# Álgebra I
# Segundo recuperatorio del Segundo parcial
# 17/12/2019

1. Hallar el resto de de la división de $12^{(2^n)}$ por 7 para cada n $\in \mathbb{N}$.
2. Probar que: $|1 + iz| = |1 - iz| \iff z \in \mathbb{R}$.
3. Sea $\omega \in G_5$ una raíz quinta primitiva de la unidad. Hallar todos los n $\in \mathbb{N}$ tales que:

$$\sum_{j=0}^{3n+2} (\overline{\omega^{-11}} + \omega^{10} + \omega^{-3} + \omega^{4} + \omega^{14^2}\overline{\omega^{12}})^j = \omega + 1$$

4. Sea $f = X^6 - 3X^4 - (2+8i)X^3 + 24iX + 16i$. Hallar todas las raíces complejas de $f$, sabiendo que tiene al menos una raíz entera.
5. Hallar $f \in \mathbb{Q}[X]$ de grado mínimo que cumpla las siguientes condiciones simultáneamente:
   - $f$ comparte una raíz con $X^3 - 3X^2 + 7X - 5$.
   - $X + 3 - \sqrt{2}$.
   - $1 - 2i$ es raíz de $f$ y $f'(X - 2i) = 0$.

   A continuación, factorizar $f$ en $\mathbb{C}[X]$, $\mathbb{R}[X]$ y $\mathbb{Q}[X]$.

[1]

## Solución de 1:

- Quiero encontrar $x = r_7((12)^{2^n})$, para esto, uso Fermat. Como 7 es primo y (12:7) = 1 $\implies (12)^{2^n} \equiv (12)^{r_6(2n)}(7)$.
- Recordemos que, dados $a$,$b \in \mathbb{Z}$ y que si $r$ es el resto de dividir a por b, $a \equiv r(b)$, $\implies (12)^{r_6(2^n)} \equiv x(7) \implies (12)^{r_6(2^n)} \equiv x(7)$. Entonces, busco $r_6(2^n)$ para seguir.
- Sea $y = r_6(2^n)$, se me ocurre encontrar $y$ mediante TCR, ya que (2:3) = 1.

$$2^n \equiv y(6) \iff \begin{cases} 2^n \equiv y(2) \\ 2^n \equiv y(3) \end{cases} \iff \begin{cases} y \equiv 0(2) \\ 2^n \equiv y(3) \end{cases}$$

[1]Código fuente

Por Fermat, $2^n \equiv 2^{r_2(n)}(3)$, los posibles restos de n son 0 ó 1, que se corresponden con n par o impar.

- Asumo n par: $\implies 2^{r_2(n)} \equiv 2^0 \equiv 1(3) \implies y \equiv 1(3)$, entonces, se tiene que:

$$\begin{cases} y \equiv 0(2) \iff y = 2q, \text{ para algún } q \in \mathbb{Z} \\ y \equiv 1(3) \iff 2q \equiv 1(3) \iff -q \equiv 1(3) \iff q \equiv -1(3) \iff q \equiv 2(3) \end{cases}$$

Así, $y = 2q = 2(3k+2) = 6k+4 \equiv 4(4)$, para algún $k \in \mathbb{Z}$
Entonces, $2^n \equiv 4(6) \implies (12)^{r_6(2^n)} \equiv 12^4 \equiv 2(7) \implies r_7(12^{2^n}) = 2$, sé que es 2 ya que el resto es único.

- Asumo n impar: se llega a que, con un proceso similar al anterior, $2^n \equiv 2(6)$ y que $r_7(12)^{(2^n)} = 4$.

# Solución de 2:

- Quiero ver que:
$$|1+iz| = |1-iz| \iff z \in \mathbb{R}$$

- $\implies$ ), qvq: $|1+iz| = |1-iz| \implies z \in \mathbb{R}$

Asumo que z $\in \mathbb{C}$ con forma binomial $z = a+bi$ con $a, b \in \mathbb{R}$ tal que $|1+iz| = |1-iz|$
$\implies |1+i(a+bi)| = |1-i(a+bi)|$
$\implies |1+ai-b| = |1-ai+b|$
$\implies |(1-b)+ai| = |(1+b)-ai|$
$\implies \sqrt{(1-b)^2+a^2} = \sqrt{(1+b)^2+a^2}$
$\implies (1-b)^2+a^2 = (1+b)^2+a^2$
$\implies (1-b)^2 = (1+b)^2$
$\implies 1-2b+b^2 = 1+2b+b^2$
$\implies -b = b$
$\implies b = 0$
$\implies z = a+0i$
$\implies z \in \mathbb{R}$

- $\impliedby$ ), qvq: $z \in \mathbb{R} \implies |1+iz| = |1-iz|$

$z = z \iff 1+z^2 = 1+z^2$
$\implies \sqrt{1+z^2} = \sqrt{1+z^2}$
$\implies \sqrt{1+z^2} = \sqrt{1+(-z^2)}$
$\implies |1+iz| = |1-iz|$

■

# Solución de 3:

- Sé que $\omega \in G_5*$, esto me dice que si tengo $\omega^n, n \in \mathbb{Z} \implies \omega^n = w^{r_5(n)}$, además, $\overline{\omega} = \omega^{-1}$ que voy a usar para reescribir la expresión de la sumatoria a algo más amigable.
  $\overline{\omega^{-11}} = \omega$, $\omega^{10} = 1$, $\omega^{-3} = \omega^2$ , $\omega^{14^2} = \omega^{196} = \omega$, $\overline{\omega}^{12} = \omega^{-12} = w^3$.
  Por lo tanto:

$$\begin{aligned}\overline{\omega^{-11}} + \omega^{10} + \omega^{-3} + \omega^4 + \omega^{14^2} + \overline{\omega^{12}} &= 1 + \omega + \omega^2 + \omega^3 + \omega^4 + \omega \\ &= (\sum_{j=0}^{4} \omega^j) + w = \frac{\omega^5 - 1}{\omega - 1} + \omega = \omega\end{aligned}$$

  Notar que $\omega - 1 \neq 0$, ya que $\omega \in G_5*$.

- Así,

$$\sum_{j=0}^{3n+2} (\overline{\omega^{-11}} + \omega^{10} + \omega^{-3} + \omega^4 + \omega^{14^2}\overline{\omega^{12}})^j = \sum_{j=0}^{3n+2} \omega^j = \frac{\omega^{3n+2+1} - 1}{\omega - 1} = \frac{\omega^{3(n+1)} - 1}{\omega - 1}$$

- Ahora, quiero ver para cuáles $n \in \mathbb{N}$ se cumple que:

$$\frac{\omega^{3(n+1)} - 1}{\omega - 1} = \omega + 1$$

$$\begin{aligned}\frac{\omega^{3(n+1)} - 1}{\omega - 1} = \omega + 1 &\iff \omega^{3(n+1)} - 1 = (\omega + 1)(\omega - 1) \\ &\iff \omega^{3(n+1)} - 1 = \omega^2 - 1 \\ &\iff \omega^{3(n+1)} = \omega^2 \\ &\iff 3(n + 1) \equiv 2(5) \\ &\iff n \equiv 3(5)\end{aligned}$$

  Entonces, los $n \in \mathbb{N}$ que cumplen son $n \equiv 3(5)$

# Solución de 4:

- Me piden todas las raíces en $\mathbb{C}$ de $f$.

- Reescribo $f$:
  $f(x) = X^6 - 3X^4 - 2X^3 - 8iX^3 + 24iX + 16i$
  $f(x) = X^6 - 3X^4 - 2X^3 + 8i(-X^3 + 3X + 2)$
  $f(x) = X^3(X^3 - 3X + 2) + 8iX^3(-X^3 + 3X + 2)$
  $f(x) = (X^3 + 8iX^3)(-X^3 + 3X + 2)$

- Sea $g(x) = -x^3 + 3x + 2$, busco sus raíces:
  Como $g(x) \in \mathbb{Z}[X]$, por Gauss, las posibles raíces de $g(x)$ en $\mathbb{Q}$ son $\{\pm 2, \pm 1\}$. De estas, 2 resulta ser raíz de $g(x)$.
  2 es raíz de $g(x) \iff X - 2 | g(x)$.
  Si divido a $g(x)$ por $X - 2$, obtengo que $g(x) = (X-2)(-X^2 - 2x - 1) = -(X - 2)(+X^2 + 2X + 1) = -(X-2)(+X+1)^2$
  Las raíces de $g(x)$ son, entonces, 2 y -1, -1 siendo doble.

- Sea $j(x) = -X^3 + 8i$, sus raíces son las soluciones de $-X^3 + 8i = 0 \iff 8i = X^3$.
  2 números complejos son iguales si comparten módulo y argumento, entonces veo para cuáles $X \in \mathbb{C}$ se cumplen ambos.
  Módulo: $|X|^3 = |8i| \iff |X^3| = \sqrt{(8^2)} \iff |X^3| = 8 \iff |X| = 2$

- Argumento: veo para cuáles $X$ se cumple que $\arg(X^3) = \arg(8i)$
  $\arg(8i) = \frac{\pi}{2}$, ya que es imaginario puro y positivo
  Planteo $\arg(X^3) = \frac{\pi}{2}$, por De Moivre, $\arg(X^3) = 3\arg(X) + 2k\pi$ donde $k \in \mathbb{Z}$ tal que $3\arg(X) + 2k\pi \in [0, 2\pi)$
  $\implies 3\arg(X) + 2k\pi = \frac{\pi}{2} \implies 3\arg(X) = -2k\pi + \frac{\pi}{2} \implies \arg(X) = \frac{\pi}{3}(\frac{1}{2} - 2k)$
  Ahora, hay que ver para cuáles $k \in \mathbb{Z}$, $\arg(X) \in [0, 2\pi)$:
  $0 \leq \frac{\pi}{3}(\frac{1}{2} - 2k) < 2\pi \iff 0 \leq 1 - 2k < 6 \iff -1 \leq -2k < 5$
  $\iff \frac{1}{2} \geq k < -\frac{5}{2} \implies k \in \{0, -1, -2\}$.
  Entonces, las soluciones de $8i = X^3$ son $a_k = 2e^{i\frac{\pi}{3}(1-2k)}$, donde $k \in \{0, -1, -2\}$.

- Así, todas las raíces de $f$ en $\mathbb{C}$ son $\{-1, 2, a_k\}$.

# Solución de 5

- Enumero cada condición:

  1. $f$ tiene una raíz de $g$.
  2. $X + (-\sqrt{2} + 3) | f$.
  3. $f(1 - 2i) = 0$ y $f'(1 - 2i) = 0$.
  4. $f \in \mathbb{Q}[X]$, y además, f tiene grado mínimo.

  1. Busco las raíces de $g$, que como pertenece a $\mathbb{Z}[X]$, veo si las puedo encontrar mediante Gauss. Las posibles raíces de $g$ en $\mathbb{Q}$ son $\{\pm 5, \pm 1\}$, de estas, 1 resulta ser raíz de $g$. Si divido a $g$ por $X-1$, se tiene que $g = (X-1)(X^2 - 2X + 5)$. El discriminante de $(X^2 - 2X + 5)$ es -36, es decir, tiene raíces en $\mathbb{C} - \mathbb{R}$. Quiero que $f$ comparta una raíz de $g$, y que sea de grado mínimo, supongamos que la raíz que comparten es una de las raíces de $(X^2 - 2X + 5)$, como se tiene que cumplir que $f \in \mathbb{Q}[X]$, si tomo una de esas raíces, necesito su conjugado, es decir, en este caso $f$ tiene 2 raíces (y mayor grado por el Teorema Fundamental del Álgebra), pero si la raíz que comparten $f$ y $g$ es 1, solamente tengo una raíz, y por consecuente, menor grado que elegir otra raíz de $g$.
  2. $X + (-\sqrt{2} + 3) | f \iff \sqrt{2} - 3$ es raíz de $f$, y como $f \in \mathbb{Q}[X]$, y ya que $\sqrt{2} \notin \mathbb{Q} \implies \sqrt{2} + 3$ también es raíz de $f \iff X + (-\sqrt{2} - 3) | f$, además,

al ser $X+(-\sqrt{2}-3)$ y $X+(-\sqrt{2}+3)$ coprimos (ambos grado 1 con distinta raíz) $\implies (X+(-\sqrt{2}+3))(X+(-\sqrt{2}-3))|f$.

3. Necesito que $f(1-2i)=0$ y $f'(1-2i)=0 \iff X-(1+2i)|f$ y $X-(1+2i)|f \implies (X-(1+2i))^2|f \implies (X-(\overline{(1+2i)})^2|f$, esta última implicación es por la condición 4.

- Entonces, un $f$ que cumple es:
  $f(x)=(X-1)(X+(-\sqrt{2}+3))(X+(-\sqrt{2}-3))(X-(1+2i))^2(X-(1+2i))^2$
  Que al ser todas expresiones de grado 1, son irreducibles en $\mathbb{C}[X]$.

- La expresión irreducible de $f$ en $\mathbb{R}[X]$ es :
  $f(x)=(X-1)(X+(-\sqrt{2}+3))(X+(-\sqrt{2}-3))(X^2-2X+4)^2$
  Que son expresiones de grado 1, y un polinomio de grado 2 con discriminante negativo, por lo que son irreducibles en $\mathbb{R}[X]$.

- En $\mathbb{Q}[X]$,la expresión irreducible de$f$ es:
  $f(x)=(X-1)(X^2+3X+5)(X^2-2X+4)^2$
  La primera y última expresión son irreducibles por la misma razón que en $\mathbb{R}[X]$, la segunda, de ser reducible en $\mathbb{Q}[X]$, deberían existir $p$ y $q$ en $\mathbb{Q}[X]$ tales que su producto sea igual a $(X^2+3X+5)$, pero ya vimos que $p$ y $q$ están en $\mathbb{R}[X]$ y sé que la factorización en irreducibles es única.

- Por último, veamos que el $f$ al que llegué, es de grado mínimo:
  Supongamos que $\exists\ w \in \mathbb{Q}[X]$, que cumple las condiciones 1 (con raíz 1), 2 y 3, y que además cumple $gr(w) < gr(f) = 7$:
  Por 1, $w$ tiene 1 raíz
  Por 2, $w$ tiene 2 raíces
  Por 3, $w$ tiene 4 raíces
  Por el Teorema Fundamental del Álgebra, $w$ tiene grado 7, pero habíamos supuesto $gr(w) < 7$, ¡Absurdo! $\implies f$ es de grado mínimo. [1]

[1] Código fuente de este pdf: