Recuperatorio segundo parcial

July 20, 2021

Contents

1 Ejercicio 1

Ejercicio 1:
Hallar todas las soluciones $(a, b) \in \mathbb{Z} \times \mathbb{Z}$ de la ecuación

$$110\,a + 250\,b = 100$$

que satisfacen simultáneamente $37^2 | (a-b)^{2021}$.

Solución: La condición $37^2 \mid (a-b)^{2021}$ parece complicada, pero en realidad se puede llevar a una condición equivalente mucho mas sencilla. Veamos que en realidad $37^2 \mid (a-b)^{2021}$ es equivalente a $37 \mid a-b$, veamoslo!

Mini observación: $37^2 \mid (a-b)^{2021}$ si y solamente si $37 \mid a-b$.

Demostración $\Rightarrow$) Como $37^2 \mid (a-b)^{2021}$ en particular tenemos que $37 \mid (a-b)^{2021}$. **Como** 37 **es primo** resulta que $37 \mid a-b$ como queríamos.
$\Leftarrow$) Si $37 \mid a-b$, entonces $37^{2021} \mid (a-b)^{2021}$. Como $37^2 \mid 37^{2021}$ y $37^{2021} \mid (a-b)^{2021}$, por la transitividad de la divisibilidad tenemos que $37^2 \mid (a-b)^{2021}$.

□

Es decir $37^2 \mid (a-b)^{2021} \Leftrightarrow 37 \mid (a-b)$. Con lo cual en realidad el ejercicio se traduce en encontrar los pares $(a, b) \in \mathbb{Z} \times \mathbb{Z}$ tales que cumplen

$$110a + 250b = 100 \quad \text{y} \quad 37 \mid a - b.$$

Tenemos la ecuación $110a + 250b = 100$ y para que sea compatible, es necesario que $(110 : 250) \mid 100$. Como $(110 : 250) = 10$, y $10 \mid 100$ es compatible y la ecuación original es equivalente a la ecuación coprimizada

$$11a + 25b = 10.$$

Hallemos las soluciones. Una solución particular es $(10, -4)$ y por lo tanto, por lo visto en clase, todas las soluciones son

$$(a, b) = (10 + 25k, -4 - 11k) \text{ con } k \in \mathbb{Z}$$

Ahora bien, según lo que hicimos tenemos que $a - b = 10 + 25k - (-4 - 11k) = 14 + 36k$. De esta manera la segunda condición se cumple si y solo si $37 \mid 14 + 36k$, o lo que es lo mismo, $36k \equiv -14 \pmod{37}$.

Pero $36k \equiv -14 \pmod{37} \Leftrightarrow -k \equiv -14 \pmod{37} \Leftrightarrow k \equiv 14 \pmod{37}$. Entonces $k = 37q + 14$ para algún $q \in \mathbb{Z}$, y en definitiva, reemplazando k, las dos condiciones se cumplen si y solamente si

$$(a, b) = (360 + 925q, -158 - 407q) \text{ con } q \in \mathbb{Z}$$

.

2 Ejercicio 2

Ejercicio 2:
Sea $a \in \mathbb{Z}$ tal que el resto de dividir $2a$ por 3 es 0, el resto de dividir $2a$ por 14 es 4 y tal que el resto de dividir $a^{2021} + a^{110}$ por 11 es 5. Hallar todos los posibles restos de dividir a por 693.

Solución: Notemos primero que 11 es primo y que $11 \nmid a$, pues si $a \equiv 0 \pmod{11}$ llegaríamos a una contradicción ya que $a^{2021} + a^{110} \equiv 0^{2021} + 0^{110} \equiv 0 \pmod{11}$, sin embargo el enunciado nos dice que $a^{2021} + a^{110} \equiv 5 \pmod{11}$. Entonces podemos usar el pequeño teorema de Fermat en su versión más fuerte, es decir podemos usar que $a^{10} \equiv 1 \pmod{11}$. De esta manera tenemos que:

$$a^{2021} + a^{110} \equiv a^1(a^{10})^{202} + (a^{10})^{11} \equiv a + 1 \pmod{11}$$

Por lo tanto, con lo hecho recién y el enunciado llegamos a lo siguiente

$$\begin{cases} 2a \equiv 0 \pmod{3} \\ 2a \equiv 4 \pmod{14} \\ a^{2021} + a^{110} \equiv 5 \pmod{11} \end{cases} \leftrightsquigarrow \begin{cases} 2a \equiv 0 \pmod{3} \\ 2a \equiv 4 \pmod{14} \\ a + 1 \equiv 5 \pmod{11} \end{cases} \leftrightsquigarrow \begin{cases} 2a \equiv 0 \pmod{3} \\ 2a \equiv 4 \pmod{14} \\ a \equiv 4 \pmod{11} \end{cases}$$

Notemos que $2a \equiv 0 \pmod 3$ es equivalente a $a \equiv 0 \pmod 3$ pues $(2:0) = 2$ es coprimo con 33, y $2a \equiv 4 \pmod{14}$ es equivalente a $a \equiv 2 \pmod 7$ pues vimos en clase que esa ecuación tiene solución si y solo si $(2:14) = 2 \mid 4$ y en ese caso la ecuación $2a \equiv 4 \pmod{14}$ es equivalente a la ecuación coprimizada $a \equiv 2 \pmod 7$.

Entonces el sistema es equivalente a

$$\begin{cases} a \equiv 0 \pmod 3 \\ a \equiv 2 \pmod 7 \\ a \equiv 4 \pmod{11} \end{cases}$$

Ahora, todos estos módulos son coprimos luego por el teorema chino del resto seguro hay solución y es única módulo $3 \cdot 7 \cdot 11 = 231$.

Hagamos un método más artesanal para resolver este sistema. De la primer ecuación sabemos que $a = 3k$ para algún $k \in \mathbb{Z}$. Luego, reemplazando esto en la segunda y tercera ecuación tenemos un sistemita de dos ecuaciones.

$$\begin{cases} 3k \equiv 2 \pmod 7 \\ 3k \equiv 4 \pmod{11} \end{cases} \overset{\substack{(5:7)=1 \\ (4:11)=1}}{\leftrightsquigarrow} \begin{cases} 5 \cdot 3k \equiv 5 \cdot 2 \pmod 7 \\ 4 \cdot 3k \equiv 4 \cdot 4 \pmod{11} \end{cases} \leftrightsquigarrow \begin{cases} k \equiv 3 \pmod 7 \\ k \equiv 5 \pmod{11} \end{cases}$$

Ahora resolvemos este pequeño sistema, resolvemos:

$$(S_1) \begin{cases} k_1 \equiv 0 \pmod 7 \\ k_1 \equiv 5 \pmod{11} \end{cases} \quad (S_2) \begin{cases} k_2 \equiv 3 \pmod 7 \\ k_2 \equiv 0 \pmod{11} \end{cases}$$

- **Resolvemos** (S_1): tenemos que $k_1 = 7 \cdot q$.

  Luego $7 \cdot q \equiv 5 \pmod{11} \underbrace{\Leftrightarrow}_{(8:11)=1} 8 \cdot 7 \cdot q \equiv 8 \cdot 5 \pmod{11} \Leftrightarrow q \equiv 7 \pmod{11}$ con lo cual $k_1 = 77 \cdot q + 49 \Leftrightarrow k_1 \equiv 49 \pmod{77}$

- **Resolvemos** (S_2): tenemos que $k_2 = 11 \cdot q$.

  Luego $11 \cdot q \equiv 3 \pmod 7 \Leftrightarrow 4 \cdot q \equiv 3 \pmod 7 \underbrace{\Leftrightarrow}_{(2:7)=1} 2 \cdot 4 \cdot q \equiv 2 \cdot 3 \pmod 7 \Leftrightarrow q \equiv 6 \pmod 7$ con lo cual $k_2 = 77 \cdot q + 66 \Leftrightarrow k_2 \equiv 66 \pmod{77}$.

De esta forma $k \equiv k_1 + k_2 \equiv 66 + 49 \equiv 38 \pmod{77}$ y por lo tanto, $a = 3 \cdot (77 \cdot q + 38) = 231q + 114$ es decir:

$$\begin{cases} a \equiv 0 \pmod 3 \\ a \equiv 2 \pmod 7 \\ a \equiv 4 \pmod{11} \end{cases} \underbrace{\Longleftrightarrow}_{\text{T.C.R}} a \equiv 114 \pmod{231}$$

Ahora bien, $693 = 3 \cdot 231$ y nosotros ya sabemos que $a = 231k + 114$. Lo que haremos es dividir a k por 3, es decir $k = 3q + r$ donde $0 \leq r < 3$, y estas son todas las posibilidades. Obtendremos que $a = 693q + 231 \cdot r + 114$ De esta manera:

- Si $r_3(k) = 0$, entonces $a = 693q + 114$ y por ende $r_{693}(a) = 114$
- Si $r_3(k) = 1$, entonces $a = 693q + 231 + 114$ y por ende $r_{693}(a) = 345$
- Si $r_3(k) = 2$, entonces $a = 693q + 231 \cdot 2 + 114$ y por ende $r_{693}(a) = 576$

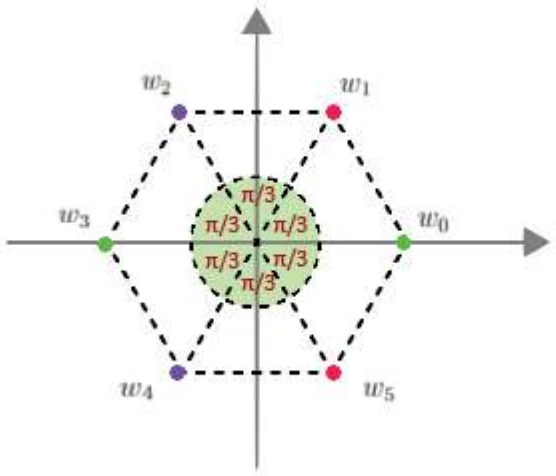
y estas son todas las posibilidades.

3 Ejercicio 3

Ejercicio 3:
Sea $f = X^4 - 2X^3 + 3X^2 - 2X + 1 \in \mathbb{C}[X]$.

(a) Probar que si $\omega \in \mathbb{C}$ es una raíz sexta primitiva de la unidad, entonces $f(\omega) = 0$.

(b) Calcular la multiplicidad de cada raíz de f.



Este es un gráfico de todas las raíces sextas de la unidad. En rojo se ven w_1 y w_5 las raíces sextas primitivas de la unidad. En violeta se ven w_2 y w_4 las raíces terceras primitivas de la unidad. En verde se ven $w_3 = -1$ la raíz primitiva cuadrada de la unidad y $w_0 = 1$.

3.1 Manera 1

(a) La estrategia que vamos a emplear es encontrar un polinomio $\Phi_6 \in \mathbb{C}[X]$ que tenga por raíces simples a las raíces primitivas sextas de las unidad y verificar que $\Phi_6 \mid f$. En cuyo caso, es automático demostrar lo que nos dice el enunciado pues en general si tenemos polinomios $g, f \in K[X]$ tales que $g \mid f$ entonces si $a \in K$ es raíz de g resulta que a es también raíz de f (o lo que es lo mismo por definición de raíz, $f(a) = 0$).

Recordemos un resultado de la teórica que dice que en $G_n = \{w_0, \ldots, w_{n-1}\}$ (todas distintas), dado $w_k = e^{\frac{2\pi k}{n}i}$ con $0 \leq k < n-1$ entonces w_k es una raíz primitiva n-ésima si y solamente si $(k : n) = 1$. En particular, en G_6 las raíces primitivas son dos distintas, w_1 y w_5 ya que 1 y 5 son los coprimos.

Luego, sabemos que las raíces primitivas sextas de la unidad son w_1 y w_5. Podemos intentar calcular $\Phi_6 = (X - w_1)(X - w_5)$. ¿Que tan traumático puede resultar calcular w_1 y w_5? resulta que no demasiado si sabemos calcular $\cos(\frac{\pi}{3})$ y $\text{sen}(\frac{\pi}{3})$ pues $w_1 = \cos(\frac{\pi}{3}) + i\text{sen}(\frac{\pi}{3})$.

Sabemos que $\cos(\frac{\pi}{3}) = \frac{1}{2}$ y $\text{sen}(\frac{\pi}{3}) = \frac{\sqrt{3}}{2}$.

Una vez que sabemos esto, tenemos que $w_1 = \cos(\frac{\pi}{3}) + i\text{sin}(\frac{\pi}{3}) = \frac{1}{2} + i\frac{\sqrt{3}}{2}$.

Por otro lado, $w_5 = w_1^5 \underbrace{=}_{5 \equiv -1 \pmod 6} w_1^{-1} = \overline{w_1} = \frac{1}{2} - i\frac{\sqrt{3}}{2}$ con lo cual

$$\Phi_6 = \Big(X - \frac{1}{2} - i\frac{\sqrt{3}}{2}\Big)\Big(X - \frac{\sqrt{1}}{2} + i\frac{\sqrt{3}}{2}\Big) = X^2 - 2Re(w_1)X + |w_1|^2 = X^2 - X + 1$$

De esta manera, dividiendo f por Φ_6 vemos que $f = (X^2 - X + 1)^2$ y por lo tanto las raíces sextas primitivas de la unidad son raíces de f.

(b) La ventaja de encarar el ejercicio de esta forma es que tenemos que

$$f = (X^2 - X + 1)^2 = (X - w_1)^2(x - w_2)^2$$

y por lo tanto es evidente por definición que la multiplicidad de cada una de las raíces es 2.

3.2 Manera 2

(a) Sea $w \in G_6^*$. De la teórica sabemos que entonces, al ser w primitiva, $(w^3)^2 = 1$ pero $w^3 \neq 1$ y por lo tanto $w^3 = -1$

Tenemos:

$$\begin{aligned} f(w) = \underbrace{w^4}_{w^3 \cdot w = -w} - 2\underbrace{w^3}_{=-1} + 3w^2 - 2w + 1 \\ = -w + 2 + 3w^2 - 2w + 1 \\ = 3w^2 - 3w + 3 \\ = 3(w^2 - w + 1) \end{aligned}$$

Pero $w - w^2 + 1 = 0$ como se puede comprobar de $w = \frac{1}{2} \pm \frac{\sqrt{3}}{2}i$ que implica $w^2 = -\frac{1}{2} \pm \frac{\sqrt{3}}{2}i$, así , $f(w) = 0$.

Además como $w \in \mathbb{C} \setminus \mathbb{R}$, tanto w como $\overline{w}$ son raíces de f pues $f \in \mathbb{R}[x]$.

(b) Por el item anterior, sabemos que si $w \in G_6^*$ entonces w es raíz de f. Ahora derivemos el polinomio f para ver si podemos sacar alguna conclusión sobre la multiplicidad de $w \in G_6^*$.

Derivando obtenemos $f' = 4X^3 - 6X^2 + 6X - 2$. Evaluando en w obtenemos

$$f'(w) = \underbrace{4w^3}_{=-4} - 6w^2 + 6w - 2 = -6(w^2 - w + 1)$$

Es decir, si $w \in G_6^*$ entonces $f(w) = 0$ y $f'(w) = 0$, es decir w es un raíz de multiplicidad al menos doble de f.

Finalmente, como w y $\overline{w}$ son raíces de f distintas de la misma multiplicidad, concluimos que ambas son raíces dobles de f pues f tiene grado 4 y tiene exactamente 4 raíces en $\mathbb{C}$ contadas con multiplicidad.

4 Ejercicio 4

Ejercicio 4:
Factorizar como producto de irreducibles en $\mathbb{Q}[X]$, $\mathbb{R}[X]$ y $\mathbb{C}[X]$ el polinomio

$$f = X^4 - 6X^3 + 11X^2 - 2X - 10,$$

sabiendo que tiene alguna raíz en común con el polinomio $g = X^4 - 5X^3 + 7X^2 - 6$.

Solución: Como sabemos que f tiene alguna raíz en común con g, simplemente vamos a buscar el máximo común divisor entre estos dos polinomios usando el algoritmo de Euclides. Efectuamos las divisiones para llevar a cabo el algoritmo.

Primero dividimos $f = X^4 - 6X^3 + 11X^2 - 2X - 10$ por $g = X^4 - 5X^3 + 7X^2 - 6$:

$$\begin{array}{l|l} X^4 - 6X^3 + 11X^2 - 2X - 10 & X^4 - 5X^3 + 7X^2 - 6 \\ \hline X^4 - 5X^3 + 7X^2 + 0X - 6 & 1 \\ \hline 0 - X^3 + 4X^2 - 2X - 4 & \end{array}$$

Ahora, vemos que el resto de esta división es $-X^3 + 4X^2 - 2X - 4$, así que para continuar con el algoritmo debemos dividir a $g = X^4 - 5X^3 + 7X^2 - 6$ por $-X^3 + 4X^2 - 2X - 4$:

$$
\begin{array}{r|l}
X^4-5X^3+7X^2+0X-6 & -X^3+4X^2-2X-4 \\
-\,X^4-4X^3+2X^2+4X & -X+1 \\
\hline
0\;\; -X^3+5X^2-4X-6 & \\
\quad -X^3+4X^2-2X-4 & \\
\hline
\quad 0\;\; X^2-2X-2 &
\end{array}
$$

Vemos que el resto de esta división es $X^2 - 2X - 2$. Si queremos seguir el algoritmo, debemos dividir a $-X^3 + 4X^2 - 2X - 4$ por $X^2 - 2X - 2$:

$$
\begin{array}{r|l}
-X^3+4X^2-2X-4 & X^2-2X-2 \\
-\,-X^3+2X^2+2X & -X+2 \\
\hline
0\;\; 2X^2-4X-4 & \\
\quad -\,2X^2-4X-4 & \\
\hline
\quad\quad 0 \;/ &
\end{array}
$$

Como el resto es 0 damos por terminado el algoritmo. El último resto no nulo divido su coeficiente principal es justamente el máximo común divisor entre f y g que en este caso es $(f : g) = X^2 - 2X - 2$.

De esta forma, sabemos que $f = X^4 - 6X^3 + 11X^2 - 2X - 10$ es divisible por $X^2 - 2X - 2$. Ahora dividimos f por $X^2 - 2X - 2$:

$$
\begin{array}{r|l}
X^4-6X^3+11X^2-2X-10 & X^2-2X-2 \\
-\,X^4-2X^3-2X^2 & X^2-4X+5 \\
\hline
0\;\; -4X^3+13X^2-2X-10 & \\
\quad -\,-4X^3+8X^2+8X & \\
\hline
\quad 0\;\; 5X^2-10X-10 & \\
\quad\quad -\,5X-10X-10 & \\
\hline
\quad\quad\quad 0 \;/ &
\end{array}
$$

De esta forma $f = (X^2 - 2X - 2)(X^2 - 4X + 5)$.

- Hallemos las raíces de $X^2 - 2X - 2$. Estas son los $x = \frac{2+w}{2}$ tales que $w^2 = 2^2 + 8 = 12$.

Como $w^2 - 12$ tiene por raíces a $w_1 = 2\sqrt{3}$ y $w_2 = -2\sqrt{3}$ resulta que:

$$X^2 - 2X - 2 = (X - 1 + \sqrt{3})(X - 1 - \sqrt{3})$$

- Hallemos las raíces de X^2-4X+5. Estas son los $x = \frac{4+w}{2}$ tales que $w^2 = 16-20 = -4$. Como $w^2 - 4$ tiene por raíces a $w_1 = 2i$ y $w_1 = -2i$ resulta que:

$$X^2 - 4X + 5 = (X - 2 + i)(X - 2 - i)$$

Finalmente estamos en condiciones de dar las factorizaciones correspondientes.

1. La factorización de f en irreducibles en $\mathbb{Q}[X]$ es $(X^2 - 2X - 2)(X^2 - 4X + 5)$ pues ambos polinomios son de grado 2 y ya vimos que ninguno de los dos tiene raíces en $\mathbb{Q}$, luego son irreducibles en $\mathbb{Q}[X]$.

2. La factorización de f en irreducibles en $\mathbb{R}[X]$ es $(X-1+\sqrt{3})(X-1-\sqrt{3})(X^2-4X+5)$ ya que tiene 2 factores de grado 1 y un factor de grado 2 que no tiene raíces en $\mathbb{R}$, luego son todos irreducibles en $\mathbb{R}[X]$

3. Finalmente $(X - 1 + \sqrt{3})(X - 1 - \sqrt{3})(X - 2 + i)(X - 2 - i)$ es la factorización de f en irreducibles en $\mathbb{C}[X]$ ya que todos los factores son de grado 1, y por lo tanto irreducibles en $\mathbb{C}[X]$.