

# Congruencias

## 1 Congruencias módulo $m$

**Definición 1.1.** *Dados los enteros  $a$ ,  $b$  y  $m$ , se dice que  $a$  es congruente con  $b$  módulo  $m$  y se escribe  $a \equiv b \pmod{m}$  (ó  $a \equiv_m b$  ó  $a \equiv b \pmod{m}$ ) si y sólo si  $m|a - b$ , es decir, existe  $k \in \mathbb{Z}$  tal que  $a - b = k.m$*

**Ejemplo 1.2.**  $4 \equiv 10 \pmod{3}$  pues  $3|4 - 10$ , ya que existe  $-2$  tal que  $4 - 10 = -6 = -2 \cdot 3$

**Proposición 1.3.** *La relación de congruencia módulo  $m$  es una relación de equivalencia*

**Demotración:** Para mostrar que la congruencia es una relación de equivalencia tenemos que probar que es reflexiva, simétrica y transitiva.

Tenemos:  $a$  es congruente con  $b$  módulo  $m$ , ó  $a \equiv_m b$  si y sólo si  $m|a - b$ , entonces,

- $\equiv_m$  es reflexiva ya que para  $a$  entero vale que  $m|a - a$  pues  $a - a = 0.m$
- $\equiv_m$  es simétrica.  
Supongamos que  $a \equiv_m b$ , entonces  $m$  divide a  $a - b$  y existe  $k$  entero tal que  $a - b = k.m$ , luego existe  $-k$  tal que  $b - a = -(a - b) = -(k.m) = (-k).m$  y por lo tanto  $m|b - a$  y  $b \equiv_m a$
- $\equiv_m$  es transitiva: esto es, si  $a \equiv_m b$  y  $b \equiv_m c$  entonces  $a \equiv_m c$   
Supongamos que  $a \equiv_m b$  entonces  $m|a - b$ , existe  $k$  entero tal que  $a - b = km$ ,  
por otro lado  $b \equiv_m c$  entonces  $m|b - c$ , existe  $h$  entero tal que  $b - c = hm$ ,  
luego  $a - c = a + (-b + b) - c = (a - b) + (b - c) = km + hm = (k + h)m$ , y existe un entero  $t = k + h$  tal que  $a - c = tm$  y así  $m$  divide a  $a - c$  y de esa forma tenemos que  $a \equiv_m c$  como queríamos probar.

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

La clase de congruencia módulo  $m$  de un número  $x$  será el conjunto  $\bar{x} = \{y \in \mathbb{Z} : y \equiv_m x\}$

**Observación 1.4.** *Dos números enteros pertenecen a la misma clase de equivalencia si y sólo si son congruentes módulo  $m$ .*

*Supongamos que  $a$  y  $b$  pertenecen a la "clase del  $x$ ", entonces  $a \equiv_m x$  y  $b \equiv_m x$ . Como la congruencia es una relación simétrica y transitiva tenemos que  $a \equiv_m b$ .*

*Por otro lado, si  $a \equiv_m b$  es claro que ambos pertenecen a la misma clase de equivalencia.*

Supongamos que  $x \equiv_m y$ , sabemos que esto equivale a decir que existe  $k$  entero tal que  $x - y = km$ , entonces podemos escribir  $x = km + y$ .

Como antes dijimos que dos enteros son congruentes si pertenecen a la misma clase podemos con ésto describir las clases de la siguiente forma:

$$\bar{x} = \{y : y \equiv_m x\} = \{y : x = km + y\} = \{y : y = x + k'm\} = \{y : y = x, y = x + 1, y = x + 2, \dots\}$$

Todo entero es **congruente módulo  $m$**  con su **resto** en la división por  $m$

**Ejemplos 1.5.** 1. Sabemos que  $x \equiv_3 y$  si y sólo si  $x - y = k \cdot 3$ .

Ahora tomemos por ejemplo al 2, como  $y \equiv_3 2$  es lo mismo que  $y - 2 = k \cdot 3$  entonces vale  $y = k \cdot 3 + 2$  (todos los puntos de "esa recta")

$$\bar{2} = \{y \in \mathbb{Z} : y \equiv_3 2\} = \{2, 5, 8, 11, \dots\}$$

2. Veamos la congruencia módulo 2, esto es  $x \equiv_2 y$  si y sólo si  $x - y = 2 \cdot m$

Tomemos al 1, Como  $1 \equiv y(2)$  es lo mismo que  $y - 1 = k \cdot 2$  entonces vale  $y = k \cdot 2 + 1$

$$\bar{1} = \{y \in \mathbb{Z} : 1 \equiv_2 y\} = \{1, 3, 5, 7, 9, 11, \dots\}$$

$$\bar{0} = \{y \in \mathbb{Z} : 0 \equiv_2 y\} = \{0, 2, 4, 6, 8, 10, \dots\}$$

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

"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**.

**Proposición 1.6.** Dos enteros son congruentes módulo  $m$  si y sólo si los respectivos restos en su división por  $m$  son iguales.

**Demostración:**

Supongamos que  $x$  e  $y$  son dos enteros congruentes módulo  $m$  y probemos que tienen el mismo resto en la división por  $m$ .

Por el algoritmo de la división, existen (y son únicos) cociente y resto enteros tales que :

$$x = k_1 m + r_1 \text{ con } 0 \leq r_1 < m$$

$$y = k_2 m + r_2 \text{ con } 0 \leq r_2 < m \quad (\text{Observemos que } |r_1 - r_2| < m)$$

$$\text{Luego, } x - y = (k_1 m + r_1) - (k_2 m + r_2) = (k_1 m - k_2 m) + (r_1 - r_2) = (k_1 - k_2)m + (r_1 - r_2)$$

Y como  $x \equiv_m y$ , existe un entero  $k$  tal que  $x - y = km$ , concluimos que debe ser  $r_1 - r_2 = 0$  y por lo tanto  $r_1 = r_2$ .

Ahora supongamos que los restos en la división por  $m$  coinciden y veremos que  $x \equiv_m y$ .

Otra vez usando el algoritmo de la división existen  $k_1, k_2, r$  enteros tales que :

$$x = k_1 m + r$$

$$y = k_2 m + r$$

$$\text{Así, } x - y = (k_1 m + r) - (k_2 m + r) = (k_1 m - k_2 m) + (r - r) = (k_1 - k_2)m = km$$

mostrando que  $m|x - y$  y por lo tanto,  $x \equiv_m y$ .

Todo entero es congruente con su resto en la división por  $m$ , entonces para cualquier entero  $x$  existe un resto  $r$  en la división por  $m$  y tenemos  $x \equiv_m r$

También sabemos que dos enteros congruentes pertenecen a la misma clase de equivalencia, y por lo tanto las clases serán iguales,  $\bar{x} = \bar{r}$ .

Por las propiedades y características de la división entera, tenemos que hay  $m$  posibles restos en la división por  $m$ . Estos son,  $0, \dots, m-1$ .

De esta forma vemos que habrá  $m$  clases de equivalencia o congruencia.

**Teorema 1.7.** Sea  $m \in \mathbb{N}$ ,  $\mathbb{Z}_m = \mathbb{Z} / \equiv_m$ , el conjunto cociente, tiene  $m$  clases de equivalencias.

## 2 Aritmética en $\mathbb{Z}_m$

Dado  $m \in \mathbb{Z}$ , definiremos la suma y el producto entre los elementos de  $\mathbb{Z}_m$ , 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 (es decir, las operaciones estarán bien definidas).

La relación de congruencia es compatible con la suma y el producto.

Dado  $a, b, c, d \in \mathbb{Z}$  tales que  $a \equiv_m b$  y  $c \equiv_m d$ . Entonces se cumple que:

- $a + c \equiv_m b + d$
- $a \cdot c \equiv_m b \cdot d$

Probemos la compatibilidad:

Sabemos que  $a - b = km$  y  $c - d = hm$  por ser congruentes módulo  $m$  por hipótesis general.

Sumando ambos miembros:  $\underbrace{(a - b) + (c - d)}_{(a+c)-(b+d)} = km + hm = \underbrace{(k + h)m}_{\in \mathbb{Z}}$

Con lo cual queda demostrado que  $m | (a + c) - (b + d)$  y por lo tanto  $a + c \equiv_m b + d$

Ahora veamos que el producto está bien definido. Al igual que con la suma tenemos que  $a - b = km$  y  $c - d = hm$  y queremos llegar a  $ac - bd = rm$  ya que esto significa que  $m$  divide a la diferencia  $ac - bd$  y por lo tanto  $ac \equiv_m bd$

Multipliquemos ambos miembros de  $a - b = km$  por  $c$ ,  $ca - cb = ckm$ ,  
y ambos miembros de  $c - d = hm$  por  $b$ ,  $bc - bd = bhm$

Sumando adecuadamente y utilizando las propiedades conmutativa y asociativa del producto de enteros nos queda:

$$\underbrace{(ca - cb) + (bc - bd)}_{ac - bd} = ckm + bhm = \underbrace{(ck + bh)m}_{\in \mathbb{Z}}$$

## 2.1 Operaciones en $Z_m$

Ya vimos que la suma y el producto son compatibles con la congruencia módulo  $m$ , ahora podemos definir las operaciones entre clases y basando esa definición en la suma y producto de enteros *heredará* varias propiedades.

**Suma:**  $\bar{x} + \bar{y} = \overline{x + y}$

La suma tiene las siguientes propiedades:

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

**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

Repetimos que éstas propiedades son válidas gracias a la definición de las operaciones entre clases basadas en la suma y el producto de enteros.

Veamos, como ejemplo solamente, que vale la propiedad distributiva del producto en la suma:

Queremos probar que :  $\bar{x} \cdot (\bar{y} + \bar{z}) = \bar{x} \cdot \bar{y} + \bar{x} \cdot \bar{z}$ ,

$$\bar{x} \cdot (\bar{y} + \bar{z}) = \bar{x} \cdot \overline{(y + z)} = \overline{x \cdot (y + z)} = \overline{xy + xz} = \overline{xy} + \overline{xz} = \bar{x} \cdot \bar{y} + \bar{x} \cdot \bar{z}$$

Igual a lo que ocurre en  $\mathbb{Z}$ , no todos los elementos tendrán opuesto para el producto.

### Elementos invertibles o unidades en $Z_m$

**Definición 2.1.** Dado  $a \in Z_m$ , decimos que  $a$  es **invertible** (o divisor de la unidad), si: existe  $c \in Z_m$  tal que  $a \cdot c = 1$

**Teorema 2.2.** Sea  $a \in Z_m$ ,  $a$  es invertible si y sólo si  $(a, m) = 1$

**Definición 2.3.** Dado  $a \in Z_m$  no nulo, decimos que  $a$  es **divisor de 0** si: existe  $b \in Z_m$ ,  $b \neq 0$  tal que  $a \cdot b = 0$

**Teorema 2.4.** Dado  $a \in Z_m$ ,  $a$  es invertible si y sólo si  $a$  NO es divisor de 0

## Tablas de operaciones

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

+	$\bar{0}$	$\bar{1}$	$\bar{2}$
$\bar{0}$	$\bar{0}$	$\bar{1}$	$\bar{2}$
$\bar{1}$	$\bar{1}$	$\bar{2}$	$\bar{0}$
$\bar{2}$	$\bar{2}$	$\bar{0}$	$\bar{1}$

*	$\bar{0}$	$\bar{1}$	$\bar{2}$
$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$
$\bar{1}$	$\bar{0}$	$\bar{1}$	$\bar{2}$
$\bar{2}$	$\bar{0}$	$\bar{2}$	$\bar{1}$

Es fácil ver desde la tabla que el opuesto del  $\bar{1}$  es el  $\bar{2}$ , (y obviamente el opuesto del  $\bar{2}$  es el  $\bar{1}$ ), el inverso del  $\bar{2}$  es el mismo; y que *dos más dos es uno y no cuatro...*