

# TP 5.1 - Aritmética Modular

## ▼ 1. Hallar los resultados de las siguientes operaciones realizadas entre enteros módulo 4 y 5:

Los elementos estarán en  $\mathbb{Z}_4 = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}\}$  y  $\mathbb{Z}_5 = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}\}$ .

$$\bar{3} + \bar{1}$$

- En módulo 4

$$\bar{3} + \bar{1} = \bar{4} = \bar{0}$$

- En módulo 5

$$\bar{3} + \bar{1} = \bar{4}$$

$$\bar{5} - \bar{9}$$

- En módulo 4

- Reducimos los términos

- $\bar{5} \equiv \bar{1} \pmod{4}$

- $\bar{9} \equiv \bar{1} \pmod{4}$

$$\bar{5} - \bar{9} = \bar{1} - \bar{1} = \bar{0}$$

- En módulo 5

- Reducimos los términos

- $\bar{5} \equiv \bar{0} \pmod{5}$

- $\bar{9} \equiv \bar{4} \pmod{5}$

$$\bar{5} - \bar{9} = \bar{0} - \bar{4} = \overline{-4} = \bar{1}$$

$$\bar{40} \cdot \bar{3}$$

- En módulo 4

- Reducimos  $\bar{40}$

- $\bar{40} \equiv \bar{0} \pmod{4}$

$$\bar{40} \cdot \bar{3} = \bar{0} \cdot \bar{3} = \bar{0}$$

- En módulo 5

- Reducimos  $\bar{40}$

- $\bar{40} \equiv \bar{0} \pmod{5}$

$$\bar{40} \cdot \bar{3} = \bar{0} \cdot \bar{3} = \bar{0}$$

$$(\bar{3} + \bar{2}) \cdot (\bar{6} \cdot \bar{8})$$

- En módulo 4

- Reducimos  $\bar{6}$  y  $\bar{8}$

- $\bar{6} \equiv \bar{2} \pmod{4}$

- $\bar{8} \equiv \bar{0} \pmod{4}$

$$(\bar{3} + \bar{2}) \cdot (\bar{6} \cdot \bar{8}) = (\bar{5}) \cdot (\bar{2} \cdot \bar{0}) = \bar{1} \cdot \bar{0} = \bar{0}$$

- En módulo 5

- Reducimos  $\bar{6}$  y  $\bar{8}$

- $\bar{6} \equiv \bar{1} \pmod{5}$

- $\bar{8} \equiv \bar{3} \pmod{5}$

$$(\bar{3} + \bar{2}) \cdot (\bar{6} \cdot \bar{8}) = (\bar{5}) \cdot (\bar{1} \cdot \bar{3}) = \bar{0} \cdot \bar{3} = \bar{0}$$

## ▼ 2. Construir las tablas de sumar y multiplicar de los enteros módulo 2 y 5

### Módulo 2

$$\mathbb{Z}_2 = \{\bar{0}, \bar{1}\}$$

Tabla de suma

Tabla de multiplicar

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

·	$\bar{0}$	$\bar{1}$
$\bar{0}$	$\bar{0}$	$\bar{0}$
$\bar{1}$	$\bar{0}$	$\bar{1}$

## Módulo 5

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

Tabla de suma

+	$\bar{0}$	$\bar{1}$	$\bar{2}$
$\bar{0}$	$\bar{0}$	$\bar{1}$	$\bar{2}$
$\bar{1}$	$\bar{1}$	$\bar{2}$	$\bar{3}$
$\bar{2}$	$\bar{2}$	$\bar{3}$	$\bar{4}$
$\bar{3}$	$\bar{3}$	$\bar{4}$	$\bar{0}$
$\bar{4}$	$\bar{4}$	$\bar{0}$	$\bar{1}$

Tabla de multiplicación

·	$\bar{3}$	$\bar{0}$	$\bar{4}$	$\bar{1}$	$\bar{2}$
$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$
$\bar{1}$	$\bar{1}$	$\bar{0}$	$\bar{0}$	$\bar{1}$	$\bar{2}$
$\bar{2}$	$\bar{2}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{4}$
$\bar{3}$	$\bar{3}$	$\bar{0}$	$\bar{2}$	$\bar{3}$	$\bar{1}$
$\bar{4}$	$\bar{4}$	$\bar{0}$	$\bar{3}$	$\bar{4}$	$\bar{3}$

### ▼ 3. Analizar si las siguientes son estructuras de grupo:

Para ver si cada estructura es un grupo, debe:

- Estar bien definida.
- Ser asociativa.
- Debe tener un elemento neutro.
- Cada elemento del conjunto debe tener su inverso.

#### (a) $(\mathbb{Z}_4, +)$ enteros módulo 4 con la suma modular

¿Esta bien definida?

- La suma de dos elementos de  $\mathbb{Z}_4$  sigue en  $\mathbb{Z}_4$ , ejemplo.
  - $\bar{3} + \bar{2} = \bar{1} \in \mathbb{Z}_4$

¿Es asociativa?

- La suma de enteros es asociativa, dicha propiedad se conserva bajo  $\mathbb{Z}_4$ .

¿Tiene elemento neutro?

- El elemento neutro para la suma es  $\bar{0}$ , ya que para cualquier  $\bar{a} \in \mathbb{Z}_4$ :  $\bar{a} + \bar{0} = \bar{a}$

¿Cada elemento del conjunto tiene su inverso?

- El inverso de  $\bar{0}$  es si mismo  $\bar{0} + \bar{0} = \bar{0}$ .
- El inverso de  $\bar{1}$  es  $\bar{3}$ :  $\bar{1} + \bar{3} = \bar{0}$
- El inverso de  $\bar{2}$  es si mismo:  $\bar{2} + \bar{2} = \bar{0}$
- El inverso de  $\bar{3}$  es  $\bar{1}$ :  $\bar{3} + \bar{1} = \bar{0}$

Demostramos las cuatro propiedades, por lo tanto,  $(\mathbb{Z}_4, +)$  es grupo.

#### (b) $(\mathbb{Z}_4, \cdot)$ enteros módulo 4 con el producto modular

¿Esta bien definida?

- El producto de dos elementos en  $\mathbb{Z}_4$  es otro elemento en  $\mathbb{Z}_4$ .
- Ejemplo:  $\bar{2} \cdot \bar{3} = \bar{2} \in \mathbb{Z}_4$

¿Es asociativa?

- La multiplicación de enteros es asociativa y esta propiedad se mantiene bajo  $\mathbb{Z}_4$ .

¿Tiene elemento neutro?

- El elemento neutro es  $\bar{1}$ , ya que para cualquier  $\bar{a} \in \mathbb{Z}_4 : \bar{a} \cdot \bar{1} = \bar{a}$ .

¿Cada elemento del conjunto tiene su inverso?

CONSULTAR

- $\bar{0}$  no tiene inverso, ya que  $\bar{0} \cdot \bar{a} = \bar{0}$ , para cualquier  $\bar{a} \in \mathbb{Z}_4$ .
- $\bar{2}$  tampoco tiene inverso, para cualquier  $\bar{a} \in \mathbb{Z}_4$ ,  $\bar{2} \cdot \bar{a}$  nunca da  $\bar{1}$ .
- Entonces, no todos los elementos de  $\mathbb{Z}_4$  tienen inverso.

Como no todos los elementos tienen inverso,  $(\mathbb{Z}_4, \cdot)$  no es grupo.

### (c) $(\mathbb{Z}_3, \cdot)$ enteros módulo 3 con el producto modular

¿Esta bien definida?

- El producto de dos elementos en  $\mathbb{Z}_3$  es otro elemento en  $\mathbb{Z}_3$ .

¿Es asociativa?

- La multiplicación es asociativa, dicha propiedad también está en  $\mathbb{Z}_3$ .

¿Tiene elemento neutro?

- El elemento neutro es  $\bar{1}$ , ya que para cualquier  $\bar{a} \in \mathbb{Z}_3 : \bar{a} \cdot \bar{1} = \bar{a}$ .

¿Cada elemento del conjunto tiene su inverso?

CONSULTAR

- $\bar{0}$  no tiene inverso, porque para cualquier  $\bar{a} \in \mathbb{Z}_3 : \bar{a} \cdot \bar{0} = \bar{0}$ .

Como no todos los elementos tienen inverso,  $(\mathbb{Z}_3, \cdot)$  no es grupo.

## ▼ 4. Sean $A_1 = \{\bar{0}, \bar{5}\}$ y $A_2 = \{\bar{0}, \bar{2}, \bar{4}, \bar{6}, \bar{8}\}$ subconjuntos de $\mathbb{Z}_{10}$

### Probar que $A_1$ y $A_2$ son subgrupos de $\mathbb{Z}_{10}$

Para que  $A_1$  y  $A_2$  sean subgrupos deben:

- Deben tener elemento neutro.
- Debe estar bien definida y probar el inverso en uno de sus elementos.

¿Es  $A_1$  subgrupo de  $\mathbb{Z}_{10}$ ?

- El elemento neutro en  $\mathbb{Z}_{10}$  es  $\bar{0}$  y está en  $A_1$ .
- Si sumamos dos elementos en  $A_1$ , el resultado está en  $A_1$ . Por lo tanto está bien definida.

$$\bar{0} + \bar{0} = \bar{0} \in A_1$$

$$\bar{0} + \bar{5} = \bar{5} \in A_1$$

$$\bar{5} + \bar{5} = \bar{0} \in A_1$$

- Podemos ver que el inverso de  $\bar{0}$  es si mismo (trivialmente para  $\bar{5}$ ), ya que la suma con ellos nos da el neutro.
- Por lo tanto,  $A_1$  es subgrupo de  $\mathbb{Z}_{10}$ .

¿Es  $A_2$  subgrupo de  $\mathbb{Z}_{10}$ ?

- El elemento neutro en  $\mathbb{Z}_{10}$  es  $\bar{0}$  y está en  $A_2$ .
- Podemos ver que la suma entre dos elementos cualesquiera de  $A_2$  nos da un elemento de  $A_2$ , por lo tanto está bien definida.
- El inverso de  $\bar{2}$  es  $\bar{8}$ , puesto que  $\bar{2} + \bar{8} = \bar{0}$ . El inverso de  $\bar{4}$  es  $\bar{6}$ , puesto que  $\bar{4} + \bar{6} = \bar{0}$ .

- Por lo tanto,  $A_2$  es subgrupo de  $\mathbb{Z}_{10}$ .

**Mostrar que todo elemento de  $\mathbb{Z}_{10}$  puede escribirse como suma de elementos de  $A_1$  y  $A_2$  (es decir, para todo  $x$  de  $\mathbb{Z}_{10}$ ,  $x = x_1 + x_2$  con  $x_1 \in A_1$  y  $x_2 \in A_2$ )**

Primero, los elementos de  $\mathbb{Z}_{10}$  son  $\{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5}, \bar{6}, \bar{7}, \bar{8}, \bar{9}\}$ .

$$\begin{array}{llll} \bar{0} = \bar{0} + \bar{0}, & x_1 = \bar{0} & \& x_2 = \bar{0} \\ \bar{1} = \bar{5} + \bar{6}, & x_1 = \bar{5} & \& x_2 = \bar{6} \\ \bar{2} = \bar{0} + \bar{2}, & x_1 = \bar{0} & \& x_2 = \bar{2} \\ \bar{3} = \bar{5} + \bar{8}, & x_1 = \bar{5} & \& x_2 = \bar{8} \\ \bar{4} = \bar{0} + \bar{4}, & x_1 = \bar{0} & \& x_2 = \bar{4} \\ \bar{5} = \bar{5} + \bar{0}, & x_1 = \bar{5} & \& x_2 = \bar{0} \\ \bar{6} = \bar{0} + \bar{6}, & x_1 = \bar{0} & \& x_2 = \bar{6} \\ \bar{7} = \bar{5} + \bar{2}, & x_1 = \bar{5} & \& x_2 = \bar{2} \\ \bar{8} = \bar{0} + \bar{8}, & x_1 = \bar{0} & \& x_2 = \bar{8} \\ \bar{9} = \bar{5} + \bar{4}, & x_1 = \bar{5} & \& x_2 = \bar{4} \end{array}$$

- Para cada  $x \in \mathbb{Z}_{10}$ , la expresamos como  $x = x_1 + x_2$ , siendo  $x_1 \in A_1 \wedge x_2 \in A_2$ .

## ▼ 5. Mostrar que $\bar{3}$ es un generador del grupo cíclico $(\mathbb{Z}_8, +)$ . Cuál es el orden del subgrupo cíclico generado por $\bar{2}$ ?

Para que  $\bar{3}$  sea generador del grupo cíclico  $(\mathbb{Z}_8, +)$  debemos ver si sus potencias generan todos los elementos de  $\mathbb{Z}_8$ .

Partiendo de que  $\mathbb{Z}_8 = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5}, \bar{6}, \bar{7}\}$

$$\begin{array}{l} \bar{3}^1 = \bar{3} \\ \bar{3}^2 = \bar{3} + \bar{3} = \bar{6} \\ \bar{3}^3 = \bar{3} + \bar{6} = \bar{9} = \bar{1} \\ \bar{3}^4 = \bar{3} + \bar{1} = \bar{4} \\ \bar{3}^5 = \bar{3} + \bar{4} = \bar{7} \\ \bar{3}^6 = \bar{3} + \bar{7} = \bar{10} = \bar{2} \\ \bar{3}^7 = \bar{3} + \bar{2} = \bar{5} \\ \bar{3}^8 = \bar{3} + \bar{5} = \bar{8} = \bar{0} \end{array}$$

- Podemos ver que obtuvimos todos los elementos de  $\mathbb{Z}_8$ , por lo tanto  $\bar{3}$  es generador de  $\mathbb{Z}_8$ .

Para encontrar el orden del subgrupo generado por  $\bar{2}$  en  $\mathbb{Z}_8$  tenemos que ver sus múltiplos:

$$\begin{array}{l} \bar{2}^1 = \bar{2} \\ \bar{2}^2 = \bar{2} + \bar{2} = \bar{4} \\ \bar{2}^3 = \bar{2} + \bar{4} = \bar{6} \\ \bar{2}^4 = \bar{2} + \bar{6} = \bar{0} \end{array}$$

- El subgrupo generado por  $\bar{2}$  es  $\{\bar{0}, \bar{2}, \bar{4}, \bar{6}\}$ , que posee 4 elementos, por lo tanto su orden es 4.

## ▼ 6. Encontrar los generadores del grupo cíclico $(\mathbb{Z}_6, +)$ .

Partiendo de que los elementos de  $\mathbb{Z}_6$  son  $\{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5}\}$ , tenemos que ver cuáles de esos elementos pueden generar a todos los de  $\mathbb{Z}_6$ .

- Un elemento  $\bar{a} \in \mathbb{Z}_6$  será un generador si es de orden 6, esto pasa si  $a$  y 6 son coprimos.
- Los números que son coprimos con 6 son 1 y 5.

Para  $\bar{1}$ :

$$\begin{aligned}\bar{1}^1 &= \bar{1} \\ \bar{1}^2 &= \bar{2} \\ \bar{1}^3 &= \bar{3} \\ \bar{1}^4 &= \bar{4} \\ \bar{1}^5 &= \bar{5} \\ \bar{1}^6 &= \bar{0}\end{aligned}$$

- Obtenemos todos los elementos de  $\mathbb{Z}_6$ , por lo tanto  $\bar{1}$  es generador.

Para  $\bar{5}$ :

$$\begin{aligned}\bar{5}^1 &= \bar{5} \\ \bar{5}^2 &= \bar{5} + \bar{5} = \bar{4} \\ \bar{5}^3 &= \bar{5} + \bar{4} = \bar{3} \\ \bar{5}^4 &= \bar{5} + \bar{3} = \bar{2} \\ \bar{5}^5 &= \bar{5} + \bar{2} = \bar{1} \\ \bar{5}^6 &= \bar{5} + \bar{1} = \bar{0}\end{aligned}$$

- Obtenemos todos los elementos de  $\mathbb{Z}_6$ , por lo tanto  $\bar{5}$  también es generador.

Por lo tanto, los generadores de  $(\mathbb{Z}_6, +)$  son  $\bar{1}$  y  $\bar{5}$ .

## ▼ 7. Si reparto en partes iguales $m$ caramelos entre 3 personas, me sobran 2, mientras que si los reparto entre 7, me sobran 4. Sabiendo que $m$ está entre 30 y 70. ¿Cuántos caramelos tengo para repartir? (Usar aritmética modular)

CONSULTAR (me volví mono haciendo esto)

Del enunciado tenemos que:

- Al repartir  $m$  caramelos entre 3 personas, sobran 2, o sea:

$$m \equiv_3 2$$

- Al repartir  $m$  caramelos entre 7 personas, sobran 4, o sea:

$$m \equiv_7 4$$

- Se nos da que  $m$  está entre 30 y 70, o sea:

$$30 < m < 70$$

Queremos encontrar un valor de  $m$  que satisfaga:

$$\begin{cases} m \equiv_3 2 \\ m \equiv_7 4 \end{cases}$$

- Teniendo  $m \equiv_7 4$ , es lo mismo que:

$$m = 7k + 4$$

- Sustituyendo  $m = 7k + 4$  en la primera congruencia nos quedaría:

$$7k + 4 \equiv_3 2$$

- Simplificamos  $7k + 4$  en  $\text{mod}(3)$ :

- $7 \equiv_3 1$ , por lo que  $7k \equiv_3 k$
- $4 \equiv_3 1$ .

- Así, la congruencia nos quedaría como:

$$k + 1 \equiv_3 2$$

- Restamos 1 en ambos lados:

$$k \equiv_3 1$$

- Esto significa que  $k = 3j + 1$ . Sustituimos en  $m = 7k + 4$ :

$$m = 7(3j + 1) + 4 = 21j + 7 + 4 = 21j + 11$$

- Por lo tanto:

$$m \equiv_{21} 11$$

- Tenemos que buscar valores  $m$  que satisfagan  $m \equiv_{21} 11$  y que estén en el intervalo  $30 < m < 70$ .
- Esos posibles valores de  $m$  son:

$$m = 21(0) + 11 = 11$$

$$m = 21(1) + 11 = 32$$

$$m = 21(2) + 11 = 53$$

$$m = 21(3) + 11 = 74$$

- Descartamos  $m = 11$  y  $m = 74$  porque se salen del rango.
- Para  $m = 32$ 
  - $\frac{32}{3} = 10$ , con resto 2, por lo tanto  $32 \equiv_3 2$ .
  - $\frac{32}{7} = 4$ , con resto 4, por lo tanto  $32 \equiv_7 4$ .
- Entonces,  $m = 32$  es un valor que satisface todas las condiciones.
- Para  $m = 53$ 
  - $\frac{53}{3} = 17$ , con resto 2, por lo tanto  $53 \equiv_3 2$ .
  - $\frac{53}{7} = 7$ , con resto 4, por lo tanto  $53 \equiv_7 4$ .
- Entonces,  $m = 53$  es un valor que satisface todas las condiciones.

Por lo tanto, los posibles valores que satisfacen las condiciones son:

- $m = 32$
- $m = 53$

## ▼ 8. Averiguar qué día de la semana cayó 05/11/1968, fecha del natalicio de Ricardo Fort

### CONSULTAR

Partiendo de 01/11/2024 (viernes) como fecha base, vamos a obtener los siguientes resultados cuando hagamos módulo 7 (7 por los días de la semana):

0. Viernes
1. Sábado
2. Domingo
3. Lunes
4. Martes
5. Miércoles
6. Jueves

Para ir desde el 1/11/2024 hasta el 5/11/1968:

- Retrocedemos 56 años. (1/11/1968 - 1/11/2024)
- Restamos 4 días adicionales.

Sabemos que entre 1/11/1968 y 1/11/2024 hay 56 años, es decir, 14 ciclos completos de 4 años ( $4 \cdot 14 = 56$ ).

- Cada ciclo de 4 años tiene 1461 días ( $3 \cdot 365 + 366$ ).
- $14 \text{ ciclos} \cdot 1461 = 20454$  días.
- Si restamos 4 días:  $20454 + 4 = 20458$
- Entonces  $20458 \bmod 7 = 3$

Por lo tanto, Ricardo Fort nació un martes

## ▼ 9. Mostrar que $\mathbb{Z}_m$ para $m$ natural y las operaciones de suma y producto tienen estructura de anillo

CONSULTAR

Un anillo es una estructura  $(R, +, \cdot)$  que cumple las siguientes propiedades:

- $(R, +)$  es abeliano.
- La multiplicación es cerrada y asociativa.
- La multiplicación se distribuye sobre la suma.

Vamos a ver si  $(\mathbb{Z}_m, +, \cdot)$  es un anillo.

¿Es abeliano?

- Sean  $a, b \in \mathbb{Z}_m$ , sabemos que  $a + b \bmod(m) \in \mathbb{Z}_m$ , ya que el resultado de sumar dos enteros módulo  $m$  es otro entero módulo  $m$ . Por lo tanto, está bien definida.
- Para cualquier  $a \in \mathbb{Z}_m$ , el elemento neutro para la suma es el  $\bar{0}$ , ya que  $a + \bar{0} = a \bmod(m)$ . Por lo tanto, el elemento neutro de la suma en  $\mathbb{Z}_m$  es  $\bar{0}$ .
- Para cualquier  $a, b, c \in \mathbb{Z}_m$ :  $(a + b) + c \equiv_m a + (b + c)$ . Entonces, la suma en  $\mathbb{Z}_m$  es asociativa.
- Para cada  $a \in \mathbb{Z}_m$ , existe un elemento  $a^{-1} \in \mathbb{Z}_m$  tal que  $a^{-1}$  es el inverso de  $a$ , es decir,  $a + (-a) \equiv_m 0$ . Por lo tanto, cada elemento de  $\mathbb{Z}_m$  tiene su inverso.
- Para cualquier  $a, b \in \mathbb{Z}_m$ , se cumple que  $a + b \equiv_m b + a$ . Por lo tanto, la suma en  $\mathbb{Z}_m$  es conmutativa.
- Demostramos que  $(\mathbb{Z}_m, +)$  está bien definida, tiene elemento neutro, es asociativa, cada elemento tiene su inverso y es conmutativa, por lo tanto es abeliano.

¿El producto es cerrado y asociativo para  $\mathbb{Z}_m$ ?

- Sean  $a, b \in \mathbb{Z}_m$ , sabemos que  $a \cdot b \bmod(m) \in \mathbb{Z}_m$ , ya que el producto de dos enteros módulo  $m$  es otro entero módulo  $m$ . Por lo tanto, el producto en  $\mathbb{Z}_m$  está bien definido.
- Para cualquier  $a, b, c \in \mathbb{Z}_m$ , se cumple que  $a \cdot (b \cdot c) \equiv_m (a \cdot b) \cdot c$ . Por lo tanto, el producto en  $\mathbb{Z}_m$  está bien definido.

¿El producto se distribuye sobre la suma?

- La distribución del producto sobre la suma se cumple (tanto en izquierda como en derecha) ya que es una propiedad heredada de los números enteros bajo la operación módulo  $m$ .
- Para cualquier  $a, b, c \in \mathbb{Z}_m$

$$\begin{aligned}a \cdot (b + c) &\equiv_m (a \cdot b) + (a \cdot c) \\(b + c) \cdot a &\equiv_m (b \cdot a) + (c \cdot a)\end{aligned}$$

Demostramos las 3 propiedades para  $(\mathbb{Z}_m, +, \cdot)$ , por lo tanto, tiene estructura de anillo.

## ▼ 10. Dar todos los elementos invertibles de $\mathbb{Z}_6$

## CONSULTAR

Los elementos invertibles en  $\mathbb{Z}_6$  son aquellos que tienen un inverso multiplicativo. Es decir, hallar todos los elementos  $a \in \mathbb{Z}_6$  tales que existe un  $b \in \mathbb{Z}_6$  :  $a \cdot b \equiv_6 1$ .

- Un elemento  $a \in \mathbb{Z}_m$  es invertible si el máximo común divisor con  $m$  (en nuestro caso 6) es 1, o sea, los coprimos con 6.
- Sabiendo que  $\mathbb{Z}_6 = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5}\}$ 
  - $\text{mcd}(0, 6) = 6$
  - $\text{mcd}(1, 6) = 1$
  - $\text{mcd}(2, 6) = 2$
  - $\text{mcd}(3, 6) = 3$
  - $\text{mcd}(4, 6) = 2$
  - $\text{mcd}(5, 6) = 1$
  - Podemos ver que los candidatos a elementos invertibles son  $\bar{1}$  y  $\bar{5}$ .
- Para  $\bar{1}$ , su inverso es  $\bar{1}$ , ya que  $1 \cdot 1 \equiv_6 1$ .
- Para  $\bar{5}$ , su inverso es  $\bar{5}$ , ya que  $5 \cdot 5 = 25 \equiv_6 1$ .

Por lo tanto, los elementos invertibles de  $\mathbb{Z}_6$  son  $\{\bar{1}, \bar{5}\}$ .

## ▼ 11. Sea $m$ un entero impar, probar que $m^2 \equiv_4 1$

Del enunciado sabemos que  $m$  es un entero impar, lo podemos escribir como:

$$\begin{aligned} m &= 2k + 1 \\ k &\in \mathbb{Z} \end{aligned}$$

Elevamos  $m$  al cuadrado:

$$m^2 = (2k + 1)^2$$

Binomio al cuadrado:

$$m^2 = 4k^2 + 4k + 1 = 4(k^2 + k) + 1$$

Podemos ver que  $4(k^2 + k)$  es múltiplo de 4, por lo tanto:

$$m^2 \equiv_4 1$$

Demostramos que si  $m$  es impar, entonces  $m^2 \equiv_4 1$ , debido a que el resto de  $m^2$  dividido 4 es 1, para cualquier  $m$  impar.

## ▼ 12. Dar todos los elementos invertibles de $\mathbb{Z}_6$

Ver inciso 10.

## ▼ 13. Si $\bar{a}$ es invertible entonces no es divisor de cero

Sea  $\bar{a} \in \mathbb{Z}_n$ ,  $\bar{a}$  es invertible si existe algún  $\bar{b} \in \mathbb{Z}_n$  tal que  $\bar{a} \cdot \bar{b} = \bar{1}$ .

- Esto es posible si  $a$  y  $n$  son coprimos, es decir,  $\text{mcd}(a, n) = 1$ .

Decimos que  $\bar{a} \in \mathbb{Z}_n$  es un divisor de cero si existe un  $\bar{c} \in \mathbb{Z}_n$  distinto de  $\bar{0}$  tal que  $\bar{a} \cdot \bar{c} = \bar{0}$ .

- El producto de  $\bar{a}$  con algún elemento no nulo da  $\bar{0}$ .

Si  $\bar{a}$  es invertible, entonces existe un  $\bar{b} \in \mathbb{Z}_n$  :  $\bar{a} \cdot \bar{b} = \bar{1}$ . Supongamos que  $\bar{a}$  es un divisor de cero, es decir, que existe un  $\bar{c} \in \mathbb{Z}_n$  no nulo que  $\bar{a} \cdot \bar{c} = \bar{0}$ .

Entonces, tenemos dos igualdades:



- $\bar{a} \cdot \bar{b} = \bar{1}$
- $\bar{a} \cdot \bar{c} = \bar{0}$

Multiplicamos  $\bar{b}$  en ambos lados de la segunda igualdad

$$\bar{b} \cdot (\bar{a} \cdot \bar{c}) = \bar{b} \cdot \bar{0}$$

Asociatividad:

$$(\bar{b} \cdot \bar{a}) \cdot \bar{c} = \bar{0}$$

Como  $\bar{b}$  es el inverso de  $\bar{a}$ :

$$\begin{aligned} \bar{1} \cdot \bar{c} &= \bar{0} \\ \bar{c} &= \bar{0} \end{aligned}$$

Llegamos a una contradicción, ya que si  $\bar{a}$  es divisor de cero, necesariamente  $\bar{c} \neq \bar{0}$ . Por lo tanto, la suposición de que  $\bar{a}$  es un divisor de cero es errónea.

Entonces, podemos decir que si  $\bar{a}$  es invertible en  $\mathbb{Z}_n$ , entonces no puede ser un divisor de cero en  $\mathbb{Z}_n$ .

## ▼ 14. Probar que $(t, m) = 1$ si y solo si $t$ es invertible módulo $m$

Si  $(t, m) = 1$ , entonces  $t$  es invertible módulo  $m$ .

- Si  $(t, m) = 1$ , significa que el MCD de ambos es 1. A partir de Bezout podemos decir que:

$$\begin{aligned} tx + my &= 1 \\ x, y &\in \mathbb{Z} \end{aligned}$$

- Tomando esa ecuación módulo  $m$  obtenemos:

$$tx \equiv_m 1$$

- Esto muestra que  $x$  es un inverso de  $t$ . Por lo tanto,  $t$  es invertible módulo  $m$  cuando  $(t, m) = 1$ .

Si  $t$  es invertible módulo  $m$ , entonces  $(t, m) = 1$ .

- Que  $t$  sea invertible módulo  $m$  significa que existe un  $x \in \mathbb{Z}$  tal que:

$$tx \equiv_m 1$$

- Lo que implica que:

$$tx - 1 = my$$

- Para algún  $y \in \mathbb{Z}$ :

$$tx + m(-y) = 1$$

- Esta es una combinación lineal de  $t$  y  $m$  que resulta ser 1, esto es similar al teorema de Bezout:

$$tx + m(-y) = 1 \rightarrow \gcd(t, m) = 1$$

Entonces, demostramos ambas implicaciones y podemos concluir con que el enunciado es verdadero.

## ▼ 15. Si $p$ es primo entonces $\mathbb{Z}_p$ es un cuerpo

Para que  $\mathbb{Z}_p$  sea un cuerpo debe cumplir:

- Ser un abeliano para la suma.
- Ser un abeliano para el producto.

- Distributiva del producto con respecto a la suma.

¿Es abeliano para la suma?

- Sean  $a, b \in \mathbb{Z}_p$ , sabemos que  $a + b \bmod(p) \in \mathbb{Z}_p$ , ya que el resultado de sumar dos enteros módulo  $p$  es otro entero módulo  $p$ . Por lo tanto, está bien definida.
- Para cualquier  $a, b, c \in \mathbb{Z}_p : (a + b) + c \equiv_p a + (b + c)$ , ya que se hereda esa propiedad de  $\mathbb{Z}$ . Entonces, la suma en  $\mathbb{Z}_p$  es asociativa.
- El elemento neutro para la suma en  $\mathbb{Z}_p$  es  $\bar{0}$ , ya que para cualquier  $\bar{a} \in \mathbb{Z}_p : \bar{a} + \bar{0} = \bar{a}$ . Por lo tanto, el elemento neutro para la suma en  $\mathbb{Z}_p$  es  $\bar{0}$ .
- Para cada  $\bar{a} \in \mathbb{Z}_p$ , existe un inverso  $\bar{a}^{-1} \in \mathbb{Z}_p$  tal que  $\bar{a} + \bar{a}^{-1} = \bar{0}$ . Por lo tanto, cada elemento de  $\mathbb{Z}_p$  tiene su inverso.
- Entonces, podemos decir que  $\mathbb{Z}_p$  para la suma es abeliano.

¿Es abeliano para el producto?

- Sean  $a, b \in \mathbb{Z}_p$ , sabemos que  $a \cdot b \bmod(p) \in \mathbb{Z}_p$ , ya que el resultado de multiplicar dos enteros módulo  $p$  es otro entero módulo  $p$ . Por lo tanto, está bien definida.
- Para cualquier  $a, b, c \in \mathbb{Z}_p : (a \cdot b) \cdot c \equiv_p a \cdot (b \cdot c)$ , ya que se hereda esa propiedad de  $\mathbb{Z}$ . Entonces, la suma en  $\mathbb{Z}_p$  es asociativa.
- El elemento neutro para el producto en  $\mathbb{Z}_p$  es  $\bar{1}$ , ya que para cualquier  $\bar{a} \in \mathbb{Z}_p : \bar{a} \cdot \bar{1} = \bar{a}$ . Por lo tanto, el elemento neutro para el producto en  $\mathbb{Z}_p$  es  $\bar{1}$ .
- Si  $p$  es primo, por Euclides sabemos que  $\text{mcd}(a, p) = 1$ , para cualquier  $a \neq 0$  en  $\mathbb{Z}_p$ . Es decir, para cada  $\bar{a} \in \mathbb{Z}_p : \bar{a} \neq \bar{0}$  existe un  $\bar{b} \in \mathbb{Z}_p : \bar{a} \cdot \bar{b} = \bar{1}$ 
  - Este inverso es garantizado porque  $a$  y  $p$  son coprimos, permitiéndonos aplicar Bézout

$$ax + py = 1$$

- De esto obtenemos  $ax \equiv_p 1$ , lo que muestra que  $x$  es el inverso de  $a$  para la multiplicación.
- Entonces, es válido decir que  $\mathbb{Z}_p$  con el producto es abeliano.

¿El producto se distribuye para la suma?

- El producto es distributivo respecto a la suma en  $\mathbb{Z}_p$ , es decir:

$$\bar{a} \cdot (\bar{b} + \bar{c}) = \bar{a} \cdot \bar{b} + \bar{a} \cdot \bar{c}$$

Demostramos que  $\mathbb{Z}_p$  cumple todas las propiedades, por lo tanto es un cuerpo cuando  $p$  es primo.