Primer examen de Matemática Discreta 2 Curso 2006 21/7/06

Ejercicio 1

1) Se tiene : N ≡ 317 (1000) ; N ≡ 1 (49) ; N + 1 ≡ 0 (3)
N + 1 ≡ 0 (3) ⇒ N ≡ -1 (3) ⇒ N ≡ 2 (3)
Queda el sistema de congruencias : N ≡ 317 (1000)
N ≡ 1 (49)
N ≡ 2 (3)
Como 1000, 49 y 3 son primos entre sí dos a dos por el Teorema Chino del Resto el sistema tiene solución.

2) $M_1 = 3*49 = 147; \quad M_2 = 3*1000 = 3000; \quad M_3 = 49*1000 = 49000$
1000 = 147*6 + 118 ; 147 = 118 – 29 ; 118 = 29*4 + 2 ; 29 = 2*14 + 1
1 = 29 – 2*14 = 29 – 14(118 – 29*4) = 57*29 – 14*118 = 57(147 – 118) – 14*118 =
57*147 – 71*118 = 57*147 – 71(1000 – 147*6) = 483*147 – 71*1000
Entonces 483*147 ≡ 1 (1000)
3000 = 49*61 + 11 ; 49 = 11*4 + 5 ; 11 = 5*2 + 1
1 = 11 – 5*2 = 11 – 2(49 – 4*11) = 9*11 – 2*49 = 9(3000 – 49*61) – 2*49 =
9*3000 – 551*49
Entonces 9*3000 ≡ 1 (49)
49000 = 3*16333 +1
1 = 49000 – 3*16333
Entonces 49000 ≡ 1 (3)
Por lo tanto N ≡ 317*483*147 + 1*9*3000 + 2*49000 (147000)
N ≡ 22632317 (147000) ⇒ N ≡ 141317 (147000)
128317 + 5*147000 = 876317
Las 6 soluciones son 141317 + k*147000 con 0 ≤ k ≤ 5

3) Si n = 3k ⇒ n^2 es $\dot{3}$
Si n = 3k + 1 ⇒ $n^2 = (3k+1)^2 = 9k^2 + 6k + 1 = \dot{3} + 1$
Si n = 3k + 2 ⇒ $n^2 = (3k+2)^2 = 9k^2 + 12k + 4 = \dot{3} + 1$
Como N es múltiplo de 3 +2 ⇒ N no puede ser cuadrado perfecto.

Ejercicio 2

1) Si I es regular entonces en A/I existe I+y/ (I+a)(I+y) = I+a = (I+y)(I+a)
⇒ I + ay = I + a = I + uy ⇒ a – ay ∈ I ; a – ya ∈ I
Si a – ay ∈ I ⇒ a ∈ I + ay ⇒ I + a = I + ay = (I + a)(I + y)
Si a – ya ∈ I ⇒ a ∈ I + ya ⇒ I + a = I + ya = (I + y)(I + a)
Por lo anterior I + y es el elemento unidad de A / I

2) Si A tiene elemento unidad u y I es un ideal de A entonces I + u es el elemento unidad de A / I ya que: (I + a)(I + y) = I + ay = I + a
(I + y)(I + a) = I + ya = I + a

3) $(r_1,0) + (r_2,0) = (r_1 + r_2,0) \in$ (R,0) ; - (r,0) = (-r,0) ∈ (R,0)
(r,0).(x,y) = (rx + 0.x + ry , 0.y) = (rx + ry , 0) ∈ (R,0)
(x,y).(r,0) = (x.r + y.r + x.0 , y.0) = (xr + yr , 0) ∈ (R,0)
Por lo anterior R x {0} es ideal de R^2
Para ver que R x {0} es regular veamos que R^2 tiene elemento unidad:
(x,y).(u,v) = (x,y) ⇒ (xu + yu + xv , yv) = (x,y) $\forall$ x, y ∈ R

yv = y $\Rightarrow$ v = 1 ; xu +yu + xv = x $\Rightarrow$ (x + y)u = 0 $\Rightarrow$ u = 0
(0,1).(x,y) = (0.x + 1.x + 0.y , 1.y) = (x,y)
Por lo anterior (0,1) es el elemento unidad de R^2
Sea $f : R \times \{0\} \to R / f((r,0)) = r$
f es biyectiva.

$$f((r_1,0)+(r_2,0)) = f((r_1+r_2,0)) = r_1+r_2 = f((r_1,0))+f((r_2,0))$$

$$f((r_1,0).(r_2,0)) = f((r_1r_2+0.r_2+r_1.0,0.0)) = f((r_1r_2,0)) = r_1r_2 = f((r_1,0)).f((r_2,0))$$

Por las dos igualdades anteriores tenemos que *f* es homomorfismo. Como es biyectivo es isomorfismo, con lo cual R x {0} es isomorfo a R.

Ejercicio 3

1) $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 3 & 6 & 9 & 2 & 5 & 8 & 1 & 4 & 7 \end{pmatrix} = (1\,3\,9\,7)(2\,6\,8\,4)$

$\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 7 & 4 & 1 & 8 & 5 & 2 & 9 & 6 & 3 \end{pmatrix} = (1\,7\,9\,3)(2\,4\,8\,6)$

Orden de σ = mcm(4,4) = 4 Paridad de σ = impar por impar = par
Orden de τ = mcm(4,4) = 4 Paridad de τ = impar por impar = par

2) σ y τ son conjugadas porque su descomposición en ciclos disjuntos es de la misma forma: producto de 2 4-ciclos.

$\gamma\tau\gamma^{-1} = \gamma(1\,7\,9\,3)(2\,4\,8\,6)\gamma^{-1} = \gamma(1\,7\,9\,3)\gamma^{-1}\gamma(2\,4\,8\,6)\gamma^{-1} = (\gamma(1)\,\gamma(7)\,\gamma(9)\,\gamma(3))\,(\gamma(2)\,\gamma(4)\,\gamma(8)\,\gamma(6))$
= σ = (1 3 9 7)(2 6 8 4) = (2 6 8 4)(1 3 9 7)
Una permutación γ posible es aquella tal que :
$\gamma(1)=1; \gamma(7)=3; \gamma(9)=9; \gamma(3)=7; \gamma(2)=2; \gamma(4)=6; \gamma(8)=8; \gamma(6)=4; \gamma(5)=5$
Otra permutación γ posible es aquella tal que :
$\gamma(1)=2; \gamma(7)=6; \gamma(9)=8; \gamma(3)=4; \gamma(2)=1; \gamma(4)=3; \gamma(8)=9; \gamma(6)=7; \gamma(5)=5$

Ejercicio 4

1) $(Z_3,+,.)$ es un cuerpo
Si P(x) de $Z_3[x]$ tiene una raíz α, entonces es divisible por $(x-\alpha) \Rightarrow P(x) = (x-\alpha)Q(x)$
donde Q(x) $\in Z_3[x]$. Por lo tanto P(x) es reducible.
Si P(x) de $Z_3[x]$ tiene grado 2 o 3 y es reducible $\Rightarrow P(x) = (ax+b)Q(x) \Rightarrow x = -ba^{-1}$ es raíz
2) c = 0 P(x) = x^2+1 $\Rightarrow$ P(0) = 1 ; P(1) = 2 ; P(2) = 2 $\Rightarrow$ es irreducible
c = 1 P(x) = x^2+x+1 $\Rightarrow$ P(0) = 1 ; P(1) = 0 $\Rightarrow$ es reducible
c = 2 P(x) = $x^2+2x+1 = (x+1)^2$ $\Rightarrow$ es reducible
3) Sea J ideal de $Z_3[x]$ tal que <P(x)> $\subset J$
Se tiene que existe Q(x) / J = <Q(x)> (alcanza con tomar Q(x) un polinomio de grado mínimo de J) Si grado de Q(x) = 0 entonces J = $Z_3[x]$
En caso contario, como P(x) $\in J = \langle Q(x) \rangle \Rightarrow P(x) = Q(x)H(x)$
Como P(x) es irreducible $\Rightarrow$ H(x) es de grado 0, o sea una constante no nula.
Pero entonces <P(x)> = <Q(x)> = J
4) P(x) = x^2+1 es irreducible en $Z_3[x]$ $\Rightarrow$ <P(x)> es ideal maximal de $Z_3[x]$
Como $Z_3[x]$ es anillo conmutativo, con elemento unidad se tiene que $Z_3[x]$ / <P(x)> es un cuerpo.

[P(x)] = [0]

$$[x^4 + x^2 + 2x + 1] = [x^2(x^2 + 1) + 2x + 1] = [x^2(x^2 + 1)] + [2x + 1] = [2x + 1]$$