

Aritmética Modular

Definición: Congruencia módulo n .

"Dados dos enteros a, b & un entero positivo n , decimos que a & b son congruentes módulo n , si is solo si,

$$n \mid (a-b) "$$

Esto lo representamos como:

$$a \equiv b \pmod{n} \quad \text{ó,}$$

$$a \equiv_n b$$

□ $n \mid (a-b)$, quiere decir también que a & b tienen el mismo residuo al ser dividido por n .

Observación:

$$\begin{array}{r} a = q_1 \cdot n + r \\ - b = q_2 \cdot n + r \\ \hline a - b = n(q_1 - q_2) + \cancel{r - r}^0 \end{array}$$

$$\frac{a-b}{n} = (q_1 - q_2) \Leftrightarrow n \mid (a-b)$$

* Por eso $n \neq 0$

Ej: El módulo 3.

- Tomemos el conjunto de todos los posibles residuos al dividir un entero por tres:

$$\{0, 1, 2\}$$

- Cada número entero puede relacionarse con uno y solo uno de los enteros en:

$$\{0, 1, 2\}$$

- Por ejemplo: relacionados con el residuo 0 están:

$$\dots -6, -3, 0, 3, 6, \dots$$

$$\boxed{\text{Dominio } 3\mathbb{Z}}$$

esto es por el módulo en el que estamos trabajando.

- estos son representados por el cero (ya que ese es su residuo al ser divididos por 3).

En otras palabras:

$$0 \equiv_3 \dots, -9, -6, -3, 0, 3, 6, 9$$

- Por otro lado, los que están relacionados con el uno son:

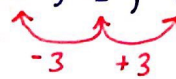
$$1 \equiv_3 \dots -5, -2, 1, 4, 7, 10, \dots$$

Dominio

$$\boxed{3\mathbb{Z} + 1}$$

■ Finalmente, los que están relacionados con el dos son:

$$2 \equiv_3 \dots -4, -1, 2, 5, 8, 11 \dots \quad 3\mathbb{Z} + 2$$



∴ Al conjunto de todos los residuos que resultan al dividir por 3, se les llama enteros módulo 3 y se les representa por \mathbb{Z}_3 (se lee "zeta tres")

$$\mathbb{Z}_3 \equiv \{0, 1, 2\}$$

┐ En general:

• Def: Enteros módulo n : Dado n un entero positivo, le llamamos enteros módulo n al conjunto de residuos posibles al dividir un entero por n ; se le representa como \mathbb{Z}_n .

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

"uno es el regalado por que

$$\mathbb{Z}_1 \equiv \{0\}$$

Ej: ¿Quién es 117 en \mathbb{Z}_6 ?

Queremos r en la ecuación:

$$117 = \square \cdot 6 + r$$

$$\left\lfloor \frac{117}{6} \right\rfloor \approx 19$$

$$r = 117 - 19 \cdot 6 = 3, \text{ en conclusión } 117 \equiv_6 3$$