Álgebra I - Verano 2020
Resolución Segundo Parcial (13/03/2020)

Ejercicio 1. Hallar todos los $n \in \mathbb{N} \cup \{0\}$ tales que

$$2^{2^n+1} + 10^{368} + 2^4 \equiv 4 \ (mod\ 34)$$

Solución:

Como $34 = 2 \cdot 17$ y $(2 : 17) = 1$ podemos quebrar la ecuación en congruencia dada en dos cuyos módulos sean primos distintos (y, entre otras cosas, nos permitan usar en cada una el Pequeño Teorema de Fermat).
Luego:

$$2^{2^n+1} + 10^{368} + 2^4 \equiv 4 \ (mod\ 34) \underset{2\perp 17}{\iff} \begin{cases} 2^{2^n+1} + 10^{368} + 2^4 \equiv 4 \ (mod\ 2) \\ 2^{2^n+1} + 10^{368} + 2^4 \equiv 4 \ (mod\ 17) \end{cases}$$

- Empecemos mirando la ecuación módulo 2:
  Dado $n \in \mathbb{N} \cup \{0\}$, se tiene que $2^n + 1 \geq 1$ y luego $2|2^{2^n+1}$. A su vez, sabemos que $2|10^{368}$, $2|2^4$ y $2|4$. Así, cada sumando es divisible por 2, es decir, es congruente a 0 módulo 2. Luego:

  $$2^{2^n+1} + 10^{368} + 2^4 \equiv 4 \ (mod\ 2) \iff 0 + 0 + 0 \equiv 0 \ (mod\ 2)$$

  Como esta última condición vale para todo $n \in \mathbb{N} \cup \{0\}$, se sigue que la primera ecuación que debíamos resolver vale para cualquier $n \in \mathbb{N} \cup \{0\}$.
  A partir de esto, deducimos que:

  $$2^{2^n+1} + 10^{368} + 2^4 \equiv 4 \ (mod\ 34) \iff 2^{2^n+1} + 10^{368} + 2^4 \equiv 4 \ (mod\ 17)$$

- Veamos ahora la ecuación módulo 17:
  Empecemos por reducir lo más posible la cantidad de sumandos. Como 17 es primo y $(10 : 17) = 1$, por el Pequeño Teorema de Fermat, se tiene que $10^{16} \equiv 1 \ (mod\ 17)$.
  Luego, como $368 = 16 \cdot 23$, se deduce que $10^{368} = (10^{16})^{23} \equiv 1 \ (mod\ 17)$.
  Así, $2^{2^n+1} + 10^{368} + 2^4 \underset{(17)}{\equiv} 2^{2^n+1} + 1 + 16 = 2^{2^n+1} + 17 \underset{(17)}{\equiv} 2^{2^n+1} + 0 = 2^{2^n+1}$, y luego:

  $$2^{2^n+1} + 10^{368} + 2^4 \equiv 4 \ (mod\ 17) \iff 2^{2^n+1} \equiv 4 \ (mod\ 17)$$

  Reescribamos $2^{2^n+1} = 2 \cdot 2^{2^n}$ y $4 = 2 \cdot 2$, y como $(2 : 17) = 1$ podemos multiplicar por el inverso multiplicativo del 2 (que se ve fácil que aquí es 9) en ambos miembros de la congruencia y así cancelar un factor 2:

  $$2 \cdot 2^{2^n} \equiv 2 \cdot 2 \ (mod\ 17) \underset{2\perp 17}{\iff} 2^{2^n} \equiv 2 \ (mod\ 17)$$

  Como 17 es primo y $(2 : 17) = 1$, por el Pequeño Teorema de Fermat, se tiene que $2^{16} \equiv 1 \ (mod\ 17)$.
  Por otro lado, por algoritmo de división existe $k_n \in \mathbb{Z}$ tal que $2^n = 16k_n + r_{16}(2^n)$.
  Se tiene entonces que $2^{2^n} = 2^{16k_n + r_{16}(2^n)} = (2^{16})^{k_n} \cdot 2^{r_{16}(2^n)} \underset{(17)}{\equiv} 1 \cdot 2^{r_{16}(2^n)} = 2^{r_{16}(2^n)}$ y así:

  $$2^{2^n} \equiv 2 \ (mod\ 17) \iff 2^{r_{16}(2^n)} \equiv 2 \ (mod\ 17)$$

  Como $16 = 2^4$, si $n \geq 4$ se tiene que $16 = 2^4 \ | 2^n$. Así, $r_{16}(2^n) = 0$ para todo $n \geq 4$ y luego, $2^{r_{16}(2^n)} = 2^0 = 1 \not\equiv 2 \ (mod\ 17)$. Esto prueba que **ningún $n \geq 4$ es solución** .
  Sólo resta ver a mano los casos con $n \in \{0; 1; 2, 3\}$:

  - Si $n = 0$:
    $2^{2^0} = 2^1 = 2 \equiv 2 \ (mod\ 17) \implies n = 0$ es solución.
  - Si $n = 1$:
    $2^{2^1} = 2^2 = 4 \not\equiv 2 \ (mod\ 17) \implies n = 1$ **no** es solución.

- Si $n = 2$:
  $2^{2^2} = 2^4 = 16 \not\equiv 2 \ (mod\ 17) \Longrightarrow n = 2$ **no** es solución.
- Si $n = 3$:
  $2^{2^3} = 2^8 = 256 \underset{(17)}{\equiv} 1 \not\equiv 2 \ (mod\ 17) \Longrightarrow n = 3$ **no** es solución.

Así, $n = 0$ es la única solución.

Ejercicio 2. En un depósito se almacenan latas de gaseosa. El viernes por la noche, un empleado realizó un control de inventario y observó que:

- Al poner las latas en cajas de 12 unidades sobraban 4.
- Al poner las latas en cajas de 63 unidades sobraban 43.
- No tomó nota de la cantidad exacta pero recuerda que había por lo menos 12.600 latas y no más de 13.000.

¿Cuántas latas de gaseosa había en el depósito el viernes a la noche?

Solución:
Llamemos X a la cantidad de latas de gaseosas que había en el depósito el viernes a la noche.

- *"Al poner las latas en cajas de 12 unidades sobraban 4"* nos dice que $r_{12}(X) = 4$. Así, $X \equiv 4 \ (mod\ 12)$.
- *"Al poner las latas en cajas de 63 unidades sobraban 43"* nos dice que $r_{63}(X) = 43$. Luego, $X \equiv 43 \ (mod\ 63)$.
- *"[...] Recuerda que había por lo menos 12.600 latas y no más de 13.000"* nos dice que $12.600 \leq X \leq 13.000$.

Debemos resolver entonces el siguiente sistema de ecuaciones en congruencia:

$$\begin{cases} X \equiv 4 \ (mod\ 12) \\ X \equiv 43 \ (mod\ 63) \end{cases}$$

Y luego quedarnos sólo con las soluciones X que satisfacen $12.600 \leq X \leq 13.000$.
Como los módulos en el sistema no son coprimos dos a dos, no podemos garantizar la existencia de solución mediante el Teorema Chino del Resto. Por tal motivo, primero quebramos el sistema en ecuaciones que permiten analizar posibles redundancias e incompatibilidades.

- Como $12 = 3 \cdot 4$ y $(3 : 4) = 1$, se tiene que:

$$X \equiv 4 \ (mod\ 12) \underset{3 \perp 4}{\Longleftrightarrow} [X \underset{(3)}{\equiv} 4 \equiv 1 \ (mod\ 3) \wedge X \underset{(4)}{\equiv} 4 \equiv 0 \ (mod\ 4)]$$

- Como $63 = 7 \cdot 9$ y $(7 : 9) = 1$, se tiene que:

$$X \equiv 43 \ (mod\ 63) \underset{7 \perp 9}{\Longleftrightarrow} [X \underset{(7)}{\equiv} 43 \equiv 1 \ (mod\ 7) \wedge X \underset{(9)}{\equiv} 43 \equiv 7 \ (mod\ 9)]$$

Así, nuestro sistema original es equivalente al sistema:

$$\begin{cases} X \equiv 1 \ (mod\ 3) \\ X \equiv 0 \ (mod\ 4) \\ X \equiv 1 \ (mod\ 7) \\ X \equiv 7 \ (mod\ 9) \end{cases}$$

De aquí vemos que la primera y la cuarta ecuación son las únicas que podrían ocasionar que haya una incompatibilidad. Analicemos esto:
Sabiendo que $X \equiv 1 \ (mod\ 3)$, ¿qué podemos decir de X módulo 9?
Por algoritmo de división existe $k \in \mathbb{Z}$ tal que $X = 9k + r_9(X)$. Luego, analizando congruencia módulo 3:
$1 \underset{(3)}{\equiv} X = 9k + r_9(X) \underset{(3)}{\equiv} r_9(X) \Longleftrightarrow r_9(X) = 1, 4$ o 7.
Esto nos dice que:

$X \equiv 1\ (mod\ 3) \iff [X \equiv 1\ (mod\ 9) \vee X \equiv 4\ (mod\ 9) \vee X \equiv 7\ (mod\ 9)]$
A partir de esto, vemos que en nuestro sistema anterior

$$\begin{cases} X \equiv 1\ (mod\ 3) \iff [X \equiv 1\ (mod\ 9) \vee X \equiv 4\ (mod\ 9) \vee X \equiv 7\ (mod\ 9)] \\ X \equiv 0\ (mod\ 4) \\ X \equiv 1\ (mod\ 7) \\ X \equiv 7\ (mod\ 9) \end{cases}$$

la cuarta ecuación implica la primera, y por lo tanto este último sistema es equivalente al sistema:

$$\begin{cases} X \equiv 0\ (mod\ 4) \\ X \equiv 1\ (mod\ 7) \\ X \equiv 7\ (mod\ 9) \end{cases}$$

Aquí, todos los módulos son coprimos 2 a 2 y entonces, por el Teorema Chino del Resto, sabemos que existe (única) solución módulo $252 = 4 \cdot 7 \cdot 9$.

- Como $X \equiv 0\ (mod\ 4)$, entonces existe $m \in \mathbb{Z}$ tal que $X = 4m$.
- A partir de que $X = 4m$, se sigue que $X \equiv 1\ (mod\ 7)$ si y sólo si $4m \equiv 1\ (mod\ 7)$, y como $(2 : 7) = 1$, podemos multiplicar por 2 ambos miembros de la congruencia y que la ecuación obtenida sea equivalente a la original. Esto es: $4m \equiv 1\ (mod\ 7) \underset{2 \perp 7}{\iff} 8m \equiv 2\ (mod\ 7) \underset{\substack{8 \equiv 1 \\ (7)}}{\iff} m \equiv 2\ (mod\ 7)$.

  Luego, como $m \equiv 2\ (mod\ 7)$, existe $s \in \mathbb{Z}$ tal que $m = 7s + 2$ y entonces $X = 4m = 4(7s + 2) = 28s + 8$.
- A partir de que $X = 28s + 8$, se sigue que $X \equiv 7\ (mod\ 9)$ si y sólo si $28s + 8 \equiv 7\ (mod\ 9)$, es decir, $28s \underset{(9)}{\equiv} 7 - 8 = -1 \equiv 8\ (mod\ 9)$, y como $28 \equiv 1\ (mod\ 9)$, concluimos que $s \underset{(9)}{\equiv} 28s \equiv 8\ (mod\ 9)$.
  Luego, como $s \equiv 8\ (mod\ 9)$, existe $t \in \mathbb{Z}$ tal que $s = 9t + 8$ y entonces

$$X = 28s + 8 = 28(9t + 8) + 8 = 252t + 232.$$

Así, el conjunto de soluciones del sistema original es: $\{X \in \mathbb{Z}\ / X = 252t + 232,\ k \in \mathbb{Z}\}$.
Ahora sólo resta buscar las soluciones X que satisfacen la relación $12.600 \leq X \leq 13.000$. Para ello, debemos resolver la inecuación $12.600 \leq 252t + 232 \leq 13.000$ para valores de $t \in \mathbb{Z}$. De aquí se obtiene que sólo $t = 50$ cumple, y entonces $X = 252 \cdot 50 + 232 =$12.832.

El viernes por la noche había 12.832 latas de gaseosa en el depósito.

Ejercicio 3. Sean $z \in G^*_{127}$ una raíz 127- ésima primitiva de la unidad, $w \in G^*_{89}$ una raíz 89- ésima primitiva de la unidad. Probar que $zw \in G^*_{11.303}$, es decir, zw es una raíz 11.303 - ésima primitiva de la unidad.

Solución:
Empecemos por observar que $11.303 = 127 \cdot 89$ y que 127 y 89 son ambos números primos.
Primero veremos que $zw \in G_{11.303}$ y luego probaremos que, efectivamente, zw es una raíz 11.303 primitiva de la unidad.

- $zw \in G_{11.303}$:
  Sabemos que $z \in G^*_{127}$ y que $w \in G^*_{89}$. En particular, esto nos dice que $z^{127} = 1$ y que w^{89}. Debemos ver que $(zw)^{11.303} = 1$. En efecto, $(zw)^{11.303} = (zw)^{127 \cdot 89} = z^{127 \cdot 89} \cdot w^{127 \cdot 89} = (z^{127})^{89} \cdot (w^{89})^{127} = 1 \cdot 1 = 1$, como queríamos ver.
- zw es una raíz 11.303 primitiva de la unidad:
  Recordemos que tenemos la siguiente igualdad de conjuntos:

$$G_{11.303} = \bigcup_{\substack{k | 11.303 \\ k > 0}}^{D} G^*_k$$

  Denotaremos " $\sqcup$ " a la unión disjunta recién mencionada.
  Como $11.303 = 127 \cdot 89$ y ambos factores son primos, se tiene que los divisores positivos de 11.303 son $\{1;\ 89;\ 127;\ 11.303\}$, y entonces:

$$G_{11.303} = G^*_{11.303} \sqcup G^*_{127} \sqcup G^*_{89} \sqcup G^*_1$$

Como ya probamos que $zw \in G_{11.303}$, ya sabemos que zw pertenece a la unión disjunta de esos 4 conjuntos. Para ver que efectivamente $zw \in G^*_{11.303}$, basta probar que $zw \notin G^*_{127}$, $zw \notin G^*_{89}$ y $zw \notin G^*_1$.

- $zw \notin G^*_1 = \{1\}$:
  Supongamos que $zw \in \{1\}$, es decir, $zw = 1$. De aquí se deduce que $z = w^{-1}$.
  Como $w \in G_{89}$, se tiene entonces también que $w^{-1} \in G_{89}$. Luego, $z \in G_{127}$ y $z = w^{-1} \in G_{89}$, es decir, $z \in G_{127} \cap G_{89} = G_{(127:89)} = G_1 = \{1\}$. Concluimos entonces que $z = 1$, pero esto contradice el hecho de que z es una raíz 127- ésima primitiva de la unidad (ya que esto último, en particular, implica que $z \neq 1$).
  La contradicción proviene de suponer que $zw \in G^*_1$, con lo cual $zw \notin G^*_1$.
- $zw \notin G^*_{89}$:
  Supongamos que $zw \in G^*_{89}$. En particular, esto implica que $zw \in G_{89}$, es decir, $(zw)^{89} = 1$.
  Así, $1 = (zw)^{89} = z^{89} \cdot w^{89} \underset{w \in G_{89}}{=} z^{89} \cdot 1 = z^{89} \Longrightarrow z \in G_{89}$.
  Luego, $z \in G_{127}$ y $z \in G_{89}$, es decir, $z \in G_{127} \cap G_{89} = G_{(127:89)} = G_1 = \{1\}$, y llegamos a la misma contradicción que en el ítem anterior.
  Concluimos entonces que $zw \notin G^*_{89}$.
- $zw \notin G^*_{127}$:
  Supongamos que $zw \in G^*_{127}$. En particular, esto implica que $zw \in G_{127}$, es decir, $(zw)^{127} = 1$.
  Así, $1 = (zw)^{127} = z^{127} \cdot w^{127} \underset{z \in G_{127}}{=} 1 \cdot w^{127} = w^{127} \Longrightarrow w \in G_{127}$.
  Luego, $w \in G_{89}$ y $w \in G_{127}$, es decir, $w \in G_{89} \cap G_{127} = G_{(89:127)} = G_1 = \{1\}$, y llegamos a una contradicción análoga a la del ítem anterior (ya que w es una raíz 89-ésima primitiva de la unidad).
  Concluimos entonces que $zw \notin G^*_{127}$.

Habiendo descartado los tres casos que dijimos, queda entonces demostrado lo enunciado.

Ejercicio 4. Calcular el resto de dividir a

$$f = X^{2811} + X^{1324} - 5X^{563} - 3X^{444} - 2X^{22} + 22X^2 + 1$$

por $g = X^2 - 2iX - 1$ en $\mathbb{C}[X]$.

Solución:

Por algoritmo de división en $\mathbb{C}[X]$, existen únicos polinomios $q, r \in \mathbb{C}[X]$ tales que $f = g \cdot q + r$ con $r = 0$ o $gr(r) < gr(g)$. Como $gr(g) = 2$, concluimos que o bien $r = 0$, o bien $gr(r) = 0$ o 1. Así, $r = aX + b$ para ciertos $a, b \in \mathbb{C}$ (eventualmente podrían ser a = 0, b = 0). De forma similar a lo visto en clase, a partir del Teorema del Resto, queremos conseguir valores donde evaluar f que nos permitan recuperar información de los coeficientes de r. Esto es: necesitamos buscar las raíces de g.
El polinomio g es de grado 2 con coeficientes complejos, por lo cual podemos buscar sus raíces mediante la fórmula resolvente para ecuaciones de segundo grado (con el cuidado de que estamos trabajando con números complejos!). Al hacer esto, obtenemos una única raíz doble: $X = i$.
A partir de esto, podemos factorizar al polinomio g como $g = (X - i)^2$. Luego, la escritura del algoritmo de división nos queda: $f = (X - i)^2 \cdot q + (aX + b)$.
Evaluando esta expresión en $X = i$ obtenemos que:
$f(i) = (i - i)^2 \cdot q(i) + (ai + b) = ai + b$.

- Calculemos $f(i)$:
  Para esto, recordemos que como $i^4 = 1$, se tiene que $i^k = i^{r_4(k)}$, para todo $k \in \mathbb{Z}$. Luego:
  $f(i) = i^{2811} + i^{1324} - 5i^{563} - 3i^{444} - 2i^{22} + 22i^2 + 1$
  $= i^3 + i^0 - 5i^3 - 3i^0 - 2i^2 + 22i^2 + 1$
  $= -i + 1 + 5i - 3 + 2 - 22 + 1$
  $= -21 + 4i$
  Luego, $-21 + 4i = f(i) = ai + b \Longrightarrow ai + b = -21 + 4i$.

Como no tenemos una raíz distinta a la que usamos recién para conseguir la última ecuación, no podemos evaluar f en otra raíz de g que nos permita conseguir más información del resto. Sin embargo, como i es raíz doble de g, sabemos que también lo será del polinomio derivado de g, que es $g' = 2(X - i)$. Por este motivo, derivamos f y su escritura vía algoritmo de división para conseguir otra relación:
$f = g \cdot q + r \Longrightarrow f' = g' \cdot q + g \cdot q' + r'$
Tenemos entonces que $f' = 2(X - i) \cdot q + (X - i)^2 \cdot q' + a = (X - i) \cdot [2 \cdot q + (X - i) \cdot q'] + a$.
Evaluando esta expresión en $X = i$ obtenemos que:
$f'(i) = (i - i) \cdot [2 \cdot q(i) + (i - i) \cdot q'(i)] + a = a$.

- Calculemos $f'(i)$:
  $f = X^{2811} + X^{1324} - 5X^{563} - 3X^{444} - 2X^{22} + 22X^2 + 1$
  $\implies f' = 2811X^{2810} + 1324X^{1323} - 2815X^{562} - 1332X^{443} - 44X^{21} + 44X$
  Evaluando en $X = i$:
  $f'(i) = 2811i^{2810} + 1324i^{1323} - 2815i^{562} - 1332i^{443} - 44i^{21} + 44i$
  $= 2811i^2 + 1324i^3 - 2815i^2 - 1332i^3 - 44i + 44i$
  $= -2811 - 1324i + 2815 + 1332i$
  $= 4 + 8i$
  Luego, $4 + 8i = f'(i) = a \implies a = 4 + 8i$.

Tenemos entonces el sistema de ecuaciones en $\mathbb{C}$:

$$\begin{cases} ai + b = -21 + 4i \\ a = 4 + 8i \end{cases}$$

del cual deducimos que $a = 4 + 8i$ y $b = -13$, por lo cual $r = (4 + 8i)X - 13$ es el resto que se obtiene de dividir a f por g.

Ejercicio 5. Sabiendo que el polinomio

$$f = X^6 - 2X^5 + 5X^4 + 3X^2 - 6X + 15$$

tiene una raíz en común con $g = X^4 + 4X^3 + 6X^2 + 4X + 65$, factorizar a f como producto de polinomios irreducibles en $\mathbb{C}[X]$, $\mathbb{R}[X]$ y $\mathbb{Q}[X]$.

Solución:
Como nos dicen que f y g tienen alguna raíz en común, al buscar el máximo común divisor entre f y g vía el algoritmo de Euclides, obtendremos seguro un factor no constante que divida a f (ya que esa raíz será raíz de $(f : g)$).
Previo a buscarlo, notemos que como f y g son ambos polinomios mónicos con coeficientes enteros, entonces $(f : g) \in \mathbb{Z}[X]$ (y ya sabemos que es mónico).
Haciendo las sucesivas divisiones del algoritmo de Euclides, conseguimos:

- $f = g \cdot (X^2 - 6X + 23) + (-60X^3 - 176X^2 + 292X - 1480)$.
- $g = (-60X^3 - 176X^2 + 292X - 1480) \cdot (-\frac{1}{60}X - \frac{4}{225}) + (-\frac{1741}{225}X^2 - \frac{3482}{225}X + \frac{1741}{45})$

Observemos que este último resto obtenido podemos escribirlo $-\frac{1741}{225}X^2 - \frac{3482}{225}X + \frac{1741}{45} = -\frac{1741}{225}(X^2 - 2X + 5)$.
Luego, seguiremos el algoritmo de Euclides con este polinomio mónico asociado al último resto obtenido:

- $-60X^3 - 176X^2 + 292X - 1480 = (X^2 - 2X + 5) \cdot (-60X - 296) + 0$.

Así, el polinomio $h = \frac{1741}{225}X^2 - \frac{3482}{225}X + \frac{1741}{45} = -\frac{1741}{225}(X^2 - 2X + 5)$ es el último resto no nulo obtenido en el Algoritmo de Euclides, y entonces $(f : g) = \frac{h}{cp(h)} = X^2 - 2X + 5$.
Dividimos ahora al polinomio f por $(f : g)$ y escribimos:
$f = (X^2 - 2X + 5) \cdot (X^4 + 3)$.

a) **Factorización en irreducibles en $\mathbb{C}[X]$:**

Sabemos que los polinomios irreducibles en $\mathbb{C}[X]$ son únicamente los de grado 1. Por tal motivo, y a partir de la correspondencia que tenemos entre factores mónicos de grado 1 y raíces de un polinomio, buscaremos las raíces en $\mathbb{C}$ de f.
Como tenemos que $f = (X^2 - 2X + 5) \cdot (X^4 + 3)$, para hallar las raíces en $\mathbb{C}$ de f debemos hallar las raíces de cada factor:

- Raíces de $h_1 = X^2 - 2X + 5$:
  Son las que se obtienen al resolver la ecuación cuadrática $X^2 - 2X + 5 = 0$ en $\mathbb{C}$. Las mismas son: $\{1 + 2i; 1 - 2i\}$. Así, podemos factorizar $h_1 = X^2 - 2X + 5 = [X - (1 + 2i)] \cdot [X - (1 - 2i)]$ en $\mathbb{C}[X]$.
- Raíces de $h_2 = X^4 + 3$:
  Son las que se obtienen al resolver en $\mathbb{C}$ la ecuación $X^4 + 3 = 0 \iff X^4 = -3$, es decir, buscamos las raíces cuartas del número complejo -3.
  A partir de que $|-3| = 3$, $arg(-3) = \pi$ y de lo visto para raíces n-ésimas de un número complejo dado, sabemos que las raíces buscadas son $\{X_k = \sqrt[4]{3} \cdot [\cos(\frac{\pi + 2k\pi}{4}) + i \operatorname{sen}(\frac{\pi + 2k\pi}{4})] \ / \ k \in \{0; 1; 2; 3\}\} = \{\frac{\sqrt[4]{12}}{2}(1 + i); \frac{\sqrt[4]{12}}{2}(1 - i); \frac{\sqrt[4]{12}}{2}(-1 - i); \frac{\sqrt[4]{12}}{2}(-1 + i)\}$.

Así, podemos factorizar en $\mathbb{C}[X]$:
$h_2 = X^4 + 3 = \left[X - \frac{\sqrt[4]{12}}{2}(1+i)\right] \cdot \left[X - \frac{\sqrt[4]{12}}{2}(1-i)\right] \cdot \left[X - \frac{\sqrt[4]{12}}{2}(-1-i)\right] \cdot \left[X - \frac{\sqrt[4]{12}}{2}(-1+i)\right]$

De aquí tenemos entonces:
$f = (X^2 - 2X + 5) \cdot (X^4 + 3)$
$= [X - (1+2i)] \cdot [X - (1-2i)] \cdot \left[X - \frac{\sqrt[4]{12}}{2}(1+i)\right] \cdot \left[X - \frac{\sqrt[4]{12}}{2}(1-i)\right] \cdot \left[X - \frac{\sqrt[4]{12}}{2}(-1-i)\right] \cdot \left[X - \frac{\sqrt[4]{12}}{2}(-1+i)\right]$
factorización de f en irreducibles en $\mathbb{C}[X]$ (y son todos irreducibles por ser de grado 1).

b) **Factorización en irreducibles en $\mathbb{R}[X]$** :

Sabemos que los polinomios irreducibles en $\mathbb{R}[X]$ son únicamente los de grado 1 y los de grado 2 con raíces complejas no reales.
A partir de lo hecho para factorizar a f en $\mathbb{C}[X]$, tenemos que $f = (X^2 - 2X + 5) \cdot (X^4 + 3)$ y esta igualdad, en particular, vale en $\mathbb{R}[X]$.

- Como ya vimos que las raíces de $h_1 = X^2 - 2X + 5$ son $\{1+2i; 1-2i\}$, concluimos entonces que h_1 es irreducible en $\mathbb{R}[X]$ por ser de grado 2 y con raíces complejas no reales.
- Como $h_2 = X^4 + 3$ es un polinomio de grado 4, **seguro** que el polinomio h_2 no es irreducible en $\mathbb{R}[X]$.
  De nuevo, a partir de lo hecho en $\mathbb{C}[X]$, ya vimos que:
  $h_2 = X^4 + 3 = \underbrace{\left[X - \frac{\sqrt[4]{12}}{2}(1+i)\right] \cdot \left[X - \frac{\sqrt[4]{12}}{2}(1-i)\right]}_{= X^2 - \sqrt[4]{12}X + \frac{\sqrt{12}}{2}} \cdot \underbrace{\left[X - \frac{\sqrt[4]{12}}{2}(-1-i)\right] \cdot \left[X - \frac{\sqrt[4]{12}}{2}(-1+i)\right]}_{= X^2 + \sqrt[4]{12}X + \frac{\sqrt{12}}{2}}$
  $\implies h_2 = X^4 + 3 = \left(X^2 - \sqrt[4]{12}X + \frac{\sqrt{12}}{2}\right) \cdot \left(X^2 + \sqrt[4]{12}X + \frac{\sqrt{12}}{2}\right)$, y aquí ambos factores son irreducibles en $\mathbb{R}[X]$ por ser de grado 2 y con raíces complejas no reales.

De aquí tenemos entonces:
$f = (X^2 - 2X + 5) \cdot (X^4 + 3)$
$= \left(X^2 - 2X + 5\right) \cdot \left(X^2 - \sqrt[4]{12}X + \frac{\sqrt{12}}{2}\right) \cdot \left(X^2 + \sqrt[4]{12}X + \frac{\sqrt{12}}{2}\right)$
factorización de f en irreducibles en $\mathbb{R}[X]$ (y son todos irreducibles por ser de grado 2 con raíces complejas no reales).

c) **Factorización en irreducibles en $\mathbb{Q}[X]$** :

Sabemos que en $\mathbb{Q}[X]$ no podemos caracterizar cuáles son todos los polinomios irreducibles (y que, de hecho, existen polinomios irreducibles en $\mathbb{Q}[X]$ de cualquier grado positivo). Sin embargo, recordemos que en $\mathbb{Q}[X]$ siempre son irreducibles los polinomios de grado 1 y también los polinomios de grado 2 o 3 sin raíces en $\mathbb{Q}$.
A partir de lo hecho para factorizar a f en $\mathbb{C}[X]$, tenemos que $f = (X^2 - 2X + 5) \cdot (X^4 + 3)$ y esta igualdad, en particular, vale en $\mathbb{Q}[X]$.

- Como ya vimos que las raíces de $h_1 = X^2 - 2X + 5$ son $\{1+2i; 1-2i\}$, concluimos entonces que h_1 es irreducible en $\mathbb{Q}[X]$ por ser de grado 2 y sin raíces en $\mathbb{Q}$.
- ¿Cómo podemos factorizar al polinomio $h_2 = X^4 + 3$ en $\mathbb{Q}[X]$? ¿Será irreducible en $\mathbb{Q}[X]$?
  Empecemos por observar que el polinomio $h_2 = X^4 + 3$ no tiene raíces racionales (y, de hecho, tampoco reales), ya que anteriormente buscamos sus raíces en $\mathbb{C}$ y obtuvimos que éstas son: $\left\{\frac{\sqrt[4]{12}}{2}(1+i); \frac{\sqrt[4]{12}}{2}(1-i); \frac{\sqrt[4]{12}}{2}(-1-i); \frac{\sqrt[4]{12}}{2}(-1+i)\right\}$ y ninguna de ellas pertenece a $\mathbb{Q}$ (ni a $\mathbb{R}$).
  Luego, al intentar factorizar $h_2 = X^4 + 3$ en $\mathbb{Q}[X]$, seguro no pueden aparecer factores de grado 1 en la factorización (ya que de haber alguno, automáticamente h_2 tendría una raíz en $\mathbb{Q}$).
  Supongamos que $h_2 = X^4 + 3$ es reducible en $\mathbb{Q}[X]$. Como $\text{gr}(h_2) = 4$ y ya vimos que h_2 no admite factores de grado 1, si h_2 fuese reducible, necesariamente debe factorizarse como $h_2 = q_1 \cdot q_2$ con $q_1, q_2 \in \mathbb{Q}[X]$ ambos mónicos y de grado 2. A su vez, como h_2 no tiene raíces en $\mathbb{R}$, se tiene que tanto q_1 como q_2 tampoco tienen raíces en $\mathbb{R}$.
  Luego, $q_1, q_2 \in \mathbb{Q}[X] \subseteq \mathbb{R}[X]$ son ambos de grado 2 y sin raíces rales, por lo cual q_1, q_2 son irreducibles en $\mathbb{R}[X]$.
  Pero entonces, a partir de lo hecho para factorizar a f en $\mathbb{R}[X]$, tenemos:
  $\underbrace{q_1}_{\in \mathbb{Q}[X]} \cdot \underbrace{q_2}_{\in \mathbb{Q}[X]} = X^4 + 3 = \underbrace{(X^2 - \sqrt[4]{12}X + \frac{\sqrt{12}}{2})}_{\notin \mathbb{Q}[X]} \cdot \underbrace{(X^2 + \sqrt[4]{12}X + \frac{\sqrt{12}}{2})}_{\notin \mathbb{Q}[X]}$

dos factorizaciones de $h_2 = X^4 + 3$ en irreducibles mónicos de $\mathbb{R}[X]$.
Por el Teorema Fundamental de la Aritmética para Polinomios, la factorización en irreducibles mónicos es única salvo el orden de los factores. De aquí concluimos que entonces $\underbrace{q_1}_{\in \mathbb{Q}[X]} = \underbrace{(X^2 - \sqrt[4]{12}X + \frac{\sqrt{12}}{2})}_{\notin \mathbb{Q}[X]}$

o bien $\underbrace{q_1}_{\in \mathbb{Q}[X]} = \underbrace{(X^2 + \sqrt[4]{12}X + \frac{\sqrt{12}}{2})}_{\notin \mathbb{Q}[X]}$, lo cual nos lleva a una contradicción.

La contradicción proviene de suponer que $X^4 + 3$ es reducible en $\mathbb{Q}[X]$, y entonces concluimos que $X^4 + 3$ es irreducible en $\mathbb{Q}[X]$.

De aquí tenemos entonces:
$f = (X^2 - 2X + 5) \cdot (X^4 + 3)$
factorización de f en irreducibles en $\mathbb{Q}[X]$ (y ambos factores son irreducibles por lo explicado anteriormente).

□