Congruencias.

Def.11. Dado un entero positivo, n, se dice que dos enteros a, b son "congruentes módulo n" si y sólo si b-a es múltiplo de n.
ojo : esto significa, como estamos trabajando en el dominio de integridad , **Z**, de los enteros, que existe un **entero**, h, tal que b-a = h.n .
En tal caso, se escribe : $a \equiv b \pmod n$ o también $a \underset{n}{\equiv} b$.

Proposición 3.
La relación $x \equiv y \pmod n$, definida en el conjunto **Z** de los enteros, es una relación de **equivalencia**.
Demostración.
1) $x-x=0=0.n$ indica que $\underset{n}{\equiv}$ es reflexiva;
2) si $y-x=h.n$ (con h entero), tenemos $x-y = -(y-x)=(-h).n$ (con -h entero) y esto indica que $\underset{n}{\equiv}$ es simétrica ;
3) si $y-x=h.n$, $z-y=k.n$ (con h, k enteros) se tiene :
$z-x = (z-y)+(y-x)= h.n+k.n = (h+k).n$, lo cual indica que $\underset{n}{\equiv}$ es transitiva.

Proposición 4.
La relación $\underset{n}{\equiv}$ es compatible con las operaciones usuales de suma y multiplicación de enteros. [ver propiedad iii) en la sección 6-B del texto de Lindsay Childs, pag. 49 o propiedades 8.5, 8.6 del texto de Saulo Rada Aranda, pag.35]
Demostración.
Antes de demostrar lo afirmado, mencionemos que significa, más en general, que una relación, T, de equivalencia es "compatible" con cierta operación * .

Def. 12. Compatibilidad de una relación de equivalencia con una operación.
[o, si se prefiere : compatibilidad de una operación con una relación de equivalencia].
Sean T una relación de equivalencia y * una operación, ambas definidas en el mismo conjunto E. Se dice que la equivalencia T es compatible con la operación * , o también que la equivalencia T es regular respecto a * si y sólo si se cumple :

$\forall (x_1,x_2,y_1,y_2 \in E)$: si $x_1 T x_2$, $y_1 T y_2$ entonces $(x_1 * y_1) T (x_2 * y_2)$.

En palabras : "si se actúa con la operación sobre elementos equivalentes, se obtienen como resultados elementos equivalentes".

Demostremos primero la compatibilidad de la congruencia módulo n con la suma usual de enteros :
si $x_1 \underset{n}{\equiv} x_2$, $y_1 \underset{n}{\equiv} y_2$ entonces $x_2-x_1=h.n$, $y_2-y_1=k.n$, (con h, k enteros), luego
$(x_2+y_2)-(x_1+y_1)=x_2-x_1+y_2-y_1=h.n+k.n=(h+k).n$
es decir $(x_1+y_1) \underset{n}{\equiv} (x_2+y_2)$;
demostremos ahora la compatibilidad de la congruencia
módulo n con la multiplicación usual de enteros :
si $x_1 \underset{n}{\equiv} x_2$, $y_1 \underset{n}{\equiv} y_2$ entonces $x_2-x_1=h.n$, $y_2-y_1=k.n$, (con h, k enteros), luego
$(x_2y_2)-(x_1y_1)=(x_1+h.n)(y_1+k.n)-(x_1y_1)= x_1y_1+x_1.k.n+h.n.y_1+h.n.k.n- x_1y_1=$
$= n.(x_1.k+h.y_1+h.k.n)$ por lo cual la resta $(x_2y_2)-(x_1y_1)$
resulta ser múltiplo de n , es decir : $(x_1y_1) \underset{n}{\equiv} (x_2y_2)$.

Observación 7 (importante).
Una de las consecuencias de la proposición que acabamos de demostrar, es poner en evidencia que las congruencias tienen propiedades parecidas a las igualdades, como por ejemplo las siguientes :
i) Dos congruencias (relativas a un mismo módulo) se pueden sumar y multiplica "miembro a miembro"; en particular :
ii) en una congruencia es lícito sumar a ambos miembros un mismo número entero. En efecto, si $a \underset{n}{\equiv} b$, como para cualquier entero k se tiene $k \underset{n}{\equiv} k$ (¿porqué?) sigue
$(a+k) \underset{n}{\equiv} (b+k)$;
iii) en una congruencia es lícito multiplicar ambos miembros por un mismo número entero.
Estas propiedades son muy importantes, ya que, por ejemplo, serán útiles para resolver el problema análogo al problema de resolver una ecuación de primer grado en una incógnita :
"Hallar todos los enteros x tales que : $a.x+b \underset{n}{\equiv} 0$ ".

Ejemplo 13.
Resolver la congruencia : $7x+4 \underset{9}{\equiv} 2x+15$.
Sumando a ambos miembros (-2x-4) obtenemos :
$7x-2x+4-4 \underset{9}{\equiv} 2x-2x+15-4$,
luego $5x \underset{9}{\equiv} 11$;
luego, multiplicando ambos miembros por 2 :
$10x \underset{9}{\equiv} 22 \underset{9}{\equiv} 4$ y como $10x \underset{9}{\equiv} x$ (¿porqué?) tenemos al final :
$x \underset{9}{\equiv} 4$ es decir x-4=t.9, x= 9t+4 (con t entero arbitrario).
Es decir : una solución es $x_1=4$ y todas las demas se obtienen sumando un múltiplo entero de 9.
Podría Ud. preguntar como se podía saber que era conveniente multiplicar ambos miembros de la congruencia por 2, de manera que resultase $5.2=10 \equiv 1 \pmod 9$ y por lo tanto $10x \equiv x$.
Para eso conviene recordar el teorema 2 [pag. 8 de esta guía] :
como (5, 9)=1 , es posible hallar enteros s, t tales que sea
5s+9t=1 (por ejemplo s=2, t= -1) . De esta manera resulta
$5s \equiv 1 \pmod 9$; entonces multiplicando ambos miembros de la congruencia $5x \equiv 11$ por "s=2" , tenemos : $10x \equiv x \equiv 22 \equiv 4 \pmod 9$.
Ilustraremos este hecho con el ejemplo siguiente.

Ejemplo 14.
Resolver la congruencia $24x+1 \underset{8}{\equiv} 15x+90$.
Primeramente podemos escribir la congruencia dada, reemplazando 24 por 0 [ya que $24 \equiv 0 \pmod 8$] , 15 por 7 y 90 por 2 : $1 \underset{8}{\equiv} 7x+2$, luego, obteniendo
(7, 8) = 1 como combinación lineal de 7, 8 : $1 = (-1).7+1.8 \underset{8}{\equiv} (-1).7$,
nos damos cuenta que multiplicando ambos miembros de la congruencia dada por (-1), obtenemos : $-1 \underset{8}{\equiv} -7x-2 \underset{8}{\equiv} x-2$ de donde $x \underset{8}{\equiv} 2-1 = 1$, x = 1+8t .

E31. Resuelva las siguientes congruencias :
a) $40x \underset{9}{\equiv} 5$; **b**) $21x \underset{10}{\equiv} 8$; **c**) $27x \underset{25}{\equiv} 88$; **d**) $35x \underset{6}{\equiv} 43$;
e) $40x+16 \underset{9}{\equiv} 5$; **f**) $31x-14 \underset{10}{\equiv} 8$; **g**) $7x+100 \underset{25}{\equiv} 88$.

E32. Usando el teorema 2 [pag. 8 de esta guía], demuestre que toda congruencia del tipo $ax \equiv b \pmod n$ tiene solución, si $(a, n) = 1$.
E33. Construya varios ejemplos que pongan en evidencia que en el caso que $(a, n)=d >1$ la congruencia $ax \equiv b$ puede tener solución o no (y esto depende del valor que tiene b).
¿ que relación debe haber , entre b , (a, n) para que la congruencia tenga solución ?
E34. Demuestre que si $(c, n) = 1$ entonces en la congruencia $ca \equiv cb$ se puede "simplificar" por c , en el sentido que : si $ca \equiv cb$ entonces necesariamente $a \equiv b$.
E35. Dada una congruencia cualquiera, $ax \equiv b \pmod n$
i)Demuestre que si x_1 es una solución de la congruencia y si $x_1 \equiv x_2 \pmod n$ entonces necesariamente x_2 también es solución ;
ii)Demuestre que si x_1, x_2 son soluciones de la congruencia dada entonces no necesariamente $x_1 \equiv x_2 \pmod n$;
iii) Demuestre que si x_1, x_2 son soluciones de la congruencia dada entonces necesariamente $x_1 \equiv x_2 \pmod{n_1}$, siendo $n_1 = n/(a, n)$;

E36. Demuestre que si $(a, n) = 1$ entonces la congruencia $ax \equiv b \pmod n$ tiene exactamente una solución x_1 tal que $0 \le x_1 < n$.
E37. En el teorema 2 [pag. 8 de esta guía] se afirma que el (a, b) se puede expresar como combinación lineal (con coeficientes enteros) de a, b.
Demuestre que si un número entero, n, se puede expresar como combinación lineal $n=s.a+t.b$ de a, b (con coeficientes s, t enteros) entonces necesariamente n es múltiplo de (a, b).
[sugerencia : recuerde el ejercicio **E10** de esta guía].
E38. Diga, justificando, si es cierto o falso que un número entero, n, se puede expresar como combinación lineal $n=s.a+t.b$ de a, b (con coeficientes s, t enteros) si y sólo si n es múltiplo del máximo común divisor de a, b.
Ejemplo 15.
Resolvamos la congruencia $15x \equiv 42 \pmod{10}$.
Como $(15, 10) = 5$ y como 5 no divide a 42, esta congruencia no tiene solución.
Ejemplo 16.
Resolvamos la congruencia $318x \equiv 42 \pmod{45}$.
Como $(318, 45) = 3$ y como 3 divide a 42 , podemos observar que la congruencia dada es equivalente a la nueva congruencia : $106x \equiv 14 \pmod{15}$;
$(106, 15)=1$,
$1 = 1.106+(-7)15$, luego $106 \underset{15}{\equiv} 1$, $106x \underset{15}{\equiv} x \underset{15}{\equiv} 14$;
la solución es : $x=14 + 15.t$ (con t entero arbitrario).
E39. Resuelva las siguientes congruencias :
a) $39x \underset{9}{\equiv} 6$; **b**) $20x \underset{10}{\equiv} 8$; **c**) $265x \underset{25}{\equiv} 85$; **d**) $33x \underset{6}{\equiv} 43$;
e) $42x+17 \underset{9}{\equiv} 5$; **f**) $33x-14 \underset{121}{\equiv} 8$; **g**) $95x+100 \underset{25}{\equiv} 2550$.
E40. Demuestre que si $d=(a, n)$ divide a b entonces la congruencia $ax \equiv b \pmod n$ tiene exactamente d diferentes soluciones $x_1, x_2,...,x_d$ tales que, si $n_1 = \frac{n}{d}$:

$$0 \le x_i < n \ , \ x_i \equiv x_k \pmod{n_1} \ , \ i, k=1, 2,..., d.$$

Ejemplo 17.
La congruencia $318x \equiv 42 \pmod{45}$ tiene d= 3 soluciones (congruentes módulo 15) en el intervalo [0, 44] , a saber :
$x_1 = 14$, $x_2 = 29$, $x_3 = 44$.

E41. Demuestre que para todo número natural, n , y para todo número primo positivo, p, se tiene : $(n+1)^p \equiv n^p + 1 \pmod{p}$.

[Sugerencia : recuerde la fórmula del binomio de Newton y observe que el coeficiente $\binom{p}{k}$ es $\underset{p}{\equiv} 0$ si $0<k<p$].

E42. Diga, justificando, cuales de las siguientes afirmaciones son ciertas y cuales falsas :

a) en la congruencia $8x \equiv 42 \pmod{n}$, siempre se puede simplificar por 2, obteniendo : $4x \equiv 21 \pmod{n}$, que es equivalente a la anterior;

b) en la congruencia $8x \equiv 42 \pmod{n}$, sólo se puede simplificar por 2 si n es par;

c) en la congruencia $8x \equiv 42 \pmod{n}$, sólo se puede simplificar por 2 si n es impar;

d) la congruencia $8x \equiv 42 \pmod{2n}$, es equivalente a : $4x \equiv 21 \pmod{n}$, cualquiera que sea el entero positivo n.

E43. Demuestre que si un entero n es divisible por n_1, n_2 y si $(n_1, n_2) = 1$ entonces n es divisible por el producto $n_1.n_2$.
[Sugerencia : como $n = h.n_1 = k.n_2$ recuerde la "aplicación 2" del algoritmo de Euclides (pag. 11 de esta guía) y observe que n_1 debe dividir k, por lo cual $k = r.n_1$, $n = k.n_2 = r.n_1n_2$].

E44. Demuestre por inducción, que si un entero n es divisible por t enteros n_1, n_2,..., n_t, y si además $(n_i, n_k) = 1$ toda vez que sea $i \neq k$, entonces n necesariamente es divisible por el producto $\prod_{i=1}^{t} n_i$. ¿ Queda válido el resultado si en lugar de la hipótesis " $(n_i, n_k) = 1$ toda vez que sea $i \neq k$ " se considera la otra hipótesis : " $(n_1, n_2, ..., n_t) = 1$ " ?
[Sugerencia : considere el ejemplo $n_1=6$, $n_2=10$, $n_3=15$].

Axiomas de anillo y cuerpos.

Ya mencionamos en esta guía las definiciones de Dominio de integridad y de cuerpo (conmutativo). [ver definiciones **1**, **1'** en la pag. 3 de esta guía]
Enunciaremos ahora la definición de **anillo** :

Def.13 . anillo.
Un conjunto D con dos operaciones (suma y producto) se llama un **anillo** si :
i)la suma es asociativa, conmutativa, con neutro , 0, y con la propiedad del simétrico;
[esto se expresa también diciendo que (D, +) es un **grupo conmutativo**]
ii) la multiplicación es asociativa ;
[la multiplicación **no** necesariamente es conmutativa **ni** necesariamente tiene neutro **ni** necesariamente tiene la propiedad del simétrico para elementos $\neq 0$]
iii) vale la propiedad distributiva de la multiplicación respecto a la suma;

Ejemplo 17.
El conjunto $M_{(2,2)}$ de todas las matrices, de componentes enteras pares, de tamaño 2x2 con la suma usual de matrices y la multiplicación usual ("filas por columnas") de matrices es un anillo.

Def.13' . anillo con unidad, anillo conmutativo.
Si en un anillo hay elemento neutro para la multiplicación, [$\neq 0$], tal anillo se llama un "anillo con unidad" ;
Si en un anillo la multiplicación es conmutativa, tal anillo se llama un "anillo conmutativo".

Ejemplo 18.
El conjunto de todas las matrices de tamaño 2x2 con componentes enteras (o racionales, o reales) es una anillo con unidad (pero no es anillo conmutativo);
El conjunto de todas las matrices de tamaño 2x2 con componentes reales **no** es un dominio de integridad,[ver def. 1, pag. 3 de esta guía] ya que la multiplicación no es conmutativa ; observe también que dos matrices no nulas pueden tener producto nulo, por ejemplo, si $A=\begin{bmatrix}1 & 2\\ 1 & 2\end{bmatrix}$, $B=\begin{bmatrix}2 & 2\\ -1 & -1\end{bmatrix}$, resulta $AB=\begin{bmatrix}0 & 0\\ 0 & 0\end{bmatrix}$.

El conjunto de todos los polinomios, K[x], con coeficientes reales (o racionales) con las definiciones usuales de suma y multiplicación, es un anillo conmutativo con unidad [es además un dominio de integridad] .

El conjunto de todas las funciones continua $R\to R$, con las usuales operaciones de suma y multiplicación [mencionado en el ejercicio **E1** en la pag. 3 de esta guía] es un anillo conmutativo con unidad [pero no es un dominio de integridad] .

Los anillos $\mathbf{Z_n}$

Dado un entero positivo n, la relación definida en el conjunto **Z** de los enteros por :
$xTy \leftrightarrow y-x = h.n$ [es decir : $\leftrightarrow x \underset{n}{\equiv} y$] es una relación de equivalencia.
Indicaremos el conjunto cociente $(Z/\underset{n}{\equiv})$ con el símbolo $\mathbf{Z_n}$.

Def.14. Clases de equivalencia [ver también guía sobre relaciones] .
Si S es una relación de equivalencia definida en el conjunto E y $a \in E$, se llama clase de equivalencia, representada por a , y se indica con el símbolo $\mathbf{[a]_S}$ [o , cuando no haya peligro de ambigüedad, simplemente con [a] o inclusive a veces, con a , sin corchete], el subconjunto de E formado por todos los elementos de E que son equivalentes al elemento a considerado, es decir : $\mathbf{[a]_S} = \{x \in E \mid x\ S a\}$

Def.15 Conjunto cociente, E/S, de un conjunto E respecto a una relación de equivalencia, **S**, definida en E.
Se llama conjunto cociente de E respecto a la equivalencia, S, definida en E, al conjunto cuyos elementos son todas las diferentes clases de equivalencia de S en E.
Ejemplo 19. Sea E= {a, b, c, d, e} y sea S la relación definda en E por :
{(a, a), (b, b), (c, c), (d, d), (e, e), a, b), (b, a), (a, c), (c, a), (b, c), (c, b), (d, e), (e, d) };
se tiene entonces : $[a]_S=[b]_S=[c]_S = \{a, b, c\}$, $[d]_S=[e]_S=\{d, e\}$;
es decir, hay dos clases de equivalencia, a saber {a, b, c}, {d, e} ;

El conjunto cociente E/S={ {a, b, c}, {d, e} } ={ [a], [e] } tiene dos elementos;
Observe que las clases de equivalencia tienen las siguiente propiedades :
i) toda clase de equivalencia tiene almenos un elemento;
ii) dos clases de equivalencia diferentes no tienen elementos comunes;
iii) la unión de todas las clases de equivalencia es el conjunto E.

E45.- Considere el conjunto cociente definido en el ejemplo anterior [ejemplo 19] y diga, justificando, cuales de las siguientes afirmaciones son ciertas y cuales falsas :
i) $[a]_S \neq [c]_S$; **ii**) $a \neq c$; **iii**) $[a]_S \neq [d]_S$; **iv**) $[c]_S \neq [e]_S$;
v) E/S={ [a], [b], [c], [d], [e]} ; **vi**) E/S= E ; **vii**) $[a]_S \cap [d]_S = \varnothing$;
viii) $[a]_S \cap [c]_S = \varnothing$; **ix**) $[a]_S \cap [c]_S = [b]_S$; **x**) $a \cap c = b$.

E46.- Sea E= {a, b, c, d, e, f} ;
i) defina una relación de equivalencia, S, en E , de manera que el conjunto cociente E/S tenga un solo elemento;
ii) defina una relación de equivalencia, T, en E , de manera que el conjunto cociente E/T tenga seis elementos;
iii) defina una relación de equivalencia, V, en E , de manera que el conjunto cociente E/V tenga tres elementos .

Ejemplo 20. sea E={1, 2, 3, 4, 5, 6} y sea S la relación definida en E en la forma siguiente : $xSy \Leftrightarrow |x-3|=|y-3|$; las clases de equivalencia son entonces :
[1]=[5]={1, 5} , [2,]=[4]={2, 4} , [3]={3}, [6]={6} ;
El conjunto cociente tiene 4 elementos :
E/S={ {1, 5}, {2, 4}, {3}, {6} } = {[1], [2], [3], [6] } .
Observe que se cumplen las tres propiedades mencionadas en el ejemplo anterior.

Def.15'. **partición** de un conjunto no vacío, E.
Una familia ,$\{U_\alpha\}_{\alpha \in A}$, de subconjuntos de E se llama una partición de E si y sólo si cumple con las siguientes tres propiedades [familia= sinónimo de conjunto] :
i) todo $U_\alpha \neq \varnothing$ [es decir : todo subconjunto que se considera tiene almenos un elemento];
ii) $U_\alpha \cap U_\beta \neq \varnothing \Rightarrow U_\alpha = U_\beta$ [es decir : suconjuntos diferentes no tienen elementos comunes];
iii) $\bigcup_{\alpha \in A} U_\alpha = E$
[es decir:la unión de todos los subconjuntos miembros de la familia considerada es E].

Ejemplo 21.
En cada uno de los dos ejemplos anteriores, el conjunto cuyos elementos son todas las diferentes clases de equivalencia forma una partición de E. Esto no es una casualidad, como se desprende del siguiente teorema :
Teorema 5.
Teorema fundamental de las equivalencias.
Dado un conjunto E, no vacío, hay una correspondencia biunívoca (es decir una función biyectiva) natural entre el conjunto G de todas las relaciones de equivalencia en E y el conjunto P de todas las particiones de E . Esta correspondencia se obtiene asociando a cada equivalencia en E la partición de E cuyos elementos son las diferentes clases de equivalencia.
[Una demostración de este teorema se halla en la guía opcional sobre **relaciones**]

Ejemplo 22. (importante)
Sean E= **Z**, **S=** ($\equiv_n$) = congruencia módulo n en **Z** ;
Las clases de equivalencia son las clases de congruencia módulo n ; el conjunto cociente tiene n elementos.
En particular, a título de ejemplo, consideremos el caso n=3.
Entonces : Z/**S**= {$[0]_3$, $[1]_3$, $[2]_3$ } ; $[0]_3$= {0, -3, 3, -6, 6, -9, 9, ..., 2457651, ...} , $[1]_3$=(1, -2, 4, -5, 7, ..., -45003218, ... } , $[2]_3$= { 2, -1, 5, -4, ..., 11111003456081,....}.

Ejemplo 23. (importante, ya que se usa desde cuarto grado de primaria....**).**
E= Zx**Z* =** conjunto de todas las fracciones enteras con denominador ≠0 ;
S = relación de equivalencia definida por : $\frac{a}{b} S \frac{c}{d} \Leftrightarrow$ a.d = c.b ;
Las clases de equivalencia son los conjuntos de fracciones "equivalentes" que representan a un mismo número racional. Desde primaria se usan las fracciones de enteros para representar los números racionales, y nadie se confunde ya que cada clase de equivalencia se representa sin usar corchetes ni llaves. Por ejemplo, para representar la clase de equivalencia :
$[\frac{3}{4}] = \{ \frac{3}{4}, \frac{-3}{-4}, \frac{12}{16}, ..., \frac{-252}{-336}, ...,$ [todas las fracciones equivalentes a $\frac{3}{4}$], ... $\}$ se usa simplemente el símbolo acostumbrado " $\frac{3}{4}$ " .

Ejemplo 24. (importante).
[Definición de los números enteros a partir de los números naturales].

Sea N= {0, 1, 2, ...} el conjunto de los números naturales, E= NxN = el conjunto de los pares ordenados de números naturales y sea S la relación de equivalencia definida en E en la forma siguiente : (a, b)S(c, d) $\Leftrightarrow$ a+d = c+b .
Se puede establecer una correspondencia biunívoca [es decir, definir una función biyectiva E/S $\rightarrow$ **Z** observando que en cada clase de equivalencia hay un único representante del tipo (a, 0), o (0, b) con a ≥ 0, b>0 y asociando a la clase [(a, 0)] el número entero natural, a, y a la clase [(0, b)] el número entero negativo -b .
Esto permite dar una definición rigurosa del conjunto de los números enteros [por medio del conjunto cociente E/S].
Por ejemplo el número natural 7 estaría representado por la clase de equivalencia : [7] = { (7, 0), (8, 1), ..., (2356, 2349), ... }
y el número -2 por [2] = {(0, 2), (1, 3), ...,(2000, 2002), ...} .

En lo que sigue, verificaremos que en cada uno de los conjuntos $\mathbf{Z_n}$ (n >1) , se pueden definir operaciones de suma y multiplicación de tal manera que :
i) $\mathbf{Z_n}$ es un anillo conmutativo con unidad ;
ii) si n=p es número primo, entonces $\mathbf{Z_p}$ no sólo es dominio de integridad sino es **cuerpo conmutativo**.
[esto sigue del hecho que en todo dominio de integridad que sea un conjunto finito, todo elemento no nulo tiene necesariamente inverso multiplicativo].

Definición de las operaciones de suma y multiplicación en Z_n.

Hemos observado anteriormente[**ver def.12 y proposición 4,** en la pg. 24 de esta guía] que la relación de congruencia es una relación de equivalencia compatible con la suma y la multiplicación usuales en **Z** ;
esto significa que si $x_1 \underset{n}{\equiv} x_2$, $y_1 \underset{n}{\equiv} y_2$ entonces $(x_1+y_1) \underset{n}{\equiv} (x_2+y_2)$ y $(x_1.y_1) \underset{n}{\equiv} (x_2.y_2)$.
Este hecho permite definir operaciones de suma y multiplicación en el conjunto cociente operando sobre representantes cualesquiera de las clases de equivalencia consideradas:
$[x]+[y] = [x+y]$;
$[x].[y] = [x.y]$;
Es decir : para sumar o multiplicar dos clases de equivalencia, elementos del conjunto cociente, se pueden escoger un representante en cada una de las clases, sumarlos o (respectivamente) multiplicarlos y luego poner como resultado de la operación, la clase de equivalencia del elemento obtenido.

Ejemplo 25. A título de ejemplo, consideremos la equivalencia $\underset{6}{\equiv}$ en el conjunto **Z** de los enteros y el correspondiente conjunto cociente

$\mathbf{Z_6} = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}, \overline{4}, \overline{5}\}$; si queremos multiplicar la clase de equivalencia $\overline{3}$ por la clase $\overline{4}$ podemos multiplicar (en Z) los representantes 3, 4, obteniendo 3.4=12 y luego poner

como resultado de la multiplicación la clase representada por el número 12 (que es $\overline{0}$ ya que $12 \underset{6}{\equiv} 0$) . Análogamente si quisiésemos sumar:

$\overline{3} + \overline{4}$, podemos escribir $\overline{3} + \overline{4} = \overline{3+4} = \overline{7} = \overline{1}$, ya que $7 \underset{6}{\equiv} 1$.
En esta manera podemos construir las tablas para la suma y para la multiplicación en $\mathbf{Z_6}$:

+	0	1	2	3	4	5
0	0	1	2	3	4	5
1	1	2	3	4	5	0
2	2	3	4	5	0	1
3	3	4	5	0	1	2
4	4	5	0	1	2	3
5	5	0	1	2	3	4

x	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

.

Def. 16. Homomorfismo.
Si (E, *), (F, #) son dos conjuntos con cierta operación, una función f: E→F se llama un homomorfismo si y sólo si se cumple, para toda escogencia de dos elementos $x, y \in E$: $f(x*y)=f(x)\#f(y)$

es decir, las dos acciones de i) aplicar la función, ii) aplicar la operación , deben conmutar;

debe dar el mismo resultado:
a) componer en el dominio dos elementos, x, y, obteniendo el elemento x*y y a este aplicar la función . obteniendo f(x*y) ;
b) primero aplicar la función a los dos elementos, obteniendo f(x), f(y) y luego componer las imágenes en el codominio : f(x)#f(y) .

Ejemplo 26.
Sean V, W dos espacios vectoriales y consideremos en cada uno la operación de suma de vectores ; entonces una transformación lineal T : V→W es un homomorfismos de (V,+) a (W,+) ya que para todo par de vectores **u**, **v** en V se tiene T(**u**+**v**)=T(**u**)+T(**v**).

Observación 9 (importante).
Dado un entero positivo n y la congruencia $\underset{n}{\equiv}$, por la manera en que se han definido las operaciones de suma y multiplicación en el conjunto cociente, $\mathbf{Z_n}$, la función p : $\mathbf{Z}\rightarrow\mathbf{Z_n}$ definida asociando a cada entero su clase de equivalencia : p(x)=[x] , resulta ser un homomorfismo ya sea considerando la operación de suma , ya sea la operación de multiplicación. [ver def. 16]
Esto significa que :
" x, y∈ **Z** : p(x+y)=p(x)+p(y) , p(xy)=p(x)p(y) .

En efecto se tiene : p(x+y) = [x+y]= [x]+[y] = p(x)+p(y) ,
p(xy) = [xy]= [x][y] = p(x)p(y) .

Proposición 6. (importante).
Sean un conjunto con operación (E, *) y una equivalencia, T, compatible con * ;
6i) Se puede entonces definir una operación *' en el conjunto cociente [que se llama la operación **inducida** por * en el cociente] con : $[x]_T *' [y]_T = [x*y]_T$;
6ii) la función $\pi : E\rightarrow E/T$, definida por $\pi(x)=[x]_T$, [que asocia a todo elemento de E la clase de equivalencia a la cual pertenece y que se llama la "**proyección natural** sobre el cociente"] resulta ser entonces un homomorfismo sobreyectivo;
6iii) del hecho que π es un homomorfismo sobreyectivo sigue que si la operación * definida en E tiene cualquiera de las siguientes propiedades que se mencionan a continuación, por consiguiente la misma propiedad la tiene también la operación *' , inducida por * en el conjunto cociente , E/T :
a) propiedad asociativa ;
b) propiedad conmutativa;
c) propiedad del neutro;
d) propiedad del simétrico;
e) en el caso que en E haya dos operaciones (suma y multiplicación) compatibles con la equivalencia, T, propiedad distributiva de la multiplicación respecto a la suma .

Una importantísima consecuencia de esta proposición es que :
como el conjunto de los números enteros Z, con las dos operaciones de suma y multiplicación es **un anillo conmutativo con unidad** entonces, igualmente, el conjunto cociente $\mathbf{Z_n}$ con las operaciones de suma y multiplicación inducidas, resulta ser un anillo conmutativo con unidad.

Proposición 7.
Si n es un número primo entonces $\mathbf{Z_n}$ es un cuerpo conmutativo.

Recuerde [def. 1' de la pag. 3 de esta guía] que un cuerpo conmutativo es un conjunto,K , con dos operaciones, indicadas como "suma", +, y "multiplicación",x , tales que :
1) (K,+) es un grupo conmutativo ;
2) (K*,x) es un grupo conmutativo [siendo K* el subconjunto de K formado por los elementos distintos del neutro de la suma] ;
3) vale la propiedad distributiva de la multiplicación respecto a la suma.

Demostración de la proposición 7.
Como ya sabemos que los conjuntos $\mathbf{Z_n}$ con suma y multiplicación inducidas por la suma y la multiplicación usuales de los números enteros, son anillos conmutativos con unidad , lo único que deberemos demostrar es que :
si n=p es número primo, entonces en $(\mathbf{Z_p})^*$ vale la propiedad del simétrico respecto a la multiplicación, es decir que :todo elemento no nulo de $\mathbf{Z_p}$ tiene inverso multiplicativo.
Sea $\mathbf{x}\in \mathbf{Z_p}$, $\mathbf{x}\neq\mathbf{0}$; como el neutro,**0** , de la suma en $\mathbf{Z_p}$ es
[0] = {... -2p, -p, 0, p, 2p, ..., np, ...}, entonces , $\mathbf{x}\neq\mathbf{0}$ significará **x**=[a] , con (a, p)=1 , por lo cual existen s, t enteros, tales que s.a+t.p=1 ; de esto sigue que [s] es inverso multiplicativo de [a] , ya que [s].[a] = [s.a] = [1-t.p] = [1] - [t.p] = [1]-[0]= [1] = neutro de la multiplicación en $\mathbf{Z_p}$.

Proposición 8.
Si n es un entero mayor que 1 y si n es un número compuesto entonces $\mathbf{Z_n}$ no es un dominio de integridad .
Demostración.
Para poner en evidencia que $\mathbf{Z_n}$ no es un dominio de integridad, bastará exhibir dos elementos no nulos de $\mathbf{Z_n}$ cuyo producto sea nulo;
si n es compuesto, existen n_1, n_2 tales que $n=n_1n_2$, $1< n_1 \leq n_2< n$,
por lo cual $[n_1]\neq \mathbf{0}=[0] \neq[n_2]$, pero $[n_1].[n_2]=[n_1n_2]=[n]=[0]=\mathbf{0}$.

E47. Halle todos los elementos $\mathbf{a}\in \mathbf{Z_{12}}$ tales que exista un $\mathbf{b}\in \mathbf{Z_{12}}$ de manera que sea $\mathbf{a}\neq\mathbf{0}$ $\neq\mathbf{b}$, $\mathbf{ab}=\mathbf{0}$.

E48. Diga , justificando, si la ecuación $\mathbf{3x}+\mathbf{1}=\mathbf{6}$ tiene solución en $\mathbf{Z_{12}}$.

Def. 17. Divisores del cero.
Sea A un anillo.
Un elemento $a\in A$, $(a\neq 0)$, se llama un divisor del cero si y sólo si existe otro elemento $b\in A$, $(b\neq 0)$ tal que a.b=0 .

Nota : en la definición de divisor del cero se exige que los elementos considerados sean $\neq 0$, ya que si así no fuese, todo elemento del anillo sería divisor del cero y la definición quedaría sin ningún interés.

Ejemplo 27. En el ejemplo **25**, consideramos el anillo conmutativo

$\mathbf{Z_6}= \{\overline{0}, \overline{1}, \overline{2}, \overline{3}, \overline{4}, \overline{5}\}$; en ese anillo, los elementos $\overline{2}, \overline{3}, \overline{4}$, son divisores del cero, ya que

$\overline{2}.\overline{3}= \overline{0}$, $\overline{3}.\overline{4} = \overline{4}.\overline{3}= \overline{0}$;

por otra parte, los elementos $\overline{1}, \overline{5}$ son unitarios (ya que tienen inverso multiplicativo : recuerde la d**ef. 6**).

E49. En el anillo $\mathbf{Z_{16}}$:
a)Halle el subconjunto, B, de todos los divisores del cero;
b) halle el subconjunto, U, de todos los elementos unitarios;

c) diga, justificando, si {{$\overline{0}$}, B, U } es o no es una partición de $\mathbf{Z_{16}}$.
E50. Lo mismo que lo del ejercicio anterior, para el anillo $\mathbf{Z_{18}}$.

E51. Escriba las tablas de las operaciones de suma y multiplicación para cada uno de los siguientes anillos :
$\mathbf{Z_2}$, $\mathbf{Z_3}$, $\mathbf{Z_4}$, $\mathbf{Z_5}$; además diga, justificando, cual o cuales de ellos son cuerpos y cuales no.

E52 . a) Escriba las tablas de la suma y de la multiplicación para el anillo $\mathbf{Z_9}$;
b) recuerde el ejemplo 12 de esta guía y considere la siguiente ecuación de primer grado en $\mathbf{Z_9}$: **7x**+**4** = **2x**+**15** , indicando aqui con letras negrita las clases de equivalencia : por ejemplo **x**=[x] , **7**=[7] etc. Indique las operaciones que Ud. efectuaría en $\mathbf{Z_9}$, para "despejar" la incógnita **x** en la ecuación dada;
[sugerencia : comience por observar que [15]=[6], ya que $15 \underset{9}{\equiv} 6$;
luego sume a los dos miembros de la ecuación el elemento **5** (=-**4**),
así como **7x** (=-**2x**) , obteniendo **5x**=**11** ; al final, vea en la tabla de multiplicar de $\mathbf{Z_9}$ cual es el inverso multiplicativo de **5** , y multiplique ambos miembros por ese inverso multiplicativo].
E53 . Usando las tablas de sumar y de multiplicar halladas en el ejercicio **E51** , resuelva las siguientes ecuaciones en $\mathbf{Z_5}$:
a) **2x**+**3**=**4** ; **b**) **x**-**3** = **3x** +**2** ; **c**) $\mathbf{x^2}$=**1** ; **d**) $\mathbf{x^3}$=**3** ; **e**) $\mathbf{x^4}$=**1** .

Def.18 :La función de Euler, $\varphi : N^* \to N^*$.
Para todo número entero positivo, n, se define $\varphi(n)$ como el número de los enteros positivos k, menores o iguales que n, tales que sea : (k, n) = 1 ;
[es decir : el número de enteros positivos menores o iguales que n y relativamente primos con n] ;
Así por ejemplo : $\varphi(2)=1$, $\varphi(3)=2$, $\varphi(4)=2$, $\varphi(6)=2$.
E54. Demuestre que :
a) si el entero positivo p es primo entonces $\varphi(p)=p-1$;
b) si el entero positivo p es primo entonces :
$$\varphi(p^n)=p^n-p^{n-1}=p^{n-1}(p-1) .$$
c) [optativo] si m, n son enteros positivos tales que (m, n)=1 entonces :
$\varphi(mn)=\varphi(m)\varphi(n)$;
E55.[optativo] Usando los resultados del ejercicio **E54** , demuestre que : **a**) si $n= p^r q^t$ (con p, q primos positivos y r, t enteros positivos) , entonces $\varphi(n)= n(1-\frac{1}{p})(1-\frac{1}{q})$;

b) si $n = \prod_{i=1}^{k} (p_i)^{r_i}$ {es decir : si n tiene k factores primos diferentes: $p_1, p_2, ..., p_k$ },

entonces $\varphi(n) = n(1-\frac{1}{p_1})(1-\frac{1}{p_2})....(1-\frac{1}{p_k})$;

por ejemplo :$\varphi(120) = 120.(1-\frac{1}{2})(1-\frac{1}{3})(1-\frac{1}{5}) = 32$.

E56. Demuestre que en $\mathbf{Z_n}$ hay exáctamente $\varphi(n)$ elementos unitarios y $n-1-\varphi(n)$ divisores del cero
[por ejemplo en $\mathbf{Z_9}$ los unitarios son **1**, **2**, **4**, **5**, **7**, **8** y los divisores del cero son **3**, **6**; por otra parte$\varphi(9)=6$, $9-1-\varphi(9) = 9-1-6 = 2$] .
E57. Averigue (y justifique) cuales conjuntos ($\mathbf{Z_0}$, $\mathbf{Z_1}$) se obtendrían como conjuntos cocientes de **Z** respecto a las congruencias $\underset{0}{\equiv}$, $\underset{1}{\equiv}$.

E58.- Para cada una de las siguientes operaciones definidas en **Z** (conjunto de los enteros), diga, justificando, :
58a) si es o no es compatible con la relación de equivalencia $\underset{n}{\equiv}$;
58b) si induce o no una operación en el conjunto cociente $\mathbf{Z}_n$.
i) $x*y = x+y+x+y$;
ii) $x*y = (x, y)$ [= MCD{x, y}];
iii) $x*y = |x-y|$;
iv) $x*y = x+2y$;
v) $x*y = 5x-3y$.

E59.- Demuestre que la ecuación $x^2-1 = 0$ tiene cuatro soluciones en $\mathbf{Z}_{15}$.

E60.- Halle halle los valores de las constantes b, $c \in \mathbf{Z}_2$, para que ecuación polinomial $x^2+bx+c=0$ no tenga soluciones en $\mathbf{Z}_2$.

E61.- Halle el inverso (multiplicativo) de [13] en $\mathbf{Z}_{17}$.

E62.-Para cada una de las siguientes afirmaciones, diga, justificando, si es cierta o falsa

a) Si p es un entero, >1, primo entonces $\mathbf{Z}_p$ tiene exactamente p-1 elementos unitarios [es decir : con inverso multiplicativo];

b) en un dominio de integridad, dos elementos unitarios siempre son asociados;

c) $\varphi(45)=24$ (siendo φ la función de Euler);

d) si en una división según Euclides el dividendo es negativo, entonces el resto puede ser negativo;

e) La ecuación polinomial $x^2+bx+c=0$ (cualesquiera que sean b, c) siempre tiene solución en $\mathbf{Z}_n$;

Soluciones de los ejercicios desde E31 hasta E62.

SE31. a) $x \underset{9}{\equiv} 8$; **b**) $x \underset{10}{\equiv} 8$; **c**) $x \underset{25}{\equiv} 19$; **d**) $x \underset{6}{\equiv} 5$;
e) $x \underset{9}{\equiv} 4$; **f**) $x \underset{10}{\equiv} 2$; **g**) $x \underset{25}{\equiv} 9$.

SE32. Si (a, n)=1 existen enteros h, k tales que ah+kn=1 luego bah+bkn=b ,

$a(bh)-b = (bk)n \underset{n}{\equiv} 0$ por lo cual x=bh es una solución de la congruencia.

SE33. La congruencia $ax \underset{n}{\equiv} b$ tiene solución si y sólo si $(a, n) \mid b$, por lo cual,
por ejemplo : $4x \underset{10}{\equiv} b$ tiene solución si b=38 , no tiene solución si b=47 .

SE34. $ca \underset{n}{\equiv} cb \Leftrightarrow ca-cb = c(a-b) = hn$ [con h entero] y como $c \mid hn$ pero (c, n)=1 sigue $c \mid h$, $h=h_1.c$, $c(a-b) = h_1.cn \Leftrightarrow (a-b) = h_1.n \Leftrightarrow a \underset{n}{\equiv} b$.

SE35. i) si x_1 es solución y si $x_1 \underset{n}{\equiv} x_2$ entonces $ax_1-b = hn$, $x_1-x_2= kn$ [h, k enteros] , luego $a(x_2+kn) -b = hn$, $ax_2-b = hn-akn = n(h-ak) \underset{n}{\equiv} 0$ por lo cual x_2 es solución de la congruencia;
ii) por ejemplo, si la congruencia es : $2x \underset{10}{\equiv} 8$, se tiene : $2x \underset{10}{\equiv} 8 \Leftrightarrow x \underset{5}{\equiv} 4$ y por ejemplo $x_1=4$, $x_2=9$ son dos soluciones que no son congruentes módulo n=10;
iii) Sean d = (a, n) , $a=a_1d$, $n=n_1d$, [[**]observe que entonces $(a_1, n_1) = 1$] ; si x_1, x_2 son dos soluciones cualesquiera de la congruencia $ax \underset{n}{\equiv} b$, entonces $ax_1 \underset{n}{\equiv} ax_2 \underset{n}{\equiv} b$, luego $a_1x_1 \underset{n_1}{\equiv} a_1x_2$, $a_1(x_1-x_2) = h\, n_1$, $a_1 \mid h$ [por[**]] luego $h=h_1a_1$, $a_1(x_1-x_2) = h\, n_1= h_1a_1n_1$ por lo cual $(x_1-x_2) = h_1\, n_1 \Rightarrow x_1 \underset{n_1}{\equiv} x_2$.

SE36. Hemos verificado en E32 que la congruencia tiene soluciones y por **E35iii**) si x_1, x_2 son dos soluciones cualesquiera entonces $x_1 \underset{n}{\equiv} x_2$, $x_2- x_1= hn$.
Por lo tanto, si $0 \le x_1 \le x_2 < n$, tenemos : $-n < x_2- x_1 < n$ luego $|x_2- x_1| < n$ y como $x_2- x_1= hn$, $|hn| < n$, con h entero. Esto es posible únicamente si h=0 , en el cual caso $x_1= x_2$. Por lo tanto hay una única solución en el intervalo [0, n) .

SE37. Sean d=(a, b) , n=sa+tb ; como d es divisor común de a, b, se tiene $a=a_1d$, $b=b_1d$, $n=sa+tb = n=sa_1d+tb_1d = (sa_1+tb_1)d$ lo cual indica que n es múltiplo de d.

SE38. Es cierto. En el ejercicio E37 se verifica que si n=sa+tb entonces n es múltiplo de d=(a, b) ; falta justificar que si n=kd entonces n es combinación lineal de a, b : como gracias al algoritmo de Euclides se puede expresar d=ua+vb entonces tenemos : n=kd = k(ua+vb) = (ku)a+(kv)b = combinación lineal de a, b.

SE39. a) $x \underset{3}{\equiv} 2$; **b, d**) no tienen solución ; **c**) $x \underset{5}{\equiv} 4$;
e) $x \underset{3}{\equiv} 1$; **f**) $x \underset{11}{\equiv} 8$; **g**) $x \underset{5}{\equiv} 0$.

SE40. Sean d=(a, n) , $a=a_1d$, $b=b_1d$, $n=n_1d$; sabemos que entonces

$ax \underset{n}{\equiv} b \Leftrightarrow a_1 x \underset{n_1}{\equiv} b_1$ y por el ejercicio **E36** hay exactamente <u>una</u> solución, x_1, en el intervalo $[0, n_1)$; por otra parte, por el ejercicio **E35** : $x_2=x_1+n_1$, $x_3=x_1+2n_1$ ... ... $x_{k+1} = x_1+kn_1$ son soluciones [k=1, 2, ..., d-1] en el intervalo [0, n).
Quedaría verificar con detalle que cualquier solución en el intervalo [0, n) es una de las x_i que hemos mencionado.

SE41. Como $\binom{p}{k} = \frac{p!}{k!\,(p-k)!}$ y como el primo p no es factor del denominador siempre y cuando sea $0 < k < p$, se tiene que en el desarrollo de la fórmula de la potencia p-ésima de (a+b) todos los sumandos, con excepción del primero y del último, son números enteros múltiplos de p (ya que p es factor del numerador);
Por lo tanto $(a+b)^p = a^p+p(\text{entero})+b^p \underset{p}{\equiv} a^p+b^p$ y en particular $(n+1)^p \underset{p}{\equiv} n^p+1$.

SE42. c es cierta; **a, b, d** son falsas.

SE43. La sugerencia lo dice todo.

SE44. Sea P(t) la propiedad :
" si un entero n es divisible por t enteros $n_1, n_2,..., n_t$, y si además $(n_i, n_k)=1$ toda vez que sea $i \neq k$, entonces n necesariamente es divisible por el producto $\prod_{i=1}^{t} n_i$ ";

P(1) es cierta ya que si t=1 el producto $\prod_{i=1}^{1} n_i$ es igual al mismo n_1 ;

Supongamos ahora cierta P(k) y sean $n_1, n_2,..., n_k, n_{k+1}$ números que satisfacen la hipótesis; por hipótesis inductiva entonces el número $h=n_1n_2...n_k$ =producto de los primeros k números dados, divide a n ; además, por el resultado del ejercicio anterior, para asegurar que el producto $n_1n_2...n_kn_{k+1}= hn_{k+1}$ divide a n es suficiente justificar que $(h, n_{k+1})=1$ lo cual es consecuencia del hecho que por hipótesis, los k+1 números asignados no tienen (dos a dos) ningún factor primo común.

SE45. Son ciertas : **ii, iii, iv, v, vii, ix** ;
son falsas : **i, vi, viii, x** .
Nota : la **v es cierta,** ya que , cuando se representa un conjunto "por extensión" es decir enumerando los elementos, no importa si se hacen repeticiones, por ejemplo : F={1, 2, 3, 4} , G= {1, 1, 2, 3, 4, 2, 3} son el mismos conjunto ya que tienen los mismos elementos.

SE46. i) La única posibilidad es que haya una sola clase de equivalencia, es decir que para todo par de elementos x, y del conjunto dado, se tenga
"x relacionado con y" ; es un caso en cierta forma trivial y la equivalencia definida en esta forma en un conjunto se llama "la equivalencia universal";
ii) este es otro caso trivial y la única posibilidad es que todo elemento del conjunto dado esté relacionado sólo consigo mismo, es decir la equivalencia deberá se la igualdad : "x relacionado con y" si y sólo si x=y;

iii) para que haya tres clases de equivalencia, basta considerar tres subconjuntos no vacíos, dos a dos sin elementos comunes y cuya unión sea el conjunto dado [es decir, considerar una "partición" con tres subconjuntos;
Hay muchas posibilidades; por ejemplo las clases de equivalencia podrían ser {a, b}, {c, d}, {e, f} y la equivalencia estaría definida por el conjunto :
{ (a, a), (b, b), (c, c), (d, d), (e, e), (f, f), (a, b), (b, a), (c, d), (d, c), (e, f), (f, e) } ;
otra posibilidad podría ser siendo las clases de equivalencia {a}, {b}, {c, d, e, f} etc.

SE47. Son los elementos representados por números, a, (del intervalo (1, 11) tales que (a, 12) >1; a saber : 2, 3, 4, 6, 8, 9, 10; a título de ejemplo : $2.6 = 12 \underset{12}{\equiv} 0$; $9.4 = 36 \underset{12}{\equiv} 0$.

SE48. No tiene solución ya que la congruencia: $3x+1 \underset{12}{\equiv} 6$ no tiene solución.

SE49. Divisores del cero en $\mathbf{Z_{16}}$: [2], [4], [6], [8], [10], [12], [14] ; por ejemplo [14][8]=[112]=[0]; unitarios : [1], [3], [5], [7], [9], [11], [13], [15] .

SE50. Divisores del cero en $\mathbf{Z_{18}}$: todos los elementos representados por :
2, 3, 4, 6, 8, 9, 10, 12, 14, 15, 16 ; por ejemplo [14][9] = [126] = [0] .
Unitarios : todos los elementos representados por 1, 5, 7, 11, 13, 17 ;

SE51. Son cuerpos $\mathbf{Z_2}$, $\mathbf{Z_3}$, $\mathbf{Z_5}$; no es cuerpo (ni dominio de integridad) $\mathbf{Z_4}$.

SE52b. Sumando **(-2x)** y **-4** a ámbos miembros se obtiene : **5x=11** , luego, observando que el inverso de **5** es **2** , ya que **2.5=10=1** , multipliquemos ámbos miembros por **2** obteniendo : **x=22=4** .

SE53. a) **x=3** , b) **x=0** , c) $\mathbf{x_1=1}$, $\mathbf{x_2=4}$, d) **x=2** , e) $\mathbf{x_1=1}$, $\mathbf{x_2=2}$, $\mathbf{x_3=3}$, $\mathbf{x_4=4}$.

SE57. $\mathbf{Z_1}$ es el anillo cociente de **Z** obtenido con la equivalencia universal, en la cual todo elemento es equivalente a cualquier otro ya que todo entero es múltiplo de 1 ; por lo tanto $\mathbf{Z_1}$ tiene un solo elemento;
$\mathbf{Z_0}$ es el anillo cociente de **Z** obtenido con la equivalencia "igualdad" de manera que todo elemento de $\mathbf{Z_0}$ es una clase de equivalencia que tiene un solo elemento; intuitivamente hablando, $\mathbf{Z_0}$ es "lo mismo que Z" , mientras que en forma rigurosa podemos decir que existe la función f : $\mathbf{Z \to Z_0}$ definida por f(n) = [n] que resulta ser un homomorfismo biyectivo.

SE58. i, iv, v son compatibles con la congruencia módulo n, y por consiguiente pueden inducir una operación en el conjunto cociente;
ii) no es compatible; por ejemplo si n=6, tenemos 4*14=(4, 14)= 2 ; $4 \underset{6}{\equiv} 10$, $14 \underset{6}{\equiv} 20$, y sin embargo 10*20=(10, 20) = 10 pero 2 no es congruente a 10 módulo 6;

iii) tampoco es compatible ; por ejemplo : 2*3 = |2-3| = 1 , $2 \underset{6}{\equiv} 8$, $3 \underset{6}{\equiv} 3$ y sin embargo
8*3 = |8-3| = 5, pero 1 no es congruente a 5 módulo 6.

SE59. las soluciones son : **1, 4, 11, 14**. **SE60** b=c=1 **SE61 4.13 = 52 = 1**

SE54. Sabemos que indicando con $|E|$ el número de elementos del conjunto E, se tiene: $\varphi(n)= |\{x\in Z|\ 1\leq x \leq n\ ,\ (x,\ n)=1\ \}|$;
54a) Si p es primo, entonces todos los p-1 números naturales del intervalo [1, p-1] son relativamente primos con p, por lo cual $\varphi(p)= p-1$;
54b) Si n=1 entonces la fórmula $\varphi(p^n)=p^{n-1}(p-1)$ se escribe $\varphi(p)= 1.(p-1)$ lo cual se demostró en 54a); si $n>1$, observemos que los únicos números del intervalo $[1,\ p^n]$ que tienen algún divisor común ,[> 1], con p^n son los múltiplos de p, a saber : $p,\ 2p,...,\ p^{n-1}p=p^n$ que son exactamente p^{n-1}; por lo tanto los restantes p^n-p^{n-1} son los $\varphi(p^n)$ naturales del intervalo $[1,\ p^n]$ relativamente primos con p^n así que :

$$\varphi(p^n)=p^n-p^{n-1}= p^{n-1}(p-1)\ ;$$

54c) Sean n, m dos naturales (>1) , relativamente primos [$(m,\ n)=1$] y sean $A=\{x_1,\ x_2,...,x_h\ \}$ el conjunto de los $\varphi(m)$ números del intervalo [1, m], relativamente primos con m , $B=\{\ y_1,\ y_2,...,y_k\ \}$ el conjunto de los $\varphi(n)$ números del intervalo [1, n], relativamente primos con n , $E=\{\ z_1,\ z_2,...,z_s\ \}$ el conjunto de los $\varphi(mn)$ números del intervalo [1, mn], relativamente primos con mn ;
consideremos la función $f : E\rightarrow AxB$ que asocia a todo número, x, natural del conjunto E, de los números relativamente primos con mn el par ordenado $f(x) =(x_j\ ,\ y_k)$ definido por : $x \underset{m}{\equiv} x_j$, $x \underset{n}{\equiv} y_k$; f está bien definida, ya que si $x\in E$ entonces x no tiene ningún factor primo común con mn y por consiguiente tampoco con m ni con n ; bastará poner en evidencia que f es biyectiva para poder afirmar que s = h.k , es decir

$$\varphi(mn)= \varphi(m)\varphi(n)\ .$$

Se tiene $f(x) =(x_j\ ,\ y_k)$ si y sólo si $x \underset{m}{\equiv} x_j$, $x \underset{n}{\equiv} y_k$, es decir, x es solución del sistema de congruencias : $\begin{cases} x \underset{m}{\equiv} x_j \\ x \underset{n}{\equiv} y_k \end{cases}$ y este sistema, [como se verifica facilmente], es equivalente a la congruencia $x \underset{mn}{\equiv} x_0$ con $x_0 = msy_k+ntx_j$, siendo s, t números enteros tales que

$ms+nt = 1$.

[nota : este es un caso particular del "teorema chino del resto", del cual se tratará más adelante].

Del hecho que la congruencia $x \underset{mn}{\equiv} x_0$ tiene una solución en el intervalo [1, mn] sigue que f es sobreyectiva y del hecho que hay una sola solución en el intervalo [1, mn] sigue que f es inyectiva.

SE55a. Sea $n= p^rq^t$ (con p, q primos distintos y r, t enteros positivos) , entonces por **SE54c** $\varphi(n)= \varphi(p^r)\varphi(q^t)$ y por **SE54b** $\varphi(p^r)\varphi(q^t)=p^{r-1}(p-1)q^{t-1}(q-1) =$
$=p^rq^t(1-\frac{1}{p})(1-\frac{1}{q}) = n(1-\frac{1}{p})(1-\frac{1}{q})$;

SE55b. Por indución : si k=1 entonces $n = \prod_{i=1}^{1}(p_i)^{r_i} = p^r$, $\varphi(n)= p^{r-1}(p-1) = n(1-\frac{1}{p})$;

si la propiedad es cierta para k=s entonces $n=\prod_{i=1}^{s+1}(p_i)^{r_i} = (\prod_{i=1}^{s}(p_i)^{r_i})p^r = n_1 p^r$,

indicando $p_{s+1}{}^{r_{s+1}}$ con p^r y $(\prod_{i=1}^{s}(p_i)^{r_i})$ con n_1. Luego, por **SE54c** y por hipótesis inductiva: $\varphi(n)= \varphi(n_1)\varphi(p^r) = n_1(1-\frac{1}{p_1})(1-\frac{1}{p_2})....(1-\frac{1}{p_s})\,(p_{s+1})^{r_{s+1}}(1-\frac{1}{p_{s+1}}) =$

$=(n_1\,(p_{s+1})^{r_{s+1}})(1-\frac{1}{p_1})(1-\frac{1}{p_2})...(1-\frac{1}{p_s})(1-\frac{1}{p_{s+1}})= n(1-\frac{1}{p_1})(1-\frac{1}{p_2})....(1-\frac{1}{p_s})(1-\frac{1}{p_{s+1}})$.

SE62.- a, b, c ciertos, **d, e** falsos.

Por ejemplo $x^2+x+1=0$ no tiene solución en $\mathbf{Z}_2$. Si n es impar entonces toda vez que en $\mathbf{Z}_n$ el elemento representado por $b^2-4ac = b^2-4c$ no es cuadrado de algún elemento, 41
[es decir, toda vez que la congruencia $x^2 \underset{n}{\equiv} b^2-4c$ no tenga solución], el polinomio x^2+bx+c no tendrá ceros.

Def. 19: **grupo** (G, *). [ver también en la pag. 3 de esta guía **def.1-i**].
Se llama grupo a un conjunto no vacío, G en el cual se haya definido una operación, * , **asociativa**, con **elemento neutro** y con la **propiedad del simétrico**.

Nota : analice todos los ejemplos de grupo que aparecen en el texto de Lindsay Chils, cap. 11 , pag.92.

E63. Sea (**G**,*) un grupo.
a) Resuelva el ejercicio E9 de la pag. 92 del texto de Lindsay Child
b) demuestre que para todo elemento, $\mathbf{a}\in\mathbf{G}$, la función f : $\mathbf{G}\to\mathbf{G}$ definida por f(x)=**a***x es inyectiva;
c) demuestre que si G es un conjunto finito entonces f es biyectiva;
d) dé un ejemplo de grupo no finito, con algún elemento $\mathbf{a}\in\mathbf{G}$, de manera que f no sea sobreyectiva ;
e) usando los resultados de las partes b, c de este ejercicio, demuestre que si **D** es un dominio de integridad con un número finito de elementos, entonces necesariamente **D** es un cuerpo conmutativo;
f) demuestre que si p es número primo entonces $\mathbf{Z}_p$ es un cuerpo conmutativo.

E64. Dado cualquier $\mathbf{Z}_n$ sea **G** el subconjunto de $\mathbf{Z}_n$ formado por los elementos [x] tales que (x, n) =1; es decir $\mathbf{G} = \{ [x]\in\mathbf{Z}_n \mid x \in \mathbf{Z} , (x, n) = 1 \}$. Demuestre que G con la multiplicación de $\mathbf{Z}_n$ es un grupo.
[sugerencia : **i**) verifique primero que multiplicando dos elementos del subconjunto **G** , se obtiene un elemento del mismo subconjunto;
ii) verifique luego que se cumple la definición de grupo [def.19];
en particular, ponga en evidencia que se cumple la propiedad del simétrico tomando en cuenta que $[1]\in\mathbf{Z}_n$ y la parte **c**) del ejercicio **E63**.

E65 Halle el grupo, **G** , que se menciona en el ejercicio **E64** para $\mathbf{Z}_4, \mathbf{Z}_6, \mathbf{Z}_7, \mathbf{Z}_9, \mathbf{Z}_{12}$. Verifique que en cada caso el número de elementos que tiene el grupo que se menciona está dado por el valor de la función de Euler, por ej. $|\mathbf{Z}_{12}| = \varphi(12) = 4$.

E66. **a**)Demuestre el "teorema abstracto de Fermat" para un genérico grupo conmutativo, G, de n elementos. [pag. 92 del texto de Lindsay Childs].
b) demuestre el teorema de Euler [pag. 94 del texto de Lindsay Childs].

Def.20 Orden de un elemento en un grupo.
Sea G un grupo y sea $a \in G$; se llama el orden de a el menor número entero positivo, n, tal que $a^n = e$ = neutro de G.
[recuerde que a^n se define por inducción : $a^0 = e$, si $k \geq 0$: $a^{k+1} = a^k * a$].

E67. Demuestre que todo elemento de un grupo finito tiene orden.

E68. Demuestre que el orden de cualquier elemento de un grupo conmutativo finito divide al número de elementos que tiene el grupo.
Nota : esta propiedad también vale si el grupo no es conmutativo.

Def.21. Grupo cíclico.
Un grupo (**G**, *) se llama **cíclico** si existe algún elemento $\mathbf{a} \in G$, tal que la función $Z \to G$ definida por $f(x) = \mathbf{a}^x$ sea sobreyectiva. Observe que esto significa que todo elemento de G se puede expresar como una potencia de **a**.
[recuerde que si $x < 0$ se define $a^x = (a^{-x})^{-1} = (a^{-1})^{(-x)}$].

Observación 10. Se puede demostrar que para todo número primo, p, el grupo multiplicativo formado por los elementos no nulos de $\mathbf{Z}_p$ con la multiplicación es cíclico;
más aún, se puede demostrar que el grupo multiplicativo formado por los elementos no nulos de cualquier cuerpo finito es cíclico [esto de debe al hecho que todo cuerpo finito [como demostró el matemático Maclagan Wedderburn] es necesariamente conmutativo y al hecho que en un cuerpo conmutativo, toda ecuación polinomial de grado k tiene a lo máximo k soluciones].

E69. Resuelva los ejercicios E17 hasta E26
de pag. 96 [parte I, cap. 11, D, E del texto de Lindsay Childs].

E70. demuestre que en un grupo cíclico de n elementos, para todo divisor , d, de n hay exáctamente $\varphi(d)$ elementos de orden d.

Soluciones de los ejercicios desde E63 hasta E70.

SE63a. "En todo grupo G: $a*b=a*c \Rightarrow b=c$ " .
En efecto, por la propiedad del simétrico, existe $d \in G$ tal que d*a=e=neutro, luego :
$a*b=a*c \underset{1}{\Rightarrow} d*(a*b) = d*(a*c) \underset{2}{\Rightarrow} (d*a)*b = (d*a)*c \underset{3}{\Rightarrow} e*b = e*c \underset{4}{\Rightarrow} b=c$.
Justificaciones : (1) multiplicando d por elementos iguales se obtienen elementos iguales; (2) propiedad asociativa ; (3) propiedad del simétrico ; (4) propiedad del neutro.
SE63b. $f(x)=f(y) \Rightarrow \mathbf{a}*x = \mathbf{a}*y \Rightarrow$ [por **a**)] $x=y$;

SE63c. Si una función es inyectiva, cualquier subconjunto, A, de su dominio, con un número m de elementos tiene imagen con el mismo número de elementos : $|A|=|f(A)|=m$; entonces la imagen, f(G), es un subconjunto de G con el mismo número (finito) de elementos que G así que necesariamente f(G)=G lo que significa que f es sobreyectiva;

SE63d. Considere la función f : $\mathbf{Z}\to\mathbf{Z}$ definida por f(x)= 2x que es inyectiva pero no sobreyectiva, ya que por ejemplo $1\notin f(\mathbf{Z})$;

SE63e. Para que un dominio de integridad sea un cuerpo es suficiente que todo elemento $\mathbf{a}\neq 0$ tenga inverso ; consideremos la función f : $\mathbf{D}\to\mathbf{D}$ definida por f(x)=**a**x y observemos que como por **b, c**) f es sobreyectiva, será $1\in f(\mathbf{D})$ es decir 1=f(**b**) con algún conveniente $\mathbf{b}\in\mathbf{D}$; pero entonces f(**b**) = **ab**= 1 , es decir , **b** es inverso de **a** ;
SE63f. Sigue de **e**) ya que $\mathbf{Z}_p$ es dominio de integridad finito.

SE64. i**)** Si (a, n)=(b, n)=1 entonces (ab, n)=1 ya que podemos observar por ejemplo que existen r, s, u, v enteros tales que ar+ns=1=bu+nv de lo cual sigue :
1 = (ar+ns)(bu+nv) = abru+n(arv+bsu+nsv) así que existen los enteros h=ru, k=(arv+bsu+nsv) tales que (ab)h+nk=1 de lo cual sigue que (ab,n)=1 ;
habiendo verificado esto, tenemos que la multiplicación en el anillo $\mathbf{Z}_n$ que estamos considerando, determina también una multiplicación en el subconjunto G;
ii) Como la multiplicación de $\mathbf{Z}_n$ es asociativa, lo es necesariamente la multiplicación de elementos de G; como (1, n)=1 el neutro pertenece a G y si $\mathbf{a}\in$ G sigue que **a** tiene simétrico en G, con el mismo procedimiento que se usó en la verificación de **SE63e** :
la función f: $\mathbf{G}\to\mathbf{G}$ definida por f(x)=**a**x es inyectiva y por ser G finito, sobreyectiva, por lo cual existe $\mathbf{b}\in\mathbf{G}$ tal que f(**b**) = $1\in\mathbf{G}$ y **b** es el simérico de **a** .
SE65. $\mathbf{G}_4 = \{ [1]_4 , [3]_4 \}$; $\varphi(4)= 2$;
$\mathbf{G}_6 = \{ [1]_6 , [5]_6 \}$; $\varphi(6)= 2$;
$\mathbf{G}_7 = \{ [1]_7 , [2]_7 , [3]_7 , [4]_7 , [5]_7 , [6]_7 \}$; $\varphi(7)=6$;
$\mathbf{G}_9 = \{ [1]_9 , [2]_9 , [4]_9 , [5]_9 , [7]_9 , [8]_9 \}$; $\varphi(9)= 6$;
$\mathbf{G}_{12} = \{ [1]_{12} , [5]_{12} , [7]_{12} , [11]_{12} \}$; $\varphi(12) = 4$.

SE66a. Sea $\mathbf{a}\in\mathbf{G}$ cualquier elemento de **G** ; la función f : $\mathbf{G}\to\mathbf{G}$ definida por f(x)=**a**x es inyectiva [ver **SE63**] y como **G** tiene un número finito de elementos, f es también, necesariamente, sobreyectiva; por lo tanto el conjunto $\{ f(x) | x\in\mathbf{G} \}$ es el mismo **G** y por consiguiente el producto de todos los elementos de **G** : $\mathbf{a}_1.\mathbf{a}_2...\mathbf{a}_n$ es el mismo que el producto $f(\mathbf{a}_1).f(\mathbf{a}_2)...f(\mathbf{a}_n) = \mathbf{a}.\mathbf{a}_1.\mathbf{a}.\mathbf{a}_2...\mathbf{a}.\mathbf{a}_n = (\mathbf{a})^n\mathbf{a}_1.\mathbf{a}_2...\mathbf{a}_n$ y multiplicando ambos miembros de la igualdad $(\mathbf{a}_1.\mathbf{a}_2...\mathbf{a}_n)=(\mathbf{a})^n(\mathbf{a}_1.\mathbf{a}_2...\mathbf{a}_n)$ por el inverso de $(\mathbf{a}_1.\mathbf{a}_2...\mathbf{a}_n)$ sigue $\mathbf{1}=(\mathbf{a})^n$.
Observación importante.
El teorema de Euler también vale en un grupo no conmutativo, sin embargo la demostración que acabamos de efectuar no es válida en ese caso ya que usamos la propiedad conmutativa.
SE66b. Tenemos que demostrar que : si (a, n)=1 entonces $[a]^{\varphi(n)} = [1]$;
ya sabemos que $\mathbf{G} = \{ [x]\in\mathbf{Z}_n | x\in\mathbf{Z}, (x, n) = 1 \}$ es un grupo conmutativo [ver **E64**];
y por la definición de la función de Euler, sabemos que el orden de **G** es $\varphi(n)$.
Por consiguiente, por el "teorema abstracto de Fermat" se tiene $[a]^{\varphi(n)} = [1]$.

SE67. Al considerar los elementos $\mathbf{a}$, $\mathbf{a}^2$,..., $\mathbf{a}^k$,... deberán presentarse repeticiones, ya que el grupo tiene un número finito de elementos. Sea entonces h el menor entero positivo para el cual $\mathbf{a}^h=\mathbf{a}$ [y por consiguiente $\mathbf{a}^{h-1}=\mathbf{e}$ = neutro] ;
La existencia de un tal entero positivo, h, la garantiza el principio del buen orden ya que el subconjunto E de los enteros positivos, m, para los cuales $\mathbf{a}^m=\mathbf{a}$, no es vacío [por el "teorema abstracto de Fermat", si n es el orden del grupo, entonces $\mathbf{a}^n=1$ luego $\mathbf{a}^{n+1}=\mathbf{a}$]; verifiquemos que los elementos $\mathbf{a}$, $\mathbf{a}^2$,..., $\mathbf{a}^{h-1}=\mathbf{e}$ son todos diferentes: en efecto si fuese $\mathbf{a}^i=\mathbf{a}^k$, con $1 \le i < k \le h-1$ tendríamos : $\mathbf{a}=\mathbf{a}^{k-i+1}$, con $k-i+1< h$ lo cual contradice que h era el menor entero para el cual se tenía $\mathbf{a}^h=\mathbf{a}$. Así que h-1 es el orden de $\mathbf{a}$.

Nota : Definiendo (en cualquier grupo, conmutativo o no), las potencias de un elemento $\mathbf{a}$ en la manera acostumbrada : si n es entero no negativo : $\mathbf{a}^0$=e=neutro, $\mathbf{a}^{n+1}=\mathbf{a}^n\mathbf{a}$; si n es negativo : $\mathbf{a}^n=(\mathbf{a}^{-1})^{-n}$ valen las usuales "reglas de los exponentes", a saber $\mathbf{a}^i\mathbf{a}^k=\mathbf{a}^{i+k}$, $(\mathbf{a}^k)^i=\mathbf{a}^{ki}$ [y si el grupo es conmutativo, $\mathbf{a}^k\mathbf{b}^k=(\mathbf{ab})^k$]; estas reglas se pueden demostrar por inducción.

SE68. Sea $\mathbf{G}$ un grupo de n elementos y sea m el orden de cierto elemento $\mathbf{a}\in\mathbf{G}$; por el teorema abstracto de Fermat tenemos que $\mathbf{a}^n$=e=neutro y por definición de orden de un elemento $\mathbf{a}^m$=e=neutro ; dividiendo n por m tenemos :
$n = m.q+r$, con $0 \le r < m$; por consiguiente $\mathbf{a}^r=\mathbf{a}^{(n-mq)}=\mathbf{e}=$ neutro y esto implica que r=0 ya que si así no fuese, m no sería el menor entero positivo para el cual $\mathbf{a}^m$=e .
Nota importante.
En la misma manera se demuestra la proposición 2 de l cap. 11 E, pag. 96 del texto de Lindsay Childs .

SE69.
[**E17 del texto**] $2^{47}=(2^{22})^2\,2^3 \underset{23}{\equiv} 1.\,2^3 \underset{23}{\equiv} 8$;
[**E18 del texto**] como $2^5 \underset{30}{\equiv} 2$ se tiene :
$2^{47}=(2^5)^9\,2^2 \underset{30}{\equiv} (2^9)\,2^2 \underset{30}{\equiv} 2^{11} \underset{30}{\equiv} (2^5)^2\,2 \underset{30}{\equiv} 2^3 \underset{30}{\equiv} 8$;
quizas más sencillo sería observar que las sucesivas potencias de 2 "módulo 30" se repiten ciclicamente : 2, 4, 8, 16, 2, 4, 8, 16, ... de manera que si el resto de la división del exponente por 4 es =1 la potencia considerada es $\underset{30}{\equiv} 2$, si el resto es 2 , $\underset{30}{\equiv} 4$, si el resto es 3 $\underset{30}{\equiv} 8$, de manera que, como el resto de la división de 47 por 4 es 3, la respuesta debía ser $\underset{30}{\equiv} 8$;
[**E19 del texto**] como $7^2 \underset{10}{\equiv} 9$, $7^4 \underset{10}{\equiv} 1$, se tiene : $7^{126}=(7^4)^{31}7^2 \underset{10}{\equiv} 9$;
También en este ejercicio es conveniente observar que :
$7^1 \underset{10}{\equiv} 7$, $7^2 \underset{10}{\equiv} 9$, $7^3 \underset{10}{\equiv} 3$, $7^4 \underset{10}{\equiv} 1$, $7^5 \underset{10}{\equiv} 7$, $7^6 \underset{10}{\equiv} 9$ ... de manera que, como el resto de la división del exponente 126 por 4 es 2 la respuesta es $\underset{10}{\equiv} 9$;

[**E20 del texto**] Como $5^2 \underset{12}{\equiv} 1$ resulta [si quiere, lo puede demostrar por inducción] que :
$5^n \underset{12}{\equiv} 1$ si n es par , $5^n \underset{12}{\equiv} 5$ si n es impar, de manera que $5^{400} \underset{12}{\equiv} 1$; análogamente
$3^n \underset{12}{\equiv} 9$ si n es par , $3^n \underset{12}{\equiv} 3$ si n es impar, de manera que $3^{400} \underset{12}{\equiv} 9$;

[**E21 del texto**] Por el teorema de Fermat tenemos $[17]^{28}=[1]$ en $\mathbf{Z}_{29}$ por lo cual $[17]^{27}$ actuará como $[17]^{-1}$;
como $[17]^2= [289]= [-1]$, resulta que
$[17]^{2n}= [-1]^n= [1]$ si n es par , $[17]^{2n}= [-1]^n= [-1]$ si n es impar ;
por lo tanto $[17]^{27}= [17]^{26}[17] = [-1][17] = [-17] = [12]$ y el inverso multiplicativo de [17] en $\mathbf{Z}_{29}$ se puede representar con 12.
Un procedimiento un poco más largo para hallar $[17]^{-1}$ hubiese sido resolver la ecuación : $17x+29y = 1$ con el algoritmo de Euclides :
$29 = 17.1+12$; $17=12.1+5$, $12=5.2+2$, $5=2.2+1$ luego $1= 5-2.2 = 5 -2(12-5.2) = =5.5+(-2)12 = 5(17-12)+(-2)12 = 5.17 +(-7)12 = 5.17+(-7)(29-17) = 17.12+(-7)29$ de lo cual sigue $x_1 = 12$.

[**E22 del texto**] Podríamos , como en el ejercicio anterior, observar que en $\mathbf{Z}_{41}$ se tiene $[12]^{-1}= [12]^{39}$ quedando la dificultad de expresar $[12]^{39}$ por medio de un representante positivo menor que 41; en este ejercicio aparentemente no hay ninguna potencia sencilla de [12] que dé como resultado [-1] ...
La otra posibilidad es aplicar nuevamente Euclides.
Una observación completamente casual que nos puede ayudar, es que $29=41-12$, por lo cual recordando la igualdad del ejercicio anterior : $17.12+(-7)29 =1$ obtenemos $\Rightarrow$
$1= 17.12+(-7)29 = 17.12 +(-7)(41-12) = (17+7).12+(-7)41 = 24.12+(-7)41$ de manera que $[12]^{-1}=[24]$.

[**E23 del texto**] **i**) orden de [11] en $\mathbf{Z}_{26}$;
como $\varphi(26)=\varphi(2)\varphi(13)= 12$ el orden de [11] es un divisor de 12 es decir , podría ser 1, 2, 3, 4, 6, 12 ;
calculemos : $11^2=121 \underset{26}{\equiv} 17 \underset{26}{\equiv} -9$, $11^3=1331 \underset{26}{\equiv} 5$, de manera que $11^6 \underset{26}{\equiv} 5^2=25 \underset{26}{\equiv} -1$; de esto sigue que ningún divisor de 6 puede ser el orden de [11] ;
por otra parte $11^4 \underset{26}{\equiv} (-9)^2 \underset{26}{\equiv} 81 \underset{26}{\equiv} 3$ así que el orden de [11] no puede ser ningún divisor de 4. Por consiguiente el orden buscado es 12;

ii) orden de [11] en $\mathbf{Z}_{23}$;
sabemos que como 23 es número primo, los 22 elementos no nulos de $\mathbf{Z}_{23}$ forman un grupo multiplicativo, así que por el teorema abstracto de Fermat cualquier elemento de este grupo tiene orden que es divisor de 22; el orden puede ser 1, 2, 11 o 22 ;
tenemos : $11^2=121 \underset{23}{\equiv} 6$, $11^4 \underset{23}{\equiv} (6)^2 \underset{23}{\equiv} 13$, $11^4 \underset{23}{\equiv} 169 \underset{23}{\equiv} 8$,
$11^{11}=11^{8+2+1} \underset{23}{\equiv} 8.6.11=529 \underset{23}{\equiv} -1$; por lo tanto el orden buscado es 22 ;
iii) orden de [11] en $\mathbf{Z}_{19}$; el orden buscado es divisor de 18 ;
$11^3= 1331 \underset{19}{\equiv} 1$ [ya que $19.70 = 1330$] por lo cual el orden es 3.

[**E24 del texto**] **i**)Posibles órdenes de elementos de $\mathbf{Z}_{13}$: todos los divisores de 12 ; tiene orden =1 sólo [1] ; orden 2 sólo [12] ; orden 3 : [3]. [9] ; orden 4 : [5], [8] ; orden 6 : [4], [10] ; orden 12 : [2], [6], [7], [11] .
ii)Posibles órdenes de elementos invertibles de $\mathbf{Z}_{20}$: todos los divisores de $8=\varphi(20)$; tiene orden =1 sólo [1] ; orden 2 : [9] , [11], [19] ; orden 4 : [3], [7], [13], [17] ; no hay ningún elemento de orden 8;

[**E25 del texto**] (**importante**) Sea ord(a)=n , $b=a^r$, (r, n)=d , $r=r_1d$, $n=n_1d$ y sabemos que $(r_1,n_1)=1$;
para demostrar que ord(b)= $n/d = n_1$ basta poner en evidencia que : **i**) $b^{n_1}= e$ = neutro; **ii**) si $b^m=e$ entonces por consiguiente $n_1 | m$.
Tenemos en efecto : $b^{n_1}= (a^r)^{n_1}= a^{r.n_1}= a^{r_1.d.n_1}= a^{r_1.n}= (a^n)^{r_1}= e$;
si $b^m=e$ entonces $(a^r)^m= a^{rm}= e$ luego rm es múltiplo de n , es decir r.m=kn .
[recuerde **SE68** de esta guía y/o la proposición 2 del cap. 11E de pag. 96 del texto de Lindsay Childs];
$r.m=kn \Rightarrow r_1.d.m = k.n_1.d \Rightarrow r_1.m = k.n_1$ y como n_1 divide $r_1.m$ pero $(r_1,n_1)=1$, sigue que n_1 divide m .

[**E26 del texto**] En la resolución del ejercicio **E23** del texto, parte **ii**) vimos que el orden de [11] en $\mathbf{Z}_{23}$ es 22; de esto sigue que las potencias de [11] de exponentes 1 hasta 22 son los 22 diferentes elementos no nulos de $\mathbf{Z}_{23}$.

SE70. Sea $\mathbf{G} =\{\mathbf{a}, \mathbf{a}^2, \mathbf{a}^3,..., \mathbf{a}^{n-1}=\mathbf{e}\}$ un grupo cíclico de n elementos y sea d un divisor de n; sea $\mathbf{b}= \mathbf{a}^k$ un elemento del grupo que tenga orden h ;
para que $\mathbf{a}^k$ tenga orden d, debe ser [ver ejercicio [**E25 del texto**] (**importante**)] :
$d = n/(k, n)$ es decir : $(k, n) = n/d$; así que la pregunta es : ¿ para cuales números enteros, k, del intervalo [1, n-1] el máximo común divisor con n es cierto divisor asignado, n/d = h ? Observemos que el mismo h es el menor de ellos y que los demás [dentro del intervalo [1, n-1]], se obtienen multiplicando h por un número relativamente primo con d. De esta forma se obtienen exáctamente $\varphi(d)$ posibles valores para k.

A título de ejemplo, sea n=60, sea **a** un elemento de orden 60 y hallemos todos los exponentes , k, tales que $\mathbf{a}^k$ tenga orden d=12. Debe ser $\frac{60}{(60, k)} = 12$, $(60, k)=5$;
evidentemente el menor valor posible para k es k=5 ; si multiplicamos k por un número, s, relativamente primo con 12, también el nuevo máximo común divisor (60, 5s) será 5, mientras que si mutliplicásemos k por un número, t, que tenga algún factor primo común [por ej. t=14] con 12, el MCD sería $(60, 5.14) = (60, 70)= 10 \neq 5$.
Como los posibles números por los cuales podemos multiplicar k obteniendo un número del intervalo [1, 59] tal que su MCD con 60 siga siendo 5 son entonces los $\varphi(5)=4$ números : 5.1 , 5.5, 5.7, 5.11 es decir 5, 25, 35, 55 , estos son los exponentes posibles.