

TP5 – Estructuras Algebraicas - Aritmética Modular

Agustina Sol Rojas

Ejercicio 1.

Hallar los resultados de las siguientes operaciones realizadas entre enteros módulo 4 y 5:

$$\bar{3} + \bar{1}; \bar{5} + \bar{9}; \overline{40.3}; (\bar{3} + \bar{2}).(\bar{6}.\bar{8})$$

Modulo 4:

- $\bar{3} + \bar{1} = \bar{0}$
- $\bar{5} + \bar{9} = \overline{14} = \bar{2}$
- $\overline{40.3} = \overline{120} = \bar{0}$
- $(\bar{3} + \bar{2}).(\bar{6}.\bar{8}) = \bar{5}.\overline{48} = \overline{240} = \bar{0}$

Modulo 5:

- $\bar{3} + \bar{1} = \bar{4}$
- $\bar{5} + \bar{9} = \overline{14} = \bar{4}$
- $\overline{40.3} = \overline{120} = \bar{0}$
- $(\bar{3} + \bar{2}).(\bar{6}.\bar{8}) = \bar{5}.\overline{48} = \overline{240} = \bar{0}$

Ejercicio 2.

Construir las tablas de sumar y multiplicar de los enteros módulo 2 y 5:

Modulo 2:

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

.	$\bar{0}$	$\bar{1}$
$\bar{0}$	$\bar{0}$	$\bar{0}$
$\bar{1}$	$\bar{0}$	$\bar{1}$

Modulo 5:

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

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

Ejercicio 3.

Analizar si las siguientes son estructuras de grupo:

a) $(Z_4, +)$ enteros módulo 4 con la suma modular

- Cerrada:

Para todo a, b en Z_4 vale que $\bar{a} + \bar{b}$ pertenece a Z_4

- Asociativa:

La operación $+$ sobre Z_4 es asociativa ya que para cualesquiera sean \bar{a}, \bar{b} y \bar{c} en Z_4 , se cumple, por la asociatividad de los enteros con respecto a la $+$ que:

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

- Elemento neutro:

Existe en Z_4 un elemento \bar{e} tal que para todo \bar{a} en Z_4 vale que $\bar{a} + \bar{e} = \bar{e} + \bar{a} = \bar{a}$ y ese $\bar{e} = 0$, el mismo elemento neutro de los enteros con respecto a la $+$.

- Elemento inverso:

Para todo elemento \bar{a} de Z_4 existe \bar{a}' en Z_4 tal que $\bar{a} + \bar{a}' = \bar{a}' + \bar{a} = \bar{e}$:

- $\bar{0} + \bar{0} = \bar{0}$
- $\bar{1} + \bar{3} = \bar{3} + \bar{1} = \bar{0}$
- $\bar{2} + \bar{2} = \bar{0}$

Como $+$ es asociativa, existe un elemento neutro y todos los elementos de Z_4 tienen un inverso $(Z_4, +)$ es un grupo.

b) (Z_4, \cdot) enteros módulo 4 con el producto modular

- Cerrada:

Para todo a, b en Z_4 vale que $\bar{a} \cdot \bar{b}$ pertenece a Z_4

- Asociativa:

La operación \cdot sobre Z_4 es asociativa ya que para cualesquiera sean \bar{a}, \bar{b} y \bar{c} en Z_4 , se cumple, por la asociatividad de los enteros con respecto a la \cdot que:

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

- Elemento neutro:

Existe en Z_4 un elemento \bar{e} tal que para todo \bar{a} en Z_4 vale que $\bar{a} \cdot \bar{e} = \bar{e} \cdot \bar{a} = \bar{a}$ y ese $\bar{e} = \bar{1}$, el mismo elemento neutro de los enteros con respecto a la \cdot .

- Elemento inverso:

No se da que para todo elemento \bar{a} de Z_4 existe \bar{a}' en Z_4 tal que $\bar{a} \cdot \bar{a}' = \bar{a}' \cdot \bar{a} = \bar{e}$:

- Operando al $\bar{0}$ con cualquier otro elemento \bar{a} de Z_4 nunca dará como resultado $\bar{1}$

Como en \cdot no todos los elementos de Z_4 tienen un inverso (Z_4, \cdot) no es un grupo.

c) (Z_3, \cdot) enteros módulo 3 con el producto modular

- Cerrada:

Para todo a, b en Z_3 vale que $\bar{a} \cdot \bar{b}$ pertenece a Z_3

- Asociativa:

La operación \cdot sobre Z_3 es asociativa ya que para cualesquiera sean \bar{a}, \bar{b} y \bar{c} en Z_3 , se cumple, por la asociatividad de los enteros con respecto a la \cdot que:

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

- Elemento neutro:

Existe en Z_3 un elemento \bar{e} tal que para todo \bar{a} en Z_3 vale que $\bar{a} \cdot \bar{e} = \bar{e} \cdot \bar{a} = \bar{a}$ y ese $\bar{e} = \bar{1}$, el mismo elemento neutro de los enteros con respecto a la \cdot .

- Elemento inverso:

No se da que para todo elemento \bar{a} de Z_3 existe \bar{a}' en Z_3 tal que $\bar{a} \cdot \bar{a}' = \bar{a}' \cdot \bar{a} = \bar{e}$:

- Operando al $\bar{0}$ con cualquier otro elemento \bar{a} de Z_3 nunca dará como resultado $\bar{1}$

Como en \cdot no todos los elementos de Z_3 tienen un inverso (Z_3, \cdot) no es un grupo.

Ejercicio 4.

Sean $A_1 = \{\bar{0}, \bar{5}\}$ y $A_2 = \{\bar{0}, \bar{2}, \bar{4}, \bar{6}, \bar{8}\}$ subconjuntos de Z_{10} .

- Probar que A_1 y A_2 son subgrupos de Z_{10} .

A_1

+	$\bar{0}$	$\bar{5}$
$\bar{0}$	$\bar{0}$	$\bar{5}$
$\bar{5}$	$\bar{5}$	$\bar{0}$

Elemento neutro:

Existe en A_1 un elemento e tal que para todo \bar{a} en A_1 vale que $\bar{a} + \bar{e} = \bar{e} + \bar{a} = \bar{a}$ y ese $\bar{e} = \bar{0}$ cómo se puede observar en la tabla. El neutro $+$ en Z_{10} , es $\bar{0}$ y este $\in A_1$.

Operación bien definida y elemento inverso:

Para todo $\bar{a}, \bar{b} \in A_1$ se da que $\bar{a} + \bar{b}^{-1} \in A_1$. Se puede observar en la tabla que se cumple que $\bar{b}^{-1} \in A_1$ (el inverso de $\bar{0}$ es $\bar{0}$ y el de $\bar{5}$ es $\bar{5}$). También se puede observar que para todo $\bar{a}, \bar{b} \in A_1$ se da que $\bar{a} + \bar{b}^{-1} \in A_1$

A_2

+	$\bar{0}$	$\bar{2}$	$\bar{4}$	$\bar{6}$	$\bar{8}$
$\bar{0}$	$\bar{0}$	$\bar{2}$	$\bar{4}$	$\bar{6}$	$\bar{8}$
$\bar{2}$	$\bar{2}$	$\bar{4}$	$\bar{6}$	$\bar{8}$	$\bar{0}$
$\bar{4}$	$\bar{4}$	$\bar{6}$	$\bar{8}$	$\bar{0}$	$\bar{2}$
$\bar{6}$	$\bar{6}$	$\bar{8}$	$\bar{0}$	$\bar{2}$	$\bar{4}$
$\bar{8}$	$\bar{8}$	$\bar{0}$	$\bar{2}$	$\bar{4}$	$\bar{6}$

Elemento neutro:

Existe en A_2 un elemento e tal que para todo \bar{a} en A_2 vale que $\bar{a} + \bar{e} = \bar{e} + \bar{a} = \bar{a}$ y ese $\bar{e} = \bar{0}$ cómo se puede observar en la tabla. El neutro $+$ en Z_{10} , es $\bar{0}$ y este $\in A_2$.

Operación bien definida y elemento inverso:

Para todo $\bar{a}, \bar{b} \in A_2$ se da que $\bar{a} + \bar{b}^{-1} \in A_2$. Se puede observar en la tabla que se cumple que $b^{-1} \in A_2$ ($\bar{0}$ con $\bar{0}$, $\bar{2}$ con $\bar{8}$, $\bar{4}$ con $\bar{6}$). También se puede observar que para todo $\bar{a}, \bar{b} \in A_2$ se da que $\bar{a} + \bar{b}^{-1} \in A_2$

- Mostrar que todo elemento de Z_{10} puede escribirse como suma de elementos de A_1 y A_2 (es decir, para todo x de Z_{10} , $x = x_1 + x_2$ con $x_1 \in A_1$ y $x_2 \in A_2$).
 - $\bar{0} = \bar{0} + \bar{0}$ con $\bar{0} \in A_1$ y $\bar{0} \in A_2$.
 - $\bar{1} = \bar{5} + \bar{6}$ con $\bar{5} \in A_1$ y $\bar{6} \in A_2$.
 - $\bar{2} = \bar{0} + \bar{2}$ con $\bar{0} \in A_1$ y $\bar{2} \in A_2$.
 - $\bar{3} = \bar{5} + \bar{8}$ con $\bar{5} \in A_1$ y $\bar{8} \in A_2$.
 - $\bar{4} = \bar{0} + \bar{4}$ con $\bar{0} \in A_1$ y $\bar{4} \in A_2$.
 - $\bar{5} = \bar{5} + \bar{0}$ con $\bar{5} \in A_1$ y $\bar{0} \in A_2$.
 - $\bar{6} = \bar{0} + \bar{6}$ con $\bar{0} \in A_1$ y $\bar{6} \in A_2$.
 - $\bar{7} = \bar{5} + \bar{2}$ con $\bar{5} \in A_1$ y $\bar{2} \in A_2$.
 - $\bar{8} = \bar{0} + \bar{8}$ con $\bar{0} \in A_1$ y $\bar{8} \in A_2$.
 - $\bar{9} = \bar{5} + \bar{4}$ con $\bar{5} \in A_1$ y $\bar{4} \in A_2$.

Ejercicio 5.

Mostrar que 3 es un generador del grupo cíclico $(Z_8, +)$. Cuál es el orden del subgrupo cíclico generado por 2?

$$Z_8 = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5}, \bar{6}, \bar{7}\}$$

g es un generador del grupo cíclico $(Z_8, +)$ si para todo elemento $a \in Z_8$ existe un entero k tal que $a = g^k$.

Elemento $\in Z_8$	Potencia de $\bar{3}$ que dan el elemento
$\bar{0}$	$\bar{3}^0 = \bar{0}$
$\bar{1}$	$\bar{3}^3 = \bar{3} + \bar{3} + \bar{3} = \bar{9}$ $= \bar{1}$
$\bar{2}$	$\bar{3}^6 = \overline{18} = \bar{2}$
$\bar{3}$	$\bar{3}^1 = \bar{3}$
$\bar{4}$	$\bar{3}^4 = \bar{3} + \bar{3} + \bar{3} + \bar{3}$ $= \overline{12}$ $= \bar{4}$
$\bar{5}$	$\bar{3}^7 = \overline{21} = \bar{5}$
$\bar{6}$	$\bar{3}^2 = \bar{6}$
$\bar{7}$	$\bar{3}^5 = \overline{15} = \bar{7}$

$$\bar{2}^0 = \bar{0}$$

$$\bar{2}^1 = \bar{2}$$

$$\bar{2}^2 = \bar{4}$$

$$\bar{2}^3 = \bar{6}$$

$$\bar{2}^4 = \bar{8} = \bar{0}$$

El orden del subgrupo cíclico generado por 2 es 4. Ese subgrupo es $\{\bar{0}, \bar{2}, \bar{4}, \bar{6}\}$ donde $\bar{6} = \bar{2}^{m-1}$ siendo m el orden del subgrupo.

Ejercicio 6.

Encontrar los generadores del grupo cíclico $(Z_6, +)$.

- $\bar{1}$
 - ☐ $\bar{1}^0 = \bar{0}$
 - ☐ $\bar{1}^1 = \bar{1}$
 - ☐ $\bar{1}^2 = \bar{2}$
 - ☐ $\bar{1}^3 = \bar{3}$
 - ☐ $\bar{1}^4 = \bar{4}$
 - ☐ $\bar{1}^5 = \bar{5}$

- Si es
- $\bar{2}$
 - ☐ $\bar{2}^0 = \bar{0}$
 - ☐ $\bar{2}^1 = \bar{2}$
 - ☐ $\bar{2}^2 = \bar{4}$
 - ☐ $\bar{2}^3 = \bar{0}$

- No es
- $\bar{3}$
 - ☐ $\bar{3}^0 = \bar{0}$
 - ☐ $\bar{3}^1 = \bar{3}$
 - ☐ $\bar{3}^2 = \bar{0}$

- No es
- $\bar{4}$
 - ☐ $\bar{4}^0 = \bar{0}$
 - ☐ $\bar{4}^1 = \bar{4}$
 - ☐ $\bar{4}^2 = \bar{2}$
 - ☐ $\bar{4}^3 = \bar{0}$

- No es
- $\bar{5}$
 - ☐ $\bar{5}^0 = \bar{0}$
 - ☐ $\bar{5}^1 = \bar{5}$
 - ☐ $\bar{5}^2 = \bar{4}$
 - ☐ $\bar{5}^3 = \bar{3}$
 - ☐ $\bar{5}^4 = \bar{2}$

$$\circ \quad \bar{5}^5 = \bar{1}$$

Ejercicio 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)

- $30 < m < 70$
- $m = 3q + 2$
- $m = 7t + 4$

1. Igualo ambas ecuaciones con m en común y despejo alguna de las incógnitas.

$$3q + 8 = 7t + 4$$

$$3q = 7t - 4$$

2. Considero a 3 como el módulo, y a $7t$ y 4 como los términos de la congruencia.

$$\overline{7 \cdot t} \equiv_3 \bar{4}$$

$$\bar{7} \cdot \bar{t} \equiv_3 \bar{4}$$

$$\bar{1} \cdot \bar{t} \equiv_3 \bar{1}$$

3. Realizo el algoritmo de Euclides para ver si el $\bar{1}$ que acompaña a la t y el 3 son coprimos

$$(3,1) = (1,0) = 1$$

4. Como son coprimos existe en Z_3 un \bar{a} tal que $\bar{a} \cdot \bar{1} \equiv \bar{1}$ y ese $\bar{a} = \bar{1}$ ya que $\bar{1} \cdot \bar{1} \equiv \bar{1}$

5. Multiplico ambos lados por $\bar{1}$

$$\bar{t} \equiv_3 \bar{1}$$

6. Obtengo la cantidad de monedas teniendo en cuenta que $30 < m < 70$, para ello reemplazo a t por algún numero perteneciente a $\bar{1}$:

$$m = 7 \cdot 4 + 4 = 32$$

$$m = 7 \cdot \bar{7} + 4 = 53$$

7. Por lo tanto se tienen 32 o 53 caramelos.

<https://www.youtube.com/watch?v=EpxyNxAauKE>

Ejercicio 8.

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

1. Primero se debe calcular $M = \text{días transcurridos}$:

i. Primero se deben calcular los años:

$$2024 - 1968 = 56 \text{ años.}$$

ii. Se deben tener en cuenta los bisiestos, sacando los seculares no divisibles por 400 (igualmente no están incluidos de por si en los 56 años tenidos en cuenta):

$$\frac{56}{4} = 14$$

iii. Calculo los días transcurridos:

$$M = 56 * 365 + 14 = 20454$$

2. A esa cantidad de días obtenidos se le calcula el módulo 7 (por la cantidad de días de la semana)

i. $M = 20454 \equiv_7 0$

3. Como 05/11 fue martes y desde el 05/11/1968 pasaron 20454 días, el cual es congruente modulo 7 con 0, entonces:

- $\text{martes, si } M \equiv_7 0$

4. Por lo tanto el 05/11 fue martes.

<https://www.youtube.com/watch?v=ByWNR2w-wAo>

Ejercicio 9.

Mostrar que Z_m para m natural y las operaciones de suma y producto tiene estructura de anillo

Si tengo dos operaciones binarias, que en general se llaman suma y producto, la terna ordenada $(A, +, \cdot)$ tiene estructura de anillo si $(A, +)$ es un grupo conmutativo, el producto es asociativo y se satisfacen:

1. Distributividad por la izquierda: para cualesquiera $a, b, c \rightarrow a(b + c) = ab + ac$

2. Distributividad por la derecha: para cualesquiera $a, b, c \rightarrow (a + b)c = ac + bc$

Se probó en el ejercicio 4 (se probó para Z_4 pero es la misma demostración) que $(Z_m, +)$ es un grupo conmutativo y que (Z_m, \cdot) es asociativo.

Falta demostrar la distributividad:

1. Por izquierda: para cualesquiera \bar{a}, \bar{b} y $\bar{c} \in Z_m$ vale que:

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

2. Por derecha: para cualesquiera \bar{a}, \bar{b} y $\bar{c} \in Z_m$ vale que:

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

Por lo tanto $(Z_m, +, \cdot)$ tiene estructura de anillo.

Ejercicio 10.

Dar todos los elementos invertibles de Z_6 .

\cdot	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$
$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$
$\bar{1}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$
$\bar{2}$	$\bar{0}$	$\bar{2}$	$\bar{4}$	$\bar{0}$	$\bar{2}$	$\bar{4}$
$\bar{3}$	$\bar{0}$	$\bar{3}$	$\bar{0}$	$\bar{3}$	$\bar{0}$	$\bar{3}$
$\bar{4}$	$\bar{0}$	$\bar{4}$	$\bar{2}$	$\bar{0}$	$\bar{4}$	$\bar{2}$
$\bar{5}$	$\bar{0}$	$\bar{5}$	$\bar{4}$	$\bar{3}$	$\bar{2}$	$\bar{1}$

Dado $\bar{a} \in Z_m$, decimos que \bar{a} es invertible (o divisor de la unidad), si: existe $\bar{c} \in Z_m$ tal que $\bar{a} \cdot \bar{c} = \bar{1}$

Los elementos invertibles son $\bar{1}$ y $\bar{5}$.

Ejercicio 11.

Sea m un entero impar, probar que $m^2 \equiv_4 1$

1. $m = 2k + 1$ con $k \in \mathbb{Z}$.

2. Elevando m al cuadrado nos queda:

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

3. Sacando factor común 4:

$$m^2 = 4(k^2 + k) + 1 = 4t + 1 \text{ con } t \in \mathbb{Z}$$

4. Como $m^2 = 4t + 1$, se está dividiendo a m^2 por 4.

5. Como el resto es 1 y se sabe todo entero es congruente módulo 4 con su resto en la división por 4, entonces $m^2 \equiv_4 1$.