Relaciones - Congruencias

Matemática IV, Facultad de Informática, UNLP.
2019

Relaciones de equivalencia definidas en Z

Dados los enteros a, b y m, se dice que *a es congruente con b módulo m* y se escribe $a \equiv b$ *(mod m)* (ó $a \equiv_m b$ ó $a \equiv b\ (m)$) si y sólo si $m|a-b$, es decir, existe $k \in Z$ tal que $a - b = k.m$

Por ejemplo: $4 \equiv 10\ (3)$ pues $3|4-10$, ya que existe -2 tal que $4 - 10 = -6 = -2 \cdot 3$

La relación de congruencia módulo m es una relación de equivalencia

Por ser la congruencia una relación de equivalencia, determina una partición del conjunto de los números enteros en clases de equivalencia que se denominan *clases de congruencia módulo m* .

Dos números enteros pertenecen a la misma clase de equivalencia si y sólo si son congruentes módulo m

Ejemplo: $m = 3$, $x \equiv y$ si y sólo si $x - y = 3 \cdot m$
Como $5 \equiv y(3)$ es lo mismo que $y - 5 = k \cdot 3$ entonces vale $y = k \cdot 3 + 5$ (todos los puntos de «esa recta»)

$$\bar{5} = \{y \in Z : 5 \equiv y(3)\} = \{2, 8, 11, \cdots\}$$

Congruencia módulo m

Ejemplo: $m = 2$, $x \equiv y$ si y sólo si $x - y = 2 \cdot m$
Como $1 \equiv y(2)$ es lo mismo que $y - 1 = k \cdot 2$ entonces vale $y = k \cdot 2 + 1$

$$\bar{1} = \{y \in Z : 1 \equiv y(2)\} = \{1, 3, 5, 7, 9, 11, \cdots\}$$

$$\bar{0} = \{y \in Z : 0 \equiv y(2)\} = \{0, 2, 4, 6, 8, 10, \cdots\}$$

Luego, $Z/\equiv_2 = \{\bar{0}, \bar{1}\}$

«Partimos» el conjunto de los números enteros en dos clases, la del $\bar{0}$ y la del $\bar{1}$, es decir, los números que tienen resto 0 cuando se los divide por 2, o resto 1.
Esto es, los números pares y los impares.

Congruencia módulo m

Observación

Dos enteros son congruentes módulo m si y sólo si los respectivos restos en su división por m son iguales

Teorema

Sea $m \in N$, $Zm = Z_m = Z/\equiv(m)$, *el conjunto cociente, tiene m clases de equivalencias.*

Aritmética en Zm

Dado $m \in Z$, definiremos la suma y el producto entre los elementos de Z_m, es decir entre las clases de equivalencia módulo m.
Esta definición no dependerá del representante elegido y así podremos sumar y multiplicar clases de equivalencias y el resultado será un representante de la misma clase.

La relación de congruencia es compatible con la suma y el producto. Dado $a, b, c, d \in Z$ tales que $a \equiv b \pmod{m}$ y $c \equiv d \pmod{m}$. Entonces se cumple que:

- $a + c \equiv b + d \pmod{m}$
- $a \cdot c \equiv b \cdot d \pmod{m}$

Esto vale porque el resto de la suma es congruente con la suma de restos, y el resto del producto es congruente con el producto de restos.

Operaciones en Zm

Suma: $\bar{x} + \bar{y} = \overline{x + y}$ La suma tiene las siguientes propiedades:

- Asociatividad
- Conmutatividad
- Existencia del neutro
- Todo elemento tiene opuesto

Operaciones en Zm

Producto: $\bar{x} \cdot \bar{y} = \overline{x \cdot y}$

El producto tiene las siguientes propiedades:

- Asociatividad
- Conmutatividad
- Existencia del neutro
- El producto se distribuye en la suma

Ejemplos de tablas de operaciones

Sea $Z_3 = \{\bar{0}, \bar{1}, \bar{2}\}$. Veamos las tablas de la suma y el producto:

+	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