Álgebra I - Final

Leandro Ezequiel Barrios

28/07/2015

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: $\forall a \in A,\ a\mathfrak{R}a$

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

  Luego, $a\mathfrak{R}a$, entonces $\mathfrak{R}$ es reflexiva.

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

$$\begin{aligned} n\mathfrak{R}m &\Leftrightarrow (n : m) \neq 1 \\ (n : m) \neq 1 \quad &\Leftrightarrow \quad (m : n) \neq 1 \\ (m : n) \neq 1 &\Leftrightarrow m\mathfrak{R}n \end{aligned}$$

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

- Antisimetría: $\forall n, m \in A,\ n\mathfrak{R}m \wedge m\mathfrak{R}n \Rightarrow n = m$
  Basta con encontrar un contraejemplo para ver que $\mathfrak{R}$ no es antisimétrica.

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

  $10\mathfrak{R}20 \wedge 20\mathfrak{R}10$, 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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

...además,

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

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

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

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

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

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

$$n^{3n} \equiv 4^{3n} \equiv \left(4^3\right)^n \equiv 64^n \equiv 1^n \equiv 1(7)$$
$$\Leftrightarrow$$
$$\boxed{n^{3n} \equiv 1(7)}$$

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

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

...además,

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

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

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

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

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

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

$$n^{3n} \equiv 6^{3n} \equiv (6^3)^n \equiv 216^n \equiv 6^n(7)$$

$$\Leftrightarrow$$

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

...además,

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

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

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

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

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

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 $\mathbb{Q}[X]$.

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