PRÁCTICA 5.2

1)

mod 4

$\overline{3} + \overline{1} = \overline{0} \rightarrow 4 \bmod 4 = 0$

$\overline{5} + \overline{9} = \overline{2} \rightarrow 14 \bmod 4 = 2$

$\overline{40} \cdot \overline{3} = \overline{0} \rightarrow 120 \bmod 4 = 0$

$(\overline{3} + \overline{2}) \cdot (\overline{6} \cdot \overline{8}) = \overline{0} \rightarrow 5 \bmod 4 = 1 \quad 48 \bmod 4 = 0$

$\overline{1} \cdot \overline{0} = \overline{0}$

mod 5

$\overline{3} + \overline{1} = \overline{4} \rightarrow 4 \bmod 5 = 4$

$\overline{5} + \overline{9} = \overline{4} \rightarrow 14 \bmod 5 = 4$

$\overline{40} \cdot \overline{3} = \overline{0} \rightarrow 120 \bmod 5 = 0$

$(\overline{3} + \overline{2}) \cdot (\overline{6} \cdot \overline{8}) = \overline{0} \rightarrow 5 \bmod 5 = 0 \quad 48 \bmod 5 = 3$

$\overline{0} \cdot \overline{3} = \overline{0}$

2)

mod 2

+	$\overline{0}$	$\overline{1}$
$\overline{0}$	$\overline{0}$	$\overline{1}$
$\overline{1}$	$\overline{1}$	$\overline{0}$

·	$\overline{0}$	$\overline{1}$
$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{1}$	$\overline{0}$	$\overline{1}$

mod 5

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

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

a) $(\mathbb{Z}_4, +)$ $\mathbb{Z}$ mod 4 y + modular Los elem. son: $\{0, 1, 2, 3\}$

CERRADA: para cualquier $a, b \in \mathbb{Z}_4$, $\bar{a} + \bar{b} \in \mathbb{Z}_4$

ASOCIATIVA: para cualquier $a, b, c \in \mathbb{Z}_4$:

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

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

por asociatividad de la + en los $\mathbb{Z}$

NEUTRO: $\exists e \in \mathbb{Z}_4 / \ \bar{a} + \bar{e} = \bar{e} + \bar{a} = \bar{a}$, $a \in \mathbb{Z}_4$

El elemento es el $\bar{0}$

INVERSO: $\exists \bar{a}^{-1} \in \mathbb{Z}_4 / \ \bar{a} + \bar{a}^{-1} = \bar{a}^{-1} + \bar{a} = \bar{e}$, $\bar{a} \in \mathbb{Z}_4$

$\therefore$ para cada elemento:

$\bar{0} + \bar{0} = \bar{0}$ $\bar{0}^{-1} = \bar{0}$

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

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

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

$\therefore$ Es un grupo

---

b) $(\mathbb{Z}_4, \cdot)$ $\mathbb{Z}$ mod 4 y · modular Los elem. son: $\{0, 1, 2, 3\}$

CERRADA: para cualquier $a, b \in \mathbb{Z}_4$, $\bar{a} \cdot \bar{b} \in \mathbb{Z}_4$

ASOCIATIVA: para cualquier $a, b, c \in \mathbb{Z}_4$:

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

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

por asociatividad del · de $\mathbb{Z}$

NEUTRO: $\exists e \in \mathbb{Z}_4 / \ \bar{a} \cdot \bar{e} = \bar{e} \cdot \bar{a} = \bar{a}$; $\bar{a} \in \mathbb{Z}_4$

El elemento es $\bar{1}$

INVERSO: $\exists \bar{a}^{-1} \in \mathbb{Z}_4 / \ \bar{a} \cdot \bar{a}^{-1} = \bar{a}^{-1} \cdot \bar{a} = \bar{e}$, $\bar{a} \in \mathbb{Z}_4$

$\therefore$ para cada elemento:

$\bar{0} \cdot \bar{0}^{-1} \neq \bar{1}$ como operando el $\bar{0}$ nunca puede dar $\bar{1}$, esta propiedad no se cumple

$\therefore$ no es un grupo

c) $(Z_3, \cdot)$ Z mod 3 y · modulos

CERRADA: para cualquier $a, b \in Z_3$; $\bar{a} \cdot \bar{b} \in Z_3$

ASOCIATIVA: para cualquier $a, b, c \in Z_3$:

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

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

por asociatividad del · de $\mathbb{Z}$

NEUTRO: $\exists e \in Z_3 \,/\, \bar{a} \cdot \bar{e} = \bar{e} \cdot \bar{a} = \bar{a}$, $\bar{a} \in Z_3$

Ese elemento es $\bar{1}$

INVERSO: $\exists \bar{a}^{-1} \in Z_3 \,/\, \bar{a} \cdot \bar{a}^{-1} = \bar{a}^{-1} \cdot \bar{a} = \bar{e}$, $\bar{a} \in Z_3$

∴ para cada elemento:

$\bar{0} \cdot \bar{0}^{-1} \neq \bar{1}$ no existe inverso para $\bar{0}$, por lo que no se cumple.

∴ no es un grupo

---

4) $A_1 = \{\bar{0}, \bar{5}\}$

NEUTRO: $\exists e \in A_1 \,/\, \bar{a} + \bar{e} = \bar{e} + \bar{a} = \bar{a}$ $\bar{a} \in A_1$

Este elemento es el $\bar{0}$

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

CIAUSURA e INVERSO: para $\bar{a}, \bar{b} \in A_1 \rightarrow \bar{a} + \bar{b}^{-1} \in A_1$

$\bar{0}^{-1} = \bar{0}$ y $\bar{5}^{-1} = \bar{5}$

y como se ve en la tabla está bien definida

∴ $\bar{a} + \bar{b}^{-1} \in A_1$

$A_2 = \{\bar{0}, \bar{2}, \bar{4}, \bar{6}, \bar{8}\}$

Neutro: $\exists e \in A_2 / \ \bar{a} + \bar{e} = \bar{e} + \bar{a} = \bar{a} \ ; \ \bar{a} \in A_2$

Cor elemento es $\bar{0}$

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

Clausura e Inverso: $\exists \bar{a}^{-1} \in A_2 / \ \bar{a} + \bar{a}^{-1} = \bar{a}^{-1} + \bar{a} = \bar{e} \ ; \ \bar{a} \in A_2$ y

$\bar{0}^{-1} = \bar{0} \ ; \ \bar{2}^{-1} = \bar{8} \ ; \ \bar{4}^{-1} = \bar{6} \ ; \ \bar{6}^{-1} = \bar{4} \ ; \ \bar{8}^{-1} = \bar{2}$

y como se ve, es cerrada.

$\therefore \bar{a} + \bar{b}^{-1} \in A^2$

$\bar{a} + \bar{b}^{-1} \in A_2$ con $\bar{a}, \bar{b} \in A_2$

---

b) $\forall \bar{a} \in Z_{10}$ puede escribirse como $\bar{a} = \bar{b} + \bar{c}$ con $\bar{b} \in A_1$ y $\bar{c} \in A_2$

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

$\bar{1} = \bar{5} + \bar{6}$

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

$\bar{3} = \bar{5} + \bar{8}$

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

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

$\bar{6} = \bar{0} + \bar{6}$

$\bar{7} = \bar{5} + \bar{2}$

$\bar{8} = \bar{0} + \bar{8}$

$\bar{9} = \bar{5} + \bar{4}$

5) $\bar{3}$ es generador de $(Z_8, +)$ si para $\forall b \in Z_8 \; \exists k / b = \bar{3}^k$

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

$\bar{0} \rightarrow \bar{3}^0 = \bar{0}$

$\bar{1} \rightarrow \bar{3}^3 = \bar{3} + \bar{3} + \bar{3} = \bar{9} = \bar{1}$

$\bar{2} \rightarrow \bar{3}^6 = \bar{3} + \bar{3} + \bar{3} + \bar{3} + \bar{3} + \bar{3} = \overline{18} = \bar{2}$

$\bar{3} \rightarrow \bar{3}^1 = \bar{3}$

$\bar{4} \rightarrow \bar{3}^4 = \bar{3} + \bar{3} + \bar{3} + \bar{3} = \overline{12} = \bar{4}$

$\bar{5} \rightarrow \bar{3}^7 = \bar{3} + \bar{3} + \bar{3} + \bar{3} + \bar{3} + \bar{3} + \bar{3} = \overline{21} = \bar{5}$

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

$\bar{7} \rightarrow \bar{3}^5 = \bar{3} + \bar{3} + \bar{3} + \bar{3} + \bar{3} = \overline{15} = \bar{7}$

Orden del subgrupo generado por $\bar{2}$:

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

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

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

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

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

$\therefore$ Orden = 4 y elementos son = $\{\bar{0}, \bar{2}, \bar{4}, \bar{6}\}$

---

6) $(Z_6, +)$ Elementos: $\{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5}\}$

$\bar{1}$ es generador

$\bar{1}^0 = \bar{0}$

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

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

$\bar{1}^3 = \bar{3}$

$\bar{1}^4 = \bar{4}$

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

$\bar{2}$ no es generador

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

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

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

$\bar{2}^3 = \bar{0}$

$\bar{3}$ no es generador

$\bar{3}^0 = \bar{0}$

$\bar{3}^1 = \bar{3}$

$\bar{3}^2 = \bar{0}$

$\bar{4}$ no es generador

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

$\bar{4}^1 = \bar{4}$

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

$\bar{4}^3 = \bar{0}$

$\bar{5}$ es generador

$\bar{5}^0 = \bar{0}$

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

$\bar{5}^2 = \bar{4}$

$\bar{5}^3 = \bar{3}$

$\bar{5}^4 = \bar{2}$

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

7) $m \equiv_3 2$ y $m \equiv_7 4$ $\quad 30 \leq m \leq 70$

$m = 3k + 2$ $\quad m = 7t + 4$

Igualamos ambas ecuaciones: $3k + 2 = 7t + 4$

$\underbrace{3k}_{a} \underbrace{-2}_{b} = \underbrace{7t}_{n}$

$\Rightarrow \overline{3k} \equiv_7 \overline{2}$

$\overline{3}.\overline{k} \equiv_7 \overline{2}$

$a \equiv_n b$

$a - b = kn$

Buscamos el inverso de $\overline{3}$: $\quad \overline{3}$ es invertible $\leftrightarrow (3,7) = 1$

usando el algoritmo de Euclides:

$7 = 3.2 + 1$

$3 = 3.1 + 0 \rightarrow$ como el resto es 0, tenemos que 1 es el MCD de (3,7)

$\overline{1} = \overline{7} - \overline{2}.\overline{3}$

$\overline{1} = \overline{0} - \overline{2}.\overline{3}$

$\overline{1} = -\overline{2}.\overline{5} \quad [-\overline{2} + \overline{7} = \overline{5}]$

$\overline{1} = \overline{5}.\overline{3}$

$\hookrightarrow \overline{5}.\overline{3}.\overline{k} \equiv_7 \overline{5}.\overline{2}$

$\overline{1}.\overline{k} \equiv_7 \overline{10}$

$\overline{k} \equiv_7 \overline{3}$

reemplazamos por elementos de $\overline{3}$ en la ecuación, por ej: 3, 10, 17, etc.

$m = 3.(10) + 2 = 32$

$m = 3.(17) + 2 = 53$

• para cualquier otro elemento de $\overline{3}$ el valor resultante no cumple $30 \leq m \leq 70$. $9 \leq k \leq 22$.

∴ Se tienen 32 o 53 caramelos

---

8) Martes $\equiv_7 0$

...

Lunes $\equiv_7 6$

∴ La fecha del matrimonio fue un martes.

calcular 05/11/1968 $\quad$ 05/11/2024 → martes

2024 - 1968 = 56.

calcular los días de años bisiestos (quitando los seculares (1900, 2000, etc) no divisibles por 400 (en este caso no hay). → 56 / 4 = 14

$365 \times 56 + 14 = 20.454 \rightarrow 20.454 \equiv_7 0$

9) $(\mathbb{Z}_m, +, \cdot)$ es un anillo con $m \in \mathbb{N}$

$(\mathbb{Z}_m, +)$ debe ser un grupo conmutativo

$(\mathbb{Z}_m, \cdot)$ debe ser asociativo y satisfacer:

* Distributividad por izquierda → $a(b+c) = ab + ac$
* Distributividad por derecha → $(a+b).c = ac + bc$

CERRADA: para todo $a, b \in \mathbb{Z}_m \rightarrow \bar{a} + \bar{b} \in \mathbb{Z}_m$ con $m \in \mathbb{N}$

ASOCIATIVA: para todo $a, b, c \in \mathbb{Z}_m$

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

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

por asociatividad de la + en $\mathbb{Z}$

NEUTRO: $\exists e \in \mathbb{Z}_m$ / $\bar{a} + \bar{e} = \bar{e} + \bar{a} = \bar{a}$; $\bar{a} \in \mathbb{Z}_m$

Ese elemento es $\bar{0}$ → $\bar{a} + \bar{0} = \overline{a+0} = \bar{a}$

INVERSO: $\exists \bar{a}^{-1} \in \mathbb{Z}_m$ / $\bar{a} + \bar{a}^{-1} = \bar{a}^{-1} + \bar{a} = \bar{e}$; $\bar{a} \in \mathbb{Z}_m$

$$\bar{a} + \overline{(m-a)} = \overline{a+(m-a)} = \overline{m} = \bar{0}$$

CONMUTATIVIDAD: $\bar{a} + \bar{b} = \overline{a+b} = \overline{b+a} = \bar{b} + \bar{a}$

por conmutatividad de la suma en $\mathbb{Z}$

$\therefore (\mathbb{Z}_m, +)$ es un grupo abeliano

ASOCIATIVO: para todo $a, b, c \in \mathbb{Z}_m$

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

por asociatividad del . en $\mathbb{Z}$

DISTRIBUTIVA → IZQUIERDA: $\bar{a} . (\bar{b} + \bar{c}) = \bar{a} . \overline{(b+c)} =$

$$= \overline{a.(b+c)} = \overline{a.b + a.c} = \overline{ab} + \overline{ac} =$$

$$= \bar{a}\,\bar{b} + \bar{a} . \bar{c}$$

↓

DERECHA:

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

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

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

Dado $\bar{a} \in \mathbb{Z}_6$, $\bar{a}$ es invertible si $\exists\, \bar{c} \in \mathbb{Z}_6 / \bar{a} \cdot \bar{c} = \bar{1}$

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

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

---

11) $\{m \in \mathbb{Z} / m = 2k+1\}$ probar $m^2 \equiv_4 1$

$m^2 - 1 = 4t$ $\qquad m^2 = (2k+1)^2$

$m^2 = 4t + 1$ $\qquad m^2 = 4k^2 + 4k + 1$

$m^2 = 2(\underbrace{2t}_{w \in \mathbb{Z}}) + 1$ $\qquad m^2 = 4(\underbrace{k^2 + k}_{z \in \mathbb{Z}}) + 1$

Como su resto es 1 y todo $\mathbb{Z}$ es congruente con su resto (en este caso para mod 4) $\rightarrow m^2 \equiv_4 1$

---

12) Ejercicio repetido (punto 10)

---

13) Si $\bar{a}$ es invertible $\rightarrow \bar{a} \neq 0$

si $\bar{a}$ es invertible $\rightarrow \exists\, \bar{b} \in \mathbb{Z}_m / \bar{a} \cdot \bar{b} = \bar{1}$; suponemos $\bar{a} \mid 0$:

Como $\bar{a} \mid 0 \rightarrow \exists\, \bar{c} \in \mathbb{Z} / \bar{a} \cdot \bar{c} = \bar{0}$ y $\bar{c} \neq \bar{0}$

Como $\bar{a}$ tiene inverso ($\bar{b}$), multiplicamos ambos lados:

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

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

$\bar{1} \cdot \bar{c} = \bar{0}$

$\bar{c} = \bar{0}$ $\qquad \therefore$ Contradice $\bar{c} \neq \bar{0}$

14) $(t, m) = 1 \leftrightarrow t$ es invertible mod m

I) suponemos $(t, m) = 1$

por el teorema de Bezout $\exists x, y \in \mathbb{Z} / tx + my = 1$

o sea $t.x + m.y \equiv_m 1$ y como $m.y \equiv_m 0$

$\rightarrow t.x \equiv_m 1$ $\therefore$ x es el inverso de t mod m, o sea t es invertible mod m.

2) suponemos t es invertible mod m

si es invertible, $\exists x \in \mathbb{Z} / t.x \equiv 1 \pmod m$

o sea $t.x - 1 = m.k$ con $k \in \mathbb{Z}$

↳ $t.x - m.k = 1$

↳ $t.x + m.(-k) = 1$

Por el teorema de Bezout, $(t, m) = 1$

---

15) Si p es primo $\rightarrow \mathbb{Z}_p$ es un cuerpo

Debemos probar:

* $(\mathbb{Z}_p, +)$ es un grupo abeliano
* $(\mathbb{Z}_p - \{\bar{0}\}, \cdot)$ es un grupo
* multiplicación distributiva con respecto a la suma.

1- CERRADA: para cualquier $\bar{a}, \bar{b} \in \mathbb{Z}_p \rightarrow \bar{a} + \bar{b} \in \mathbb{Z}_p$

ya que $\overline{a+b} \in \{0, 1, \dots, p-1\}$

ASOCIATIVA: dado $\bar{a}, \bar{b}, \bar{c} \in \mathbb{Z}_p$

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

por asociatividad de + para $\mathbb{Z}$

NEUTRO: $\exists \bar{e} \in \mathbb{Z}_p / \bar{a} + \bar{e} = \bar{e} + \bar{a} = \bar{a}$ con $\bar{a} \in \mathbb{Z}_p$

Ese elemento es $\bar{0} \Longrightarrow \bar{a} + \bar{0} = \overline{a+0} = \bar{a}$

por neutro de $\mathbb{Z}$

Inverso: para cada $\bar{a} \in \mathbb{Z}_p$, $\exists \bar{a}' \in \mathbb{Z}_p / \bar{a} + \bar{a}' = \bar{a}' + \bar{a} = \bar{e}$

Ese elemento es $\overline{p-a} \Rightarrow \bar{a} + \overline{p-a} = \overline{a+p-a} = \bar{p} = \bar{0}$

Conmutativa: $\bar{a} + \bar{b} = \overline{a+b} = \overline{b+a} = \bar{b} + \bar{a}$ para $\forall a, b \in \mathbb{Z}_p$
por conmutatividad de la + en $\mathbb{Z}$

$\therefore (\mathbb{Z}_p, +)$ es un grupo abeliano

2- Cerrada para cualquier $a, b \in \mathbb{Z}_p \rightarrow \bar{a} \cdot \bar{b} \in \mathbb{Z}_p$

ya que $\overline{a \cdot b} \in \{0, 1, \ldots, p-1\}$

Asociativa: dado $\bar{a}, \bar{b}, \bar{c} \in \mathbb{Z}_p$

$(\bar{a} \cdot \bar{b}) \cdot \bar{c} = \overline{(a \cdot b) \cdot c} = \overline{a \cdot (b \cdot c)} = \bar{a} \cdot (\bar{b} \cdot \bar{c})$
por asociatividad del $\cdot$ en $\mathbb{Z}$

Neutro: $\exists \bar{e} \in \mathbb{Z}_p / \bar{a} \cdot \bar{e} = \bar{e} \cdot \bar{a} = \bar{a}$; $\bar{a} \in \mathbb{Z}_p$

Ese elemento es $\bar{1} \Rightarrow \bar{a} \cdot \bar{1} = \overline{a \cdot 1} = \bar{a}$

Inverso: para cualquier $\bar{a} \neq \bar{0}$ (por el teorema de Bezout)

como $(a, p) = 1$ (porque p es primo y $\bar{a} \neq \bar{0}$) $\rightarrow$

$\exists b \in \mathbb{Z} / a \cdot b \equiv_p 1$

O sea $\bar{b}$ es el inverso de $\bar{a}$

$\therefore (\mathbb{Z}_p, \cdot)$ es un grupo

3-

Dado $\bar{a}, \bar{b}, \bar{c} \in \mathbb{Z}_p$

$\bar{a} \cdot (\bar{b} + \bar{c}) = \bar{a} \cdot (\overline{b+c}) = \overline{a \cdot (b+c)} = \overline{ab + ac} = \overline{ab} + \overline{ac}$
distrib. del $\cdot$ con respecto a la + en $\mathbb{Z}$

y

$\overline{ab} + \overline{ac} = \overline{ab + ac} = \overline{a \cdot (b+c)} = \bar{a} \cdot (\overline{b+c}) = \bar{a} \cdot (\bar{b} + \bar{c})$
Factor común de $\mathbb{Z}$

$\therefore \mathbb{Z}_p$ es un cuerpo cuando p es primo.