

Matemática Discreta 2
(Solución)

Examen Febrero 2003

Nº Examen =

Apellidos

Nombre

C.I.

- 1) a) Hallar el menor x entero positivo que verifica : $16x + 5 \equiv 21 \pmod{99}$
 $9x + 7 \equiv 32 \pmod{70}$

Justificar desarrollando un método para hallar el tal x

- 2) **Solución: $x = 3565$.** El sistema es equivalente a $16x \equiv 16 \pmod{99}$
 $9x \equiv 25 \pmod{70}$

De lo cual $x \equiv 1 \pmod{99}$ (pues $\text{mcd}(16,99)=1$)

$x \equiv -5 \pmod{70}$ (pues $39 \cdot 9 \equiv 1 \pmod{70}$ y $39 \cdot 25 \equiv -5 \pmod{70}$)

Por el teorema Chino de los Restos existe un único x positivo menor que $99 \cdot 70 = 6930$ que verifica dicho sistema y el mismo verifica $x \equiv a70 + b99 \pmod{6930}$ siendo a y b tales que $a70 \equiv 1 \pmod{99}$ y $b99 \equiv -5 \pmod{70}$ de aquí que $a = 58$ y $b = -5$ y $x \equiv 58 \cdot 70 - 5 \cdot 99 \pmod{6930}$, pero $58 \cdot 70 - 5 \cdot 99 = 3565 < 6930$, por lo tanto $x = 3565$.

- b) Hallar a y b enteros positivos tales que :

$$a + b = 1271$$

$$\text{mcm}(a,b) = 330 \text{ mcd}(a,b)$$

Justificar

Solución: $a = 930$ y $b = 341$ o al revés. Como $a + b = 1271 = 31 \cdot 41$, entonces el $\text{mcd}(a,b)$ puede ser o bien 1 o bien 31 o bien 41 o bien 1271. Si $\text{mcd}(a,b) = 1$ entonces $\text{mcm}(a,b) = 330$, pero $a, b < \text{mcm}$ por lo que $a+b < 2\text{mcm} = 660 < 1271$. Si $\text{mcd}(a,b) = 31$, entonces existen k y h tales que $a = 31k$, $b = 31h$ y

$$k \cdot h = a \cdot b / 31^2 = \text{mcm}(a,b) = 330 = 2 \cdot 3 \cdot 5 \cdot 11,$$

$$k+h = (a+b)/31 = 41. \quad (E)$$

Por lo tanto, tendremos que los factores de h y k son particionan los factores 2, 3, 5 y 11 en dos conjuntos disjuntos. Antes de enumerar las posibilidades observemos que el factor 11 no podrá aparecer junto con el factor 5 pues superaría 41, ni con el 2 y el 3, ni con el 3 y el 5, ni con el 2 y el 5 por la misma razón. Las posibilidades son:

$$\{\{11\}, \{2,3,5\}\}, \{\{11,2\}, \{3,5\}\} \text{ y } \{\{11,3\}, \{2,5\}\}, \text{ que dan}$$

$$11 + 30 = 41, \quad 22 + 15 = 37 \text{ y } 33 + 10 = 43 \text{ respectivamente. La primera es la}$$

única opción que verifica la ecuación (E) y es la solución del problema. Los demás casos ($\text{mcd}(a,b) = 41$ o 1271) se estudian en forma similar al anterior.

- 2) Demostrar que un grupo de menos de 6 elementos es abeliano.

Solución: Si tiene un solo elemento es obvio. Si tiene un número primo de elementos, tiene que ser cíclico y por tanto abeliano, cosa que se cumple para $n = 2, 3$ y 5 . Resta ver que sucede para $n = 4$. En este caso el subgrupo generado por un elemento diferente a la

unidad puede tener orden 2 o 4. Si tiene orden 4 entonces el grupo es cíclico y por tanto, conmutativo. Supongamos entonces que todo elemento diferente de la unidad tiene orden 2. Sea x e y dos de dichos elementos diferentes entre sí. Es decir x e y tienen orden 2, son diferentes de la unidad y entre sí. Por lo tanto tenemos por ahora tres elementos: la unidad u , x e y . Nos falta el cuarto elemento que afirmamos es xy . Efectivamente, xy no puede ser ni x ni y pues si $xy = x$ entonces $y = u$. De la misma forma si $xy = y$ entonces $x = u$. Además si $xy = u$ entonces $xyx = x \Rightarrow y = x$. Basta ahora probar que los elementos conmutan. Primero veamos que $xy = yx$. Efectivamente, yx no puede ser x porque sino y sería u , ni puede ser y porque sino x sería u , ni puede ser u porque sino $x=y$, por lo tanto el único elemento que puede ser es xy . Por otra parte $x(xy) = x(yx) = (xy)x$; $y(xy) = (yx)y = (xy)y$.

3) Se considera S_9 (grupo simétrico)

a) Exhibir un elemento de este grupo de orden 20. Elevar a la potencia 5 dicho elemento.

Solución: un posible elemento, expresado como producto de ciclos es $x = (1234)(56789)$. Su potencia quinta es $x^5 = (1234)^5(56789)^5 = (1234)^{4+1} = (1234)^4(1234)^1 = (1234)$.

b) Demostrar que en este grupo no existen elementos de orden 18.

Solución: Si existiera un tal elemento su descomposición en ciclos disjuntos con longitudes L_1, L_2, \dots, L_n , deberían verificar $\text{mcm}(L_1, L_2, \dots) = 18$ y $L_1 + L_2 + \dots + L_n = 9$. De la primera condición deducimos que alguno de los L_i debe ser un múltiplo de 9. Pero por la segunda igualdad la única posibilidad es que sea 9 y que $n = 1$, lo cual impide que se verifique la primera condición.

4) En $Z_7[x]$ se consideran los polinomios :

$$P(x) = x^4 + 2x^3 + 3x^2 + 6x + 4 \quad ; \quad Q(x) = 3x^3 + 4x^2 + 5x + 4$$

Hallar $\text{mcd}(P, Q)$ en $Z_7[x]$ (es un polinomio mónico)

Solución: $\text{mcd}(P, Q) = x+1$. Efectivamente

$$x^4 + 2x^3 + 3x^2 + 6x + 4 = (x^3 - x^2 - 4x - 1)(x+3) + 2x^2 + 2x,$$

y

$$x^3 - x^2 - 4x - 1 = (x^2 + x)(x-2) + 6x$$

y

$$x^2 + x = x(x+1).$$

Podemos verificar que -1 es raíz de ambos polinomios: $P(-1) = 1 - 2 + 3 - 6 + 4 = 0$ y $Q(-1) = -3 + 4 - 5 + 4 = 0$.

5) Sea $(A, +, \cdot, \bar{}, 0, 1)$ un álgebra booleana. Demuestre que (A, \otimes) es un grupo conmutativo, donde \otimes está definida como :

$$a \otimes b = a \cdot \bar{b} + \bar{a} \cdot b$$

Solución:

$$\text{Neutro } a \otimes 0 = a \cdot 1 + \bar{a} \cdot 0 = a + 0 = a$$

$$\text{Inverso } a \otimes a = a \cdot \bar{a} + \bar{a} \cdot a = 0 + 0 = 0$$

$$\text{Conmutativa: } a \otimes b = a \cdot \bar{b} + \bar{a} \cdot b = \bar{a} \cdot b + a \cdot \bar{b} = b \cdot \bar{a} + \bar{b} \cdot a = b \otimes a.$$

$$\begin{aligned}
\text{Asociativa: } a \otimes (b \otimes c) &= a \otimes (b.\bar{c} + \bar{b}.c) = a.(\overline{b.\bar{c} + \bar{b}.c}) + \bar{a} (b.\bar{c} + \bar{b}.c) \\
&= a.(\overline{(b.\bar{c}).(\bar{b}.c)}) + \bar{a}.b.\bar{c} + \bar{a}.\bar{b}.c = a.((\bar{b} + c).(b + \bar{c})) + \bar{a}.b.\bar{c} + \bar{a}.\bar{b}.c \\
&= a.(\bar{b}.b + \bar{b}.\bar{c} + c.b + c.\bar{c}) + \bar{a}.b.\bar{c} + \bar{a}.\bar{b}.c = a.(0 + \bar{b}.\bar{c} + c.b + 0) + \bar{a}.b.\bar{c} + \bar{a}.\bar{b}.c = a.\bar{b}.\bar{c} + a.c.b + \bar{a}.b.\bar{c} + \bar{a}.\bar{b}.c.
\end{aligned}$$

Por otro lado

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

Que tiene los mismos términos que la suma anterior salvo reordenamiento.

- Puntajes : 1) 26 : a) 14 b) 12
2) 18
3) 20 : a) 10 b) 10
4) 18
5) 18