

## **Trabajo Práctico N° 5.2:** **Aritmética Modular.**

### **Ejercicio 1.**

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

**(a)**  $\bar{3} + \bar{1}$ .

$$\begin{aligned}\bar{3} + \bar{1} &= \overline{3 + 1} \\ \bar{3} + \bar{1} &= \bar{4}.\end{aligned}$$

$$\begin{aligned}\bar{3} + \bar{1} &= 4 \bmod 4 \\ \bar{3} + \bar{1} &= 0.\end{aligned}$$

$$\begin{aligned}\bar{3} + \bar{1} &= 4 \bmod 5 \\ \bar{3} + \bar{1} &= 4.\end{aligned}$$

**(b)**  $\bar{5} + \bar{9}$ .

$$\begin{aligned}\bar{5} + \bar{9} &= \overline{5 + 9} \\ \bar{5} + \bar{9} &= \overline{14}.\end{aligned}$$

$$\begin{aligned}\bar{5} + \bar{9} &= 14 \bmod 4 \\ \bar{5} + \bar{9} &= 2.\end{aligned}$$

$$\begin{aligned}\bar{5} + \bar{9} &= 14 \bmod 5 \\ \bar{5} + \bar{9} &= 4.\end{aligned}$$

**(c)**  $\overline{40} * \bar{3}$ .

$$\begin{aligned}\overline{40} * \bar{3} &= \overline{40 * 3} \\ \overline{40} * \bar{3} &= \overline{120}.\end{aligned}$$

$$\begin{aligned}\overline{40} * \bar{3} &= 120 \bmod 4 \\ \overline{40} * \bar{3} &= 0.\end{aligned}$$

$$\begin{aligned}\overline{40} * \bar{3} &= 120 \bmod 5 \\ \overline{40} * \bar{3} &= 0.\end{aligned}$$

**(d)**  $(\bar{3} + \bar{2}) * (\bar{6} * \bar{8})$ .

$$(\bar{3} + \bar{2}) * (\bar{6} * \bar{8}) = (\overline{3 + 2}) * (\overline{6 * 8})$$

$$(\bar{3} + \bar{2}) * (\bar{6} * \bar{8}) = \bar{5} * \bar{48}$$

$$(\bar{3} + \bar{2}) * (\bar{6} * \bar{8}) = \overline{5 * 48}$$

$$(\bar{3} + \bar{2}) * (\bar{6} * \bar{8}) = \overline{240}.$$

$$(\bar{3} + \bar{2}) * (\bar{6} * \bar{8}) = 240 \bmod 4$$

$$(\bar{3} + \bar{2}) * (\bar{6} * \bar{8}) = 0.$$

$$(\bar{3} + \bar{2}) * (\bar{6} * \bar{8}) = 240 \bmod 5$$

$$(\bar{3} + \bar{2}) * (\bar{6} * \bar{8}) = 0.$$

**Ejercicio 2.**

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

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

Tabla de sumar (mod 2):

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

Tabla de multiplicar (mod 2):

| *         | $\bar{0}$ | $\bar{1}$ |
|-----------|-----------|-----------|
| $\bar{0}$ | 0         | 0         |
| $\bar{1}$ | 0         | 1         |

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

Tabla de sumar (mod 5):

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

Tabla de multiplicar (mod 5):

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

**Ejercicio 3.**

*Analizar si las siguientes son estructuras de grupo:*

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

$$\mathbb{Z}_4 = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}\}.$$

Cerradura: Para cada  $a, b \in \mathbb{Z}_4$ ,  $(a + b) \bmod 4 \in \mathbb{Z}_4$ .

Asociatividad: La operación  $+$  en  $\mathbb{Z}_4$  es asociativa porque se cumple que, para cada  $a, b, c \in \mathbb{Z}_4$ ,  $[(a + b) + c] \bmod 4 = [a + (b + c)] \bmod 4$ .

Elemento neutro: Existe un elemento  $e \in \mathbb{Z}_4$  tal que, para todo  $a \in \mathbb{Z}_4$ , se cumple que  $(a + e) \bmod 4 = (e + a) \bmod 4 = a \bmod 4$ . En particular, 0 es el elemento neutro  $\in \mathbb{Z}_4$ , ya que  $(a + 0) \bmod 4 = (0 + a) \bmod 4 = a \bmod 4 \Leftrightarrow a \bmod 4 = a \bmod 4 = a \bmod 4$ .

Inversos: Un elemento  $a \in \mathbb{Z}_4$  tiene inverso si existe  $a' \in \mathbb{Z}_4$  tal que  $(a + a') \bmod 4 = (a' + a) \bmod 4 = e$ . En particular, el inverso de 0 es 0  $\in \mathbb{Z}_4$ , el inverso de 1 es 3  $\in \mathbb{Z}_4$ , el inverso de 2 es 2  $\in \mathbb{Z}_4$  y el inverso de 3 es 1  $\in \mathbb{Z}_4$ , por lo que existe inverso para todo  $a \in \mathbb{Z}_4$ .

Por lo tanto,  $(\mathbb{Z}_4, +)$  es un grupo, ya que satisface cerradura, asociatividad, elemento neutro e inversos.

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

$$\mathbb{Z}_4 = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}\}.$$

Cerradura: Para cada  $a, b \in \mathbb{Z}_4$ ,  $(a * b) \bmod 4 \in \mathbb{Z}_4$ .

Asociatividad: La operación  $*$  en  $\mathbb{Z}_4$  es asociativa porque se cumple que, para cada  $a, b, c \in \mathbb{Z}_4$ ,  $[(a * b) * c] \bmod 4 = [a * (b * c)] \bmod 4$ .

Elemento neutro: Existe un elemento  $e \in \mathbb{Z}_4$  tal que, para todo  $a \in \mathbb{Z}_4$ , se cumple que  $(a * e) \bmod 4 = (e * a) \bmod 4 = a \bmod 4$ . En particular, 1 es el elemento neutro  $\in \mathbb{Z}_4$ , ya que  $(a * 1) \bmod 4 = (1 * a) \bmod 4 = a \bmod 4 \Leftrightarrow a \bmod 4 = a \bmod 4 = a \bmod 4$ .

Inversos: Un elemento  $a \in \mathbb{Z}_4 \setminus \{0\}$  tiene inverso si existe  $a' \in \mathbb{Z}_4$  tal que  $(a * a') \bmod 4 = (a' * a) \bmod 4 = e$ . En particular, esto sólo se cumple para 1 (cuyo inverso es 1  $\in \mathbb{Z}_4$ ) y 3 (cuyo inverso es 3  $\in \mathbb{Z}_4$ ), por lo que no existe inverso para todo  $a \in \mathbb{Z}_4 \setminus \{0\}$ .

Por lo tanto,  $(\mathbb{Z}_4, *)$  no es un grupo, ya que satisface cerradura, asociatividad y elemento neutro, pero no satisface inversos.

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

$$\mathbb{Z}_3 = \{\bar{0}, \bar{1}, \bar{2}\}.$$

Cerradura: Para cada  $a, b \in \mathbb{Z}_3$ ,  $(a * b) \bmod 3 \in \mathbb{Z}_3$ .

Asociatividad: La operación  $*$  en  $\mathbb{Z}_3$  es asociativa porque se cumple que, para cada  $a, b, c \in \mathbb{Z}_3$ ,  $[(a * b) * c] \bmod 3 = [a * (b * c)] \bmod 3$ .

Elemento neutro: Existe un elemento  $e \in \mathbb{Z}_3$  tal que, para todo  $a \in \mathbb{Z}_3$ , se cumple que  $(a * e) \bmod 3 = (e * a) \bmod 3 = a \bmod 3$ . En particular, 1 es el elemento neutro  $\in \mathbb{Z}_3$ , ya que  $(a * 1) \bmod 3 = (1 * a) \bmod 3 = a \bmod 3 \Leftrightarrow a \bmod 3 = a \bmod 3 = a \bmod 3$ .

Inversos: Un elemento  $a \in \mathbb{Z}_3 \setminus \{0\}$  tiene inverso si existe  $a' \in \mathbb{Z}_3$  tal que  $(a * a') \bmod 3 = (a' * a) \bmod 3 = e$ . En particular, 1 es el inverso de 1 y 2 es el inverso de 2, por lo que existe inverso para todo  $a \in \mathbb{Z}_3 \setminus \{0\}$ .

Por lo tanto,  $(\mathbb{Z}_3, *)$  es un grupo, ya que satisface cerradura, asociatividad, elemento neutro e inversos.

**Ejercicio 4.**

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

(a) Probar que  $A_1$  y  $A_2$  son subgrupos de  $\mathbb{Z}_{10}$ .

$$A_1 \subset \mathbb{Z}_{10}.$$

Cerradura: Para cada  $a, b \in A_1$ ,  $(a + b) \bmod 10 \in A_1$ .

Asociatividad: La operación  $+$  en  $A_1$  es asociativa porque se hereda del grupo original  $(\mathbb{Z}_{10}, +)$ .

Elemento neutro: El elemento neutro de  $+$  en  $\mathbb{Z}_{10}$  también existe en  $A_1$ . En particular,  $0 \in A_1$ .

Inversos: Un elemento  $a \in A_1$  tiene inverso si existe  $a' \in A_1$  tal que  $(a + a') \bmod 10 = (a' + a) \bmod 10 = e$ . En particular, el inverso de 5 es  $5 \in A_1$ , por lo que existe inverso para todo  $a \in A_1 \setminus \{0\}$ .

Por lo tanto, queda demostrado que  $(A_1, +)$  es un subgrupo del grupo  $(\mathbb{Z}_{10}, +)$ , ya que satisface cerradura, elemento neutro e inversos.

$$A_2 \subset \mathbb{Z}_{10}.$$

Cerradura: Para cada  $a, b \in A_2$ ,  $(a + b) \bmod 10 \in A_2$ .

Asociatividad: La operación  $+$  en  $A_2$  es asociativa porque se hereda del grupo original  $(\mathbb{Z}_{10}, +)$ .

Elemento neutro: El elemento neutro de  $+$  en  $\mathbb{Z}_{10}$  también existe en  $A_2$ . En particular,  $0 \in A_2$ .

Inversos: Un elemento  $a \in A_2$  tiene inverso si existe  $a' \in A_2$  tal que  $(a + a') \bmod 10 = (a' + a) \bmod 10 = e$ . En particular, el inverso de 2 es  $8 \in A_2$ , el inverso de 4 es  $6 \in A_2$ , el inverso de 6 es  $4 \in A_2$  y el inverso de 8 es  $2 \in A_2$ , por lo que existe inverso para todo  $a \in A_2 \setminus \{0\}$ .

Por lo tanto, queda demostrado que  $(A_2, +)$  es un subgrupo del grupo  $(\mathbb{Z}_{10}, +)$ , ya que satisface cerradura, elemento neutro e inversos.

(b) 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  $x_2 \in A_2$ ).

$$\mathbb{Z}_{10} = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5}, \bar{6}, \bar{7}, \bar{8}, \bar{9}\}.$$

Si  $x_1 = \bar{0}$ , entonces,  $x = x_2$ . Como  $A_2$  contiene  $\bar{0}, \bar{2}, \bar{4}, \bar{6}, \bar{8}$ , los valores posibles de  $x_2$  cubren los elementos pares de  $\mathbb{Z}_{10}$  ( $\bar{0}, \bar{2}, \bar{4}, \bar{6}, \bar{8}$ ).

Si  $x_1 = \bar{5}$ , entonces,  $x = (\bar{5} + x_2) \bmod 10$ . Esto genera:  $\bar{5} + \bar{0} = \bar{5}$ ;  $\bar{5} + \bar{2} = \bar{7}$ ;  $\bar{5} + \bar{4} = \bar{9}$ ;  $\bar{5} + \bar{6} = \bar{1}$ ;  $\bar{5} + \bar{8} = \bar{3}$ . Los valores posibles de  $x_2$  cubren los elementos impares de  $\mathbb{Z}_{10}$  ( $\bar{1}, \bar{3}, \bar{5}, \bar{7}, \bar{9}$ ).

Por lo tanto, todo elemento de  $\mathbb{Z}_{10}$  puede escribirse como la suma de elementos de  $A_1$  y  $A_2$ .

**Ejercicio 5.**

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

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

Un elemento  $g \in \mathbb{Z}_8$  es un generador si y sólo si los múltiplos de  $g$  (es decir,  $g, 2g, \dots$  módulo 8) generan todos los elementos de  $\mathbb{Z}_8$ .

$$g = \bar{3}: \bar{1} * \bar{3} = \bar{3}; \bar{2} * \bar{3} = \bar{6}; \bar{3} * \bar{3} = \bar{1}; \bar{4} * \bar{3} = \bar{4}; \bar{5} * \bar{3} = \bar{7}; \bar{6} * \bar{3} = \bar{2}; \bar{7} * \bar{3} = \bar{5}; \bar{8} * \bar{3} = \bar{0}.$$

Por lo tanto,  $\bar{3}$  es un generador del grupo cíclico  $(\mathbb{Z}_8, +)$ .

El orden de un elemento en un grupo cíclico es el menor  $n$  tal que  $ng = \bar{0}$ , donde  $g$  es el elemento que se está considerando.

$$g = \bar{2}: \bar{1} * \bar{2} = \bar{2}; \bar{2} * \bar{2} = \bar{4}; \bar{3} * \bar{2} = \bar{6}; \bar{4} * \bar{2} = \bar{0}.$$

Por lo tanto, el orden del subgrupo cíclico generado por  $\bar{2}$  es 4.



**Ejercicio 6.**

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

$$\mathbb{Z}_6 = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5}\}.$$

Un elemento  $g \in \mathbb{Z}_6$  es un generador si y sólo si los múltiplos de  $g$  (es decir,  $g, 2g, \dots$  módulo 6) generan todos los elementos de  $\mathbb{Z}_6$ .

$g = \bar{0}$ : La suma de  $\bar{0}$  consigo mismo siempre da 0.

$$g = \bar{1}: \bar{1} * \bar{1} = \bar{1}; \bar{2} * \bar{1} = \bar{2}; \bar{3} * \bar{1} = \bar{3}; \bar{4} * \bar{1} = \bar{4}; \bar{5} * \bar{1} = \bar{5}; \bar{6} * \bar{1} = \bar{0}.$$

$$g = \bar{2}: \bar{1} * \bar{2} = \bar{2}; \bar{2} * \bar{2} = \bar{4}; \bar{3} * \bar{2} = \bar{0}.$$

$$g = \bar{3}: \bar{1} * \bar{3} = \bar{3}; \bar{2} * \bar{3} = \bar{0}.$$

$$g = \bar{4}: \bar{1} * \bar{4} = \bar{4}; \bar{2} * \bar{4} = \bar{2}; \bar{3} * \bar{4} = \bar{0}.$$

$$g = \bar{5}: \bar{1} * \bar{5} = \bar{5}; \bar{2} * \bar{5} = \bar{4}; \bar{3} * \bar{5} = \bar{3}; \bar{4} * \bar{5} = \bar{2}; \bar{5} * \bar{5} = \bar{1}; \bar{6} * \bar{5} = \bar{0}.$$

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

**Ejercicio 7.**

*Si se reparte en partes iguales  $m$  caramelos entre 3 personas me sobran 2, mientras que, si se reparten entre 7, me sobran 4. Sabiendo que  $m$  está entre 30 y 70. ¿Cuántos caramelos se tienen para repartir? (Usar aritmética modular).*

$$m \equiv_3 2$$

$$m = 3k + 2, \text{ con } k \in \mathbb{Z}.$$

$$m \equiv_7 4.$$

$$3k + 2 \equiv_7 4$$

$$3k \equiv_7 4 - 2$$

$$3k \equiv_7 2$$

$$5 * 3k \equiv_7 5 * 2$$

$$15k \equiv_7 10$$

$$15k \bmod 7 = 10$$

$$15 \bmod 7 * k \bmod 7 = 3$$

$$1 * k \bmod 7 = 3$$

$$k \bmod 7 = 3$$

$$k = 7n + 3, \text{ con } n \in \mathbb{Z}.$$

$$m = 3(7n + 3) + 2$$

$$m = 21n + 9 + 2$$

$$m = 21n + 11.$$

Con  $n = 1$ :

$$m = 21 * 1 + 11$$

$$m = 21 + 11$$

$$m = 32.$$

Con  $n = 2$ :

$$m = 21 * 2 + 11$$

$$m = 42 + 11$$

$$m = 53.$$

Con  $n = 3$ :

$$m = 21 * 3 + 11$$

$$m = 63 + 11$$

$$m = 74.$$

Por lo tanto, se tienen para repartir 32 o 53 caramelos.

**Ejercicio 8.**

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

Se utilizará el algoritmo de Zeller, que es una fórmula para calcular el día de la semana de cualquier fecha:

$$h = (q + \left\lfloor \frac{13(m+1)}{5} \right\rfloor + K + \left\lfloor \frac{K}{4} \right\rfloor + \left\lfloor \frac{J}{4} \right\rfloor - 2J) \bmod 7, \text{ donde:}$$

h: día de la semana (0: sábado, 1: domingo, 2: lunes, 3: martes, 4: miércoles, 5: jueves, 6: viernes),

q: día del mes,

m: mes (los meses de enero y febrero se consideran como los meses 13 y 14 del año anterior),

K: últimos dos dígitos del año,

J: primeros dos dígitos del año.

$$h = (5 + \left\lfloor \frac{13(11+1)}{5} \right\rfloor + 68 + \left\lfloor \frac{68}{4} \right\rfloor + \left\lfloor \frac{19}{4} \right\rfloor - 2 * 19) \bmod 7$$

$$h = (5 + \left\lfloor \frac{13*12}{5} \right\rfloor + 68 + 17 + 4 - 38) \bmod 7$$

$$h = (5 + \left\lfloor \frac{156}{5} \right\rfloor + 68 + 17 + 4 - 38) \bmod 7$$

$$h = (5 + 31 + 68 + 17 + 4 - 38) \bmod 7$$

$$h = 87 \bmod 7$$

$$h = 3.$$

Por lo tanto, el día de la semana que cayó 05/11/1968 fue martes.

**Ejercicio 9.**

*Mostrar que  $\mathbb{Z}_m$  para  $m$  natural y las operaciones de suma y producto tiene estructura de anillo.*

$$\mathbb{Z}_m = \{\bar{0}, \bar{1}, \bar{2}, \dots, \overline{m-1}\}.$$

La terna ordenada  $(\mathbb{Z}_m, +, *)$  tiene estructura de anillo si  $(\mathbb{Z}_m, +)$  es un grupo conmutativo y si el producto es cerrado, asociativo y se satisface distributividad del producto respecto de la suma.

Cerradura de la suma: Para cada  $a, b \in \mathbb{Z}_m$ ,  $(a + b) \bmod m \in \mathbb{Z}_m$ .

Asociatividad de la suma: La operación  $+$  en  $\mathbb{Z}_m$  es asociativa porque se cumple que, para cada  $a, b, c \in \mathbb{Z}_m$ ,  $[(a + b) + c] \bmod m = [a + (b + c)] \bmod m$ .

Elemento neutro de la suma: Existe un elemento  $e \in \mathbb{Z}_m$  tal que, para todo  $a \in \mathbb{Z}_m$ , se cumple que  $(a + e) \bmod m = (e + a) \bmod m = a \bmod m$ . En particular,  $0$  es el elemento neutro  $\in \mathbb{Z}_m$ , ya que  $(a + 0) \bmod m = (0 + a) \bmod m = a \bmod m \Leftrightarrow a \bmod m = a \bmod m = a \bmod m$ .

Inversos aditivos: Un elemento  $a \in \mathbb{Z}_m$  tiene inverso si existe  $a' \in \mathbb{Z}_m$  tal que  $(a + a') \bmod m = (a' + a) \bmod m = e$ . En particular, para todo  $a \in \mathbb{Z}_m$ , su inverso es  $a' = (m - a) \in \mathbb{Z}_m$ , por lo que existe inverso para todo  $a \in \mathbb{Z}_m$ .

Conmutatividad de la suma: La operación  $+$  en  $\mathbb{Z}_m$  es conmutativa porque se cumple que, para cada  $a, b \in \mathbb{Z}_m$ ,  $(a + b) \bmod m = (b + a) \bmod m$ .

Por lo tanto,  $(\mathbb{Z}_m, +)$  es un grupo conmutativo, ya que satisface cerradura, asociatividad, elemento neutro, inversos y conmutatividad.

Cerradura del producto: Para cada  $a, b \in \mathbb{Z}_m$ ,  $(a * b) \bmod m \in \mathbb{Z}_m$ .

Asociatividad del producto: La operación  $*$  en  $\mathbb{Z}_m$  es asociativa porque se cumple que, para cada  $a, b, c \in \mathbb{Z}_m$ ,  $[(a * b) * c] \bmod m = [a * (b * c)] \bmod m$ .

Distributividad del producto respecto de la suma: La operación  $*$  en  $\mathbb{Z}_m$  es distributiva respecto de la operación  $+$  porque se cumple que, para cada  $a, b, c \in \mathbb{Z}_m$ ,  $[a * (b + c)] \bmod m = (a * b + a * c) \bmod m$  y  $[(a + b) * c] \bmod m = (a * c + b * c) \bmod m$ .

Por lo tanto, queda demostrado que  $(\mathbb{Z}_m, +, *)$  tiene estructura de anillo.

**Ejercicio 10.**

*Dar todos los elementos invertibles de  $\mathbb{Z}_6$ .*

$$\mathbb{Z}_6 = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5}\}.$$

Un elemento  $a \in \mathbb{Z}_6$  es invertible si existe  $b \in \mathbb{Z}_6$  tal que  $(a * b) \bmod 6 = 1$ .

Un elemento  $a \in \mathbb{Z}_6$  es invertible si y sólo si  $\text{mcd}(a, 6) = 1$  (es coprimo con 6).

$$a = 0: \text{mcd}(0, 6) = 6.$$

$$a = 1: \text{mcd}(1, 6) = 1.$$

$$a = 2: \text{mcd}(2, 6) = 2.$$

$$a = 3: \text{mcd}(3, 6) = 3.$$

$$a = 4: \text{mcd}(4, 6) = 2.$$

$$a = 5: \text{mcd}(5, 6) = 1.$$

En particular, los inversos de  $\bar{1}$  y  $\bar{5}$  son  $\bar{1}$  y  $\bar{5}$ , respectivamente.

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

**Ejercicio 11.**

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

Si  $m$  es un entero impar, entonces:

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

Elevando al cuadrado ambos lados de la ecuación anterior, se tiene:

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

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

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

Tomando la congruencia módulo 4, se tiene:

$$m^2 \bmod 4 = [4(k^2 + k) + 1] \bmod 4$$

$$m^2 \bmod 4 = [4(k^2 + k)] \bmod 4 + 1 \bmod 4$$

$$m^2 \bmod 4 = 4 \bmod 4 * (k^2 + k) \bmod 4 + 1$$

$$m^2 \bmod 4 = 0 * (k^2 + k) \bmod 4 + 1$$

$$m^2 \bmod 4 = 0 + 1$$

$$m^2 \bmod 4 = 1$$

$$m^2 \equiv_4 1.$$

Por lo tanto, queda demostrado que, dado un número impar  $m$ ,  $m^2 \equiv_4 1$ .

**Ejercicio 12.**

*Si  $\bar{a}$  es invertible, entonces, no es divisor de cero.*

Si  $\bar{a}$  es invertible, entonces, existe  $\bar{b} \in \mathbb{Z}_m$  tal que:

$$\bar{a} * \bar{b} = \bar{1}.$$

Ahora, se supone, por contradicción, que  $\bar{a}$  también es divisor de 0. Entonces, existe  $\bar{c} \neq 0 \in \mathbb{Z}_m$  tal que:

$$\bar{a} * \bar{c} = \bar{0}.$$

Pre-multiplicando a ambos lados de la ecuación anterior por el inverso de  $\bar{a}$  ( $\bar{b}$ ), se tiene:

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

Usando la propiedad asociativa, se tiene:

$$\begin{aligned} (\bar{b} * \bar{a}) * \bar{c} &= \bar{0} \\ (\bar{a} * \bar{b}) * \bar{c} &= \bar{0}. \end{aligned}$$

Usando que  $\bar{b}$  es el inverso de  $\bar{a}$ , se tiene:

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

Lo cual contradice la suposición de que  $\bar{c} \neq 0$ .

Por lo tanto, queda demostrado que, si  $\bar{a}$  es invertible, entonces, no es divisor de cero.

**Ejercicio 13.**

*Probar que  $(t, m) = 1$  si y sólo si  $t$  es invertible módulo  $m$ .*

Si  $\text{mcd}(t, m) = 1$ , entonces, por el teorema de Bézout, existen enteros  $x$  e  $y$  tales que  $tx + my = 1$ . Tomando la congruencia módulo  $m$ , se tiene:

$$tx + my \equiv_m 1$$

$$(tx + my) \bmod m = 1$$

$$tx \bmod m + my \bmod m = 1$$

$$tx \bmod m + m \bmod m * y \bmod m = 1$$

$$tx \bmod m + 0 * y \bmod m = 1$$

$$tx \bmod m + 0 = 1$$

$$tx \bmod m = 1$$

$$tx \equiv_m 1.$$

Por lo tanto,  $t$  es invertible módulo  $m$ .

Si  $t$  es invertible módulo  $m$ , entonces, existe  $t' \in \mathbb{Z}_m$  tal que  $tt' \equiv_m 1$ , lo que implica que  $tt' = mk + 1$ , para algún  $k \in \mathbb{Z}$ . La ecuación  $tt' - mk = 1$  es una combinación lineal de  $t$  y  $m$  que da como resultado 1. Por lo tanto, por el teorema de Bézout,  $\text{mcd}(t, m) = 1$ .

Por lo tanto, queda demostrado que  $(t, m)$  si y sólo si  $t$  es invertible módulo  $m$ .



**Ejercicio 14.**

Si  $p$  es primo, entonces,  $\mathbb{Z}_p$  es un cuerpo.

$$\mathbb{Z}_p = \{\bar{0}, \bar{1}, \bar{2}, \dots, \overline{p-1}\}.$$

La terna ordenada  $(\mathbb{Z}_p, +, *)$  tiene estructura de cuerpo si  $(\mathbb{Z}_p, +)$  es un grupo conmutativo, si el producto es cerrado, asociativo, tiene un elemento neutro y es conmutativo y si todo elemento no nulo tiene un inverso multiplicativo.

Cerradura de la suma: Para cada  $a, b \in \mathbb{Z}_p$ ,  $(a + b) \bmod p \in \mathbb{Z}_p$ .

Asociatividad de la suma: La operación  $+$  en  $\mathbb{Z}_p$  es asociativa porque se cumple que, para cada  $a, b, c \in \mathbb{Z}_p$ ,  $[(a + b) + c] \bmod p = [a + (b + c)] \bmod p$ .

Elemento neutro de la suma: Existe un elemento  $e \in \mathbb{Z}_p$  tal que, para todo  $a \in \mathbb{Z}_p$ , se cumple que  $(a + e) \bmod p = (e + a) \bmod p = a \bmod p$ . En particular,  $0$  es el elemento neutro  $\in \mathbb{Z}_p$ , ya que  $(a + 0) \bmod p = (0 + a) \bmod p = a \bmod p \Leftrightarrow a \bmod p = a \bmod p = a \bmod p$ .

Inversos aditivos: Un elemento  $a \in \mathbb{Z}_p$  tiene inverso si existe  $a' \in \mathbb{Z}_p$  tal que  $(a + a') \bmod p = (a' + a) \bmod p = e$ . En particular, para todo  $a \in \mathbb{Z}_p$ , su inverso es  $a' = (p - a) \in \mathbb{Z}_p$ , por lo que existe inverso para todo  $a \in \mathbb{Z}_p$ .

Conmutatividad de la suma: La operación  $+$  en  $\mathbb{Z}_p$  es conmutativa porque se cumple que, para cada  $a, b \in \mathbb{Z}_p$ ,  $(a + b) \bmod p = (b + a) \bmod p$ .

Por lo tanto,  $(\mathbb{Z}_p, +)$  es un grupo conmutativo, ya que satisface cerradura, asociatividad, elemento neutro, inversos y conmutatividad.

Cerradura del producto: Para cada  $a, b \in \mathbb{Z}_p$ ,  $(a * b) \bmod p \in \mathbb{Z}_p$ .

Asociatividad del producto: La operación  $*$  en  $\mathbb{Z}_p$  es asociativa porque se cumple que, para cada  $a, b, c \in \mathbb{Z}_p$ ,  $[(a * b) * c] \bmod p = [a * (b * c)] \bmod p$ .

Elemento neutro del producto: Existe un elemento  $e \in \mathbb{Z}_p$  tal que, para todo  $a \in \mathbb{Z}_p$ , se cumple que  $(a * e) \bmod p = (e * a) \bmod p = a \bmod p$ . En particular,  $1$  es el elemento neutro  $\in \mathbb{Z}_p$ , ya que  $(a * 1) \bmod p = (1 * a) \bmod p = a \bmod p \Leftrightarrow a \bmod p = a \bmod p = a \bmod p$ .

Conmutatividad del producto: La operación  $*$  en  $\mathbb{Z}_p$  es conmutativa porque se cumple que, para cada  $a, b \in \mathbb{Z}_p$ ,  $(a * b) \bmod p = (b * a) \bmod p$ .

Inversos multiplicativos: Como  $p$  es primo, para todo  $a \in \mathbb{Z}_p \setminus \{0\}$ ,  $\text{mcd}(a, p) = 1$ . Por el teorema de Bézout, existen enteros  $x$  e  $y$  tales que  $ax + py = 1$ . Tomando la congruencia módulo  $p$ , se tiene que  $ax + py \equiv_p 1 \Leftrightarrow ax \equiv_p 1$ , lo que implica que  $x$  es el inverso multiplicativo de  $a$  módulo  $p$ . Por lo tanto, todo elemento no nulo de  $\mathbb{Z}_p$  tiene un inverso multiplicativo.

Por lo tanto, queda demostrado que, si  $p$  es primo, entonces,  $(\mathbb{Z}_p, +, *)$  es un cuerpo.