Álgebra I
Examen III

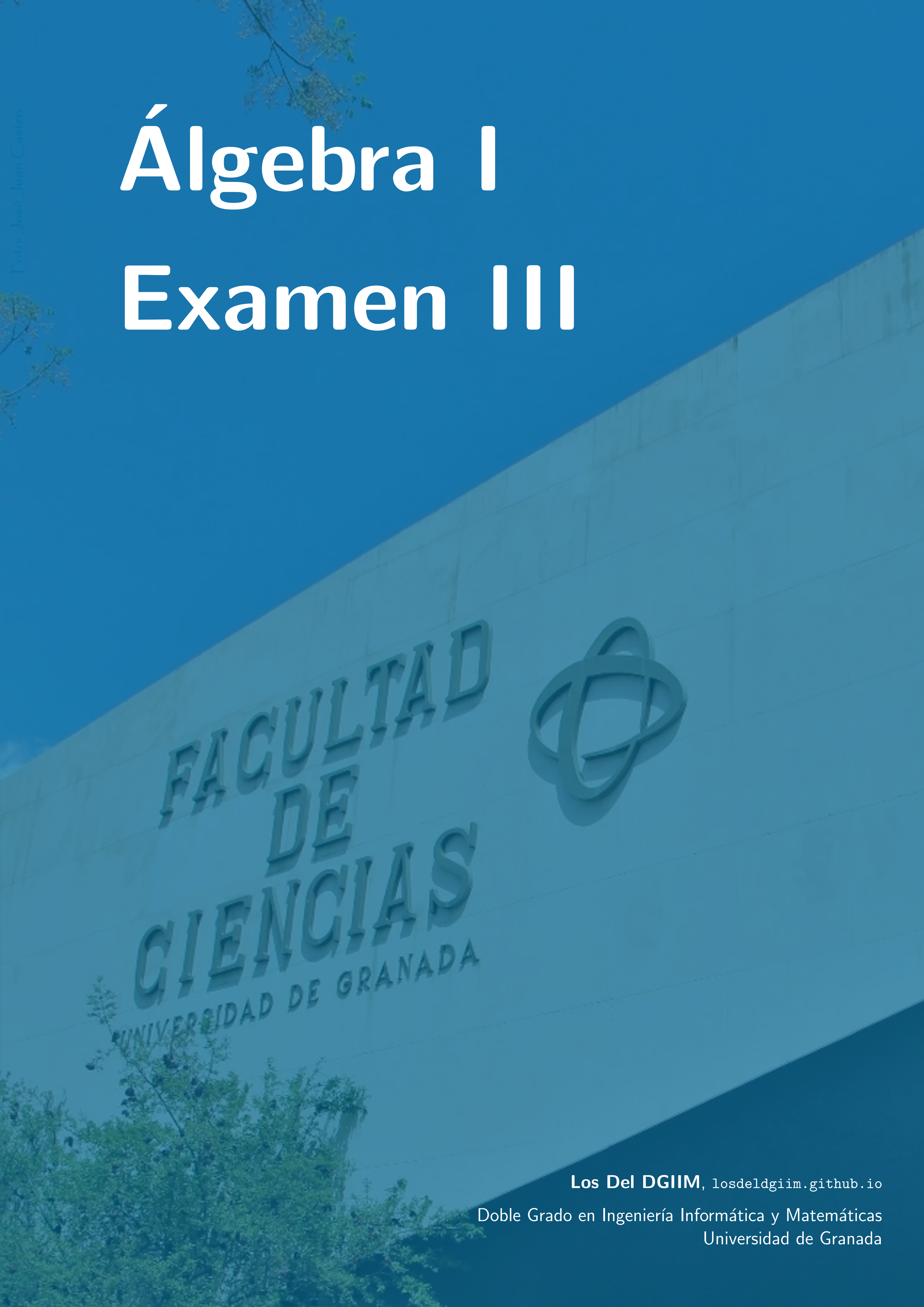

Foto: José Juan Castro

Los Del DGIIM, `losdeldgiim.github.io`

Doble Grado en Ingeniería Informática y Matemáticas
Universidad de Granada

Álgebra I
Examen III

Los Del DGIIM, `losdeldgiim.github.io`

José Juan Urrutia Milán
Arturo Olivares Martos

Granada, 2023-2024

Asignatura Álgebra I.

Curso Académico 2021-22.

Grado Doble Grado en Ingeniería Informática y Matemáticas.

Grupo Único.

Profesor María Pilar Carrasco Carrasco.

Descripción Examen Extraordinario.

Fecha 7 de febrero de 2022.

Duración 3 horas.

Ejercicio 1 (4 puntos).

1. (0.5 puntos) Sea X un conjunto y A, B y C subconjuntos de X. Suponiendo que $A \cap C = \emptyset$, probad que $(A \cup B) - C = A \cup (B - C)$.

2. (1 punto) Sea $f : \mathbb{R} \to \mathbb{R}$ la aplicación definida para cada $x \in \mathbb{R}$, por $f(x) = x^2 - 3x + 1$. Sea R_f la relación de equivalencia en $\mathbb{R}$ definida por la aplicación f. Describid el conjunto cociente. ¿Cuántos elementos tiene cada clase?

3. (0.5 puntos) En el anillo $\mathbb{Z}_8$, sea $I = 4\mathbb{Z}_8$, el ideal principal generado por 4. Describid $\mathbb{Z}_8/I$ listando todos sus elementos.

4. (1 punto) Sea A un dominio euclídeo con función euclídea $\phi : A \setminus \{0\} \to \mathbb{N}$. Demostrad que para todo $a \neq 0$, se tiene que $\phi(a) \geqslant \phi(1)$ y que se da la igualdad si, y sólo si $a \in U(A)$.

5. (0.5 puntos) Demostrad que $n^{13} - n$ es divisible por 2 y 5 para todo $n \in \mathbb{Z}$.

6. (0.5 puntos) Demostrad que en $\mathbb{Z}[i]$ se tiene que $\mathrm{mcd}(n, n+i) = 1$, para todo $n \in \mathbb{Z}$, $n \neq 0$.

Ejercicio 2 (3.5 puntos).

1. (2.5 puntos) Factorizar en $\mathbb{Z}[x]$ y en $\mathbb{Q}[x]$ los siguientes polinomios:

   a. $48x^4 + 24x^3 - 72x + 80$

   b. $x^6 + 8x^4 + 4x^3 + 5x^2 + 4x + 1$

   c. $10x^5 + 23x^4 - 20x^3 + 5x^2 + 5x - 3$

2. Sea $f(x) \in \mathbb{Z}[x]$ un polinomio primitivo de grado $n > 0$ y tal que existe un primo $p \in \mathbb{Z}$ verificando:

   (i) Su reducido módulo p es de la forma $R_p(f(x)) = \alpha x^n$, con $\alpha \in \mathbb{Z}$ no nulo.

   (ii) $p^2 \nmid f(p)$.

   Demostrad que $f(x)$ es irreducible.

Ejercicio 3 (2.5 puntos). Dado el sistema de congruencias en $\mathbb{Z}[\sqrt{-2}]$

$$\begin{cases} \mathrm{x} \equiv 1 & \text{mód } (1+\sqrt{-2}) \\ \mathrm{x} \equiv 2 & \text{mód } (3+\sqrt{-2}) \\ \mathrm{x} \equiv 4 & \text{mód } (3+2\sqrt{-2}) \end{cases}$$

Demostrad que tiene solución sin resolverlo. Resolverlo, dando una solución óptima y la solución general.
¿Es posible encontrar una solución a $a + b\sqrt{-2}$ tal que $30 < a < 56$?

Ejercicio 1 (4 puntos)**.**

1. (0.5 puntos) Sea X un conjunto y A, B y C subconjuntos de X. Suponiendo que $A \cap C = \emptyset$, probad que $(A \cup B) - C = A \cup (B - C)$.

2. (1 punto) Sea $f : \mathbb{R} \to \mathbb{R}$ la aplicación definida para cada $x \in \mathbb{R}$, por $f(x) = x^2 - 3x + 1$. Sea R_f la relación de equivalencia en $\mathbb{R}$ definida por la aplicación f. Describid el conjunto cociente. ¿Cuántos elementos tiene cada clase?

3. (0.5 puntos) En el anillo $\mathbb{Z}_8$, sea $I = 4\mathbb{Z}_8$, el ideal principal generado por 4. Describid $\mathbb{Z}_8/I$ listando todos sus elementos.

$$\mathbb{Z}_8/I = \{[a] \mid a \in \mathbb{Z}_8\} = \{a + I \mid a \in \mathbb{Z}_8\}$$

$$[0] = \{b \in \mathbb{Z}_8 \mid b \equiv 0 \pmod{4}\} = \{b \in \mathbb{Z}_8 \mid b = 0 \text{ en } \mathbb{Z}_4\} = \{0, 4\}$$

$$[1] = \{b \in \mathbb{Z}_8 \mid b \equiv 1 \pmod{4}\} = \{b \in \mathbb{Z}_8 \mid b = 1 \text{ en } \mathbb{Z}_4\} = \{1, 5\}$$

$$[2] = \{b \in \mathbb{Z}_8 \mid b \equiv 2 \pmod{4}\} = \{b \in \mathbb{Z}_8 \mid b = 2 \text{ en } \mathbb{Z}_4\} = \{2, 6\}$$

$$[3] = \{b \in \mathbb{Z}_8 \mid b \equiv 3 \pmod{4}\} = \{b \in \mathbb{Z}_8 \mid b = 3 \text{ en } \mathbb{Z}_4\} = \{3, 7\}$$

Luego:

$$\mathbb{Z}_8/I = \{0 + I, 1 + I, 2 + I, 3 + I\}$$

4. (1 punto) Sea A un dominio euclídeo con función euclídea $\phi : A \setminus \{0\} \to \mathbb{N}$. Demostrad que para todo $a \neq 0$, se tiene que $\phi(a) \geqslant \phi(1)$ y que se da la igualdad si, y sólo si $a \in U(A)$.

$$\phi(a) = \phi(a \cdot 1) \geqslant \phi(1) \quad \forall a \in A \setminus \{0\}$$

$\Rightarrow$) Supongamos que $\phi(a) = \phi(1)$:
Dividimos 1 entre a, $1 = qa + r$ con:

$$\begin{cases} \text{r} = 0 \\ \vee \\ \phi(r) < \phi(a) = \phi(1) \end{cases}$$

• Supongamos que $r \neq 0$, luego $\phi(r) < \phi(1)$, pero:

$$\phi(b) \geqslant \phi(1) \quad \forall b \in A \setminus \{0\} \Rightarrow \phi(r) \geqslant \phi(1)$$

<u>Contradicción</u>. Luego $r = 0$.
Por tanto: $1 = qa \Rightarrow a \in U(A)$.

$\Leftarrow$) Supongamos que $a \in U(A) \Rightarrow \exists a^{-1} \in A \mid aa^{-1} = 1 \Rightarrow \phi(aa^{-1}) = \phi(1)$

$$\left.\begin{array}{r} \phi(1) = \phi(aa^{-1}) \geqslant \phi(a) \\ \phi(a) \geqslant \phi(1) \quad \forall a \in A \setminus \{0\} \end{array}\right\} \Rightarrow \phi(a) = \phi(1)$$

5. (0.5 puntos) Demostrad que $n^{13} - n$ es divisible por 2 y 5 para todo $n \in \mathbb{Z}$.

Demostremos primero que $2 \mid n^{13} - n \quad \forall n \in \mathbb{Z}$:
• Supongamos que $2 \mid n \Rightarrow \exists k \in \mathbb{Z}$ tal que $n = 2k$.

$$n^{13} - n = n(n^{12} - 1) = 2k(n^{12} - 1) = 2k'$$

Con $k' = k(n^{12} - 1) \Rightarrow 2 \mid n^{13} - n$.

• Supongamos que $2 \nmid n$:
Como 2 es primo, $\text{mcd}(2, n) = 1$. Por el Teorema de Fermat:

$$n^{\varphi(2)} = n \equiv 1 \pmod{2} \Rightarrow n^{12} \equiv 1 \pmod{2} \Rightarrow n^{13} \equiv n \pmod{2} \Rightarrow$$

$$\Rightarrow n^{13} - n \equiv 0 \pmod{2} \Rightarrow 2 \mid n^{13} - n$$

Veamos que $5 \mid n^{13} - n \quad \forall n \in \mathbb{Z}$:
• Supongamos que $5 \mid n \Rightarrow \exists k \in \mathbb{Z}$ tal que $n = 5k$.

$$n^{13} - n = n(n^{12} - 1) = 5k(n^{12} - 1) = 5k'$$

Con $k' = k(n^{12} - 1) \Rightarrow 5 \mid n^{13} - n$.

• Supongamos que $5 \nmid n$:
Como 5 es primo, $\text{mcd}(5, n) = 1$. Por el Teorema de Fermat:

$$n^{\varphi(5)} = n^4 \equiv 1 \pmod{5} \Rightarrow n^{12} \equiv 1 \pmod{5} \Rightarrow n^{13} \equiv n \pmod{5} \Rightarrow$$

$$\Rightarrow n^{13} - n \equiv 0 \pmod{5} \Rightarrow 5 \mid n^{13} - n$$

6. (0.5 puntos) Demostrad que en $\mathbb{Z}[i]$ se tiene que $\text{mcd}(n, n+i) = 1$, para todo $n \in \mathbb{Z}$, $n \neq 0$.

Supongamos que $\exists n \in \mathbb{Z}^+ \mid \text{mcd}(n, n+i) \neq 1$.
Como el máximo común divisor es único salvo asociados y:
$1 \sim a$ con $a \in U(\mathbb{Z}[i])$:

$$\text{mcd}(n, n+i) = \alpha \mid \alpha \notin U(A)$$

$$\begin{cases} \alpha \mid n & \Rightarrow \quad \text{N}(\alpha) \mid N(n) & \Rightarrow \quad \text{N}(\alpha) \mid n^2 \\ \wedge & & \\ \alpha \mid n+i & \Rightarrow \quad \text{N}(\alpha) \mid N(n+i) & \Rightarrow \quad \text{N}(\alpha) \mid n^2+1 \end{cases}$$

Veamos ahora el siguiente resultado:
Sean a, $b \in \mathbb{Z}^+$: $a \mid b \wedge a \mid b+1 \Leftrightarrow a = \pm 1$

$\Leftarrow$) Supongamos que $a = \pm 1 \Rightarrow a \in U(A) \Rightarrow a \mid b \wedge a \mid b+1$
$\Rightarrow$) Supongamos que $a \mid b \wedge a \mid b+1$:

$$\left.\begin{array}{lcr} \text{a} \mid b & \Rightarrow & \exists k \in \mathbb{Z} \mid b = ka \\ \text{a} \mid b+1 & \Rightarrow & \exists k' \in \mathbb{Z} \mid b+1 = k'a \end{array}\right\} \Rightarrow ka + 1 = k'a \Rightarrow$$

$$\Rightarrow 1 = a(k' - k) \Rightarrow a \mid 1 \Rightarrow a \in U(\mathbb{Z}) \Rightarrow a = \pm 1$$

$$\left.\begin{array}{l} \mathrm{N}(\alpha) \mid n^2 \\ \wedge \\ \mathrm{N}(\alpha) \mid n^2 + 1 \end{array}\right\} \Rightarrow N(\alpha) = \pm 1 \Rightarrow \alpha \in U(A)$$

Lo que es una <u>contradicción</u>.

Luego $mcd(n, n+i) = 1 \quad \forall n \in \mathbb{Z}^+$.

Ejercicio 2 (3.5 puntos)**.**

1. (2.5 puntos) Factorizar en $\mathbb{Z}[x]$ y en $\mathbb{Q}[x]$ los siguientes polinomios:

a. $48x^4 + 24x^3 - 72x + 80$

Sea $f = 48x^4 + 24x^3 - 72x + 80$, $f = 8g$ con $g = 6x^4 + 3x^3 - 9x + 10 \in \mathbb{Z}[x]$. g es irreducible en $\mathbb{Z}[x]$ por Eisenstein para $p = 3$. Por la misma razón, también lo es en $\mathbb{Q}[x]$.

$$f = 2^3(6x^4 + 3x^3 - 9x + 10) \text{ en } \mathbb{Z}[x]$$

$$f = 8(6x^4 + 3x^3 - 9x + 10) \text{ en } \mathbb{Q}[x]$$

b. $x^6 + 8x^4 + 4x^3 + 5x^2 + 4x + 1$

Sea $f = x^6 + 8x^4 + 4x^3 + 5x^2 + 4x + 1$.
Las posibles raíces de f en $\mathbb{Q}$ son $\{\pm 1\}$:

$$\left.\begin{array}{l} f(1) = 1 + 8 + 4 + 5 + 4 + 1 = 23 \neq 0 \\ f(-1) = 1 + 8 - 4 + 5 - 4 + 1 = 7 \neq 0 \end{array}\right\} \Rightarrow \begin{array}{l} f \text{ no tiene factores} \\ \text{de grado 1 ni 5} \end{array}$$

• Reducimos módulo 2:

$R_2(f) = x^6 + x^2 + 1 = (x^3 + x + 1)^3 \Rightarrow R_2(f)$ no tiene factores de grado 2 ni 4

Luego f tampoco tiene factores de grado 2 ni 4.

• Reducimos módulo 3:

$$R_3(f) = x^6 + 2x^4 + x^3 + 2x^2 + x + 1 \in \mathbb{Z}_3[x]$$

$$\left.\begin{array}{l} R_3(f)(0) = 1 \neq 0 \\ R_3(f)(1) = 8 \neq 0 \\ R_3(f)(2) = 115 = 1 \neq 0 \end{array}\right\} \Rightarrow \begin{array}{l} R_3(f) \text{ no tiene factores} \\ \text{de grado 1 ni 5} \end{array}$$

Al dividir $R_3(f)$ entre $x^2 + 1$ obtenemos que:

$$x^6 + 2x^4 + x^3 + 2x^2 + x + 1 = (x^2 + 1)(x^4 + x^2 + x + 1) \Rightarrow (x^2 + 1) \mid R_3(f)$$

$$R_3(f) = (x^2 + 1)g \text{ con } g = x^4 + x^2 + x + 1 \in \mathbb{Z}_3[x]$$

Como $R_3(f)$ no tiene factores de grado 1 $\Rightarrow g$ no tiene de grado 1 ni 3.
$R_3(f)$ no tiene factores de grado 3 $\Rightarrow f$ tampoco.

Concluimos que f es irreducible en $\mathbb{Z}[x]$ y en $\mathbb{Q}[x]$.

c. $10x^5 + 23x^4 - 20x^3 + 5x^2 + 5x - 3$

Sea $f = 10x^5 + 23x^4 - 20x^3 + 5x^2 + 5x - 3$. Es primitivo.

$$Div(-3) = \{\pm 1, \pm 3\}$$

$$Div(10) = \{\pm 1, \pm 2, \pm 5, \pm 10\}$$

Por lo que las posibles raíces de f en $\mathbb{Q}$ son:

$$\left\{\pm 1, \pm 3, \pm\frac{1}{2}, \pm\frac{3}{2}, \pm\frac{1}{5}, \pm\frac{3}{5}, \pm\frac{1}{10}, \pm\frac{3}{10}\right\}$$

$$f(1) \neq 0 \quad f(-1) \neq 0 \quad f(3) \neq 0$$

$$f(-3) = 0 \Rightarrow (x+3) \mid f$$

Al dividir f entre $(x+3)$ obtenemos:

$$f = (x+3)g \text{ con } g = 10x^4 - 7x^3 + x^2 + 2x - 1 \in \mathbb{Z}[x]$$

Con g primitivo. Las posibles raíces de g en $\mathbb{Q}$ son:

$$\left\{\pm 1, \pm\frac{1}{2}, \pm\frac{1}{5}, \pm\frac{1}{10}\right\}$$

$$g(1) \neq 0 \quad g(-1) \neq 0$$

$$g\left(\frac{1}{2}\right) = 0 \Rightarrow \left(x - \frac{1}{2}\right) \mid g \Rightarrow (2x-1) \mid g$$

Al dividir g entre $(2x-1)$ obtenemos:

$$g = (2x-1)(5x^3 - x^2 + 1)$$

Luego:

$$f = (x+3)(2x-1)h \text{ con } h = 5x^3 - x^2 + 1 \in \mathbb{Z}[x]$$

Con h primitivo.

Las posibles ríaces de h en $\mathbb{Q}$ son: $\left\{\pm 1, \pm\frac{1}{5}\right\}$

$$h(1) \neq 0 \quad h(-1) \neq 0 \quad h\left(\frac{1}{5}\right) \neq 0 \quad h\left(-\frac{1}{5}\right) \neq 0$$

Luego h es irreducible por el criterio de la raíz.

$$f = (x+3)(2x-1)(5x^3 - x^2 + 1) \text{ en } \mathbb{Z}[x]$$

$$f = \frac{5}{2}(x+3)(x - \frac{1}{2})(x^3 - \frac{1}{2}x^2 + \frac{1}{5}) \text{ en } \mathbb{Q}[x]$$

2. Sea $f(x) \in \mathbb{Z}[x]$ un polinomio primitivo de grado $n > 0$ y tal que existe un primo $p \in \mathbb{Z}$ verificando:

(i) Su reducido módulo p es de la forma $R_p(f(x)) = \alpha x^n$, con $\alpha \in \mathbb{Z}$ no nulo.

(ii) $p^2 \nmid f(p)$.

Demostrad que $f(x)$ es irreducible.

Sea $f = \displaystyle\sum_{i=0}^{n} a_i x^i \in \mathbb{Z}[x]$:

Como $R_p(f) = \alpha x^n \Rightarrow p \nmid a_n \wedge p \mid a_i \ \ \forall i \in \{0, \ldots, n-1\}$
Para poder aplicar Eisenstein, es necesario demostrar que $p^2 \nmid a_0$:

$$f(p) = \sum_{i=0}^{n} a_i p^i = \sum_{i=1}^{n}(a_i p^i) + a_0 = \sum_{i=2}^{n}(a_i p^i) + a_1 p + a_0 = p^2 \sum_{i=2}^{n}(a_i p^{i-2}) + a_1 p + a_0$$

Como $p \mid a_1 \Rightarrow \exists k \in \mathbb{Z} \mid a_1 = pk$

$$f(p) = p^2 \sum_{i=2}^{n}(a_i p^{i-2}) + (pk)p + a_0 = p^2 \left[\sum_{i=2}^{n}(a_i p^{i-2}) + k\right] + a_0$$

- Supongamos que $p^2 \mid a_0 \Rightarrow \exists k' \in \mathbb{Z} \mid a_0 = p^2 k'$

$$f(p) = p^2 \left[\sum_{i=2}^{n}(a_i p^{i-2}) + k\right] + p^2 k' = p^2 \left[\sum_{i=2}^{n}(a_i p^{i-2}) + k + k'\right] \Rightarrow p^2 \mid f(p)$$

Lo que es una contradicción. Luego $p^2 \nmid a_0$.

Como f es primitivo y $\exists p \in \mathbb{Z}$ primo tal que:

$$p^2 \nmid a_0 \wedge p \mid a_i \ \ \forall i \in \{0, \ldots, n-1\}$$

Entonces, f es irreducible por Eisenstein para p

Ejercicio 3 (2.5 puntos)**.** Dado el sistema de congruencias en $\mathbb{Z}[\sqrt{-2}]$

$$\begin{cases} \text{x} \equiv 1 \mod (1+\sqrt{-2}) \\ \text{x} \equiv 2 \mod (3+\sqrt{-2}) \\ \text{x} \equiv 4 \mod (3+2\sqrt{-2}) \end{cases}$$

Demostrad que tiene solución sin resolverlo. Resolverlo, dando una solución óptima y la solución general.
¿Es posible encontrar una solución $a + b\sqrt{-2}$ tal que $30 < a < 56$?

Primero, calculamos:
$\text{mcd}(1+\sqrt{-2}, 3+\sqrt{-2})$, $\text{mcd}(1+\sqrt{-2}, 3+2\sqrt{-2})$ y $\text{mcd}(3+\sqrt{-2}, 3+2\sqrt{-2})$:

- En $\mathbb{Q}[\sqrt{-2}]$:

$$\frac{3+\sqrt{-2}}{1+\sqrt{-2}} = \frac{(3+\sqrt{-2})(1-\sqrt{-2})}{3} = \frac{3-3\sqrt{-2}+\sqrt{-2}+2}{3} = \frac{5}{3} - \frac{2}{3}\sqrt{-2} \Rightarrow$$

$$\Rightarrow 3+\sqrt{-2} = (2-\sqrt{-2})(1+\sqrt{-2}) - 1$$

$$\begin{array}{rcl} r_i & u_i & v_i \\ 3+\sqrt{-2} & 1 & 0 \\ 1+\sqrt{-2} & 0 & 1 \\ \text{-1} & 1 & -(2-\sqrt{-2}) \end{array}$$

Luego $\text{mcd}(1+\sqrt{-2}, 3+\sqrt{-2}) = -1 \sim 1$

• En $\mathbb{Q}[\sqrt{-2}]$:

$$\frac{3+2\sqrt{-2}}{1+\sqrt{-2}} = \frac{(3+2\sqrt{-2})(1-\sqrt{-2})}{3} = \frac{3+2\sqrt{-2}+3\sqrt{-2}+4}{3} = \frac{7}{3}+\frac{1}{3}\sqrt{-2} \Rightarrow$$

$$\Rightarrow 3+2\sqrt{-2} = (1+\sqrt{-2})(2)+1$$

$$\begin{array}{rcc} r_i & u_i & v_i \\ 3+2\sqrt{-2} & 1 & 0 \\ 1+\sqrt{-2} & 0 & 1 \\ 1 & 1 & \text{-2} \end{array}$$

Luego $\text{mcd}(1+\sqrt{-2}, 3+2\sqrt{-2}) = 1$

• En $\mathbb{Q}[\sqrt{-2}]$:

$$\frac{3+2\sqrt{-2}}{3+\sqrt{-2}} = \frac{(3+2\sqrt{-2})(3-\sqrt{-2})}{9+2} = \frac{9+6\sqrt{-2}-3\sqrt{-2}+4}{11} = \frac{13}{11}+\frac{3}{11}\sqrt{-2} \Rightarrow$$

$$\Rightarrow (3+2\sqrt{-2}) = (3+\sqrt{-2})(1)+\sqrt{-2}$$

En $\mathbb{Q}[\sqrt{-2}]$:

$$\frac{3+\sqrt{-2}}{\sqrt{-2}} = \frac{(3+\sqrt{-2})(\sqrt{-2})}{-2} = \frac{3\sqrt{-2}-2}{-2} = 1-\frac{3}{2}\sqrt{-2} \Rightarrow$$

$$\Rightarrow (3+\sqrt{-2}) = (\sqrt{-2})(1-\sqrt{-2})+1$$

$$\begin{array}{rcc} r_i & u_i & v_i \\ 3+2\sqrt{-2} & 1 & 0 \\ 3+\sqrt{-2} & 0 & 1 \\ \sqrt{-2} & 1 & \text{-1} \\ 1 & -(1-\sqrt{-2}) & 2-\sqrt{-2} \end{array}$$

Luego $\text{mcd}(3+\sqrt{-2}, 3+2\sqrt{-2}) = 1$

Como:

$$\left.\begin{array}{l} \text{mcd}(1+\sqrt{-2}, 3+\sqrt{-2}) = 1 \\ \text{mcd}(1+\sqrt{-2}, 3+2\sqrt{-2}) = 1 \\ \text{mcd}(3+\sqrt{-2}, 3+2\sqrt{-2}) = 1 \end{array}\right\}$$

Por el Teorema Chino del resto generalizado, sabemos que el sistema tiene solución.

Pasamos a resolver el sistema.
Resolvemos en primer lugar:

$$\begin{cases} x \equiv 1 \mod (1+\sqrt{-2}) \\ x \equiv 2 \mod (3+\sqrt{-2}) \end{cases}$$

De la primera ecución, tenemos que:

$$x = 1 + (1+\sqrt{-2})\alpha \mid \alpha \in \mathbb{Z}[\sqrt{-2}]$$

De la segunda:

$$x = 1 + (1+\sqrt{-2})\alpha \equiv 2 \mod (3+\sqrt{-2}) \Leftrightarrow$$

$$\Leftrightarrow (1+\sqrt{-2})\alpha \equiv 1 \mod (3+\sqrt{-2})$$

Sabemos que $-1 = 3+\sqrt{-2} - (2-\sqrt{-2})(1+\sqrt{-2})$. Luego:

$$(1+\sqrt{-2})(2-\sqrt{-2}) \equiv 1 \mod (3+\sqrt{-2})$$

Luego $\alpha_0 = 2-\sqrt{-2}$ es una solución particular.
De hecho, se trata de la solución óptima, luego las soluciones son:

$$\alpha = (2-\sqrt{-2}) + (3+\sqrt{-2})\beta \mid \beta \in \mathbb{Z}[\sqrt{-2}]$$

Por lo que las soluciones del sistema son ($\forall \beta \in \mathbb{Z}[\sqrt{-2}]$):

$$x = 1 + (1+\sqrt{-2})\alpha = 1 + (1+\sqrt{-2})[(2-\sqrt{-2}) + (3+\sqrt{-2})\beta] =$$

$$= 1 + (1+\sqrt{-2})(2-\sqrt{-2}) + (1+\sqrt{-2})(3+\sqrt{-2})\beta =$$
$$= 1 + 2 - \sqrt{-2} + 2\sqrt{-2} + 2 + (1+\sqrt{-2})(3+\sqrt{-2})\beta =$$
$$= 5 + \sqrt{-2} + (1+\sqrt{-2})(3+\sqrt{-2})\beta$$

Luego:

$$x \equiv 5+\sqrt{-2} \mod [(1+\sqrt{-2})(3+\sqrt{-2})]$$

Por lo que el sistema inicial es equivalente a:

$$\begin{cases} \text{x} \equiv 5+\sqrt{-2} \mod [(1+\sqrt{-2})(3+\sqrt{-2})] \\ \text{x} \equiv 4 \mod (3+2\sqrt{-2}) \end{cases}$$

De la segunda ecución, obtenemos que:

$$x = 4 + (3+2\sqrt{-2})\phi \mid \phi \in \mathbb{Z}[\sqrt{-2}]$$

Y de la segunda:

$$x = 4 + (3+2\sqrt{-2})\phi \equiv 5+\sqrt{-2} \mod [(1+\sqrt{-2})(3+\sqrt{-2})] \Leftrightarrow$$

$$\Leftrightarrow (3+2\sqrt{-2})\phi \equiv 1+\sqrt{-2} \mod [(1+\sqrt{-2})(3+\sqrt{-2})] \Leftrightarrow$$
$$\Leftrightarrow (3+2\sqrt{-2})\phi \equiv 1+\sqrt{-2} \mod (1+4\sqrt{-2})$$

Calculamos $\text{mcd}(3+2\sqrt{-2}, 1+4\sqrt{-2})$:
En $\mathbb{Q}[\sqrt{-2}]$:

$$\frac{1+4\sqrt{-2}}{3+2\sqrt{-2}} = \frac{19}{17} + \frac{10}{17}\sqrt{-2} \Rightarrow$$

$$\Rightarrow (1+4\sqrt{-2}) = (3+2\sqrt{-2})(1+\sqrt{-2}) + (2-\sqrt{-2})$$

En $\mathbb{Q}[\sqrt{-2}]$:

$$\frac{3+2\sqrt{-2}}{2-\sqrt{-2}} = \frac{1}{3} + \frac{7}{6}\sqrt{-2} \Rightarrow$$

$$\Rightarrow (3+2\sqrt{-2}) = (2-\sqrt{-2})(\sqrt{-2}) + 1$$

r_i	u_i	v_i
$1+4\sqrt{-2}$	1	0
$3+2\sqrt{-2}$	0	1
$2-\sqrt{-2}$	1	$-(1+\sqrt{-2})$
1	$-\sqrt{-2}$	$1+\sqrt{-2}(1+\sqrt{-2})$

Luego $\text{mcd}(3+2\sqrt{-2}, 1+4\sqrt{-2}) = 1$ con identidad de Bezout:

$$1 = -\sqrt{-2}(1+4\sqrt{-2}) + (3+2\sqrt{-2})(-1+\sqrt{-2}) \Rightarrow$$

$$\Rightarrow 1+\sqrt{-2} = -\sqrt{-2}(1+\sqrt{-2})(1+4\sqrt{-2}) + (3+2\sqrt{-2})(-1+\sqrt{-2})(1+\sqrt{-2})$$

Por lo que:

$$(3+2\sqrt{-2})(-1+\sqrt{-2})(1+\sqrt{-2}) \equiv 1+\sqrt{-2} \mod (1+4\sqrt{-2})$$

Luego $\phi_0 = (-1+\sqrt{-2})(1+\sqrt{-2}) = -3$ es una solución particular.
De hecho es la óptima, luego la solución general es:

$$\phi = -3 + (1+4\sqrt{-2})\psi = -3 + (1+\sqrt{-2})(3+\sqrt{-2})\psi \mid \psi \in \mathbb{Z}[\sqrt{-2}]$$

$$\begin{aligned} x = 4 + (3+2\sqrt{-2})\phi &= 4 + (3+2\sqrt{-2})[-3 + (1+\sqrt{-2})(3+\sqrt{-2})\psi] = \\ &= 4 + (3+2\sqrt{-2})(-3) + (3+2\sqrt{-2})(1+\sqrt{-2})(3+\sqrt{-2})\psi = \\ &= 4 - 9 - 6\sqrt{-2} + (3+2\sqrt{-2})(1+\sqrt{-2})(3+\sqrt{-2})\psi = \\ &= -5 - 6\sqrt{-2} + (3+2\sqrt{-2})(1+\sqrt{-2})(3+\sqrt{-2})\psi \mid \psi \in \mathbb{Z}[\sqrt{-2}] \end{aligned}$$

$$N(-5-6\sqrt{-2}) = 5^2 + 6^2 \cdot 2 = 97$$

$$N[(3+2\sqrt{-2})(1+\sqrt{-2})(3+\sqrt{-2})] = N(3+2\sqrt{-2})N(1+\sqrt{-2})N(3+\sqrt{-2}) =$$

$$= (3^2 + 2^2 \cdot 2)(1+2)(3^2+2) = 17 \cdot 3 \cdot 11 = 561$$

Como $97 < 561 \Rightarrow x_0 = -5 - 6\sqrt{-2}$ es la solución óptima del sistema.

Por tanto, la solución general del sistema es:

$$x = -5 - 6\sqrt{-2} + (3+2\sqrt{-2})(1+\sqrt{-2})(3+\sqrt{-2})\psi \mid \psi \in \mathbb{Z}[\sqrt{-2}]$$

Veamos si es posible encontrar una solución $a + b\sqrt{-2} \mid 30 < a < 56$:

$$x = -5 - 6\sqrt{-2} + (-13 + 14\sqrt{-2})\psi \mid \psi \in \mathbb{Z}[\sqrt{-2}]$$

Con $\psi = c + d\sqrt{-2}$ para ciertos c, $d \in \mathbb{Z}$.

$$x = -5 - 6\sqrt{-2} + (-13 + 14\sqrt{-2})(c + d\sqrt{-2}) =$$

$$= -5 - 6\sqrt{-2} - 13c + 14\sqrt{-2}c - 13d\sqrt{-2} - 28d =$$

$$= (-5 - 13c - 28d) + (-6 + 14c - 13d)\sqrt{-2} \mid c, d \in \mathbb{Z}$$

Como $30 < a < 56 \Rightarrow 30 < -5 - 13c - 28d < 56 \Rightarrow \psi = -1 - \sqrt{-2}$ es una solución posible.
Luego $x = 36 - 7\sqrt{-2}$ es una solución particular luego sí, es posible.