

APELLIDOS:

GRUPO:

NOMBRE:

**Cuestión 1 (2 pt)** (a) Resuelve, si es posible, la ecuación en congruencias  $234x \equiv 6 \pmod{366}$ .

*Solución:* La ecuación tiene soluciones, ya que el máximo común divisor de 234 y 366 es 6, y 6 también es divisor de 6. Por este motivo, podemos simplificarla dividiendo entre 6, con lo cual obtenemos la ecuación transformada  $39x \equiv 1 \pmod{61}$ .

Comenzamos aplicando el algoritmo de Euclides:

$$\begin{array}{r} 61 \mid 39 \quad 39 \mid 22 \quad 22 \mid 17 \quad 17 \mid 5 \quad 5 \mid 2 \quad 2 \mid 1 \\ 22 \mid 1 \quad 17 \mid 1 \quad 5 \mid 1 \quad 2 \mid 3 \quad 1 \mid 2 \quad 0 \mid 2 \end{array}$$

La solución de la ecuación es  $x = (-1)^{n-1} P_{n-1} b \pmod{61}$ , donde  $n = 6$ ,  $b = 1$  y  $P_{n-1}$  se obtiene aplicando el algoritmo siguiente:

$k$	0	1	2	3	4	5	6
$q_k$		1	1	1	3	2	2
$P_k$	1	1	2	3	11	25	61

Por tanto la solución será

$$\begin{aligned} x &= (-1)^{n-1} P_{n-1} b \pmod{61} \\ x &= (-1)^5 \cdot 25 \cdot 1 \pmod{61} \\ x &= -25 \pmod{61} = 36 \pmod{61} \end{aligned}$$

Las soluciones de la ecuación original serán entonces (sumando a la solución obtenida el módulo de la ecuación transformada, es decir, 61):

$$\begin{aligned} x &\equiv 36 \pmod{366} & x &\equiv 97 \pmod{366} & x &\equiv 158 \pmod{366} \\ x &\equiv 219 \pmod{366} & x &\equiv 280 \pmod{366} & x &\equiv 341 \pmod{366} \end{aligned}$$

(b) Calcula  $\overline{73} \cdot \overline{65} + \overline{39}^{-1}$  en  $\mathbb{Z}_{61}$ .

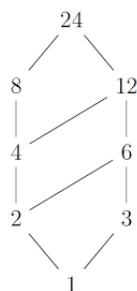
*Solución:*

Por el apartado anterior, sabemos que  $39^{-1} \pmod{61} = 36 \pmod{61}$ . Por tanto

$$73 \cdot 65 + 39^{-1} \pmod{61} = 12 \cdot 4 + 36 \pmod{61} = 48 + 36 \pmod{61} = 84 \pmod{61} = 23 \pmod{61}$$

**Cuestión 2 (2.5 pt)** Consideremos el retículo  $D_{24}$  de los divisores naturales de 24, con la relación de divisibilidad.

(a) Dibuja el correspondiente diagrama de Hasse.



(b) Calcula los elementos de  $D_{24}$  que tengan complementario.

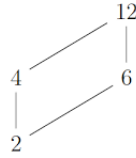
*Solución:* Los únicos elementos que tienen complementario son  $\bar{1} = 24$ ,  $\overline{24} = 1$ ,  $\bar{3} = 8$  y  $\bar{8} = 3$ .

- (c) ¿Es un álgebra de Boole? ¿Por qué?

*Solución:* No es un álgebra de Boole, ya que no todo elemento tiene complementario. Observemos además que  $24 = 2^3 \cdot 3$ , luego no es libre de cuadrados.

- (d) Calcula, si existen, cotas superiores e inferiores, supremo e ínfimo del subconjunto  $B = \{2, 4, 6, 12\}$  en  $D_{24}$ .

*Solución:* En primer lugar el diagrama de Hasse de  $B$  es:



Las cotas superiores de  $B$  en  $D_{24}$  son  $\{12, 24\}$ , y por tanto el supremo de  $B$  en  $D_{24}$  es 12. De forma análoga las cotas inferiores serán  $\{1, 2\}$ , y el ínfimo será 2.

- (e) ¿Es  $B$  un álgebra de Boole? Justifica tu respuesta.

*Solución:* En este caso, sí que se trata de un Álgebra de Boole. Podemos ver claramente que se trata de un retículo. Es acotado, el máximo es 12 y el mínimo 2. Además todo elemento está complementado,  $\bar{2} = 12, \bar{12} = 2, \bar{4} = 6, \bar{6} = 4$ , y es distributivo puesto que en todas las ternas de elementos de  $B$ , o hay dos elementos repetidos, o uno de ellos es el máximo o el mínimo. Otra forma de verlo, sería darnos cuenta de que tiene la misma estructura que el retículo de divisores del 6 y, por tanto, sería retículo de Boole.

**Cuestión 3 (2 pt)** (a) En el conjunto  $\mathbb{Z}$  de los números enteros se define la siguiente relación binaria

$$aRb \leftrightarrow a \neq b$$

Justifica cuáles de las propiedades siguientes cumple: reflexiva, simétrica, antisimétrica, transitiva.

*Solución:*

**Reflexiva:** No es reflexiva, ya que  $\forall a \in \mathbb{N} \ a \neq a$ .

**Simétrica:** Es simétrica, ya que si  $aRb$ , entonces  $a \neq b$ , luego  $b \neq a$  y  $bRa$ .

**Antisimétrica:** No es antisimétrica, por ejemplo  $2R3$  y  $3R2$  y  $2 \neq 3$ .

**Transitiva:** No es transitiva, por ejemplo  $2R3$  y  $3R2$ , pero 2 no está relacionado con 2.

- (b) En el conjunto  $A = \{1, 2, 3, 4, 5, 6, 7, 8, 9\}$  dos elementos están relacionados,  $aRb$ , si y sólo si el producto  $a \cdot b$  es el cuadrado de algún número entero. ¿Es  $R$  una relación binaria de equivalencia? En caso afirmativo, calcula las clases de equivalencia de los elementos de  $A$  y el conjunto cociente correspondiente.

*Solución:* Vamos a calcular el grafo de la relación:

$$R = \{(1, 1), (2, 2), (3, 3), (4, 4), (5, 5), (6, 6), (7, 7), (8, 8), (9, 9), (1, 4), (4, 1), (1, 9), (9, 1), (2, 8), (8, 2), (4, 9), (9, 4)\}$$

Como podemos comprobar en el grafo la relación es reflexiva, simétrica y transitiva, por tanto es una relación binaria de equivalencia.

Las clases de equivalencia son:

$$\bar{1} = \{1, 4, 9\} = \bar{4} = \bar{9}$$

$$\bar{2} = \bar{8} = \{2, 8\}$$

$$\bar{3} = \{3\}$$

$$\bar{5} = \{5\}$$

$$\bar{6} = \{6\}$$

$$\bar{7} = \{7\}$$

Y, el conjunto cociente,  $A/\mathcal{R} = \{\bar{1}, \bar{2}, \bar{3}, \bar{5}, \bar{6}, \bar{7}\} = \{\{1, 4, 9\}, \{2, 8\}, \{3\}, \{5\}, \{6\}, \{7\}\}$ .

**Cuestión 4 (2 pt)** (a) Simplifica, especificando las propiedades del álgebra de Boole que utilizas, la siguiente función booleana:

$$f(x, y, z) = \bar{x} + ((y + z) \cdot (x + y + z))$$

*Solución:*

$$\begin{aligned} f(x, y, z) &= \bar{x} + \overline{(y + z) \cdot (x + y + z)} \\ &= \bar{x} + \bar{y}\bar{z}\bar{x}\bar{y}\bar{z} && \text{Leyes de De Morgan} \\ &= \bar{x} + \bar{x}\bar{y}\bar{z} && \text{Idempotencia} \\ &= \bar{x} && \text{Simplificativa} \end{aligned}$$

(b) Calcula la forma más simplificada de la siguiente función booleana mediante el método de Quine-McCluskey. Si hay más de una, escríbelas todas.

$$f(x, y, z) = \bar{x}\bar{y}\bar{z} + \bar{x}y\bar{z} + x\bar{y}z + xyz$$

*Solución:*

Método de Quine:

Número de unos	T. minimales	1a comparación	2a comparación
0	000*	0-0	No hay
1	010*	-10	
2	101* 110*	1-1 11-	
3	111*		

Simplificación:  $f(x, y, z) = \bar{x}\bar{z} + y\bar{z} + xz + xy$ . Rejilla de McCluskey:

	0 0 0	0 1 0	1 0 1	1 1 0	1 1 1
0 - 0	X	X			
- 1 0		X		X	
1 - 1			X		X
1 1 -				X	X

Como en las columnas primera y tercera hay una única marca, los implicantes primos  $\bar{x}\bar{z}$  y  $xz$  son esenciales. Por otro lado, con estos dos implicantes primos, solamente nos quedaría un término minimal por cubrir, el  $xy\bar{z}$ . Para ello podemos utilizar o bien el implicante primo  $y\bar{z}$ , o bien el  $xy$ . Por tanto tenemos dos posibles simplificaciones:

$$f(x, y, z) = \bar{x}\bar{z} + xz + y\bar{z}$$

$$f(x, y, z) = \bar{x}\bar{z} + xz + xy$$

**Cuestión 5 (1.5 pt)** (a) Dado el conjunto  $A = \{a, b, c, 8, 13\}$ , completa la relación binaria en  $A$  definida por el grafo  $R = \{(a, b), (b, c), (8, 13)\}$ , con el menor número de elementos posible, para que sea de equivalencia.

*Solución:*  $R = \{(a, a), (b, b), (c, c), (8, 8), (13, 13), (a, b), (b, c), (8, 13), (b, a), (c, b), (13, 8), (a, c), (c, a)\}$

(b) Demuestra que la relación de divisibilidad en  $\mathbb{N}$  es una relación transitiva.

*Solución:* Supongamos que  $a, b, c \in \mathbb{N}$  tales que  $a \mid b$  y  $b \mid c$ . De aquí, existen  $k \in \mathbb{N}$  y  $s \in \mathbb{N}$  tales que  $b = ka$  y  $c = bs$ . Por tanto sustituyendo obtenemos  $c = ksa$  con  $ks \in \mathbb{N}$ . Luego  $a \mid c$  y la relación es transitiva.

(c) Resuelve la siguiente ecuación en el Álgebra de Boole de cuatro elementos  $A = \{0, 1, a, b\}$ :

$$ax^n + ax^{n-1} + \dots + ax + bx = 1 + x$$

*Solución:* Por idempotencia podemos simplificar la ecuación hasta obtener la siguiente  $ax + bx = 1 + x$ . Aplicando la propiedad absorbente obtenemos  $ax + bx = 1$ . Aplicando ahora la propiedad distributiva  $(a+b)x = 1$ . Teniendo en cuenta que estamos en el Álgebra de Boole de cuatro elementos, sabemos que  $a$  y  $b$  son complementarios, por tanto  $a + b = 1$ . De aquí  $x = 1$  es la solución buscada.