Álgebra I - Examen Final
28/07/2015

Leandro Ezequiel Barrios
(lbarrios at dc.uba.ar)

1. Sea $\mathfrak{R}$ la relación en $A := \{10, ..., 1000\}$ definida por $(n : m) \neq 1$.

1.a. Determine si $\mathfrak{R}$ es reflexiva, simétrica, antisimétrica o transitiva.

- Reflexividad: $\mathfrak{R}$ es reflexiva si $\forall a \in A,\ a\mathfrak{R}a$

$$\begin{aligned} a\mathfrak{R}a \Leftrightarrow (a : a) &\neq 1 \\ (a : a) &= a \\ a \in A \Rightarrow a &\neq 1 \end{aligned}$$

  Luego, $(a : a) \neq 1 \Rightarrow a\mathfrak{R}a$, entonces $\mathfrak{R}$ es reflexiva.

- Simetría: $\mathfrak{R}$ es simétrica si $\forall n, m \in A,\ n\mathfrak{R}m \Leftrightarrow m\mathfrak{R}n$

$$n\mathfrak{R}m \Leftrightarrow (n : m) \neq 1$$
$$(n : m) \neq 1 \quad \Leftrightarrow \quad (m : n) \neq 1$$
$$(m : n) \neq 1 \Leftrightarrow m\mathfrak{R}n$$

  Luego, $n\mathfrak{R}m \Leftrightarrow m\mathfrak{R}n$, entonces $\mathfrak{R}$ es simétrica.

- Antisimetría: $\mathfrak{R}$ es antisimétrica si $\forall n, m \in A,\ n\mathfrak{R}m \wedge m\mathfrak{R}n \Rightarrow n = m$

  Basta con encontrar un contraejemplo para ver que $\mathfrak{R}$ no es antisimétrica.

$$(10 : 20) \neq 1 \Leftrightarrow 10\,\mathfrak{R}\,20$$
$$(20 : 10) \neq 1 \Leftrightarrow 20\,\mathfrak{R}\,10$$

  Luego, $10\mathfrak{R}20 \wedge 20\mathfrak{R}10$, pero $10 \neq 20$, por lo que $\mathfrak{R}$ no es antisimétrica.

- Transitividad: $\forall a, b, c \in A,\ a\mathfrak{R}b \wedge b\mathfrak{R}c \Rightarrow a\mathfrak{R}c$

  Dados $a, b, c \in A$, $a\mathfrak{R}b$, $b\mathfrak{R}c$, se que

$$a\mathfrak{R}b \Leftrightarrow (a : b) \neq 1$$
$$b\mathfrak{R}c \Leftrightarrow (b : c) \neq 1$$

  Basta con encontrar un contraejemplo para ver que $\mathfrak{R}$ no es transitiva.
  Dados $a = 2,\ b = 6,\ c = 3$,

$$(2 : 6) = 2 \neq 1 \Rightarrow 2\,\mathfrak{R}\,6$$
$$(6 : 3) = 3 \neq 1 \Rightarrow 6\,\mathfrak{R}\,3$$

  pero $(2 : 3) = 1$, por lo que $2\,\not{\mathfrak{R}}\,3$. Luego, $\mathfrak{R}$ no es transitiva.

1.b. Encuentre la cantidad de $m \in A$ tales que $m \,\mathfrak{R}\, 12$

Quiero encontrar todos los m tales que $m \,\mathfrak{R}\, 12$, siendo que $m \,\mathfrak{R}\, 12 \Leftrightarrow (m : 12) \neq 1$.
Factorizando 12 en primos, se que

$$12 = 2^2 \cdot 3$$

Entonces, dado d el mcm entre m y 12, se cumple que

$$d = (m : 12) \neq 1 \Leftrightarrow (d \neq 1 \wedge d \mid m \wedge d \mid 12)$$

En particular,

$$(d \mid 12 \wedge 12 = 2^2 \cdot 3) \Rightarrow d \mid 2^2 \cdot 3 \Rightarrow (2 \mid d \vee 3 \mid d)$$

Es decir que d es múltiplo de 2 o de 3. Luego, por transitividad

$$\begin{gathered}(d \mid m) \wedge (2 \mid d \vee 3 \mid d)\\ (2 \mid d \wedge d \mid m) \vee (3 \mid d \wedge d \mid m)\\ (2 \mid m) \vee (3 \mid m)\end{gathered}$$

Lo que singnifica que basta con ver cuántos $m \in A$ cumplen esta última condición.

- Múltiplos de 2:

  Si tomo el conjunto A, y para cada número calculo el resto módulo 2, voy a formar un nuevo conjunto

  $$A_2 = \{0, 1, 0, \cdots, 1, 0\}$$

  en donde, sin contar el caso del último número, cada dos números uno de ellos es divisible por 2.

  Luego, dado que A tiene 990 números (sin contar el último), la cantidad de números divisibles por 2 es $990/2 + 1 = 496$.

- Múltiplos de 3:

  Usando un razonamiento similar al descripto arriba, formo el conjunto

  $$A_3 = \{\underbrace{1, 2}_{2}, \underbrace{0, 1, 2, 0, \cdots, 0, 1, 2}_{987}, \underbrace{0, 1}_{2}\}$$

  en donde, sin contar los primeros y últimos dos números, cada 3 de ellos uno es divisible por 3. Luego, tengo $987/3 + 1 = 990/3 = 330$ números divisibles por 3.

- Múltiplos de 6:

  Ahora bien, si yo sumo la cantidad de múltiplos de 2 más la cantidad de múltiplos de 3, estoy contando 2 veces a los números que son múltiplos de 6, que son múltiplos de 2 y de 3. Para evitar esto, voy a calcular la cantidad de múltiplos de 2 más la cantidad de múltiplos de 3 menos la cantidad de múltiplos de 6.

  Usando el mismo razonamiento, formo el conjunto

  $$B_6 = \{\underbrace{4, 5}_{2}, \underbrace{0, 1, 2, 3, 4, 5, \cdots, 0, 1, 2, 3, 4, 5}_{984}, \underbrace{0, 1, 2, 3, 4}_{5}\}$$

  en donde, sin contar los primeros 2 y los últimos 5, tengo 984 números en donde cada 6 números, uno de ellos es múltiplo de 6.

  Luego, tengo $984/6 + 1 = 990/6 = 165$ múltiplos de 6.

Finalmente, tengo $496 + 330 - 165 = 661$ múltiplos de 2 o de 3 que pertenecen a A.
Es decir que tengo 661 posibles m tales que $m \,\mathfrak{R}\, 12$.

2. Sea $a \in \mathbb{Z}$ tal que $(a^{182} - 26 : 130) = 13$. Calcule $(a^{25} - 39 : 2 \cdot 5^3 \cdot 13^2)$

$$\begin{aligned}(a^{182} - 26 : 130) = 13 &\Rightarrow 13 \mid a^{182} - 26\\ &\Leftrightarrow 13 \mid a^{182} - 26 + (13 \cdot 2)\\ &\Leftrightarrow 13 \mid a^{182}\\ &\Leftrightarrow 13 \mid a\end{aligned}$$

$$\begin{aligned}2 \mid 130 \wedge 2 \nmid (a^{182} - 26 : 130) &\Rightarrow 2 \nmid a^{182} - 26\\ &\Leftrightarrow 2 \nmid a^{182} - 26 + (2 \cdot 13)\\ &\Leftrightarrow 2 \nmid a^{182}\\ &\Leftrightarrow 2 \nmid a\end{aligned}$$

$$\begin{aligned}13 \mid a &\Leftrightarrow 13^{25} \mid a^{25}\\ 13^2 \mid 13^{25} \wedge 13^{25} \mid a^{25} &\Rightarrow 13^2 \mid a^{25}\\ 13 \mid 39 \wedge 13^2 \mid a^{25} &\Rightarrow 13^2 \mid a^{25} + 39\end{aligned}$$

$$\begin{aligned}2 \nmid a &\Rightarrow 2 \nmid a^2 5\\ 2 \nmid 39 \wedge 2 \nmid a^{25} &\Rightarrow 2 \mid a^{25} - 39\end{aligned}$$

$$5 \mid 130 \wedge 5 \nmid (a^{182} - 26 : 130) \Rightarrow 5 \nmid a^{182} - 26$$

Caso $a \underset{(5)}{\equiv} 0$:

$$\begin{aligned}a \underset{(5)}{\equiv} 0 \Rightarrow a^{182} - 26 &\underset{(5)}{\equiv} 0^{182} - 26\\ \Leftrightarrow a^{182} - 26 &\underset{(5)}{\equiv} -26\\ \Leftrightarrow a^{182} - 26 &\underset{(5)}{\equiv} -1\\ \Leftrightarrow a^{182} - 26 &\underset{(5)}{\equiv} 4\\ a \underset{(5)}{\equiv} 0 \Rightarrow a^{25} - 39 &\underset{(5)}{\equiv} 0^{25} - 39\\ \Leftrightarrow a^{25} - 39 &\underset{(5)}{\equiv} -39\\ \Leftrightarrow a^{25} - 39 &\underset{(5)}{\equiv} -4\\ \Leftrightarrow a^{25} - 39 &\underset{(5)}{\equiv} 1\end{aligned}$$

es decir que, para $a \underset{(5)}{\equiv} 0$, $a^{25} - 39$ no es múltiplo de 5.

Caso $a \underset{(5)}{\equiv} 1$:

$$\begin{aligned}a \underset{(5)}{\equiv} 1 \Rightarrow a^{182} - 26 &\underset{(5)}{\equiv} 1^{182} - 26\\ \Leftrightarrow a^{182} - 26 &\underset{(5)}{\equiv} 1 - 1\\ \Leftrightarrow a^{182} - 26 &\underset{(5)}{\equiv} 0\end{aligned}$$

pero $5 \nmid a^{182} - 26$ por lo que $a \underset{(5)}{\not\equiv} 1$.

Caso $a \underset{(5)}{\equiv} 2$:

$$\begin{aligned}
a \underset{(5)}{\equiv} 2 \Rightarrow a^{182} - 26 &\underset{(5)}{\equiv} 2^{182} - 26 \\
\Leftrightarrow a^{182} - 26 &\underset{(5)}{\equiv} (2^2)^{91} - 1 \\
\Leftrightarrow a^{182} - 26 &\underset{(5)}{\equiv} 4^{90+1} - 1 \\
\Leftrightarrow a^{182} - 26 &\underset{(5)}{\equiv} (4^2)^{45} \cdot 4^1 - 1 \\
\Leftrightarrow a^{182} - 26 &\underset{(5)}{\equiv} 16^{45} \cdot 4 - 1 \\
\Leftrightarrow a^{182} - 26 &\underset{(5)}{\equiv} 1^{45} \cdot 4 - 1 \\
\Leftrightarrow a^{182} - 26 &\underset{(5)}{\equiv} 3 \\
a \underset{(5)}{\equiv} 2 \Rightarrow a^{25} - 39 &\underset{(5)}{\equiv} 2^{25} - 39 \\
\Leftrightarrow a^{25} - 39 &\underset{(5)}{\equiv} 2^{24+1} + 1 \\
\Leftrightarrow a^{25} - 39 &\underset{(5)}{\equiv} (2^2)^{12} \cdot 2 + 1 \\
\Leftrightarrow a^{25} - 39 &\underset{(5)}{\equiv} 4^{12} \cdot 2 + 1 \\
\Leftrightarrow a^{25} - 39 &\underset{(5)}{\equiv} (4^2)^{6} \cdot 2 + 1 \\
\Leftrightarrow a^{25} - 39 &\underset{(5)}{\equiv} 16^{6} \cdot 2 + 1 \\
\Leftrightarrow a^{25} - 39 &\underset{(5)}{\equiv} 1^{6} \cdot 2 + 1 \\
\Leftrightarrow a^{25} - 39 &\underset{(5)}{\equiv} 2 + 1 \\
\Leftrightarrow a^{25} - 39 &\underset{(5)}{\equiv} 3
\end{aligned}$$

es decir que, para $a \underset{(5)}{\equiv} 2$, $a^{25} - 39$ no es múltiplo de 5.

Caso $a \underset{(5)}{\equiv} 3$:

$$
\begin{aligned}
a \underset{(5)}{\equiv} 2 \Rightarrow a^{182} - 26 &\underset{(5)}{\equiv} 3^{182} - 26 \\
\Leftrightarrow a^{182} - 26 &\underset{(5)}{\equiv} (3^2)^{91} - 1 \\
\Leftrightarrow a^{182} - 26 &\underset{(5)}{\equiv} 9^{91} - 1 \\
\Leftrightarrow a^{182} - 26 &\underset{(5)}{\equiv} 4^{90+1} - 1 \\
\Leftrightarrow a^{182} - 26 &\underset{(5)}{\equiv} (4^2)^{45} \cdot 4^1 - 1 \\
\Leftrightarrow a^{182} - 26 &\underset{(5)}{\equiv} 16^{45} \cdot 4 - 1 \\
\Leftrightarrow a^{182} - 26 &\underset{(5)}{\equiv} 1^{45} \cdot 4 - 1 \\
\Leftrightarrow a^{182} - 26 &\underset{(5)}{\equiv} 4 - 1 \\
\Leftrightarrow a^{182} - 26 &\underset{(5)}{\equiv} 3 \\
a \underset{(5)}{\equiv} 2 \Rightarrow a^{25} - 39 &\underset{(5)}{\equiv} 3^{25} - 39 \\
\Leftrightarrow a^{25} - 39 &\underset{(5)}{\equiv} 3^{24+1} + 1 \\
\Leftrightarrow a^{25} - 39 &\underset{(5)}{\equiv} (3^2)^{12} \cdot 3 + 1 \\
\Leftrightarrow a^{25} - 39 &\underset{(5)}{\equiv} 9^{12} \cdot 3 + 1 \\
\Leftrightarrow a^{25} - 39 &\underset{(5)}{\equiv} 4^{12} \cdot 3 + 1 \\
\Leftrightarrow a^{25} - 39 &\underset{(5)}{\equiv} (4^2)^{6} \cdot 3 + 1 \\
\Leftrightarrow a^{25} - 39 &\underset{(5)}{\equiv} (16)^{6} \cdot 3 + 1 \\
\Leftrightarrow a^{25} - 39 &\underset{(5)}{\equiv} (1)^{6} \cdot 3 + 1 \\
\Leftrightarrow a^{25} - 39 &\underset{(5)}{\equiv} 3 + 1 \\
\Leftrightarrow a^{25} - 39 &\underset{(5)}{\equiv} 4
\end{aligned}
$$

es decir que, para $a \underset{(5)}{\equiv} 3$, $a^{25} - 39$ no es múltiplo de 5.

Caso $a \underset{(5)}{\equiv} 4$:

$$\begin{aligned}
a \underset{(5)}{\equiv} 2 \Rightarrow a^{182} - 26 &\underset{(5)}{\equiv} 4^{182} - 26 \\
\Leftrightarrow a^{182} - 26 &\underset{(5)}{\equiv} (4^2)^{91} - 1 \\
\Leftrightarrow a^{182} - 26 &\underset{(5)}{\equiv} 16^{91} - 1 \\
\Leftrightarrow a^{182} - 26 &\underset{(5)}{\equiv} 1^{91} - 1 \\
\Leftrightarrow a^{182} - 26 &\underset{(5)}{\equiv} 0
\end{aligned}$$

pero $5 \nmid a^{182} - 26$ por lo que $a \underset{(5)}{\not\equiv} 4$.

Entonces, cualquiera sea el a, siempre que cumpla $(a^{182} - 26 : 130) = 13$, se que $5 \nmid a^{182} - 26$. Finalmente, dadas las siguientes condiciones,

$$\begin{gathered}
2 \mid 2 \cdot 5^3 \cdot 13^2 \wedge 2 \mid a^{25} - 39 \\
5 \mid 2 \cdot 5^3 \cdot 13^2 \wedge 5 \nmid a^{25} - 39 \\
13 \mid 2 \cdot 5^3 \cdot 13^2 \wedge 13 \mid a^{25} - 39 \\
13^2 \mid 2 \cdot 5^3 \cdot 13^2 \wedge 13^2 \nmid a^{25} - 39
\end{gathered}$$

es posible concluir que

$$\boxed{(a^{25} - 39 : 2 \cdot 5^3 \cdot 13^2) = 2 \cdot 13 = 26}$$

3. Para cada $n \in \mathbb{N}$, encuentre el resto de dividir por 7 a n^{3n}en términos de una congruencia apropiada de n.

- Supongo $n \underset{(7)}{\equiv} 0$,

$$n^{3n} \underset{(7)}{\equiv} 0^{3n} \underset{(7)}{\equiv} 0$$
$$\Leftrightarrow$$
$$\boxed{n^{3n} \underset{(7)}{\equiv} 0}$$

- Supongo $n \underset{(7)}{\equiv} 1$,

$$n^{3n} \underset{(7)}{\equiv} 1^{3n} \underset{(7)}{\equiv} 1$$
$$\Leftrightarrow$$
$$\boxed{n^{3n} \underset{(7)}{\equiv} 1}$$

- Supongo $n \underset{(7)}{\equiv} 2$,

$$n^{3n} \underset{(7)}{\equiv} 2^{3n} \underset{(7)}{\equiv} \left(2^3\right)^n \underset{(7)}{\equiv} 8^n(7) \underset{(7)}{\equiv} 1^n \underset{(7)}{\equiv} 1$$
$$\Leftrightarrow$$
$$\boxed{n^{3n} \underset{(7)}{\equiv} 1}$$

- Supongo $n \underset{(7)}{\equiv} 3$,

$$n^{3n} \underset{(7)}{\equiv} 3^{3n} \underset{(7)}{\equiv} \left(3^3\right)^n \underset{(7)}{\equiv} 27^n \underset{(7)}{\equiv} 6^n$$
$$\Leftrightarrow$$
$$n^{3n} \underset{(7)}{\equiv} 6^n$$

...además,

$$n \underset{(7)}{\equiv} 3 \Rightarrow \exists k \in \mathbb{Z} : n = 7k + 3$$

...entonces, para algún $k \in \mathbb{Z}$,

$$n^{3n} \underset{(7)}{\equiv} 6^n = 6^{7k+3}$$
$$n^{3n} \underset{(7)}{\equiv} \left(6^7\right)^k * 6^3$$
$$n^{3n} \underset{(7)}{\equiv} \left(6 * \left(6^2\right)^3\right)^k * 6 * 6^2$$
$$n^{3n} \underset{(7)}{\equiv} 6^k * \left(36^3\right)^k * 6 * 36$$
$$n^{3n} \underset{(7)}{\equiv} 6^k * \left(1^3\right)^k * 6 * 1$$
$$n^{3n} \underset{(7)}{\equiv} 6^k * 1^k * 6$$
$$n^{3n} \underset{(7)}{\equiv} 6^k * 6$$
$$n^{3n} \underset{(7)}{\equiv} 6^{k+1}$$

$$\begin{cases} Caso: \ k \underset{(2)}{\equiv} 0 & \Leftrightarrow k+1 \underset{(2)}{\equiv} 1 \quad \Leftrightarrow n = 7k+3 \underset{(2)}{\equiv} 3 \underset{(2)}{\equiv} 1 \\ & \Rightarrow n^{3n} \underset{(7)}{\equiv} 6^{k+1} \\ & \cdots \underset{(7)}{\equiv} 6^k * 6 \\ & \cdots \underset{(7)}{\equiv} (6^2)^{k/2} * 6 \\ & \cdots \underset{(7)}{\equiv} 1^k * 6 \\ & \cdots \underset{(7)}{\equiv} 6 \\ \\ Caso: \ k \underset{(2)}{\equiv} 1 & \Leftrightarrow k+1 \underset{(2)}{\equiv} 0 \quad \Leftrightarrow n = 7k+3 \underset{(2)}{\equiv} 7+3 \underset{(2)}{\equiv} 0 \\ & \Rightarrow n^{3n} \underset{(7)}{\equiv} 6^{k+1} \\ & \cdots \underset{(7)}{\equiv} (6^2)^{(k+1)/2} \\ & \cdots \underset{(7)}{\equiv} 1^{(k+1)/2} \\ & \cdots \underset{(7)}{\equiv} 1 \end{cases}$$

$$\boxed{\begin{array}{c} n \underset{(2)}{\equiv} 0 \Rightarrow n^{3n} \underset{(7)}{\equiv} 1 \\ n \underset{(2)}{\equiv} 1 \Rightarrow n^{3n} \underset{(7)}{\equiv} 6 \end{array}}$$

- Supongo $n \equiv 4(7)$,

$$n^{3n} \equiv 4^{3n} \equiv (4^3)^n \equiv 64^n \equiv 1^n \equiv 1(7)$$

$$\Leftrightarrow$$

$$\boxed{n^{3n} \equiv 1(7)}$$

- Supongo $n \underset{(7)}{\equiv} 5$,

$$n^{3n} \underset{(7)}{\equiv} 5^{3n} \underset{(7)}{\equiv} (5^3)^n \underset{(7)}{\equiv} 125^n \underset{(7)}{\equiv} 6^n$$

$$\Leftrightarrow$$

$$n^{3n} \underset{(7)}{\equiv} 6^n$$

...además,

$$n \underset{(7)}{\equiv} 5 \Rightarrow \exists k \in \mathbb{Z} : n = 7k+5$$

...entonces, para algún $k \in \mathbb{Z}$,

$$\begin{aligned}
n^{3n} &\underset{(7)}{\equiv} 6^n \\
n^{3n} &\underset{(7)}{\equiv} 6^{7k+5} \\
n^{3n} &\underset{(7)}{\equiv} \left(6^7\right)^k * 6^5 \\
n^{3n} &\underset{(7)}{\equiv} \left(6 * \left(6^2\right)^3\right)^k * 6 * \left(6^2\right)^2 \\
n^{3n} &\underset{(7)}{\equiv} 6^k * \left(36^3\right)^k * 6 * 36^2 \\
n^{3n} &\underset{(7)}{\equiv} 6^k * \left(1^3\right)^k * 6 * 1^2 \\
n^{3n} &\underset{(7)}{\equiv} 6^k * 1^k * 6 \\
n^{3n} &\underset{(7)}{\equiv} 6^k * 6 \\
n^{3n} &\underset{(7)}{\equiv} 6^{k+1}
\end{aligned}$$

$$\begin{cases}
Caso: \ k \underset{(2)}{\equiv} 0 \quad \Leftrightarrow k+1 \underset{(2)}{\equiv} 1 \quad \Leftrightarrow n = 7k+5 \underset{(2)}{\equiv} 5 \underset{(2)}{\equiv} 1 \\
\qquad\qquad\qquad\qquad \Rightarrow n^{3n} \underset{(7)}{\equiv} 6 \\
\\
Caso: \ k \underset{(2)}{\equiv} 1 \quad \Leftrightarrow k+1 \underset{(2)}{\equiv} 0 \quad \Leftrightarrow n = 7k+5 \underset{(2)}{\equiv} 7+5 \underset{(2)}{\equiv} 0 \\
\qquad\qquad\qquad\qquad \Rightarrow n^{3n} \underset{(7)}{\equiv} 1
\end{cases}$$

$$\boxed{\begin{array}{c} n \underset{(2)}{\equiv} 0 \Rightarrow n^{3n} \underset{(7)}{\equiv} 1 \\ n \underset{(2)}{\equiv} 1 \Rightarrow n^{3n} \underset{(7)}{\equiv} 6 \end{array}}$$

- Supongo $n \equiv 6(7)$,

$$\begin{gathered}
n^{3n} \equiv 6^{3n} \equiv \left(6^3\right)^n \equiv 216^n \equiv 6^n(7) \\
\Leftrightarrow \\
n^{3n} \equiv 1(7)
\end{gathered}$$

...además,

$$n \underset{(7)}{\equiv} 6 \Rightarrow \exists k \in \mathbb{Z} : n = 7k+6$$

...entonces, para algún $k \in \mathbb{Z}$,

$$\begin{aligned}
n^{3n} &\underset{(7)}{\equiv} 6^n \\
n^{3n} &\underset{(7)}{\equiv} 6^{7k+6} \\
n^{3n} &\underset{(7)}{\equiv} \left(6^7\right)^k * 6^6 \\
n^{3n} &\underset{(7)}{\equiv} \left(6 * \left(6^2\right)^3\right)^k * \left(6^2\right)^3 \\
n^{3n} &\underset{(7)}{\equiv} 6^k * \left(36^3\right)^k * 36^3 \\
n^{3n} &\underset{(7)}{\equiv} 6^k * \left(1^3\right)^k * 1^3 \\
n^{3n} &\underset{(7)}{\equiv} 6^k * 1^k \\
n^{3n} &\underset{(7)}{\equiv} 6^k
\end{aligned}$$

$$
\begin{cases}
Caso: \; k \underset{(2)}{\equiv} 0 & \Leftrightarrow k+1 \underset{(2)}{\equiv} 1 & \Leftrightarrow n = 7k+6 \underset{(2)}{\equiv} 6 \underset{(2)}{\equiv} 0 \\
 & \Rightarrow n^{3n} & \underset{(7)}{\equiv} 6^k \\
 & \cdots & \underset{(7)}{\equiv} (6^2)^{k/2} \\
 & \cdots & \underset{(7)}{\equiv} 36^{k/2} \\
 & \cdots & \underset{(7)}{\equiv} 1^{k/2} \\
 & \cdots & \underset{(7)}{\equiv} 1 \\
Caso: \; k \underset{(2)}{\equiv} 1 & \Leftrightarrow k+1 \underset{(2)}{\equiv} 0 & \Leftrightarrow n = 7k+6 \underset{(2)}{\equiv} 7+6 \underset{(2)}{\equiv} 1 \\
 & \Rightarrow n^{3n} & \underset{(7)}{\equiv} 6^k \\
 & \cdots & \underset{(7)}{\equiv} 6^{k-1+1} \\
 & \cdots & \underset{(7)}{\equiv} 6^{k-1} * 6 \\
 & \cdots & \underset{(7)}{\equiv} 6^{2*(k-1)/2} * 6 \\
 & \cdots & \underset{(7)}{\equiv} (6^2)^{(k-1)/2} * 6 \\
 & \cdots & \underset{(7)}{\equiv} 36^{(k-1)/2} * 6 \\
 & \cdots & \underset{(7)}{\equiv} 1^{(k-1)/2} * 6 \\
 & \cdots & \underset{(7)}{\equiv} 1^{k/2} * 6 \\
 & \cdots & \underset{(7)}{\equiv} 6
\end{cases}
$$

$$
\boxed{\begin{array}{c} n \underset{(2)}{\equiv} 0 \Rightarrow n^{3n} \underset{(7)}{\equiv} 1 \\ n \underset{(2)}{\equiv} 1 \Rightarrow n^{3n} \underset{(7)}{\equiv} 6 \end{array}}
$$

4. Sea $f \in \mathbb{Q}[X]$ el polinomio $f = X^4 + X^3 + X^2 + X + 1$.

4.a. Pruebe que f es irreductible en $\mathbb{Q}[X]$.

Primero, voy a intentar reducir el polinomio por alguna de sus raíces enteras, utilizando el método de Gauss. El término independiente es 1, y el coeficiente principal es 1, por lo que las posibles raíces son 1 y -1.

$$\begin{aligned} f(1) &= 1^4 + 1^3 + 1^2 + 1 + 1 = 5 \\ f(-1) &= (-1)^4 + (-1)^3 + (-1)^2 + (-1) + 1 = \cancel{1-1} + \cancel{1-1} + 1 = 1 \end{aligned}$$

Como el polinomio no tiene raíces enteras, voy a intentar expresarlo de una forma que me quede más cómoda.

$$\begin{aligned} (X^4 + X^3 + X^2 + X + 1) &= (X^4 + X^3 + X^2 + X + 1) \cdot \frac{X-1}{X-1} \\ (X^4 + X^3 + X^2 + X + 1) &= \frac{X(X^4 + X^3 + X^2 + X + 1) - (X^4 + X^3 + X^2 + X + 1)}{X-1} \\ (X^4 + X^3 + X^2 + X + 1) &= \frac{(X^5 + X^4 + X^3 + X^2 + X) - (X^4 + X^3 + X^2 + X + 1)}{X-1} \\ (X^4 + X^3 + X^2 + X + 1) &= \frac{X^5 + (X^4 - X^4) + (X^3 - X^3) + (X^2 - X^2) + (X - X) - 1}{X-1} \\ (X^4 + X^3 + X^2 + X + 1) &= \frac{X^5 + \cancel{(X^4 - X^4)} + \cancel{(X^3 - X^3)} + \cancel{(X^2 - X^2)} + \cancel{(X - X)} - 1}{X-1} \\ (X^4 + X^3 + X^2 + X + 1) &= \frac{X^5 - 1}{X-1} \end{aligned}$$

$$(X^4 + X^3 + X^2 + X + 1) = \frac{X^5 - 1}{X-1}$$
$$\Rightarrow$$
$$(X^4 + X^3 + X^2 + X + 1) = 0 \Leftrightarrow \frac{X^5 - 1}{X-1} = 0$$

Luego, asumo $X_0 \neq 1 \Leftrightarrow (X-1) \neq 0$, y puedo despejar multiplicando por $(X-1)$ en ambos lados.

$$\begin{aligned} \frac{X^5 - 1}{X-1} \cdot (X-1) &= 0 \cdot (X-1) \\ \frac{X^5 - 1}{\cancel{X-1}} \cdot \cancel{(X-1)} &= 0 \cdot \cancel{(X-1)} \\ X^5 - 1 &= 0 \\ X^5 &= 1 \\ X &= \sqrt[5]{1} \end{aligned}$$

Por definición,

$$\begin{aligned} X = \sqrt[5]{1} &\Leftrightarrow X \in G_5 = \{e^{\frac{2k\pi}{5}i}, 0 \leq k < 5\} \\ X = \sqrt[5]{1} &\Leftrightarrow X \in \{e^{0i}, e^{\frac{2\pi}{5}i}, e^{\frac{4\pi}{5}i}, e^{\frac{6\pi}{5}i}, e^{\frac{8\pi}{5}i}\} \end{aligned}$$

entonces las raíces del polinomio son 5, y excepto $X_0 = e^{0i} = 1$ el resto pertenecen a $\mathbb{C}$ (puesto que la única raíz que no pertenecería a $\mathbb{C}$ es -1, y es fácil ver que $(-1)^5 \neq 1$).

Luego, como $(X^4+X^3+X^2+X+1)=\frac{X^5-1}{X-1}$, las raíces de f son las mismas que las de X^5-1, sin contar $X_0=1$. Y estas pertenecen a $\mathbb{C}$, por lo que no pertenecen a $\mathbb{Q}$, por lo que f no es divisible por ningún polinomio de grado 1 en $\mathbb{Q}$.

Para probar que f es irreducible en $\mathbb{Q}[X]$, basta con mostrar que f no tampoco es divisible por ningún polinomio de grado 2 o 3 en $\mathbb{Q}$. Dicho polinomio, si existe, debe ser producto por los polinomios de grado 1 formados con las raíces encontradas anteriormente.

Entonces dadas las raíces $Z_i=a+bi\neq 1, Z'_i=a'+b'i\neq 1$, sabemos que los polinomios $X-(a+bi)$ y $X-(a'+b'i)$ dividen a f, por lo que

$$(X-a-bi)\cdot(X-a'-b'i)=X^2-Xa'-Xb'i-aX+aa'+ab'i-biX+bia+bib'i$$
$$(X-a-bi)\cdot(X-a'-b'i)=X^2-a'X-b'iX-aX-biX+aa'+ab'i+bia+bib'i$$
$$(X-a-bi)\cdot(X-a'-b'i)=X^2+(-a'-a-b'i-bi)X+aa'+ab'i+bia+(-1)bb'$$
$$(X-a-bi)\cdot(X-a'-b'i)=X^2+(-(a'+a)-(b'i+bi))X+aa'+ab'i+bia-bb'$$

divide a f. Para ver que este polinomio no pertenece a $\mathbb{Q}[X]$, debemos mirar si los coeficientes pertenecen a $\mathbb{Q}[X]$. En particular, si miramos el coeficiente de grado 1, podemos notar que su parte imaginaria debería ser necesariamente igual a cero.

$$-(a'+a)-(b'i+bi)\in\mathbb{Q}\Leftrightarrow \mathfrak{Im}(-(a'+a)-(b'i+bi))=0$$
$$-(a'+a)-(b'i+bi)\in\mathbb{Q}\Leftrightarrow -(b'i+bi)=0\Leftrightarrow b'i+bi=0$$
$$-(a'+a)-(b'i+bi)\in\mathbb{Q}\Leftrightarrow b'i=-bi$$

Y dado que Z_i y Z'_i son raíces quintas de la unidad,

$$b'i=-bi\Leftrightarrow Z'_i=\overline{Z_i}$$

Siendo las raíces y sus conjugados,

$$Z_1=e^{\frac{2\pi}{5}i}\Rightarrow\overline{Z_1}=e^{\frac{-2\pi}{5}i}=e^{\frac{10\pi-2\pi}{5}i}=e^{\frac{8\pi}{5}i}=Z_4$$
$$Z_2=e^{\frac{4\pi}{5}i}\Rightarrow\overline{Z_2}=e^{\frac{-4\pi}{5}i}=e^{\frac{10\pi-4\pi}{5}i}=e^{\frac{6\pi}{5}i}=Z_3$$
$$Z_3=e^{\frac{6\pi}{5}i}\Rightarrow\overline{Z_3}=e^{\frac{-6\pi}{5}i}=e^{\frac{10\pi-6\pi}{5}i}=e^{\frac{4\pi}{5}i}=Z_2$$
$$Z_4=e^{\frac{8\pi}{5}i}\Rightarrow\overline{Z_4}=e^{\frac{-8\pi}{5}i}=e^{\frac{10\pi-8\pi}{5}i}=e^{\frac{2\pi}{5}i}=Z_1$$

los posibles valores para Z_i y Z'_i son

$$\begin{cases} Z_i=Z_1\wedge Z'_i=Z_4\\ Z_i=Z_2\wedge Z'_i=Z_3\end{cases}$$

Quiero ver si $(X-Z_1)(X-Z_4)\in\mathbb{Q}[X]$ o $(X-Z_2)(X-Z_3)\in\mathbb{Q}[X]$.

$$(X-Z_1)(X-Z_4)\in\mathbb{Q}[X]\Leftrightarrow a_1,b_1,c_1\in Q,(X-Z_1)(X-Z_4)=a_1X^2+b_1X+c_1$$
$$(X-Z_2)(X-Z_3)\in\mathbb{Q}[X]\Leftrightarrow a_2,b_2,c_2\in Q,(X-Z_2)(X-Z_3)=a_2X^2+b_2X+c_2$$

$$a_1X^2+b_1X+c_1=(X-z_1)(X-z_4)$$
$$a_1X^2+b_1X+c_1=X^2+X(-z_4)-z_1X-z_1(-z_4)$$
$$a_1X^2+b_1X+c_1=X^2+(-z_4-z_1)X+z_1\cdot z_4$$

Entonces, $a_1,b_1,c_1\in\mathbb{Q}\Leftrightarrow a_1=1\ \wedge\ b_1=-(z_4+z_1)\ \wedge\ c_1=z_1\cdot z_4$. Luego, $a_1\in\mathbb{Q}$ trivialmente, y b_1 ya vimos que también está en $\mathbb{Q}$. Pero c_1 es el producto de dos números complejos, y sabemos que $c_1\in\mathbb{Q}\Leftrightarrow\mathfrak{Im}(c_1)=0$ o, lo que es lo mismo, si el argumento de c_1 es 0, es decir, si $arg(z_1\cdot z_4)=0$. Pero $arg(z_1\cdot z_4)=arg(z_1)+arg(z_4)$

En este punto me cansé...

Sea $f \in \mathbb{Q}[X]$ el polinomio $f = X^4 + X^3 + X^2 + X + 1$.
Pruebe que f es irreductible en $\mathbb{Q}[X]$.

Sean z_1, z_2, z_3 y z_4 las raíces del polinomio f, tal que

$$X^4 + X^3 + X^2 + X + 1 = (a_1x - z_1)(a_2x - z_2)(a_3x - z_3)(a_4x - z_4)$$

Distribuyendo los factores,

$$(a_1x - z_1)(a_2x - z_2)(a_3x - z_3)(a_4x - z_4) = a_1a_2a_3a_4x^4 \cdots + (z_1z_2z_3z_4)$$

es fácil ver que el término independiente está dado por $(z_1z_2z_3z_4)$, de lo que se desprende que

$$\begin{aligned} a_1a_2a_3a_4x^4 \cdots + (z_1z_2z_3z_4) &= X^4 + X^3 + X^2 + X + 1 \\ (z_1z_2z_3z_4) &= 1 \end{aligned}$$

4.b. Para cada número natural n calcule $(f : X^n - 1)$.

4.c. Pruebe que si $p \in \mathbb{Q}[X]$ tiene como raíz a alguna raíz quinta primitiva de la unidad, entonces todas las raíces quintas primitivas de la unidad son raíces de p