

Álgebra I - Segundo cuatrimestre de 2024
Primer Recuperatorio del Segundo Parcial - 10/12/2024

1. Hallar todos los números primos $p \in \mathbb{N}$ tales que

$$p \mid ((11!)^{p-1} + 220 : 142^{5p} + 40).$$

2. Hallar todos los $a \in \mathbb{Z}$, $0 \leq a < 360$, tales que $a^3 \equiv 197 \pmod{360}$.

3. Sea $f = X^5 - \left(\frac{1}{2} + \frac{\sqrt{3}i}{2}\right)$.

a) Probar que $f \mid X^{30} - 1$

b) Hallar el polinomio $g \in \mathbb{R}[X]$ mónico de grado mínimo tal que $f \mid g$.

4. Sea $f = X^6 + X^5 + aX^4 + 2X^3 + aX^2 + X + 1 \in \mathbb{R}[X]$. Hallar todos los valores de a tales que $f(1) \neq 0$ y f tiene una raíz $\omega \in \mathbb{C}$ que verifica $\omega^3 = 1$. Para cada uno de los valores hallados, factorizar f en $\mathbb{R}[X]$ y en $\mathbb{C}[X]$.

*Complete esta hoja con sus datos y entréguela con el resto del examen.
Justifique todas sus respuestas.*

Mariangeles Porro
4611334

①

① Hallar todos los p primos $\in \mathbb{N} /$
 $p \mid \left(\underbrace{(11!)^{p-1} + 220}_a : \underbrace{142^{5p} + 40}_b \right)$

\Rightarrow Se que si $p \mid (a:b) \Leftrightarrow p \mid a \wedge p \mid b$.
análisis cada congruencia:

$p \mid a$: $p \mid a \Leftrightarrow a \equiv 0(p) / (11!)^{p-1} + 220 \equiv 0(p)$,
si $p \nmid (11!)$ puedo usar Fermat (luego
análisis cuando $p \mid (11!)$) ~~caso particular~~

[PTE]: $(11!)^{p-1} \equiv 1(p) \Leftrightarrow p$ primo y $(11! \cdot p) = 1$.

reemplazo.

$$1 + 220 \equiv 0(p) \Leftrightarrow 221 \equiv 0(p) /$$

$p = 13$; $p = 17$. Veo si alguno de estos
 p cumple que $p \mid b$.

$p = 13$: $\underbrace{142^{5 \cdot 13}}_{\equiv 12(13)} + \underbrace{40}_{\equiv 1} \equiv 0(13) \rightarrow (12^{13})^5 + 1 \equiv 0(13)$

[PTE]: $12^{13} \equiv 12(13) \rightarrow 12^5 + 1 \equiv 0(13)$, $12^2 \equiv 1(13)$

$12^2 \cdot 12^2 \cdot 12 + 1 \equiv 12 + 1 \equiv 13 \equiv 0(13) \checkmark$ $p = 13$ \checkmark

$p = 17$: $\underbrace{(142^{17})^5}_{142 \equiv 6(17)} + \underbrace{40}_{\equiv 6(17)} \equiv 0(17) \rightarrow \underbrace{(6^{17})^5}_{\text{[PTE]: } 6^{17} \equiv 6(17)} + 6 \equiv 0(17)$

$6^5 + 6 \equiv 0(17) \rightarrow 7776 + 6 \equiv 7 + 6 \equiv 13 \not\equiv 0(17) \times$

$p \neq 17$ \times

→) Ahora me fijo que pasa con los factores de (111) / los primos que aparecen en su factorización son: $p=2, p=3, p=5, p=7, p=11$. Me fijo cada uno

$p=2$: $(111)^{2-1} + 220 \equiv 0(2)$ \wedge $(42^2)^5 + 40 \equiv 0(2)$
 $11! \text{ contiene a } 2, \text{ así que}$ $192 \equiv 0(2)$ y $40 \equiv 0(2)$
 $es \equiv 0(2), 220 \equiv 0(2)$

conclusión, 2 divide a ambas expresiones
 $(p=2) \checkmark$

$p=3$: $(111)^{3-1} + 220 \equiv 0(3)$ \wedge $(42^3)^5 + 40 \equiv 0(3)$
 $\text{contiene a } 3$ $\text{como } 3|a, 3|(a:b)$
 $\text{así que el resto es } 0$ $\text{así que no analizo si } 3|b \text{ y}$
 $\text{mod. } 3$ $\text{concluyo que } (p \neq 3) \checkmark$

$p=5$: $(111)^{5-1} + 220 \equiv 0(5)$ \wedge $(42^5)^5 + 40 \equiv 0(5)$
 $\text{contiene al } 5, 220 \equiv 0(5)$ $\text{queda } 2 + 40 = 42(5)$
 $\text{su resto es } 0, 5|a$ $2^5 \equiv 2 \rightarrow (2^5)^5 \equiv 2(5)$ y $42 \not\equiv 0(5)$
 $(p \neq 5) \checkmark$

$p=7$: $(111)^{7-1} + 220 \equiv 0(7)$ \wedge $(42^7)^5 + 40 \equiv 0(7)$
 $\text{contiene a } 7$ $\text{como } 7 \nmid a$
 $\text{es congruente a } 0 \Rightarrow 0+3 \not\equiv 0(7)$ $\text{como } 7 \nmid a$
 $\text{mod. } 7$ $\text{no } 7|(a:b), (p \neq 7) \checkmark$

$p=11$: $(111)^{11-1} + 220 \equiv 0(11)$ \wedge $(42^{11})^5 + 40 \equiv 0(11)$
 $\equiv 0(11)$ $\equiv 0(11)$ $\text{queda } 2 + 40 = 42(11)$
 $10^{11} \equiv 10(11)$ $(p \neq 11) \checkmark$

Los p primos $\in \mathbb{N}$ que cumplen son $p=13$ y $p=2$
 $p|(a:b)$

$10^5 + 7 \not\equiv 0(11)$

Mari Angeles Pardo
46113741

(2)

② Hallar todos los $a \in \mathbb{Z} / 0 \leq a < 360 /$
 $a^3 \equiv 197 \pmod{360}$

\Rightarrow Comienzo factorizando a 360/
 $360 = 2^3 \cdot 3^2 \cdot 5$ / 8, 9 y 5 son coprimos

$2 \nmid a$ / $a^3 \equiv 197 \pmod{360}$ $\xrightarrow{\text{TCR}}$ $\begin{cases} a^3 \equiv 197 \pmod{8} \text{ ①} \\ a^3 \equiv 197 \pmod{9} \text{ ②} \\ a^3 \equiv 197 \pmod{5} \text{ ③} \end{cases}$

Planteo congruencia con los módulos /

① $\Rightarrow a^3 \equiv 197 \pmod{8} \rightarrow a^3 \equiv 5 \pmod{8}$; ¿cuando a^3 es congruente a 5 módulo 8?

a	0	1	2	3	4	5	6	7
a^2	0	1	4	1	0	1	4	1
a^3	0	1	0	3	0	5	0	7

solo pasa cuando
 $[a \equiv 5 \pmod{8}]$ ✓

② $\Rightarrow a^3 \equiv 197 \pmod{9} \rightarrow a^3 \equiv 8 \pmod{9}$; ¿cuando pasa $a^3 \equiv 8 \pmod{9}$?

a	0	1	2	3	4	5	6	7	8
a^3	0	1	8	0	1	8	0	1	8

pasa cuando
 $a \equiv 2 \pmod{9}$, $a \equiv 5 \pmod{9}$
y $a \equiv 8 \pmod{9}$.

③ $\Rightarrow a^3 \equiv 197 \pmod{5} \rightarrow a^3 \equiv 2 \pmod{5}$

a	0	1	2	3	4
a^3	0	1	3	2	4

pasa solo cuando $[a \equiv 3 \pmod{5}]$ ✓

⇒) Juntando todo me queda que: $a \equiv 5(8)$

$a \equiv 3(5)$ y $\textcircled{A} a \equiv 2(9)$, voy a plantear 3

- $\textcircled{B} a \equiv 5(9)$
- $\textcircled{C} a \equiv 8(9)$

los sistemas que van a ser equivalentes al original teniendo las mismas soluciones

- \textcircled{A}
- $a \equiv 3(5)$
 - $a \equiv 5(8)$
 - $a \equiv 2(9)$

$\textcircled{S_1} \begin{cases} a \equiv 3(5) \\ a \equiv 0(72) \end{cases}$

$a = 72k, 72k \equiv 3(5) \rightarrow 2k \equiv 3(5)$
 $2 \nmid 5$ $\textcircled{A} \rightarrow k \equiv 4(5) \rightarrow a = 72 \cdot 4 = 288$ (360)

$\textcircled{S_2} \begin{cases} a \equiv 5(8) \\ a \equiv 0(45) \end{cases}$

$a = 45k \rightarrow 45k \equiv 5(8) \rightarrow 5(9)k \equiv 5(8)$
 $45 \nmid 8$ y $a \equiv b(d) \Leftrightarrow a \equiv bd$ hence d
 $\Rightarrow 9k \equiv 1(8) \rightarrow k \equiv 1(8)$
 $[a = 45 \cdot 1 = 45]$ (360)

$\textcircled{S_3} \begin{cases} a \equiv 2(9) \\ a \equiv 0(40) \end{cases}$

$a = 40k, 40k \equiv 2(9)$
 $40 \nmid 9 \rightarrow 2(20)k \equiv 2(9) \rightarrow 20k \equiv 1(9) \rightarrow 2k \equiv 1(9)$
 $2 \nmid 9 \rightarrow k \equiv 5(9)$
 $[a = 40 \cdot 5 = 200]$

$a \equiv 288 + 45 + 200$ (360) $\rightarrow a \equiv 533$ (360) $533 = 360 \cdot 1 + 173$
 solución de \textcircled{A} : $[a \equiv 173$ (360)] \checkmark Buscamos $0 < r < d$.

- \textcircled{B}
- $a \equiv 3(5)$
 - $a \equiv 5(8)$
 - $a \equiv 5(9)$

$\textcircled{S_1} \begin{cases} a \equiv 3(5) \\ a \equiv 0(72) \end{cases}$

$a = 72k, 72k \equiv 3(5)$
 $72 \equiv 2(5) \rightarrow 2k \equiv 3(5)$
 $2 \nmid 5 \rightarrow k \equiv 4(5)$
 $[a = 72 \cdot 4 = 288]$

$\textcircled{S_2} \begin{cases} a \equiv 5(8) \\ a \equiv 0(45) \end{cases}$

$a = 45k, 45k \equiv 5(8)$
 $5 \cdot 9k \equiv 5(8) \Leftrightarrow 9k \equiv 1(8)$
 $9 \nmid 8$
 $k \equiv 1(8), [a = 45]$

$\textcircled{S_3} \begin{cases} a \equiv 5(9) \\ a \equiv 0(40) \end{cases}$

$a = 40k, 40k \equiv 5(9)$
 $5 \cdot 8k \equiv 5(9) \Leftrightarrow 8k \equiv 1(9)$
 $8 \nmid 9$
 $k \equiv 8(9), [a = 40 \cdot 8 = 320]$

$a = 288 + 45 + 320$ (360) $\rightarrow a \equiv 653$ (360) $653 = 360 \cdot 1 + 293$
 $[a \equiv 293$ (360)] s.c. de \textcircled{B} \checkmark

Maria Angeles Pardo
46113341

(3)

⇒) continuación de (2) : $\begin{cases} a \equiv 3(5) \\ a \equiv 5(8) \\ a \equiv 8(9) \end{cases}$

(S₁) $\begin{cases} a \equiv 3(5) \\ a \equiv 0(72) \end{cases}$

$a = 72k, \quad 72k \equiv 3(5)$
 $2k \equiv 3(5) \leftarrow k \equiv 4(5)$
 $5 \nmid 2$

$[a = 72 \cdot 4 = 288$

$a \equiv 288 + 45 + 80 \equiv 413(360)$

$413 = 360 \cdot 1 + 53$, (C) $a \equiv 53(360)$ ✓

Todos los $a \in \mathbb{Z}$ entre $0 \leq a < 360$ ✓

Son $a \equiv 173(360)$, $a \equiv 293(360)$ y $a \equiv 53(360)$
 (cuando $a \equiv 2(9)$) (cuando $a \equiv 5(9)$) (cuando $a \equiv 8(9)$)

es siempre

$0 \leq a < 360$ $a = 173, a = 293, a = 53$!!

(S₂) $\begin{cases} a \equiv 5(8) \\ a \equiv 0(45) \end{cases}$

$a = 45k, \quad 45k \equiv 5(8)$
 $5 \cdot 9k \equiv 5 \cdot 1(8) \Leftrightarrow 9k \equiv 1(8)$
 $8 \nmid 5$
 $\Leftrightarrow k \equiv 1(8) \quad [a = 45]$
 $9 \nmid 8$

(S₃) $\begin{cases} a \equiv 8(9) \\ a \equiv 0(40) \end{cases}$

$a = 40k, \quad 40k \equiv 8(9)$
 $8 \cdot 5k \equiv 8 \cdot 1(9)$
 $8 \nmid 9$
 $\Leftrightarrow 5k \equiv 1(9)$
 $9 \nmid 5$
 $\Leftrightarrow k \equiv 2(9)$
 $5 \nmid 9$

$a = 40 \cdot 2 = 80$

\Rightarrow) 4) continuación: $a = -3$ y $g = x^4 + 2x^2 + 1$
~~sigo factorizando g . Busco sus raíces
 por Gauss / $p = a_0 = -5$ / $p = \{\pm 1, \pm 5\}$
 veo cual divide $g = a_n = 1$ / g
 por Ruffini /
 $1 \mid 0 \quad -4 \quad 6 \quad -5$~~

\Rightarrow) Noto que $g = (x^2)^2 + 2(x^2) + 1$, si hago un
 cambio de variable / $x^2 = y$, $y^2 + 2y + 1$, busco
 raíces por Baskara / $y_{1,2} = \frac{-2 \pm \omega}{2}$ con $\omega^2 = (-2)^2 - 4 \cdot 1 \cdot 1$

\Rightarrow) $\omega^2 = 4 - 4 \Rightarrow \omega = 0$ (se sea ω) me queda que -1
 $\frac{-2 \pm 0}{2} = \frac{-2}{2} = -1$ $y_1 = -1$ y $y_2 = -1$ es raíz cuadrada /

$x = -1$, $g(x) = (-1)^2 + 2 \cdot (-1) + 1 = -2 + 2 = 0$ /

se sea -1 es raíz doble de g / $x^2 + 1 = 0$

$(x^2 + 1) \mid g$ / $x^4 + 2x^2 + 1 \mid x^2 + 1$ (verifico)

$$\begin{array}{r} x^4 + 2x^2 + 1 \\ -(x^4 + x^2) \\ \hline x^2 + 1 \\ -(x^2 + 1) \\ \hline 0 \end{array}$$

$(x^2 + 1)$ es de multiplicidad
 doble. $(x^2 + 1)^2$ //

Ya puedo factorizar en $\mathbb{R}[x]$ ya que
 $(x^2 + 1)$ y $(x^2 + x + 1)$ son ambos polinomios de
 grado 2 irreducibles en $\mathbb{R}[x]$ /

factorización en $\mathbb{R}[x]$: $f = (x^2 + x + 1) \cdot (x^2 + 1)^2$

$$\begin{matrix} -3+a+1 \\ a-2 \end{matrix}$$

$$\begin{matrix} 2-a+1=3-a \\ a-a+1 \end{matrix}$$

④ Sea $f = x^6 + x^5 + ax^4 + 2x^3 + ax^2 + x + 1 \in \mathbb{R}[x]$
 Hallar todos los valores de a /
 $f(a) \neq 0$ y f tiene una raíz $w \in \mathbb{C} / w^3 = 1$.
 Factorizar en $\mathbb{R}[x]$ y $\mathbb{C}[x]$.

\Rightarrow f tiene una raíz $w / w^3 = 1$, o sea
 $w \in G_3$, se que G_3 tiene al 1, pero por
 enunciado, $f(a) \neq 0$, luego las únicas 2
 posibilidades de raíces en G_3 son:

$w_0 = 1$, no es raíz. $w_1 = e^{\frac{2\pi i}{3}}$ $w_2 = e^{\frac{4\pi i}{3}}$
 con $\omega = e^{\frac{2k\pi i}{3}} / 0 \leq k \leq 2$
 $w_1 = e^{\frac{2\pi i}{3}} = -\frac{1}{2} + \frac{\sqrt{3}}{2}i$ y $w_2 = e^{\frac{4\pi i}{3}} = -\frac{1}{2} - \frac{\sqrt{3}}{2}i$
 (porque estos en \mathbb{R})



o sea, básicamente, voy a tener a w_1 y $\bar{w}_1 = w_2$
 los multiplico para que esté en $\mathbb{R}[x]$

$$(x - (-\frac{1}{2} + \frac{\sqrt{3}}{2}i))(x - (-\frac{1}{2} - \frac{\sqrt{3}}{2}i)) = x^2 + x + \frac{1}{4} + \frac{3}{4} = x^2 + x + 1 = g$$

Se que $g | f$ dividido /
 $x^6 + x^5 + ax^4 + 2x^3 + ax^2 + x + 1 \mid x^2 + x + 1$
 $(x^6 + x^5 + x^4)$ $x^4 + (a-1)x^2 + (3-a)x + (a-2)$

$(a-1)x^4 + 2x^3 + ax^2 + x + 1$
 $(a-1)x^4 + (a-1)x^3 + (a-1)x^2$

Como $g | a$, el resto es 0 /
 $3-a=0 \Leftrightarrow [a=3]$

$(3-a)x^3 + 1x^2 + x + 1$
 $((3-a)x^3 + (3-a)x^2 + (3-a)x)$

hemplazo / $a=3$
 $g = x^4 + 2x^2 + 1$

$(a-2)x^2 + (a-2)x + 1$
 $((a-2)x^2 + (a-2)x + (a-2))$
 $1 - a + 2$

Hoy que $a=3$ que para $a=3$,
 no dando, luego si no no
 haberlo así.

③ Sea $f = x^5 - \left(\frac{1}{2} + \frac{\sqrt{3}}{2}i\right)$.

a) Probar que $f \mid (x^{30} - 1)$

~~Se describe con $z = \frac{1}{2} + \frac{\sqrt{3}}{2}i$
se cortes por la con~~

$\Rightarrow (x^{30} - 1) = h$, ¿cuáles son las raíces de h ?

$h = x^{30} - 1 = 0 \quad [x^{30} = 1 \text{ de las raíces de } h$
 $\in G_{30} \quad / \quad G_{30} = \{e^{\frac{2k\pi}{30}} \text{ con } 0 \leq k \leq 29\}$ ✓

De la misma forma, igualo f a 0 /

$x^5 - \frac{1}{2} - \frac{\sqrt{3}}{2}i = 0 \Leftrightarrow x^5 = \frac{1}{2} + \frac{\sqrt{3}}{2}i$ igualo números
complejos, para ver z_1 z_2

las raíces / igualo sus módulos y argumentos.

~~z_1~~ $z_1 : \begin{cases} |z_1| = x^5 \\ \arg(z_1) = 0.5 \end{cases} \quad z_2 : \begin{cases} |z_2| = \sqrt{\left(\frac{1}{2}\right)^2 + \left(\frac{\sqrt{3}}{2}\right)^2} = 1 \\ \arg(z_2) = \frac{\pi}{3} \end{cases}$

$z_1 = z_2 \Leftrightarrow \begin{cases} x^5 = 1 \rightarrow x = 1 \\ 5 \cdot 0 = \frac{\pi}{3} + 2k\pi \rightarrow 0 = \frac{\pi}{3} + \frac{2k\pi}{5} \end{cases}$ sacando factor común

$0 \leq \frac{1}{3} + \frac{2k}{5} < 2k \rightarrow 0 \leq \frac{1}{3} + 2k < 10k \rightarrow -\frac{1}{3} \leq 2k < \frac{29}{3}k$

$-\frac{1}{6} \leq \frac{2k}{5} < \frac{29}{6} / k \in \{0, 1, 2, 3, 4\}$ las 5 raíces de f

$[k_0 = e^{\frac{1}{5}i} \quad [k_2 = e^{\frac{13}{5}i} \quad [k_4 = e^{\frac{29}{5}i}$
 $[k_1 = e^{\frac{7}{5}i} \quad [k_3 = e^{\frac{19}{5}i}$



\Rightarrow $e^{\frac{k_0}{30}i}$, $e^{\frac{k_1}{30}i}$, $e^{\frac{k_2}{30}i}$, $e^{\frac{k_3}{30}i}$, $e^{\frac{k_4}{30}i}$ son las raíces de f , pero, también de h ✓
 Cuando en $G_{30} / e^{\frac{2k}{30}i}$ conjugado y g

- Si $j=1$, $e^{\frac{2 \cdot 1 \cdot \pi i}{30}} = e^{\frac{1 \cdot \pi i}{15}} = k_0$
 - Si $j=7$, $e^{\frac{14 \cdot \pi i}{30}} = e^{\frac{7 \cdot \pi i}{15}} = k_1$
 - Si $j=13$, $e^{\frac{26 \cdot \pi i}{30}} = e^{\frac{13 \cdot \pi i}{15}} = k_2$
 - Si $j=19$, $e^{\frac{38 \cdot \pi i}{30}} = e^{\frac{19 \cdot \pi i}{15}} = k_3$
 - Si $j=25$, $e^{\frac{50 \cdot \pi i}{30}} = e^{\frac{5 \cdot \pi i}{3}} = k_4$
- } $f \in G_{30}$ ✓

sea, todas las raíces de f se encuentran en G_{30} , y como h sería el polinomio "asociado" a G_{30} , $f|h$ ✓
 Si tengo que cada raíz de f de la forma $(x - k_n) | h$, entonces:

$$(x - k_0)(x - k_1)(x - k_2)(x - k_3)(x - k_4) | h$$

que es f factorizado. ✓

b) $g \in \mathbb{R}_x$ monico gr minimo / $f|g$.

\Rightarrow trato de buscar un polinomio g en \mathbb{R}_x que sea divisible por f , o sea en un principio va a tener que tener las raíces de f , pero como $g \in \mathbb{R}_x$ y las raíces de g son complejas, entonces voy a tener al conjugado, o sea, cada raíz

va a ser de multiplicidad 2 /

$$g = (x - e^{\frac{1 \cdot \pi i}{15}})^2 (x - e^{\frac{5 \cdot \pi i}{3}})^2 (x - e^{\frac{13 \cdot \pi i}{15}})^2 (x - e^{\frac{7 \cdot \pi i}{15}})^2 (x - e^{\frac{19 \cdot \pi i}{15}})^2$$

No! Solo tiene los conjugados, o sea $e^{\frac{1 \cdot \pi i}{15}}$ y $e^{-\frac{1 \cdot \pi i}{15}}$, etc.