

Ejercicios Capítulo 7

- 1) Demuestra que todo numero entero divide a cero

Dem.

Sabemos que por la def de producto, para todo

$a \in \mathbb{Z}$, $a \cdot 0 = 0$, por lo tanto para todos los enteros existe un r (en todos los casos 0) tal que $ar = 0$

□

- 2) Demuestra que si 0 es divisor de a, entonces $a = 0$

Dem.

Supongamos que $a \neq 0$

por hipótesis que 0/a es decir $0 \cdot r = a$ con $r \in \mathbb{Z}$

y como $a \neq 0$ entonces $0 \cdot r \neq 0$! pero por la definición

de multiplicación se $a \cdot 0 = 0$ entonces llegamos a una contradicción,

por lo tanto $a = 0$

□

- 3) Demuestra que las unidades en $\mathbb{Z} \{1, -1\}$ son divisores de cualquier entero

Sea $a \in \mathbb{Z}$ cualquiera. Veamos si existe un $r \in \mathbb{Z}$

tal que $1/a$, $-1/a$ es decir $1 \cdot r = a$ y $-1 \cdot r = a$

Veamos que en el caso I $r=a$ ya se por def de producto.

I. $a \cdot a = a$, $a \in \mathbb{Z}$ entonces $r \in \mathbb{Z}$ y por lo tanto

$|/a$

el caso II $r=-a$ ya se por def de producto \rightarrow "leyes

de signos" $-1 \cdot -a = a$, $a \in \mathbb{Z}$ entonces $r \in \mathbb{Z}$ y por lo

tanto $-1/a$

□

- 4) Demuestra que si u es un divisor común a todos los enteros entonces u es una medida

Dem

Como u divide a todos los enteros entonces $u/1$ es

medio $u=1$ con $v \in \mathbb{Z}$ cumpliendo la condición de medida

□

- 5) Demuestra que lo siguiente es equivalente

i) a divide a b

ii) $-a$ divide a b

iii) a divide a $-b$

iv) $-a$ divide a $-b$

Dem

PD i) \Rightarrow ii)

Sup se a/b

PO $-a/b$

Pr hip $a \cdot r = b$ con $r \in \mathbb{Z}$

entonces $-a \cdot -r = a \cdot r$ por "ley de signos"

entonces $-a \cdot -r = b$ y $-r \in \mathbb{Z}$, entonces $-a \mid b$

□

PD ii) \Rightarrow iii)

sup $-a \mid b$ PD $a \mid -b$

por hip $-a \cdot r = b$ con $r \in \mathbb{Z}$

entonces $a \cdot r = -(-a \cdot r)$ por "ley de signos"

entonces $a \cdot r = -b$ y $r \in \mathbb{Z}$ y $-a \in \mathbb{Z}$ entonces $a \mid -b$

□

PD iii) \Rightarrow iv)

sup $a \mid -b$ PD $-a \mid b$

por hip $a \cdot r = -b$ con $r \in \mathbb{Z}$

entonces $-a \cdot -r = a \cdot r$ por "ley de signos"

entonces $-a \cdot -r = -b$ y $-r \in \mathbb{Z}$, $-a \in \mathbb{Z}$ entonces $-a \mid b$

$$-2 \cdot 3 = -6$$

sup $-a \mid b$ PD $a \mid b$

por hip $-a \cdot r = b$ con $r \in \mathbb{Z}$, entonces $a \cdot r = -(-a \cdot r)$ por

"ley de signos" y entonces $a \cdot r = b$, como $a \in \mathbb{Z}$ y $r \in \mathbb{Z}$

$$\therefore a \mid b \quad \square$$

-) 6) Prueba que 52 no es combinación de 20 y 15
- sabemos que $5|20$, $5|15$, pero $5\nmid 52$ entonces
 52 no es combinación de 20 y 15
-) 7) Encuentra un número que no sea combinación de 30 y 70
- 144 ya que $5|30$, $5\nmid 70$ pero $5\nmid 144$
-) 8) Pruébese que si c es un entero impar entonces
 c no es combinación lineal de 98 y 102
- como c es impar entonces $2 \nmid c$ pero $2|98 \rightarrow 2|102$
entonces c no es combinación lineal
-) 9) Prueba que si $c = 3n \pm 1$ (entre), entonces c no es combinación de 45 y 125
- veamos que $9|45$, $9|125$ por 9 no es de la forma
 $3n \pm 1$ es de la forma $3n$ entonces $3n \nmid 9$
-) 10) Prueba que si $c = 30n \pm 6$ (entre), entonces c no es combinación de 1020 y 210
- veamos que $30|1020$ y $30|210 \rightarrow 30$ es de la forma $30n$
no de $30n \pm 6$ entonces $30 \nmid 30n \pm 6$

• 11) Probar que si c es combinación de a y b , entonces rc también lo es.

por hipótesis $c = ap + bs$ para $p, s \in \mathbb{Z}$

$$\Rightarrow rc = r(ap + bs) \quad y \quad rp, rs \in \mathbb{Z}$$

$$= a(rp) + b(rs)$$

entonces rc es combinación

□

• 12) Probar que si d es combinación de a y b , y b es combinación lineal de a y c entonces d es combinación de a y c .

Sea c una división de a y b entonces

$\rightarrow c$ es una división de a y c entonces

por hipótesis $a = el_a$ y $b = el_b$ y $d = el_d$

entonces $1l_a$ y $1l_c$ y $1l_b$

$$d = ar + bs$$

$$y \quad b = ax + cy$$

$$\text{entonces } d = ar + (ax + cy)s$$

$$= ar + axs + cys$$

$$d = a(r + xs) + c(ys) \quad r + xs \in \mathbb{Z} \quad ys \in \mathbb{Z}$$

entonces d es combinación de a y c

□

• 13) Demuestre que si a divide a los enteros b_1, b_2, \dots, b_n entonces

a divide a cualquier combinación de b_1, b_2, \dots, b_n e igualmente



$$a/b_1, a/b_2, \dots, a/b_k \Rightarrow a/b_1x_1 + \dots + b_kx_k \text{ para } x_1, \dots, x_k \in \mathbb{Z}$$

por inducción sobre k

• caso base $k=1$

$$\text{entonces } a/b_1 \quad \text{p.d. } a/b_1x_1$$

$$\text{por def. existe } a \cdot r = b \Rightarrow a \cdot (r x_1) = b x_1 \Rightarrow a/b x_1$$

ahora sup. qe $a/b_1, a/b_2, \dots, a/b_n \Rightarrow a/b_1x_1 + \dots + b_nx_n$
con $n < k$

• Paso Inducción

sup. $a/b_1, a/b_2, \dots, a/b_n, a/b_k$ p.d. $a/b_1x_1 + \dots + b_nx_n + b_kx_k$

por hip. $a/b_1x_1 + \dots + b_nx_n$, como a/b_k

entonces a/b_kx_k y p.d lo visto en clase

$$a/b_1x_1 + \dots + b_nx_n + b_kx_k$$

$$\boxed{\Rightarrow a/b_1x_1 + \dots + b_nx_n + b_kx_k \Rightarrow a/b_1, a/b_2, \dots, a/b_k}$$

por inducción sobre k

• caso base $k=1$

entonces $a/b_1x_1 \vdash a/b_1$

por hip $a \cdot q = b_1x_1$

$\Rightarrow a/b_1$

• hip sup se cumple para $m < k$

• paso inducción

entonces $a/b_1x_1 + \dots + b_kx_k$

por hip $a/b_1, a/b_2, \dots, a/b_{k-1}$

$\Rightarrow a/b_k$

□

$$a = bq + r$$

→ 1) Encuentra q y r para los siguientes pares de a y b

a) $a=0, b=-3 \quad 0 = -3(0) + 0$

b) $a=12, b=59 \quad 12 = 59(0) + 12$

c) $a=59, b=12 \quad 59 = 12(4) + 11$

d) $a=-59, b=12 \quad -59 = 12(-5) + 1$

e) $a=59, b=-12 \quad 59 = -12(-4) + 11$

f) $a=-59, b=-12 \quad -59 = -12(5) + 1$

g) $a=8611, b=-37 \quad 8611 = -37(232) + 27$

h) $a=-8611, b=-37 \quad -8611 = -37(233) + 10$

i) $a=-37, b=8611 \quad -37 = 8611(-1) + 8574$

j) $a=p^3+2p^2+2p+2 \quad p^3+2p^2+2p+2 = p+1(p^2+p+1) + 1$

$$b = p+1$$

$$p > 0$$

→ 2) Algoritmo de la división casos

i) $a < 0, b < 0$

consideren $B := \{a - bk \mid k \in \mathbb{Z}\} \cap (\text{NUEO})$

B no es vacío ya que $-ab \leq a < 0$ entonces $a - (-ab) > 0$

$\Rightarrow a - b(-a) > 0$

para el PBO $\exists r := a - bq$ para $q \in \mathbb{Z}$

y $a = b \cdot q + r = b \cdot q (a - bq)$
q es cero (demonstrar antes)

ii) $a < 0, b > 0$

consideremos $B := \{a - bk \mid k \in \mathbb{Z}\} \cap (\mathbb{N} \cup \{0\})$

B no es vacío ya que $b \geq 1$ entonces

$$-ab \geq -a \Rightarrow a - ab \geq 0$$

por el PBO $\exists r : a - bq \text{ con } q \in \mathbb{Z}$

$$a = bq + r = bq + (a - bq)$$

iii) $a > 0, b < 0$

consideremos $B := \{a - bk \mid k \in \mathbb{Z}\} \cap (\mathbb{N} \cup \{0\})$

B no es vacío ya que $a \in B$ ya que $a > 0$ y $a = a - b(0)$

por el PBO $\exists r : a - bq \text{ con } q \in \mathbb{Z}$

$$\text{tal que } a = bq + r = bq + (a - bq)$$

$r \in \mathbb{N}$

□

• 1) Demuestre que

$$(a, 0) = a \quad (\text{en particular } (0, 0) = 0)$$

sabemos que $a|a$ y pero sabemos que solo $0|0$

entonces a debe ser 0 y así $(0, 0) = 0$

$$(a, b) = 0 \Rightarrow a=0, b=0$$

supongamos que $a \neq 0$

entonces sabemos que cada entero se divide así mismo y

entonces $r, 0 \equiv a$ pero por def de null, a debe ser 0 .

análogamente b entonces $a, b = 0$

• 2) Demuestre

$$(a, b) = (|a|, |b|)$$

sabemos que el mcd siempre es positivo a y $|a|$ tiene

los mismos divisores entonces a tiene los mismos

por el PBC debe ser el mismo



• 3) Demuestre que $d = as + bt$ es la combinación menor y $\{da, db\}$
 y d es combinación de a y b en igualdad.

$\Rightarrow \exists$ sup $d = as + bt$, es la menor.

por los pasos anteriores sabemos que todo divisor de d también divide
 da y db

y d es menor que da y db

$\Leftarrow \exists$ sup d es combinación de a y b $\rightarrow da$ y db

(señalando) $da \mid d$ y $db \mid d$ (es divisor)

combinación menor que da y db es la menor

□

• 4) si $d = (a, b)$ y $d = ar + bs$ entonces r, s son primos entre sí

sea $k \in \mathbb{Z}$ tal que $kdr + kbs = kd$

sabemos que $da \mid kdr$ $\Rightarrow kd \mid da$

además $db \mid kbs$ $\Rightarrow kd \mid db$

$\Rightarrow kd \mid da + bs \Rightarrow kd \mid d \Rightarrow k \leq 1$ por
 lo tanto $(r, s) = 1$

• 5) Si $d = (a, b) \Rightarrow a = a'd, b = b'd$ probar que $a' \geq b'$:

son primos

como d divide tanto los factores primos de a y b ,
 a' y b' tienen que ser primos relativos.

$$\left. \begin{array}{l} d = as + bt \\ d = a'ds + b'dt \\ d = d(a's + b't) \end{array} \right\} \quad \left. \begin{array}{l} \text{1} \\ \text{1} \\ \square \end{array} \right.$$

• 6) Si $(a, b) = 1$ entonces $(b, c) = 1$

$$1 = as + bt \quad , \quad a = cq$$

$$1 = (cq)s + bt$$

$$1 = c(qs) + bt \quad \square$$

• 7) Si $d \mid a, d \nmid bc \quad y \quad (a, b) = 1$ Probar $d \mid c$

$$1 = as + bt \Rightarrow c = asc + bct$$

\therefore $d \mid a \Rightarrow d \mid asc \quad y \quad d \nmid bc \Rightarrow d \nmid bct$

$$\Rightarrow d \mid asc + bct$$

$$\therefore d \mid c \quad \square$$

• 8) Si a, b son primos entre sí, prueba que el mcd de a, bc es igual al de a, c

sea S el conjunto tal qe $S = \{x \in \mathbb{Z} \mid x \mid a \text{ y } x \mid bc\}$

sea S' el conjunto tal qe $S' = \{y \in \mathbb{Z} \mid y \mid a \text{ y } y \mid bc\}$

sea $x \in S'$ cualquiera por def $x \mid a$ y $x \mid bc$

sabes qe $(a, b) = 1$ entonces para el ejercicio 7

tienes qe $w \mid c$ por lo tanto $S' \subseteq S$

, $S \subseteq S'$ da qe $x \mid c \Rightarrow x \mid bc$

$\Rightarrow S = S'$

y por lo tanto el mcd de a, bc = al mcd de a, c

• 9) si $m^l > 0$ multiplo comn de a, b disto a todos

los multiplos comns de a, b entonc $m^l = m$

coms $m^l \mid$ todos los multiplos de a, b entonces debe

$m^l \mid m$ p. syp qe $m^l \neq m$ entonces $m^l < m$

pues m es el mnmo \therefore ento $m^l = m$ \square

$a \wedge b$

- 10) Probar que el mcm de dos primos entre si es $\text{lcm}[a, b]$ producto

por lo visto en lc pg 192

$$ab = [a, b] [a, b]$$

y como $a \wedge b$ son primos entre si $(a, b) = 1$

$$\Rightarrow ab = 1 [a, b] \Rightarrow ab = [a, b] \quad \square$$

- 11) Si a, b son primos entre si y $a|c, b|c$

entonces $[a, b] = ab$ y como el mcm divide a todos

los multiplos comunes entre $ab|c$ \square

- 12) Dados $d = (a, b)$, $a = a'd$, $b = b'd$. Si $a|c, b|c$

entonces $a'b'd|c$

por el ejercicio 5 $a \wedge b$ son primos entre si y

por el ejercicio 11 $ab|c$ entonces $d = 1$



$$a'db'd|c = a'b'd|c$$

$$= a'b'd|c \quad \square$$

• (3) Si a, b relativos entre $ab = (a,b)[a,b]$
 $a_0 \vee b_0$

Sea $(a,b) = d$ ento d es primo relativo tal q

$$a = da_0 \Rightarrow b = db_0$$

$$\text{PO } [a,b] = da_0b_0$$

da_0b_0 es múltiplo de a, b veas q es el menor!

Sea m otro mltiplo de a, b PO $da_0b_0 \mid m$

$$m = kq, q \text{ es al n} \quad m \neq kq \Rightarrow m \neq ka_0b_0$$

$$\Rightarrow \text{entro } b_0 \mid m \Rightarrow b_0 \mid kq_0$$

y como $a_0 \vee b_0$ son primos relativos $b_0 \mid k$ cmo

$da_0b_0 \mid m$ \square

• (4) Si $k > 0$ demostrar

$$(ka, kb) = k(a, b)$$

$$(ka, kb) = kas + kbt \Rightarrow (a, b) = ast + bt$$

$$k(a, b) = k(ast + bt) = kas + kbt$$

$$kas + kbt \mid ka \quad \text{por q } ast + bt \mid k$$

$$\Rightarrow kas + kbt \mid kb$$

$$\text{entonces } kas + kbt = (ka, kb) = k(a, b)$$

$$[ka, kb] = k[a, b]$$

sabemos que $(ka, kb) = k(a, b)$

$$[ka, kb]k(a, b) = k^2 ab = k^2 a, b$$

$$[ka, kb] = k[a, b] \quad \square ?$$

• 15) Si: a_1, a_2, \dots, a_n enteros, $d_i = (a_1, a_2, \dots, a_n)$

$$\text{para } 2 \leq i \leq n \text{ pu } d_i = (d_{i-1}, a_i)$$

Case base $T=2$

$$\text{entonces } d_2 = (a_1, a_2) \quad \text{y} \quad d_2 = (d_1, a_2)$$

entonces se cumple

sup que si $i < n$

por inducción $T=n$

$$\text{sea } d_n = (a_1, a_2, \dots, a_n) \Rightarrow a_1 x_1 + a_2 x_2 + \dots + a_{n-1} x_{n-1} + a_n x_n$$

$$d_n = (d_{n-1}, a_n) \Rightarrow (a_1 x_1 + a_2 x_2 + \dots + a_{n-1} x_{n-1}) x_{n-1} + a_n x_n$$

por hip

$d_n | a_1, d_n | a_2, \dots, d_n | a_n$

□

$d_n | d_{n-1}$ y $d_n | a_n$

por hip se cumple?

• 16) Si $a_1, a_2, \dots, a_n \rightarrow d_1 = [a_1, a_2, \dots, a_n]$

per $d_i = [d_{i-1}, a_i]$

caso base $i=2$

a_1

↑

$$d_2 = [a_1, a_2] \rightarrow d_2 = [d_1, a_2] \quad \checkmark$$

hp sup se cumple per i en

PO para $i=1$

$$d_1 = [a_1, a_2, \dots, a_n] \Rightarrow a_1/d_1, a_2/d_1, \dots, a_n/d_1$$

$$\rightarrow d_n = [d_{n-1}, a_n] \rightarrow d_{n-1}/d_n \rightarrow a_n/d_n$$

per hp

$$a_1/d_1, \dots, a_n/d_{n-1}$$

$$\Rightarrow a_1/d_n, \dots, a_n/d_n$$

□

- 1) Si $a = bq + r$ entonces $(a, b) = (b, r)$
- Sea S el conjunto de los divisores de a, b
 v sea S' el conjunto de los divisores de b y r
- sea $d \in S$ entonces $d | a$ y $d | b$ entonces $d | (a - bq)$
 entonces $d | r$ entonces $d | r$ y $d \in S'$
- sea $d \in S'$ entonces $d | b$, $d | r$ entonces $d | (bq + r)$
- entonces $d | a$ entonces $d \in S$
- entonces $S = S'$ \square
- 2) Encuentra el mcd de
- 329, 1005 = 1
 - 1302, 1224 = 6
 - 1816, -1789 = 1
 - 666, -12309 = 3
- 3) el mcd de
- $\overbrace{2784, 4988, 8944}^{112} = 4$
 - $\overbrace{103224, 31416, 3932, 840}^{\sqrt{4488}} = 24$

4) $2n+1 = 2n - 3$

$$2n^2 - 2n - 40 = 0 + 7$$

o 4) combi, teard de

a) $228, 348 \Rightarrow 12 = -3 + 228 + 2 + 348$

b) $15, 21 \Leftarrow 3 = 3 * 15 - 2 * 21$

$$4_1 = (2n+1) + (2n-1)$$

c) $2n+1, 4_1 = 21 = n \cdot (4_1) + -(2n-1)(2+1) 2n+1 = (2n-1) + 2$

$$2n-1 = 2(n-1) + 1$$

d) $4_1^2 + 2n - 40, 2n+7 = 1 \in 4_1^2 + 2n - 40 (-n-3) + 2n+7 (2_1^2 - 6n+1)$

o 5) \sim si tiene solucns enteras

a) $35x + 17y = 14 \quad (35, 17) = 1 \quad (\text{tiene solucion})$

b) $1242x + 1476y = 49 \quad (1242, 1476) = 18 \quad (\text{no tiene solucion})$

c) $15x + 21y = 10 \quad (15, 21) = 3 \quad (\text{no tiene solucion})$

o 6) solucns

a) $696x + 408y = 48 \quad (696, 408) = 24 = -7 \cdot 696 + 12 \cdot 408$

$$\begin{cases} x = -14 \\ y = 24 \end{cases} \quad 48 = 24 + 2$$

b) $(6n+1)x + 3ny = 12 \quad (6n+1, 3n) = 1 = 6n+1 - 2 \cdot 3n$

$$\begin{cases} x = 12 \\ y = -24 \end{cases} \quad 12 = 1 \cdot 12$$

• 7) calah tots laagelwant

$$a) 15x + 21y = 300$$

$$\begin{array}{r} 3x \\ \times 7 \\ \hline 21x \end{array}$$

$$(15, 21) = 3 = 3 \cdot 15 - 2 \cdot 21$$

$$1 \cdot x = 300 \quad x = -200$$

$$x = 300 - 7t \quad y = -200 + 5t$$

$$\begin{array}{r} 12x 19 \\ 12x 29 \\ \hline \end{array}$$

$$b) 228x - 348y = 1368$$

$$(228, -348) = 12 = -3 \cdot 228 + 2 \cdot -348$$

$$x = -342 + 27t$$

$$y = -228 + 19t$$

$$x = -342 \quad y = -228$$

$$\begin{array}{r} 18x 67 \\ 18x 82 \\ \hline \end{array}$$

$$c) 1242x + 1476y = 90$$

$$(1242, 1476) = 18 = -18 \cdot 1242 + 16 \cdot 1476$$

$$x = -95 - 82t$$

$$y = 80 + 69t$$

$$x = -95 \quad y = 80$$

$$d) (4n+1)x + 2ny = n$$

$$(4n+1, 2n) = 1 = (4n+1) \cdot 1 + (2n) \cdot -2$$

$$x = n - 2nt \quad y = -2n + (4n+1)t$$

$$x = n \quad y = -2n$$

$$(2n+1) \cdot 1 \quad (4n) \cdot -1$$

$$e) (2n+1)x + 4ny = n$$

$$(2n+1, 4n) = 1 = (4n) \cdot n + (2n+1) \cdot -(2n-1)$$

$$x = -2n^2 + n \quad y = n^2 + (2n+1)t$$

$$x = -2n^2 + n \quad y = n^2$$

• 1) Si a es divisible por p , a demostrar que $p | ab \Rightarrow p | a \circ p | b$

- suposición que p no divide a ninguno de los dos

$$\text{entonces } (p, a) = 1 = (p, b)$$

$$ps + at = 1 \quad pr + bq = 1$$

$$1 = pspr + psbq + atr + atbq$$

$$1 = p(pr + sbq + atr) + ab(tq) \Rightarrow$$

$$1 = (p, ab)$$

□

• 2) Si p y q son primos distintos entonces $(p, q) = 1$

los divisores de p son $\{\pm 1, \pm p\} = A$

y los de q son $\{\pm 1, \pm q\} = B$

$$A \cap B = \{\pm 1\} \text{ por PBO } (p, q) = 1$$

□

• 3) Si $p | a_1 a_2 \dots a_n \Rightarrow p | a_i$ para $1 \leq i \leq n$

Inducir sobre n

Caso base $n=1$

$$p_1 = a = q_1 \dots q_s$$

$$q_1 = p_1 \Rightarrow j = q_2 \dots q_s$$

$$\therefore s=1 \therefore p_1 = q_1$$

$$\sup \text{ que } p_1 \cdots p_n \cdots p_{n+1} = q_1 \cdots q_s$$

$$\Rightarrow p_1 = q_1 \quad \text{y} \quad p_2 \cdots p_{n+1} = q_2 \cdots q_s$$

$$p \leftarrow \text{hyp} \quad p_2 = q_2 \cdots \quad q_n = q_{s-1} \quad \Rightarrow \quad p_{n+1} = q_s \quad \square$$

• 4) Si $p \mid b^n \Rightarrow p \mid b$

$$p \mid b^n = b \cdot b \cdots b \quad \xrightarrow{\text{mres}} \quad p \mid \text{ejercicio anterior}$$

$p \mid b$ a alguna

□

• 5) Demstrar que 3×4 son falsos si p no es primo

$$4) \quad 14 \mid 2^5 \quad \text{poc} \quad 4 \nmid 2$$

$$3) \quad 4 \mid 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \quad \text{poc} \quad 4 \nmid 2 \quad \square$$

• 6) Demstrar por PBO que todo entero mayor que 1 es divisible

por un primo

cada entero se puede poner como factorización de primos
entre ellos al menos uno de esos lo divide

□

• 7) Demuestra que hay una infinidad de primos

Supongamos que solo hay p_1, \dots, p_n primos

Sea P el producto de todos $P = p_1 p_2 \dots p_n$ y sea

$$q = P + 1 \quad , \text{ dos casos.}$$

(1) q es primo \rightarrow no está en la lista y termina.

(2) no es primo, entonces un p_k divide a q .

Si esta p_k está en la lista más $p_k \mid P$ por $p_k \mid P + 1 \Rightarrow q$

Si p_k divide a P y q entonces $(P+1) - P = 1$, y como ningún primo divide a 1, p_k no aparecerá en la lista.

entonces hay uno más \square

• 8) si a es un entero positivo y a no es primo, entonces existe

un primo de p que $p \leq \sqrt{a}$

Sea a un número compuesto, entonces tiene un factor b que $1 < b < a$

$$\text{entonces } p \mid a = bq \text{ con } q \in \mathbb{Z} \text{ y } q > 1 \quad (1)$$

$$\text{PD } b \leq \sqrt{a} \text{ o } q \leq \sqrt{a}$$

Si $b > \sqrt{a}$, $\therefore q > \sqrt{a}$ entonces $bq > \sqrt{a} \cdot \sqrt{a} = a$!

entonces $b \leq \sqrt{a}$ o $q \leq \sqrt{a}$

como b y q dividen a entonces a tiene una descomposición

el cual es primo o tiene un divisor primo

entonces a tiene un divisor primo $\leq \sqrt{a}$ 77

• 9) encontrar los primos menores que 150 y mayores 113

113, 127, 131, 137, 139, 149, 151

• 10) a, b enteros $\neq 0$

$$(1) (a, b) = p_1^{\delta_1} p_2^{\delta_2} \cdots p_n^{\delta_n} \text{ con } \delta_i = \min\{\alpha_i, \beta_i\}$$

$$a = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_n^{\alpha_n} \quad b = p_1^{\beta_1} p_2^{\beta_2} \cdots p_n^{\beta_n}$$

$$\therefore \text{PD } (p_1^{\delta_1}, p_2^{\delta_2}, \cdots, p_n^{\delta_n}) \mid a \quad \text{y} \quad p_1^{\delta_1} \cdot p_2^{\delta_2} \cdots p_n^{\delta_n} \mid b$$

$$\text{veremos que } \delta_i + z_i = \alpha_i \quad \text{con} \quad z_i \in \mathbb{N} \cup \{0\}$$

$$\therefore \delta_i + w_i = \beta_i \quad \text{con} \quad w_i \in \mathbb{N} \cup \{0\}$$

entonces

$$(p_1^{z_1} p_2^{z_2} \cdots p_n^{z_n}) \cdot (p_1^{\delta_1} \cdot p_2^{\delta_2} \cdots p_n^{\delta_n}) = a$$

$$(p_1^{w_1} p_2^{w_2} \cdots p_n^{w_n}) \cdot (p_1^{\delta_1} \cdot p_2^{\delta_2} \cdots p_n^{\delta_n}) = b \quad \therefore (a, b) \mid a$$

$$\times (a, b) \mid b$$

Norma

ii) si $\text{clay} \subsetneq p\mathbb{Q}$, $p \mid \frac{\alpha_1}{p_1} \cdots \frac{\alpha_k}{p_k}$

$\sup_{p \in \mathbb{P}}$ $q \in p\mathbb{Z}$ $p \mid \frac{\alpha_1}{p_1} \cdots \frac{\alpha_k}{p_k} \Rightarrow p \in \{p_1, \dots, p_k\}$

$p \in \mathbb{P}$, $q \in p\mathbb{Z}$ $\Rightarrow p \mid q$

$\Rightarrow p \mid \frac{\alpha_1}{p_1} \cdots \frac{\alpha_k}{p_k} \Rightarrow p \mid \frac{\alpha_i}{p_i} \Rightarrow p \mid p_i \Rightarrow p = p_i$

$\therefore p \in \{p_1, \dots, p_k\}$

ahora si $p_i \mid c$ veas $q \in \mathbb{Z}$ $x_i \leq a_i$

si $x_i > a_i \Rightarrow p_i^{x_i} \mid c \wedge \text{clay} \Rightarrow p_i^{x_i} \mid c$

$$\Rightarrow p_i^{x_i} \cdot q = \frac{a_1}{p_1} \cdot \frac{a_2}{p_2} \cdots \frac{a_i}{p_i} \cdots \frac{a_k}{p_k}$$

$x_i > a_i \Rightarrow \exists n \in \mathbb{N} \quad \exists h \in \mathbb{Z} \quad x_i = a_i + h$

$$\Rightarrow \frac{a_i + h}{p_i} \cdot q = \frac{a_1}{p_1} \cdot \frac{a_2}{p_2} \cdots \frac{a_i}{p_i} \cdots \frac{a_k}{p_k}$$

$$\Rightarrow p_i^h \left(\frac{a_i + h}{p_i} \cdot q \right) = p_i^h \left(\frac{a_1}{p_1} \cdots \frac{a_{i-1}}{p_{i-1}} \frac{a_{i+1}}{p_{i+1}} \cdots \frac{a_k}{p_k} \right)$$

$$\Rightarrow p_i^h \cdot q = p_1^{a_1} \cdots p_{i-1}^{a_{i-1}} p_{i+1}^{a_{i+1}} \cdots p_k^{a_k}$$

$$\therefore p_i \mid p_1^{a_1} \cdots p_{i-1}^{a_{i-1}} p_{i+1}^{a_{i+1}} \cdots p_k^{a_k}$$

$\therefore p_i = p_i$ para $j \in \{1, \dots, i-1, i+1, \dots, k\}$!

$\therefore x_i \leq a_i$

analogamente $x_i \leq b_i$

$$(2) [a, b] = p_1^{\delta_1} p_2^{\delta_2} \cdots p_k^{\delta_k} \text{ con } \delta_i = \max\{\alpha_i, \beta_i\}$$

$$\text{i) } a \text{ PD } a \mid p_1^{\delta_1} \cdots p_k^{\delta_k} \quad b \mid p_1^{\delta_1} \cdots p_k^{\delta_k}$$

$$\exists n_i \in \mathbb{N} \cup \{0\} \quad \alpha_i + n_i = \delta_i$$

$$\exists m_i \in \mathbb{N} \cup \{0\} \quad \beta_i + m_i = \delta_i$$

$$p_1^{\delta_1} \cdots p_k^{\delta_k} = p_1^{\alpha_1 + n_1} \cdots p_k^{\alpha_k + m_k}$$

$$= p_1^{\alpha_1} \cdots p_k^{\alpha_k} (p_1^{n_1} \cdots p_k^{m_k})$$

$$= c_1 (p_1^{n_1} \cdots p_k^{m_k}) \quad \therefore a \mid p_1^{\delta_1} \cdots p_k^{\delta_k}$$

$$\text{analogamente } b \mid p_1^{\delta_1} \cdots p_k^{\delta_k}$$

$$\text{ii) sup } a \text{LCM } b \text{LCM } \text{PD } p_1^{\delta_1} \cdots p_k^{\delta_k} \mid c$$

$$\text{per h.p. } p_1^{\alpha_1} \cdots p_k^{\alpha_k} \mid c \vee p_1^{\beta_1} \cdots p_k^{\beta_k} \mid c$$

$$\text{enthus } C = p_1^{x_1} \cdots p_k^{x_k} \cdots p_l^{x_l} \Rightarrow \text{solo hen k factors (?)}$$

vears que $x_i \geq \alpha_i$

$$\text{sup } \alpha_i > x_i \quad \times \text{con } p_i^{\alpha_i} \mid c \quad \vee \text{aLCM}$$

$$\alpha_i = x_i + n$$

enthus

$$p_i^{\alpha_i} \cdot q = p_1^{x_1} \cdots p_k^{x_k}$$

$$p_i^{x_i+n} \cdot q = p_1^{x_1} \cdots p_k^{x_k}$$

$$p_i^{x_i} \cdot p_i^n \cdot q = p_i^{x_i} (p_1^{x_1} \cdots p_{i-1}^{x_{i-1}} \cdot p_{i+1}^{x_{i+1}} \cdots p_k^{x_k})$$

$$p_i \cdot q = p_1^{x_1} \cdot p_{i-1}^{x_{i-1}} \cdot p_{i+1}^{x_{i+1}} \cdots p_k^{x_k}$$

$$\Rightarrow p_i | p_i^n \Rightarrow p_i | p_1^{x_1} \cdot p_{i-1}^{x_{i-1}} \cdot p_{i+1}^{x_{i+1}} \cdots p_k^{x_k}$$

$$\therefore p_i = p_j \text{ for } j \in \{1, \dots, i-1, \dots, k\}!$$

i. $x_i \geq a_i$

ausgenom $x_i \geq a_i$

□

$$\text{def) } m, n \in \mathbb{Z} \quad p(m+n) = \min\{m, n\} + \max\{m, n\}$$

-caso 1 $m=n$

$$\text{entw: } m+n=2m \Rightarrow \min\{m, n\} = \max\{m, n\} = m$$

$$\Rightarrow m+n=2m = m+m = \min + \max$$

-caso 2 $m < n$

$$\text{entw: } \min\{m, n\} = m \Rightarrow \max\{m, n\} = n$$

$$\Rightarrow m+n = m+n$$

-caso 3 $n < m$

$$\text{entw: } mn = n \Rightarrow \max = n$$

$$\Rightarrow m+n = n+m$$

□

$$\bullet 12) \quad \text{PD} \quad ab = [a, b] [a, b]$$

$$\begin{aligned}
 ab &= \left(p_1^{\alpha_1} \cdots p_k^{\alpha_k} \right) \left(p_1^{\beta_1} \cdots p_k^{\beta_k} \right) \\
 &= p_1^{\max\{\alpha_1, \beta_1\}} \cdots p_k^{\max\{\alpha_k, \beta_k\}} \\
 &= p_1^{\max\{\alpha_1, \beta_1\} + \min\{\alpha_1, \beta_1\}} \cdots p_k^{\max\{\alpha_k, \beta_k\} + \min\{\alpha_k, \beta_k\}} \\
 &= \left(p_1^{\max\{\alpha_1, \beta_1\}} \cdots p_k^{\max\{\alpha_k, \beta_k\}} \right) \left(p_1^{\min\{\alpha_1, \beta_1\}} \cdots p_k^{\min\{\alpha_k, \beta_k\}} \right) \\
 &= [a, b] (a, b) \quad \square
 \end{aligned}$$

• 1) - P.D. si $a \equiv b \pmod{m}$ y $b \equiv c \pmod{m}$, entonces $a \equiv c \pmod{m}$

por hip $m \mid a-b \Rightarrow m \mid b-c$

$$\Rightarrow m \mid (a-b) + (b-c)$$

$$\Rightarrow m \mid a-c \Rightarrow a \equiv c \pmod{m} \quad \square$$

• 2) $a \equiv 0 \pmod{m}$ si y solo si $m \mid a$

$$a \equiv 0 \pmod{m} \Leftrightarrow m \mid a-0 \Leftrightarrow m \mid a \quad \square$$

• 3) si $a \equiv b \pmod{m}$ entonces $ac \equiv bc \pmod{m}$

por hip $m \mid a-b \Rightarrow m \mid c(a-b) \Rightarrow m \mid ca-cb$

$$\Rightarrow ac \equiv bc \pmod{m}$$

• 4) si $a+c \equiv b+c \pmod{m}$, entonces $a \equiv b \pmod{m}$

por hip $m \mid (a+c) - (b+c)$

$$(a+c) - (b+c) = a+c - b - c = a - b$$

$$\Rightarrow m \mid a - b \Rightarrow a \equiv b \pmod{m} \quad \square$$

05) Si $a \equiv b \pmod{m}$ y m, c son primos si

entonces $a \equiv b$

pr hip $m \mid (ac - bc) \Rightarrow m \mid c(a - b)$

y como $(m, c) = 1 \Rightarrow m \mid a - b \Rightarrow a \equiv b \pmod{m}$

06) Da ejemplo de si la condición del ejercicio anterior es falsa

$$5 \mid (15 \cdot 10 - 6 \cdot 10)$$

$$\text{pero } 5 \nmid (15 - 6)$$

07) PO

Si

$$a = mq_1 + r_1$$

$$0 \leq r_1 < m$$

$$b = mq_2 + r_2$$

$$0 \leq r_2 < m$$

entonces $a \equiv b \pmod{m}$ si y solo si $q_1 = r_2$

$\Rightarrow \boxed{\text{sup } a \equiv b \pmod{m}}$

pr hip $m \mid a - b \Rightarrow m \mid (mq_1 + r_1) - (mq_2 + r_2)$

sup que $r_1 \neq r_2$ entonces $m \mid m(q_1 - q_2) + r_3$ lo cual no se cumple
 $\rightarrow r_1 - r_2 = r_3$

$\Leftarrow \boxed{\text{sup } r_1 = r_2}$

entonces $a - b = (mq_1 + r_1) - (mq_2 + r_2) = m(q_1 - q_2)$

entonces $m \mid a - b \Rightarrow a \equiv b \pmod{m}$

\square

*) 8) En módulo 5, todo número es congruente con 0, 1, 2, 3 o 4

Sea $x \in \mathbb{Z}$ algún

Casos:

-caso 1 x de la forma $n5+0$ entonces $5|x \Rightarrow 5|x-0 \Rightarrow x \equiv 0 \pmod{5}$

-caso 2 x de la forma $n5+1$ entonces $5|x-1 \Rightarrow x \equiv 1 \pmod{5}$

-caso 3 x de la forma $n5+2$ entonces $5|x-2 \Rightarrow x \equiv 2 \pmod{5}$

-caso 4 x de la forma $n5+3$ entonces $5|x-3 \Rightarrow x \equiv 3 \pmod{5}$

-caso 5 x de la forma $n5+4$ entonces $5|x-4 \Rightarrow x \equiv 4 \pmod{5}$

*) 9) Si p es primo positivo ent. $ab \equiv 0 \pmod{p}$ implica

$$a \equiv 0 \pmod{p} \text{ o } b \equiv 0 \pmod{p}$$

por hip $p | ab \rightarrow p -$ lo visto arriba

$$p | a \Rightarrow p | a - 0 \Rightarrow a \equiv 0 \pmod{p}$$

$$p | b \Rightarrow p | b - 0 \Rightarrow b \equiv 0 \pmod{p}$$

*) 10) Da ejemplos en que $ab \equiv 0 \pmod{m}$ con $a \neq 0 \pmod{m}$ y $b \neq 0 \pmod{m}$

$$36 \equiv 0 \pmod{6} \quad \text{pero} \quad 9 \not\equiv 0 \pmod{6} \quad y \quad 4 \not\equiv 0 \pmod{6}$$

$$36 \equiv 0 \pmod{12} \quad \text{pero} \quad 9 \not\equiv 0 \pmod{12} \quad y \quad 4 \not\equiv 0 \pmod{12}$$

• 11) \exists $a \equiv b \pmod{m}$ \wedge $c \equiv d \pmod{m}$ entw.

$$a \pm c \equiv b \pm d \pmod{m} \quad \wedge \quad ac \equiv bd \pmod{m}$$

per hip $m \mid a-b$ \wedge $m \mid c-d$

$$\Rightarrow m \mid (a-b) + (c-d) \Rightarrow m \mid a+c - b-d$$

$$\Rightarrow a \pm c \equiv b \pm d \pmod{m}$$

$$\wedge \exists k_1 \in \mathbb{Z} \text{ s.t. } a = b + k_1 m \quad \wedge \quad \exists k_2 \in \mathbb{Z} \text{ s.t. } c = d + k_2 m$$

$$\text{entw. } ac = (b+k_1 m)(d+k_2 m) = bd + (bk_2 + dk_1)m + k_1 k_2 m^2$$

$$\wedge \text{ per def. } ac \equiv bd \pmod{m} \quad \square$$

• 12) \exists $a \equiv b \pmod{m}$ entw. $b = a + km$ prado de 1c

per hip $m \mid a-b$ entw.

$$a-b = m k \quad \text{entw. } b = a + m(k)$$

\square

• 13) \exists $a \equiv b \pmod{m}$ con $0 \leq a < m$, $0 \leq b < m$ restw. $a = b$

sup $a \neq b$ \wedge $m \nmid a-b$

restw. $a-b \neq 0 \quad \wedge \quad -m < a-b < m$ per lo tabo $m \nmid a-b$

$$\therefore a = b \quad \square$$

• 14) sup x_1 y x_2 soluciones p.d. $x_1 \equiv x_2 \pmod{m}$

p.h.p. $ax_1 + b \equiv 0 \pmod{m}$

$$ax_2 + b \equiv 0 \pmod{m}$$

$$n | x_1 - x_2$$

entonces $m | ax_1 + b$ y $m | ax_2 + b$

$$\Rightarrow m | (ax_1 + b) - (ax_2 + b)$$

$$\Rightarrow m | a(x_1 - x_2) \text{ y como } (a, m) = 1 \text{ ent.}$$

$$m | (x_1 - x_2) \Rightarrow x_1 \equiv x_2 \pmod{m} \quad \square$$

• 15) si $ax + b \equiv 0 \pmod{m}$ tiene solucn s1 y s2 solo si

$$(a, m) | b$$

\Rightarrow supongamos $ax + b \equiv 0 \pmod{m}$ tiene solucn y por la prop 3

como tiene solucn otros existe $x' y' \in \mathbb{Z}$ tales que

$$b = ax + my \quad \text{sen } d = (a, m)$$

$$d | a \rightarrow d | m \Rightarrow d | ax \rightarrow d | my \Rightarrow d | (ax + my) \\ d | b$$

\Leftarrow supongamos $(a, m) = d \neq 1 \wedge d | b$

$$\text{existe } r, s \in \mathbb{Z} \text{ tal que } d = ra + sm$$

$$\text{ent. } b = cd \Rightarrow b = c(ra + sm) = a(cr) + m(cs)$$

$$\Rightarrow ax + b \equiv 0 \pmod{m} \text{ tiene solucn}$$



• 6) Si x_1 y x_2 son soluciones del sistema en $x_1 \equiv x_2 \pmod{mn}$

hay una solución t tal que $0 \leq t < rs$.

$$\text{P.D.: } x_1 \equiv x_2 \pmod{mn}$$

sabemos que $x_1 - x_2$ es múltiplo de $m \cdot n$

$$\therefore [m, n] \mid x_1 - x_2$$

$$\Rightarrow mn \mid x_1 - x_2$$

$$\therefore x_1 \equiv x_2 \pmod{mn} \quad \square$$

• 7) Si m_1, m_2, \dots, m_n son primos relativos dos a dos

entonces $x \equiv a_1 \pmod{m_1}, x \equiv a_2 \pmod{m_2}, \dots, x \equiv a_n \pmod{m_n}$

tienen solución en común

por inducción sobre n

• caso base

si $n=1$ entonces si tiene solución

• hipótesis para $n=j$ con $1 < j < k$ tiene solución en común

• paso de inducción $n=k$

sea x una solución de

$$\begin{cases} x \equiv a_1 \pmod{m_1} \\ x \equiv a_2 \pmod{m_2} \\ \vdots \\ x \equiv a_{k-1} \pmod{m_{k-1}} \end{cases} \quad (t+)$$

• si $k \in \mathbb{Z}$ ento $s + n_1 n_2 \cdots n_{k-1}^k \rightarrow$ solución de $(t+)$

ahora encontramos un k_0 tal que $s + n_1 n_2 \cdots n_{k-1} k_0 \equiv a_k \pmod{n_k}$

basta resolver la congruencia

$$n_1 n_2 \cdots n_{k-1} x + (s - a_k) \equiv 0 \pmod{n_k} \quad (\star \star)$$

para un teorema $(\star \star)$ bien sabremos si $(n_1 n_2 \cdots n_{k-1}, n_k) = 1$

sea $(n_1 n_2 \cdots n_{k-1}, n_k) = d$ PD $d = 1$

si $d > 1$ entonces considera p un primo divisor de d

$$\Rightarrow p | n_1 n_2 \cdots n_{k-1} \Rightarrow p | n_k$$

$$\Rightarrow p | n_1 \Rightarrow p | n_k$$

$$\Rightarrow (n_1, n_k) \geq p > 1 \quad ! \quad p = 900 \quad (n_1, n_k) = 1$$

$$\therefore (n_1 n_2 \cdots n_{k-1}, n_k) = 1$$

$$\square \quad ax + b \equiv 0 \pmod{n}$$

$$\begin{aligned} t &= -b \\ &\rightarrow axt \equiv -b \\ &\rightarrow xt \equiv -b \\ &\rightarrow x \equiv -b^{-1}t \end{aligned}$$

• 18) resolver las siguientes congruencias

a) $16x - 9 \equiv 0 \pmod{35}$ $x = (+9 \cdot 11) = 99 = 29 + 35k$

b) $200x + 315 \equiv 0 \pmod{441}$ $x = (-315 \cdot 86) = -27090 =$

c) $(2n+1)x + 7 \equiv 0 \pmod{4n}$ $x = (-7 \cdot 2n+1)) = -14n + 7 =$

d) $(3n-2)x + 5n \equiv 0 \pmod{9n-9}$ $x = (-5n \cdot -3n+4) = 15n^2 - 20n =$

103

20

$$x = 3(8f) = 24k \quad (24)$$

• 19) resuelve

$$\rightarrow 0+3k$$

a) $x \equiv 0 \pmod{3}$
 $x \equiv 0 \pmod{8}$

$$3k + (0-0) \equiv 0 \pmod{8}$$

$$3k \equiv 0 \pmod{8}$$

$$k = 0+8f$$

b) $x \equiv 1 \pmod{25}$
 $x \equiv 7 \pmod{35}$

no hay solución ya que $(25, 35) \neq 1$

c) $x \equiv 3 \pmod{11} \rightarrow 3+11k \quad |$
 $x \equiv 4 \pmod{21} \quad |$
 $x \equiv 5 \pmod{25} \quad |$

$$11k + (3-4) \equiv 0 \pmod{21}$$

$$k = (+1 \cdot 5) = 5$$

$$\rightarrow 5+21f$$

$$21f + (5-5) \equiv 0 \pmod{25}$$

$$21f \equiv 0 \pmod{25}$$

$$f = (6+25g) \quad ??$$

①

$$x = 8925f + 2230$$

o 19)

a)

$$\begin{aligned}x &\equiv 0 \pmod{3} \\x &\equiv 8 \pmod{8}\end{aligned}$$

$$x=0$$

$$x=24$$

$$N = 8 \times 3$$

$$N_i = \frac{N}{n_i}$$

$$b_i \quad N_i \quad x_i \quad b_i N_i x_i$$

$$0 \quad 0 \quad 8$$

$$0$$

$$0$$

b)

$$x \equiv 1 \pmod{25}$$

$$x \equiv 7 \pmod{35}$$

no other solution

$$x \equiv 0 \pmod{24}$$

c)

$$x \equiv 3 \pmod{17}$$

$$x \equiv 4 \pmod{21}$$

$$x \equiv 5 \pmod{25}$$

$$N = 17 + 21 + 25$$

$$N_i = \frac{N}{n_i}$$

$$b_i \quad N_i \quad x_i \quad b_i N_i x_i$$

$$3$$

$$525$$

$$25$$

$$39357$$

$$4$$

$$425$$

$$38$$

$$64600$$

$$5$$

$$357$$

$$43$$

$$76755$$

$$15x_1$$

$$11$$

$$525x_1 \equiv 1 \pmod{17}$$

$$425x_2 \equiv 1 \pmod{21}$$

$$357x_3 \equiv 1 \pmod{25}$$

$$x \equiv 180730 \pmod{8925}$$

$$x \equiv 2230 \pmod{8925}$$

$$2230 = 180730 - (20 \cdot 8925)$$

•20) Los tablas están bien

•21) Tabla de multiplicación

\mathbb{Z}_2

\times	0	1
0	0	0
1	0	1

\mathbb{Z}_3

\times	0	1	2
0	0	0	0
1	0	1	2
2	0	2	1

\mathbb{Z}_4

\times	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

\mathbb{Z}_5

\times	0	1	2	3	4	5
0	0	0	0	0	0	0
1	0	1	2	3	4	5
2	0	2	4	0	2	4
3	0	3	0	3	0	3
4	0	4	2	0	4	2
5	0	5	4	3	2	1

•22) suma y producto en \mathbb{Z}_m

$+ : \mathbb{Z}_m \times \mathbb{Z}_m \rightarrow \mathbb{Z}_m$

$a+b \mapsto r$

$$r = (a+b) - mq$$

$$(a+b) \% m$$

$\times : \mathbb{Z}_m \times \mathbb{Z}_m \rightarrow \mathbb{Z}_m$

$ab \mapsto s$

$$s = (ab) - mq'$$

$$(ab) \% m$$

•23) ver que \mathbb{Z}_m valen las leyes de los números (ra distributiva)

i) commutativa $\forall a, b \in \mathbb{Z}_m \quad ab = ba$

$$ab = mq_1 + r$$

$$ba = mq_2 + s$$

com

$$r \equiv (ab) = (ba) \equiv s \pmod{m} \Rightarrow r = s$$

ejer ejercito 13

Norma

$$\therefore a+b = b+a$$

ii) asociativa Sean $a, b, c \in \mathbb{Z}_m$ PO $(a+b)+c = a+(b+c)$

$$(a+b)+c = mq_1+r \quad \Rightarrow \quad a+(b+c) = mq_2+s$$

$$r \equiv (a+b)+c = a+(b+c) \equiv s \pmod{m}$$

$$\Rightarrow r=s \Rightarrow (a+b)+c = a+(b+c)$$

ejercicio 13

iii) elemento neutro PO $a+0 = 0+a = a$ Sea $a \in \mathbb{Z}_m$

por la suma de naturales sabemos que $a+0=a$

iv) inverso aditivo Sean $a \in \mathbb{Z}_m$ PO $a+x=0$

$$\text{sea } x=-a$$

entonces $a+(-a)=0$ por la t^{er} en IN

v) commutativa Sean $a, b \in \mathbb{Z}_m$ PO $ab = ba$

$$ab = mq_1+r \quad \Rightarrow \quad ba = mq_2+s$$

$$r \equiv ab = ba \equiv s \pmod{m}$$

$$r=s \Rightarrow ab = ba$$

vi) asociativa Sean $a, b, c \in \mathbb{Z}_m$ PO $(ab)c = a(bc)$

$$(ab)c = mq_1+r \quad \Rightarrow \quad a(bc) = mq_2+s$$

$$r \equiv (ab)c = a(bc) \equiv s \pmod{m}$$

$$r=s \Rightarrow (ab)c = a(bc)$$

vii) a es de neutro $\exists a \in \mathbb{Z}_m \quad m \geq 1$

entonces para todo $m = \{0, 1, \dots, m-1\}$ estu cl 1

$$y a \cdot 1 = a$$

viii) Ya demostrado

* 24) Demostremos que \mathbb{Z}_p es un dominio entero con primos

$$\mathbb{Z}_p = \{0, 1, \dots, p-1\} \text{ enteros nulos dividible por } p$$

entonces si $ab=0$ las únicas opciones son que

$a=0$ o $b=0$ ya que como nulos dividible a p siempre

$p \nmid ab$

* 25) $\mathbb{Z}_4 \times \mathbb{Z}_6$ no son dominios enteros

en \mathbb{Z}_4

$$2 \cdot 2 = 0$$

pero $2 \neq 0$

y en \mathbb{Z}_6

$$4 \cdot 3 = 0$$

pero $4, 3 \neq 0$