ADADAH

Apellidos y nombre

AMPLIACIÓN DE MATEMÁTICAS 2019-2020
TRABAJO PRÁCTICO 9: Homomorfismos y Teorema Chino de los Restos

Se dice que $\alpha \in \mathbb{K}$ es una raíz de f con **multiplicidad** r si $(x-\alpha)^r | f$ y $(x-\alpha)^{r+1} \nmid f$. Una **raíz múltiple** es aquella cuya multiplicidad es 2 ó más. Halla las raíces múltiples del polinomio

$$f(x) = 9x^4 + x^2 + 9$$

en $\mathbb{C}$ y $\mathbb{Z}_{17}$.

$= 9(x^4+2x^2+1) = 9(x^2+1)^2 =$ ⊛ en $\mathbb{Z}_{17}$

En $\mathbb{C}$: Hacemos el cambio $t = x^2$ y usamos la fórmula

$$t = x^2 = \frac{-1 \pm \sqrt{1^2 - 4(9)(9)}}{2\cdot 9} = \frac{-1}{18} \pm i\,\frac{\sqrt{323}}{18}$$

} no puede haber raíces múltiples

$= 9(x+4)^2(x-4)^2 =$

⊛ $= (x-4)^2(x-13)^2 \rightsquigarrow$ raíces dobles: **4, 13**

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 49 centavos en sellos, y entonces, para su sorpresa, vio que la cantidad de dinero en efectivo que tenía era el doble al valor del cheque de viaje que había cambiado. Determina el valor mínimo que podría tener dicho cheque.

x = número de dólares del cheque { valor del cheque: $100x+y$ centavos
y = número de centavos del cheque { lo que da el cajero: $100y+x$ centavos

$\rightsquigarrow 100y + x - 49 = 2(100x+y) \iff 199x - 98y = -49$ ecuación Diofántica

$\mathrm{mcd}(199,-98) = 1 \mid 49 \rightsquigarrow$ tiene sol.

$1 = 199\cdot 33 + (-98)\cdot 67 \Rightarrow \begin{cases} x = -1617 + 98\lambda \\ y = -3283 + 199\lambda \end{cases} \lambda \in \mathbb{Z}$ $\rightsquigarrow$ valor mínimo $\begin{cases} x = 49 \\ y = 100 \end{cases}$ N = 5

Estudiar (justificando) si son isomorfos los siguientes pares de anillos:

(i) $\frac{\mathbb{R}[x]}{(x^2+1)}$ y $\frac{\mathbb{R}[x]}{(x^2-1)}$. **No** pueden ser isomorfos porque el primero es cuerpo y el segundo no es si quiera DI.

(ii) $\mathbb{Z}_9$ y $\frac{\mathbb{Z}_3[x]}{(x^2+1)}$. **No** pueden ser isomorfos porque el primero no es DI, mientras que el otro es cuerpo (pese a tener mismo cardinal)

(iii) $\frac{\mathbb{Z}_2[x]}{(x^3+x+1)}$ y $\frac{\mathbb{Z}_2[x]}{(x^3+x^2+1)}$. **SI** que son isomorfos porque son cuerpos ambos de mismo cardinal $2^3 = 8$. El isomorfismo es

$$\{\varphi(ax^2+bx+c) = a\varphi(x)^2 + b\varphi(x) + c$$

donde $\varphi(x)$ se determina obligando a este a que esté bien definido. Para ello

$$\{\varphi(x)^3 + \varphi(x) + 1 = 0\};$$

pero $x^3+x^2+1 = 0 \Rightarrow 1 + x^{-1} + (x^{-1})^3 = 0$ (mult. por $(x^{-1})^3$ i.e.) basta tomar

$$\boxed{\varphi(x) = x^{-1} = x^2 + x}$$ alg. Euclides.

(iv) $\mathbb{Z}_4[x]$ y $\mathbb{Z}_2[x]$.

No pueden ser isomorfos porque $\mathbb{Z}_2$ es cuerpo, y por tanto $\mathbb{Z}_2[x]$ es DI, mientras que $\mathbb{Z}_4[x]$ no es si quiera DI por no serlo $\mathbb{Z}_4$ ($[2]_4 \cdot [2]_4 = [0]_4$, con $[2]_4 \neq 0$ y $[2]_4 \neq 0$).

El **Teorema Chino de los Restos** dice que, si tenemos un sistema de n congruencias del tipo

$$x \equiv a_i (\text{mód } m_i),$$

este **tiene solución** cuando $\text{mcd}(m_i, m_j) = 1$ para todo $i \neq j$ con $i, j \in \{1, \ldots, n\}$ dados, y dicha solución es única módulo $m_1 \cdots m_n$. Vamos a resolver un sistema de congruencias:

$$\begin{cases} x & \equiv & 2 \text{ (mód 7)}; \\ x & \equiv & 8 \text{ (mód 15)}. \end{cases}$$

Para ello, calcula los coeficientes para la identidad de Bezout $7u + 15v = 1$. Nótese que u es el inverso de 7 en $\mathbb{Z}_{15}$ claramente, mientras que v es el inverso de 15 en $\mathbb{Z}_7$.

$u = 13$; $v = 1$

Considera el número $\alpha = 8 \cdot u \cdot 7 + 2 \cdot v \cdot 15$. Comprueba que este es solución del sistema dado. En definitiva, tenemos que toda solución de este sistema es del tipo $\alpha + (7 \cdot 35)\, k = \alpha + 105k$ con $k \in \mathbb{Z}$ arbitrario y $\alpha \in \mathbb{Z}$ por determinar.

$\alpha = 8 \cdot 13 \cdot 7 + 2 \cdot 1 \cdot 15 \equiv \underline{23 \text{ (mod. } 105)}$

En general, si tenemos $x \equiv a (\text{mód } m)$ y $x \equiv b (\text{mód } n)$ dos congruencia, con $1 = um + vn$ identidad de Bezout, se tiene que las soluciones de esta son del tipo $umb + vna + mnk$ con $k \in \mathbb{Z}$ arbitrario.

Acumula esto para resolver:

$$\begin{cases} x & \equiv & 1 \text{ (mód 11)}; \\ x & \equiv & 12 \text{ (mód 24)}; \\ x & \equiv & 3 \text{ (mód 25)}. \end{cases}$$

Por el Teorema Chino de los Restos, hay que resolver

$600u \equiv 1 \text{ (mód. } 11)$; $275v \equiv 1 \text{ (mód. } 24)$; $264w \equiv 1 \text{ (mod. } 25)$

$\hookrightarrow u = 2$ $\hookrightarrow v = 11$ $\hookrightarrow w = 9$

$\alpha = 600 \cdot 2 \cdot 1 + 275 \cdot 11 \cdot 12 + 264 \cdot 9 \cdot 3 \equiv \underline{5028 \text{ (mod. } 6600)}$

Por el Teorema Chino de los Restos, como x^2+x y x^2+1 son coprimos, hay que resolver

$(x^2+x)\,u(x) \equiv 1 \text{ (mód. } x^2+1)$; $(x^2+1)\,v(x) \equiv 1 \text{ (mód } x^2+x)$

¿Te atreves a hacerlo con polinomios? $\begin{cases} f(x) & \equiv & x & (\text{mód } x^2+x); \\ f(x) & \equiv & 1 & (\text{mód } x^2+1), \end{cases}$ (en $\mathbb{Z}_3[x]$).

$u(x) = x+1$ $\qquad$ $v(x) = 2x+1$

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

$\equiv \underline{2x^2 \text{ (mód. } x^4+x^3+x^2+x)}$