

PRIMER PARCIAL DE MATEMÁTICA DISCRETA 2

Nombre	C.I.	No. de prueba
--------------	-----------	---------------------

Duración: 3:30 horas. Sin material y sin calculadora.

Es necesario mostrar la resolución de los ejercicios, presentar únicamente la respuesta final carece de valor.

SOLUCIONES.

Ejercicio 1.

- (a) Si a, n son enteros tales que $\text{mcd}(a, n) = 1$, entonces $a^{\varphi(n)} \equiv 1 \pmod{n}$.
- (b) Tenemos que $\varphi(35) = \varphi(5 \times 7) = \varphi(5)\varphi(7) = 4 \times 6 = 24$. Como $\text{mcd}(102, 35) = 1$, por el Teorema de Euler tenemos que $102^{24} \equiv 1 \pmod{35}$; además $102 \equiv 32 \pmod{35} \equiv -3 \pmod{35}$. Por lo tanto $102^{201} \equiv 102^{24 \times 8 + 9} \pmod{35} \equiv 102^9 \pmod{35} \equiv (-3)^9 \pmod{35}$. Ahora calculamos directamente (se puede usar el Teo Chino de resto también): $(-3)^9 \equiv (-27)^3 \pmod{35} \equiv 8^3 \pmod{35} \equiv 64 \times 8 \pmod{35} \equiv (-6) \times 8 \pmod{35} \equiv -48 \pmod{35} \equiv 22 \pmod{35}$. Por lo tanto $x = 22$.
- (c) Como 4001 es primo, tenemos que $\varphi(4001) = 4000$. Como $\text{mcd}(30, 4001) = 1$, por Euler tenemos que $30^{4000} \equiv 1 \pmod{4001}$ y por lo tanto $30^{3998} 30^2 \equiv 1 \pmod{4001}$, es decir, $30^{3998} 900 \equiv 1 \pmod{4001}$. Entonces 30^{3998} es el inverso de 900 módulo 4001; esto es, buscamos $x \in \{0, \dots, 4000\}$ tal que $900x \equiv 1 \pmod{4001}$. Para hallar x basta con resolver $900x + 4001y = 1$ y esto lo hacemos con el algoritmo de Euclides extendido: tenemos que $4001 = 900(4) + 401$, $900 = 401(2) + 98$, $401 = 98(4) + 9$, $98 = 9(10) + 8$ y $9 = 8(1) + 1$, y utilizando estos datos obtenemos $1 = (4001)(101) + 900(-449)$, así que $x \equiv -449 \pmod{4001}$ y por lo tanto $x = 4001 - 449 = 3552$.

Ejercicio 2.

(a) y (b) Ver Teórico.

(c) Veamos tres formas posibles, una es con la fórmula:

$$\varphi(dn) = dn \prod_{\substack{p \text{ primo} \\ p|dn}} (1 - 1/p) = dn \prod_{\substack{p \text{ primo} \\ p|n}} (1 - 1/p) = d\varphi(n)$$

donde en la segunda igualdad se usa que $d|n$.

Otra forma es contando: si $x \in \mathbb{Z}$ es tal que $1 \leq x < nd$ y $\text{mcd}(x, dn) = 1$ entonces $x = nq + r$ con $0 \leq r < n$. Como $d|n$, $\text{mcd}(x, dn) = 1 \Rightarrow \text{mcd}(x, n) = 1$ de donde $\text{mcd}(r, n) = 1$ puesto que $r = x - nq$. Por otra parte q puede ser cualquier entero que cumpla $0 \leq q < d$ (pues $x < nd$). De esa forma tenemos d posibilidades para q y $\varphi(n)$ posibilidades para r , por lo tanto tenemos $d\varphi(n)$ posibilidades para x y se cumple

$$d\varphi(n) = \varphi(dn).$$

La tercer forma es usando la descomposición factorial de d y m ; sea $m = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$ la descomposición factorial de m (donde los p_i son primos y los α_i enteros positivos). Como $d|m$ entonces $d = p_1^{\beta_1} p_2^{\beta_2} \dots p_k^{\beta_k}$ con $0 \leq \beta_i \leq \alpha_i$ para $i = 1, 2, \dots, k$. Se tiene que:

$$\begin{aligned} \varphi(md) &= \varphi(p_1^{\alpha_1+\beta_1} p_2^{\alpha_2+\beta_2} \dots p_k^{\alpha_k+\beta_k}) = (p_1-1)(p_2-1) \dots (p_k-1) p_1^{\alpha_1+\beta_1-1} p_2^{\alpha_2+\beta_2-1} \dots p_k^{\alpha_k+\beta_k-1} \\ &= (p_1-1)(p_2-1) \dots (p_k-1) p_1^{\alpha_1-1} p_2^{\alpha_2-1} \dots p_k^{\alpha_k-1} \cdot p_1^{\beta_1} p_2^{\beta_2} \dots p_k^{\beta_k} = \varphi(m) \cdot d \end{aligned}$$

como queríamos probar.

- (d) Sea n un entero compuesto. Si $n = md$ con $1 < m < d \leq n-1$ entonces m y d aparecen como factores en $(n-1)!$ y por lo tanto $n|(n-1)!$. Si es imposible descomponer a n en la forma anterior entonces $n = p^2$ con p primo (y $p > 2$ pues $n > 4$), pero en este caso p y $2p$ aparecen como factores en $(n-1)!$ (pues $n-1 = p^2-1 > 2p$ pues $p > 2$) así que también se verifica que $n|(n-1)!$.
- (e) Si n es primo entonces $\text{mcd}(n, (n-1)!) = 1$ así que usando la propiedad multiplicativa tenemos que $\varphi(n!) = \varphi(n \cdot (n-1)!) = \varphi(n)\varphi((n-1)!) = (n-1)\varphi((n-1)!)$. Si $n = 4$ entonces $\varphi(4!)/\varphi(3!) = \varphi(24)/\varphi(6) = 8/2 = 4$. En último caso, si n es compuesto y $n > 4$ entonces $n|(n-1)!$ así que usando la parte iii) tenemos que $\varphi(n!) = n\varphi((n-1)!)$.

En resumen tenemos que:

$$\frac{\varphi(n!)}{\varphi(n-1)!} = \begin{cases} n-1 & \text{si } n \text{ es primo.} \\ n & \text{si } n \text{ es compuesto} \end{cases}$$

Ejercicio 3.

- (a) Si $x \cdot g_0 = g_0 \Rightarrow (x \cdot g_0) \cdot g_0^{-1} = g_0 \cdot g_0^{-1} \Rightarrow x \cdot (g_0 \cdot g_0^{-1}) = g_0 \cdot g_0^{-1} \Rightarrow x \cdot e = e \Rightarrow x = e$; por lo tanto $x \cdot g = e \cdot g = g$ para todo $g \in G$.
- (b) Si en la fila correspondiente a g , un elemento h aparece dos veces, es porque existen $g_1 \neq g_2 \in G$, tales que $h = g \cdot g_1$ y $h = g \cdot g_2$. Pero entonces $g \cdot g_1 = g \cdot g_2$ y por lo tanto $g^{-1} \cdot (g \cdot g_1) = g^{-1} \cdot (g \cdot g_2)$. Entonces, por asociativa y propiedad del inverso y del neutro tendríamos que $g_1 = g_2$, lo cual es absurdo. Para columnas el argumento es análogo con $g_1 \cdot g = g_2 \cdot g$ y multiplicando a la derecha por g^{-1} .
- (c) (i) Por (b) el último elemento de la 2da columna es g_2 . Por lo tanto $g_6 \cdot g_2 = g_2$ y por (a) tenemos que g_6 es el neutro.
- (ii) Tenemos que $g_2 \neq g_6$, $g_2^2 = g_1 \neq g_6$ y $g_2^3 = g_2^2 \cdot g_2 = g_1 \cdot g_2 = g_6$ y g_6 es el neutro, así que $\text{o}(g_2) = 3$.
- (iii) Usamos primero que g_6 es el neutro y obtenemos

\cdot	g_1	g_2	g_3	g_4	g_5	g_6
g_1		g_6		g_5		g_1
g_2		g_1				g_2
g_3	g_5	g_4	g_6			g_3
g_4		g_5		g_6		g_4
g_5		g_3			g_6	g_5
g_6	g_1	g_2	g_3	g_4	g_5	g_6

Luego, utilizando por ejemplo que como $g_1g_2 = g_6$, (entonces $g_1^{-1} = g_2$) por lo tanto $g_2g_1 = g_6$

\cdot	g_1	g_2	g_3	g_4	g_5	g_6
g_1		g_6		g_5		g_1
g_2	g_6	g_1				g_2
g_3	g_5	g_4	g_6			g_3
g_4		g_5		g_6		g_4
g_5		g_3			g_6	g_5
g_6	g_1	g_2	g_3	g_4	g_5	g_6

Ahora usemos varias veces la propiedad asociativa:

- $g_3(g_2g_4) = (g_3g_2)g_4 = g_4g_4 = g_6 = g_3g_3$ así que por cancelativa: $g_2g_4 = g_3$.
- $g_2g_5 = g_2(g_4g_2) = (g_2g_4)g_2 = g_3g_2 = g_4$
- $g_1^2 = g_1(g_2g_2) = (g_1g_2)g_2 = g_6g_2 = g_2$
- $(g_3g_5)g_2 = g_3(g_5g_2) = g_3g_3 = g_6 = g_1g_2$ así que por cancelativa: $g_3g_5 = g_1$.
- $(g_4g_3)g_2 = g_4(g_3g_2) = g_4g_4 = g_6 = g_1g_2$ así que por cancelativa $g_4g_3 = g_1$

Nos va quedando:

\cdot	g_1	g_2	g_3	g_4	g_5	g_6
g_1	g_2	g_6				g_1
g_2	g_6	g_1		g_3	g_4	g_2
g_3	g_5	g_4	g_6		g_1	g_3
g_4		g_5	g_1	g_6		g_4
g_5		g_3			g_6	g_5
g_6	g_1	g_2	g_3	g_4	g_5	g_6

Finalmente utilizamos reiteradamente la parte b (propiedad Sudoku) para completar los lugares que falta:

- $g_5 = g_2g_3$ • $g_2 = g_3g_4$ • $g_4 = g_5g_1$ • $g_3 = g_4g_1$ • $g_2 = g_4g_5$
- $g_1 = g_5g_4$ • $g_2 = g_5g_3$ • $g_3 = g_1g_5$ • $g_5 = g_1g_4$ • $g_4 = g_1g_3$

Quedándonos la siguiente tabla:

\cdot	g_1	g_2	g_3	g_4	g_5	g_6
g_1	g_2	g_6	g_4	g_5	g_3	g_1
g_2	g_6	g_1	g_5	g_3	g_4	g_2
g_3	g_5	g_4	g_6	g_2	g_1	g_3
g_4	g_3	g_5	g_1	g_6	g_2	g_4
g_5	g_4	g_3	g_2	g_1	g_6	g_5
g_6	g_1	g_2	g_3	g_4	g_5	g_6