

**SOLUCIONES DEL EXAMEN DE MATEMÁTICA DISCRETA II**  
21 DE JULIO DE 2005.

**Ejercicio 1**

(1)  $n \equiv -3 \pmod{n+3}$ ,  $\Rightarrow n^3 \equiv -27 \pmod{n+3}$ ,  $\Rightarrow 3n^3 - 11n + 48 \equiv -81 + 33 + 48 \equiv 0 \pmod{n+3}$ , de donde se deduce que  $3n^3 - 11n + 48$  es múltiplo de  $n+3$  como se quería demostrar.

(2) Sea  $h = \text{mcd}(a, b) \geq 1$ .  $h$  divide a  $a$  y divide a  $b$ , luego  $h$  divide a cualquier múltiplo  $bc$  de  $b$ , y como divide a  $a$ , divide también a la diferencia  $bc - a$ . Tenemos entonces que  $h$  es un divisor común de  $b$  y de  $bc - a$ . Luego divide al  $\text{mcd}(bc - a, b)$ . (i)

Sea  $k = \text{mcd}(bc - a, b) \geq 1$ .  $k$  divide a  $bc - a$  y divide a  $b$ ; luego  $k$  divide a cualquier múltiplo  $bc$  de  $b$ , y como divide a  $bc - a$ , divide también a la diferencia  $bc - (bc - a) = a$ . Tenemos entonces que  $k$  es un divisor común de  $b$  y de  $a$ . Luego divide al  $\text{mcd}(a, b)$ . (ii)

De (i) y (ii) se deduce que  $h$  y  $k$  son enteros  $\geq 1$  tales que uno divide al otro y recíprocamente. Entonces  $h = k$  como queríamos demostrar.

(3) Sea  $a = 3n^3 - 11n$ . Como  $n \geq 2$  se tiene  $a \geq 3 \cdot 2^3 - 11 \cdot 2 = 2$ .

Sea  $b = n + 3 \geq 5$ . Sea  $c$  entero positivo tal que  $bc - a = 48$ . Debemos probar que existe tal  $c$ . En efecto, queremos que  $(n + 3)c = a + 48 = 3n^3 - 11n + 48$ , o lo que es equivalente

$$c = \frac{3n^3 - 11n + 48}{n + 3}$$

El numerador es igual a  $a + 48 \geq 50$  y el denominador es mayor o igual que 5. Luego  $c$  es mayor que 0. Por la parte 1) el numerador es múltiplo entero del denominador, entonces  $c$  es entero.

Por la parte 2) se tiene

$$\text{mcd}(a, b) = \text{mcd}(bc - a, b) \quad (iii)$$

para todos  $a, b$  y  $c$  enteros no nulos, en particular para  $a, b$  y  $c$  los enteros positivos elegidos antes en función de  $n$ . Sustituyendo en (iii) las expresiones  $a = 3n^3 - 11n$ ,  $b = n + 3$  y  $bc - a = 48$  se deduce  $\text{mcd}(3n^3 - 11n, n + 3) = \text{mcd}(48, n + 3)$  como se quería demostrar.

(4) Descomponiendo en factores primos:  $48 = 2^4 \cdot 3$ . Luego, los divisores positivos de 48 son 1, 2, 4, 8, 16, 3, 6, 12, 24 y 48.

$(3n^3 - 11n)/(n + 3)$  es entero si y solo si  $3n^3 - 11n$  es múltiplo entero de  $n + 3$ . (iv)

Por la parte 1 se tiene que  $3n^3 - 11n + 48$  es siempre múltiplo entero de  $n + 3$ . Entonces restando esta condición y la (iv) deducimos que

$(3n^3 - 11n)/(n + 3)$  es entero si y solo si 48 es múltiplo de  $(n + 3)$ , o lo que es equivalente,  $n + 3$  es divisor de 48 (v).

Por otro lado, sabiendo que  $n$  es natural, se tiene que  $(3n^3 - 11n)/(n + 3)$  es no negativo. Por lo tanto, cuando es entero, es natural.

De (v) deducimos que los valores naturales de  $n$  buscados son aquellos que sumados a 3 dan como resultado alguno de los divisores positivos de 48, o sea  $n = 1, 5, 13, 0, 3, 9, 21$  y 45.

**Ejercicio 2.**

(1) El producto de clases de congruencia  $\text{mod}12$  se define como la clase de congruencia  $[n][m] = [nm]$ . Esta operación es cerrada en  $U_{12}$  pues si  $\text{mcd}(n, 12) = 1$  y  $\text{mcd}(m, 12) = 1$  entonces  $\text{mcd}(nm, 12) = 1$ . Luego el resto  $r$  de dividir  $nm$  entre 12 también cumple  $\text{mcd}(r, 12) = 1$ , de donde  $[nm] = [r] \in U_{12}$ .

La propiedad asociativa se cumple porque el producto de clases de congruencia en  $Z_{12}$  es asociativo (enunciado en el teórico). Luego lo es en particular restringido al subconjunto  $U_{12}$ .

El neutro  $[1] \text{ mod}12$  del producto en  $Z_{12}$  pertenece a  $U_{12}$  porque  $\text{mcd}(1, 12) = 1$ .

Finalmente resta probar que todo  $[n] \in Z_{12}$  tiene un inverso en  $Z_{12}$ . Sea  $n$  tal que  $\text{mcd}(n, 12) = 1$ . Por la propiedad de combinación lineal del máximo común divisor, se tiene que existen  $a$  y  $b$  enteros tales que  $na + 12b = 1$ . Entonces también se cumple  $\text{mcd}(a, 12) = 1$  y  $[a] \in U_{12}$ . Además  $[na + 12b] = [1] \text{ mod}12$ , luego  $[n][a] + [12][b] = [1] \text{ mod}12$ . En  $Z_{12} : [12][b] = [0][b] = [0]$  y  $[n][a] + [0] = [n][a]$ . Luego obtuvimos  $[a] \in U_{12}$  tal que  $[n][a] = [1]$ , o sea existe inverso de  $[n]$  en  $U_{12}$  como queríamos demostrar.

(2)

$$U_{12} = \{[1], [5], [7], [11]\} \subset Z_{12}$$

Para construir la tabla de operación efectuamos los productos entre dos elementos cualesquiera de  $U_{12}$ . Si uno de los factores es  $[1]$ , el resultado es el otro factor. Con eso completamos la primera fila y la primera columna de la tabla (A) que está más abajo. Además el producto es conmutativo, así que llenando los espacios de la tabla en la diagonal principal y por encima de ella, se completa por simetría abajo de la diagonal. Operando con el producto de las clases de congruencia módulo 12, se tiene:

$$[5][5] = [25] = [1], \quad [5][7] = [35] = [11], \quad [5][11] = [55] = [7],$$

$$[7][7] = [49] = [1], \quad [7][11] = [77] = [5], \quad [11][11] = [121] = [1]$$

Luego la tabla es:

$(U_{12}, \cdot)$		[1]	[5]	[7]	[11]
(A)	[1]	[1]	[5]	[7]	[11]
	[5]	[5]	[1]	[11]	[7]
	[7]	[7]	[11]	[1]	[5]
	[11]	[11]	[7]	[5]	[1]

(3) Sea  $G = \{e, a, b, c\}$  un grupo, con cuatro elementos (o sea todos diferentes entre sí), donde  $e$  es el neutro y tal que  $a^2 = e$ ,  $b^2 = e$ ,  $c^2 = e$ . Construyamos la tabla de operación del grupo. Como  $e$  es el neutro  $ex = xe = x$  para todo  $x \in G$ . Con ello se completa la primera fila y la primera columna de la tabla (B) que está más abajo. Ahora completemos la segunda fila:  $aa = e$  por hipótesis.  $ab \neq a$  porque de lo contrario, por la propiedad cancelativa, tendríamos  $b = e$  lo que es absurdo.  $ab \neq e$  porque de lo contrario tendríamos  $ab = aa$  y por la propiedad cancelativa, deduciríamos  $b = a$  lo que es absurdo. Finalmente  $ab \neq b$  porque de lo contrario por la propiedad cancelativa tendríamos  $a = e$  lo que es absurdo. Por lo tanto la única posibilidad que resta es  $ab = c$ . Análogamente obtenemos

$$ac = b, \quad ba = c, \quad bc = a, \quad ca = b, \quad cb = a$$

lo que permite completar la siguiente tabla:

	$(G, \cdot)$	$e$	$a$	$b$	$c$
	$e$	$e$	$a$	$b$	$c$
(B)	$a$	$a$	$e$	$c$	$b$
	$b$	$b$	$c$	$e$	$a$
	$c$	$c$	$b$	$a$	$e$

Sea  $\varphi : U_{12} \mapsto G$  la aplicación biunívoca tal que

$$\varphi([1]) = e, \quad \varphi([5]) = a, \quad \varphi([7]) = b, \quad \varphi([11]) = c$$

Se observa, comparando las tablas (A) y (B) que al elemento de  $U_{12}$  que está en la fila  $[i]$ , columna  $[j]$  de la tabla (A) (es decir al elemento  $[i] \cdot [j] \in U_{12}$ ) le corresponde por  $\varphi$  el elemento de  $G$  en la tabla (B) que está en la fila  $\varphi([i])$ , columna  $\varphi([j])$ , (es decir el elemento  $\varphi([i]) \cdot \varphi([j])$ ). Por lo tanto

$$\varphi([i] \cdot [j]) = \varphi([i]) \cdot \varphi([j])$$

concluyendo que  $\varphi$  es un homomorfismo de grupos. Como además  $\varphi$  es biyectivo por construcción, se tiene que es un isomorfismo. Luego  $U_{12}$  y  $G$  son grupos isomorfos como queríamos demostrar.

### Ejercicio 3

(1) Sea  $\varphi : G \mapsto G$  definida por  $\varphi(g) = g^m$  para todo  $g \in G$ .

Sabiendo que  $G$  es abeliando se tiene  $(g_1 g_2)^m = g_1^m g_2^m$ . Luego:

$$\varphi(g_1 g_2) = (g_1 g_2)^m = g_1^m g_2^m = \varphi(g_1) \varphi(g_2)$$

lo que prueba que  $\varphi$  es un homomorfismo del grupo  $G$  en sí mismo. Ahora probemos que es inyectivo y sobreyectivo.

$\text{Ker} \varphi = \{g \in G : g^m = e\}$ . Si un elemento  $g \in G$  cumple  $g^m = e$  entonces  $m$  es múltiplo del orden de  $g$ . Pero por el teorema de Lagrange el orden de  $g$  divide a  $|G| = n$ . Entonces el orden de  $g$  es un divisor común de  $n$  y de  $m$ . Por hipótesis  $\text{mcd}(n, m) = 1$ , de donde se deduce que el orden de  $g$  es 1. Entonces  $g = e$ . Hemos probado que todo elemento  $g$  del núcleo de  $\varphi$  es igual a  $e$ . Entonces  $\text{Ker} \varphi = \{e\}$  y por el teorema visto en el teórico  $\varphi$  es inyectiva.

Ahora probemos que  $\varphi$  es sobreyectiva, o sea demosremos que el grupo  $G'$  imagen de  $G$  por  $\varphi$  coincide con todo  $G$ . Sabemos que  $G'$  está contenido en  $G$ . Por el primer teorema de los homomorfismos  $G/\text{Ker} \varphi$  es isomorfo a  $G'$ . Entonces tienen la misma cantidad de elementos:

$$|G'| = \left| \frac{G}{\text{Ker} \varphi} \right| = \frac{|G|}{|\text{Ker} \varphi|} = \frac{|G|}{1} = |G|$$

Luego  $G'$  es un subconjunto de  $G$  que tiene la misma cantidad (finita  $n$ ) de elementos que  $G$ . Entonces  $G' = G$  y  $\varphi$  es sobreyectivo.

Como  $\varphi$  es un homomorfismo biyectivo, es un isomorfismo como queríamos demostrar.

(2) Por la parte anterior tenemos que  $\varphi : G \mapsto G$  definida por  $\varphi(g) = g^m$  es biyectiva. Entonces es invertible, es decir, para todo  $a \in G$  existe (y es único) un  $g \in G$  tal que  $g^m = a$ . Esto prueba que para todo  $a \in G$  existe (y es única) una solución  $x = g$  de la ecuación  $x^m = a$  como queríamos probar.

#### Ejercicio 4.

(1) Si  $f$  y  $g$  pertenecen a  $N_1$  entonces  $f(1) = 0$ ,  $g(1) = 0$ . Luego  $(f + g)(1) = f(1) + g(1) = 0 + 0 = 0$  y se cumple que  $f + g \in N_1$ . Además  $-f(1) = -0 = 0$  y se cumple  $-f \in N_1$ . Lo anterior prueba que  $(N_1, +)$  es un subgrupo de  $(A, +)$ . Ahora probemos que para toda  $f \in N_1$  y para toda  $h \in A$  el producto  $hf \in N_1$ . Como el producto es funciones es conmutativo esto implica también  $fh \in N_1$ . Si  $f \in N_1$  entonces  $f(1) = 0$ , luego  $(hf)(1) = h(1)f(1) = h(1)0 = 0$ , de donde  $hf \in N_1$ , terminando de probar que  $N_1$  es un ideal de  $A$ .

Si  $f$  y  $g$  pertenecen a  $N_2$  entonces  $f(1) = f(2) = 0$ ,  $g(1) = g(2) = 0$ . Luego  $(f + g)(1) = f(1) + g(1) = 0 + 0 = 0$  y  $(f + g)(2) = f(2) + g(2) = 0 + 0 = 0$ . Por lo tanto  $f + g \in N_2$ . Además  $-f(1) = -0 = 0$  y  $-f(2) = -0 = 0$ . Entonces se cumple  $-f \in N_2$ . Lo anterior prueba que  $(N_2, +)$  es un subgrupo de  $(A, +)$ . Ahora probemos que para toda  $f \in N_2$  y para toda  $h \in A$  el producto  $hf \in N_2$ . Como el producto es funciones es conmutativo esto implica también  $fh \in N_2$ . Si  $f \in N_2$  entonces  $f(1) = f(2) = 0$ , luego  $(hf)(1) = h(1)f(1) = h(1)0 = 0$  y  $(hf)(2) = h(2)f(2) = h(2)0 = 0$ , de donde  $hf \in N_2$ , terminando de probar que  $N_2$  es un ideal de  $A$ .

(2) Sea  $\Phi : A \mapsto \mathbb{R}$  definida por  $\Phi(f) = f(1)$ . Se cumple:

$$\Phi(f + g) = (f + g)(1) = f(1) + g(1) = \Phi(f) + \Phi(g)$$

$$\Phi(fg) = (fg)(1) = f(1)g(1) = \Phi(f)\Phi(g)$$

Luego  $\Phi$  es un homomorfismo de anillos.

Además  $\Phi$  es sobreyectiva pues dado  $a \in \mathbb{R}$  sea la función  $f = a$  constante. Se cumple  $\Phi(f) = f(1) = a$ . Todo número real  $a$  es imagen por  $\Phi$  de alguna función  $f \in A$ .

Hallemos el núcleo de  $\Phi$ :  $\text{Ker}\Phi = \{f \in A : f(1) = 0\} = N_1$ . Por el primer teorema de los homomorfismos de anillos  $A/\text{Ker}\Phi = A/N_1$  es isomorfo a  $\mathbb{R}$  como queríamos demostrar.

(3)  $N_1$  es un ideal maximal porque el anillo cociente  $A/N_1$  es un cuerpo, ya que por la parte anterior es isomorfo al cuerpo de los reales. Se aplica el siguiente teorema visto en el teórico:

(\*) Un ideal  $N$  de un anillo  $A$  es maximal si y solo si el anillo cociente  $A/N$  es un cuerpo.

(4)  $N_2$  es un ideal de  $N_1$  porque  $N_2 \subset N_1 \subset A$ ,  $N_2$  es un ideal de  $A$  y  $N_1$  es un subanillo de  $A$  (por ser un ideal).

Sea  $\phi : N_1 \mapsto \mathbb{R}$  la aplicación  $\phi(f) = f(2)$ . Análogamente a lo demostrado en la parte 2,  $\phi$  es un homomorfismo de anillos. Es sobreyectivo porque dado  $a \in \mathbb{R}$  la función  $f(x) = a(x-1)$  cumple  $f(1) = 0, f(2) = a$ , entonces, para todo  $a \in \mathbb{R}$  existe alguna función  $f \in N_1$  tal que  $\phi(f) = a$ . Hallemos el núcleo de  $\phi$ :  $\text{Ker}\phi = \{f \in N_1 : f(2) = 0\} = \{f \in A : f(1) = 0, f(2) = 0\} = N_2$ . Por el primer teorema de los homomorfismos de anillos se tiene  $N_1/\text{Ker}\phi = N_1/N_2$  es isomorfo a  $\mathbb{R}$ . Como  $\mathbb{R}$  es un cuerpo, por el teorema (\*) enunciado en la parte 3) se cumple que  $N_2$  es un ideal maximal de  $N_1$  como queríamos demostrar.

Por otra parte  $N_2$  no es un ideal maximal de  $A$  porque existe el ideal  $N_1$  tal que  $N_2 \subset N_1 \subset A$  y  $N_1$  no es ni  $A$  ni  $N_2$ . (En efecto la función  $f(x) = (x-1)$  está en  $N_1$  y no está en  $N_2$ , lo que prueba que  $N_1$  no es  $N_2$ ; y la función  $g(x) = 5$  constante está en  $A$  y no está en  $N_1$ , lo que prueba que  $N_1$  no es  $A$ ).