Apellidos y nombre

AMPLIACIÓN DE MATEMÁTICAS
TRABAJO PRÁCTICO 10: Homomorfismos y teorema chino del resto

Se dice que $\alpha \in \mathbb{K}$ es una raíz de f de **multiplicidad** r si $(x-\alpha)^r | f$ y $(x-\alpha)^{r+1} \not| f$. Una **raíz múltiple** es una raíz cuya multiplicidad es 2 o más. Halla las raíces múltiples de $3x^4 + x^2 + 3$ en $\mathbb{C}$ y en $\mathbb{Z}_5$.

$3x^4+x^2+3=0 \Leftrightarrow x^2 = \frac{-1 \pm \sqrt{1^2-36}}{6} = \frac{-1}{6} \pm \frac{\sqrt{-35}}{6}$

$\Rightarrow$ No raíces múltiples en $\mathbb{C}$

$3x^4+x^2+3 = 3\underbrace{(x+3)^2}_{\hookrightarrow 2}\underbrace{(x+2)^2}_{\to 3} \Rightarrow$ las raíces dobles son: 2 y 3

Estando en Estados Unidos el Sr. Herrera se quedó sin dinero en efectivo y fue al banco a cambiar un cheque de viaje. El cajero al pagarle confundió el número de dólares con el número de centavos y viceversa. Sin darse cuenta de este hecho el Sr. Herrera gastó 68 centavos en sellos, y entonces vio para su sorpresa que la contidad de dinero en efectivo que tenía era exactamente el doble del valor del cheque de viaje que había cambiado. Determina el valor mínimo que podría tener dicho cheque.

$68 \cdot 67 = 476 + 408 = 45{,}56$

$68 \cdot 33 = 204 + 204 = 2244$

x = número de dólares del cheque

y = " " centavos " "

Valor del cheque $= 100x + y$ centavos

El cajero da: $100y + x$ "

$100y + \cancel{x} - 68 = 2(100x+y)$

199		1	0
98		0	1
3	2	1	-2
2	32	-32	65
1	1	33	-67

$\Rightarrow 199x - 98y = -68$

$1 = 199 \cdot 33 - 98 \cdot 67$

$\Rightarrow x = -33 \cdot 68 + 98k > 0 \quad k > \frac{2244}{98} = 22'89$

$\Leftrightarrow y = -67 \cdot 68 + 199k > 0 \quad k > \frac{4556}{199} = 22'89$

Si $k = 23 \Rightarrow x = 10 \quad y = 21$

Estudiar si hay isomorfismos entre los siguientes anillos:

$$\mathbb{Z}_2 \times \mathbb{Z}_2, \quad \mathbb{Z}_4, \quad \mathbb{Z}_2[x]/(x^2+x+1), \quad \mathbb{Z}_2[x]/(x^3+x+1), \quad \mathbb{Z}_2[x]/(x^3+x^2+1), \quad \mathbb{Z}_2[x]/(x^2),$$

justificando la respuesta en cada caso.

$1_{\mathbb{Z}_2\times\mathbb{Z}_2} + 1_{\mathbb{Z}_2\times\mathbb{Z}_2} = 0_{\mathbb{Z}_2\times\mathbb{Z}_2} \Rightarrow \mathbb{Z}_2\times\mathbb{Z}_2 \not\cong \mathbb{Z}_4$

$\mathbb{Z}_2\times\mathbb{Z}_2$; $\mathbb{Z}_4$ no cuerpos $\Rightarrow$

279
39
2511
837
10881

El **Teorema Chino de los Restos** dice que, si tenemos un sistema de congruencias $x \equiv a_i (\text{mód } m_i)$, hay solucin cuando los $(m_i, m_j) = 1$ para todo $i \neq j$, y dicha solución es única módulo $\prod_i m_i$. Vamos a resolver un sistema de congruencias:

$$\left.\begin{array}{rcl} x & \equiv & 2 \quad (\text{mód } 4) \\ x & \equiv & 3 \quad (\text{mód } 5) \end{array}\right\}$$

Para ello, calcula los coeficientes de la identidad de Bezout $4u + 5v = 1 = (4, 5)$. Nótese que u es el inverso de 4 en $\mathbb{Z}_5$ y v el inverso de 5 en $\mathbb{Z}_4$ (si prefieres, puedes trabajar con los representantes positivos de la clase de equivalencia).

$u = -1 \, , \, v = 1$

Considera el número $\alpha = 3 * u * 4 + 2 * v * 5$ y comprueba que es solución. Por tanto, Toda solución es de tipo $\alpha + 20k$, $k \in \mathbb{Z}$.

$\equiv 2 \text{ mód } 4$

$\alpha = 3 \cdot (-1) \cdot 4 + 2 \cdot 1 \cdot 5 = -2$

$\equiv 3 \text{ mód } 5$

En general, si tenemos $x \equiv a (\text{mód } m)$ y $x \equiv b (\text{mód } n)$, con $(m, n) = 1 = um + vn$, las soluciones son de tipo $umb + vna + mnk$, con $k \in \mathbb{Z}$. Acumula esto para resolver:

$$\left.\begin{array}{rcl} 3x & \equiv & 2 \quad (\text{mód } 7) \\ x & \equiv & 1 \quad (\text{mód } 10) \\ 2x & \equiv & 1 \quad (\text{mód } 9) \end{array}\right\} \to \left.\begin{array}{l} x \equiv 3 \text{ mód } 7 \\ x \equiv 1 \text{ mód } 10 \\ x \equiv 5 \text{ mód } 9 \end{array}\right\}$$

$1 = 7 \cdot 3 + 10 \cdot (-2) \Rightarrow \alpha = 7 \cdot 3 \cdot 1 + 10 \cdot (-2) \cdot 3 = 21 - 60 =$
$= -39$

$\Rightarrow x \equiv -39 \text{ mód } 70$
$x \equiv 5 \text{ mód } 9$

70		1	0
9		0	1
7	7	1	-7
2	1	-1	8
1	3	4	-31

$1 = 4 \cdot 70 - 31 \cdot 9$

$\beta = 4 \cdot 70 \cdot 5 - 31 \cdot 9 \cdot (-39) = 1400 + 10881 = 12281$
$\equiv -319 \text{ mod } 630 \equiv \underline{311} \text{ mód } 630$

¿Te atreves a hacerlo con polinomios? $\left.\begin{array}{rcl} P(x) & \equiv & x \quad (\text{mód } x^2 + x) \\ P(x) & \equiv & 1 \quad (\text{mód } x^2 + 1) \end{array}\right\}$ (En $\mathbb{Z}_3[x]$)

x^2+x		1	0
x^2+1		0	1
$x+2$	1	1	2
2	$x+1$	$2x+2$	$x+2$

$2 = (2x+2)(x^2+x) + (x+2)(x^2+1) \Rightarrow$

$\Rightarrow 1 = (x+1)(x^2+x) + (2x+1)(x^2+1) \Rightarrow$

$\Rightarrow \alpha = (x+1)(x^2+x) \cdot 1 + (2x+1)(x^2+1) \cdot x$