ÁLGEBRA 1

CURSO 20-21

RELACIÓN DE EJERCICIOS 1

1.1. Decidir si $A = B$, $A \subset B$ ó $A \in B$ en los siguientes casos:

i) $A = \{\emptyset\}$, $B = \{\{\emptyset\}\}$

ii) $A = \{\emptyset, \{\emptyset\}\}$, $B = \{\emptyset, \{\emptyset, \{\emptyset\}\}\}$

iii) $A = \{\{\emptyset\}, \{\emptyset, \emptyset\}\}$, $B = \{\{\emptyset\}\}$

1.2. Dar por extensión los siguientes conjuntos:
a) $\mathcal{P}(\emptyset)$; b) $\mathcal{P}(\{\emptyset\})$; c) $\mathcal{P}(\mathcal{P}(\mathcal{P}(\emptyset)))$

1.3. Demostrar las siguientes afirmaciones:

i) $\{a\} = \{b, c\}$ sí, y sólo sí $a = b = c$

ii) Si $a \neq b$ y $c \neq d$ entonces $\{\{a\}, \{a, b\}\} = \{\{c\}, \{c, d\}\}$ sí, y sólo sí $a = c$ y $b = d$

1.4. Si A y B son subconjuntos de un conjunto E demostrar:

i) $A \cap B = \emptyset \iff A \subseteq \overline{B} \iff B \subseteq \overline{A}$

ii) $A \cup B = E \iff \overline{B} \subseteq A \iff \overline{A} \subseteq B$

1.5. Sea X un conjunto y A, B, C subconjuntos de X. Demostrar que si $A \cup B \subseteq A \cup C$ y $A \cap B \subseteq A \cap C$ entonces $B \subseteq C$. Como consecuencia demostrar que si $A \cup B = A \cup C$ y $A \cap B = A \cap C$ entonces $B = C$.

1.6. (Leyes de De Morgan) Si A y B son subconjuntos de un conjunto X, demostrar:

$$i)\ \overline{A \cap B} = \overline{A} \cup \overline{B}\ ;\ ii)\ \overline{A \cup B} = \overline{A} \cap \overline{B}$$

1.7. Verificar las siguientes fórmulas donde A, B y C son subconjuntos de un conjunto X y $A \setminus C = \{x \in X / x \in A \wedge x \notin C\}$:

i) $(A \setminus C) \setminus (B \setminus C) = (A \setminus B) \setminus C$

ii) $(A \setminus C) \cup (B \setminus C) = (A \cup B) \setminus C$

iii) $(A \setminus C) \cap (B \setminus C) = (A \cap B) \setminus C$

iv) $(A \setminus B) \setminus (A \setminus C) = A \cap (C \setminus B)$

v) $(A \setminus B) \cup (A \setminus C) = A \setminus (B \cap C)$

vi) $(A \setminus B) \cap (A \setminus C) = A \setminus (B \cup C)$

1.8. Se define la diferencia simétrica de dos subconjuntos A y B de un conjunto X por

$$A \triangle B = (A \setminus B) \cup (B \setminus A)$$

Demostrar que $A \triangle B = (A \cup B) \setminus (A \cap B)$ y que $A \triangle B = \emptyset$ sí, y sólo sí $A = B$.

1.9. Sean $A, B \subseteq X$. Demostrar:

i) $A = (A \cap B) \cup (A \setminus B)$ es una representación de A como una unión disjunta.

ii) $A \cup B = A \cup (B \setminus A)$ es una representación de $A \cup B$ como una unión disjunta.

1.10. Sean $A, B \subseteq X$. Si A tiene n elementos y B tiene m elementos ¿Cuántos elementos tiene $A \cup B$?.

1.11. Sean $A, B \subseteq X$. Demostrar que si $A \subseteq B$ entonces $\mathcal{P}(A) \subseteq \mathcal{P}(B)$.

1.12. Se consideran los subconjuntos de $\mathbb{R}$, $A = [-1, 1]$ y $B = [-3, 4]$. Describir los siguientes subconjuntos de $\mathbb{R} \times \mathbb{R}$: $A \times B$, $B \times A$, $(A \times B) \cap (B \times A)$, $(A \times B) \setminus (B \times A)$, $(A \times B) \cup (B \times A)$.

ÁLGEBRA 1

CURSO 20-21

RELACIÓN DE EJERCICIOS 2

2.1. Construir todas las aplicaciones del conjunto $X = \{a, b, c\}$ en el conjunto $Y = \{1, 2\}$ y clasificarlas según sean inyectivas, sobreyectivas, biyectivas ó de ninguno de estos tipos.

2.2. Sea $f : \mathbb{R} \to \mathbb{R}$ definida por $f(x) = 5x - 3$. Demostrar que existe $g : \mathbb{R} \to \mathbb{R}$ tal que $g \circ f = 1_{\mathbb{R}}$. ¿Es cierto también que $f \circ g = 1_{\mathbb{R}}$?

2.3. Sean $f : X \to Y$ una aplicación y $A \subseteq X$, $B \subseteq Y$. Demostrar:

i) $f_*(f^*(B)) \subseteq B$ y se da la igualdad si f es sobreyectiva.

ii) $A \subseteq f^*(f_*(A))$ y se da la igualdad si f es inyectiva.

2.4. Se consideran las aplicaciones

$$A \xrightarrow{f} B \xrightarrow{g} C \quad \text{y} \quad X \xrightarrow{h} Y \xrightarrow{k} Z\ .$$

Demostrar que f y h inducen una única aplicación $f \times h : A \times X \to B \times Y$ verificando que

$$f \circ p_1 = p_1 \circ (f \times h) \ \text{ y } \ h \circ p_2 = p_2 \circ (f \times h).$$

Demostrar que $(g \times k) \circ (f \times h) = (g \circ f) \times (k \circ h)$.

2.5. Sea $f : X \to Y$ una aplicación, $A \subseteq X$ y $B \subseteq Y$. Demostrar

$$f_*(A \cap f^*(B)) = f_*(A) \cap B$$

2.6. Dada una aplicación $f : X \to Y$ y $A \subseteq X$, se llama saturación de A al conjunto $f^*(f_*(A))$. Se dice que A es saturado si $A = f^*(f_*(A))$.

i) Caracterizar los subconjuntos saturados de f si $X = Y = \mathbb{R}$ y f es la aplicación definida por $f(x) = x^2 + 1$.

ii) Hallar la saturación del conjunto $\{\pi\}$ si $X = Y = \mathbb{R}$ y f es la aplicación coseno.

2.7. Sea $f : X \to Y$ una aplicación. Demostrar que son equivalentes las siguientes afirmaciones:

i) f es inyectiva

ii) $\forall A, B \in P(X), f_*(A \cap B) = f_*(A) \cap f_*(B)$.

2.8. Sean $f : X \to Y$ y $g : Y \to Z$ dos aplicaciones y sea $h = g \circ f$ la composición de dichas aplicaciones. Demostrar:

i) Si h es inyectiva entonces f es inyectiva.

ii) Si h es sobreyectiva entonces g es sobreyectiva.

iii) Si h es inyectiva y f es sobreyectiva entonces g es inyectiva.

iv) Si h es sobreyectiva y g es inyectiva entonces f es sobreyectiva.

2.9. Sean las aplicaciones $f : X \to Y$, $g : Y \to Z$ y $h : Z \to X$ tales que $h \circ g \circ f$ es inyectiva, $g \circ f \circ h$ es inyectiva y $f \circ h \circ g$ es sobreyectiva. Demostrar que las aplicaciones f, g y h son biyectivas.

ÁLGEBRA 1

CURSO 20-21

RELACIÓN DE EJERCICIOS 3

3.1. Dar ejemplos de relaciones binarias en un conjunto que verifiquen una sola de las siguientes propiedades: reflexiva, simétrica, antisimétrica, transitiva.

3.2. Sea $X = \{1, 2, 3\}$. Calcular todas las particiones de X.

3.3. Sea $X = \{0, 1, 2, 3\}$, $Y = \{a, b, c\}$ y $f : X \to Y$ la aplicación dada por: $f(0) = c$; $f(1) = f(2) = a$; $f(3) = b$. Considerar la aplicación $f^* : \mathcal{P}(Y) \to \mathcal{P}(X)$ que a cada subconjunto $B \subseteq Y$ le hace corresponder su imagen inversa por f.

i) ¿Es f^* inyectiva, sobreyectiva o biyectiva?

ii) Calcular la relación $\sim_{f^*}$ en $\mathcal{P}(Y)$ asociada a f^* y el conjunto cociente $\mathcal{P}(Y)/\sim_{f^*}$.

iii) Hallar la descomposición canónica de f^*.

3.4. Sean X e Y dos conjuntos tales que $Y \subseteq X$. En el conjunto $\mathcal{P}(X)$ se define la siguiente relación binaria:

$$A \sim B \iff A \cap Y = B \cap Y$$

Demostrar que dicha relación es de equivalencia y describir el conjunto cociente.

3.5. Si X e Y son dos conjuntos y R y S son relaciones de equivalencia en X e Y respectivamente, definir en el conjunto $X \times Y$ una relación de equivalencia T tal que exista una biyección

$$(X \times Y)/T \cong (X/R) \times (Y/S)$$

3.6. Encontrar el error en la siguiente demostración:

"Una relación binaria sobre un conjunto X que es simétrica y transitiva es reflexiva porque $\forall x_1, x_2 \in X, x_1 R x_2 \Rightarrow x_2 R x_1$ (por simetría) y de aquí, por transitividad, $x_1 R x_1$".

3.7. Encontrar todos los órdenes parciales que se pueden definir en un conjunto de 3 elementos.

3.8. Sean X e Y conjuntos ordenados y definamos en $X \times Y$ la siguiente relación binaria:

$$(x, y) \leq (x', y') \Leftrightarrow x \leq x' \ \wedge \ y \leq y'$$

Demostrar que "$\leq$" es una relación de orden en $X \times Y$ pero que este orden no es total (incluso en el caso de que X e Y fueran totalmente ordenados) salvo en en el caso de que X ó Y consistan de un solo elemento.

3.9. Sea X un conjunto no vacío e $Y \in \mathcal{P}(X)$. Definimos la aplicación $f : X \to \mathcal{P}(X)$ por $f(x) = Y \cup \{x\}$, para $x \in X$, y consideramos la la relación de equivalencia $\sim_f$ asociada a f. Describir el conjunto cociente $X/\sim_f$. Si X es finito y tiene n elementos e Y tiene m elementos, calcular el cardinal (o sea, el número de elementos) de $X/\sim_f$.

3.10. Consideremos el plano vectorial real $\mathbb{R}^2 = \mathbb{R} \times \mathbb{R}$ y el conjunto $X = \mathbb{R}^2 \setminus \{(0,0)\}$. Definimos la relación R en X por uRv si existe $\lambda \in \mathbb{R}$ tal que $u = \lambda v$, para $u, v \in X$. Describir el conjunto cociente $\mathbb{P}^1 = X/R$.

ÁLGEBRA 1

CURSO 20-21

DOBLE GRADO MATEMÁTICAS INFORMÁTICA

RELACIÓN DE EJERCICIOS 4

4.1. Si A y B son anillos conmutativos, probar que el conjunto producto cartesiano $A \times B$, con las operaciones

$$(a,a') + (b,b') = (a+b, a'+b'), \quad (a,a')(b,b') = (ab, a'b').$$

es efectivamente un anillo conmutativo. Se llama el "*anillo producto cartesiano*" de A y B. Escribir las tablas de sumar y multiplicar del anillo producto $\mathbb{Z}_2 \times Z_2$.

4.2. En el conjunto $\mathbb{Z}$ definimos las operaciones de suma $\oplus$ y producto $\otimes$ por

$$a \oplus b = a + b - 1,$$

$$a \otimes b = a + b - ab.$$

Así, por ejemplo, $2 \oplus 3 = 4$ y $2 \otimes 3 = -1$. ¿Es $\mathbb{Z}$ un anillo conmutativo con estas operaciones?

4.3. En $\mathbb{Z} \times \mathbb{Z}$ definimos las operaciones

$$(a,a') + (b,b') = (a+b, a'+b'),$$

$$(a,a') \cdot (b,b') = (ab, ab' + a'b).$$

¿Es $\mathbb{Z} \times \mathbb{Z}$ un anillo conmutativo con estas operaciones?

4.4. Escribir las tablas de sumar y multiplicar de los anillos $\mathbb{Z}_5$ y $\mathbb{Z}_6$.

4.5. Efectuar los siguientes cálculos en el anillo $\mathbb{Z}[\sqrt{3}]$:

$$(3+2\sqrt{3}) + (4-5\sqrt{3}), \quad (3+2\sqrt{3})(4-5\sqrt{3}), (2-\sqrt{3})^3.$$

4.6. ¿Cuáles de los siguientes son subanillos de los anillos indicados?
(i) $\{a \in \mathbb{Q} \mid 3a \in \mathbb{Z}\} \subseteq \mathbb{Q}$,
(ii) $\{m + 2n\sqrt{3} \mid m, n \in \mathbb{Z}\} \subseteq \mathbb{R}$.

4.7. Determinar las unidades del anillo definido por el conjunto $\mathbb{Z} \times \mathbb{Z}$, con las operaciones $(a,a') + (b,b') = (a+b, a'+b')$ y $(a,a') \cdot (b,b') = (ab, ab' + a'b)$ (ver el Ejercicio 3).

4.8. Encontrar todas las unidades de los anillos $\mathbb{Z}_6$, $\mathbb{Z}_7$ y $\mathbb{Z}_8$.

4.9. Efectuar las siguientes operaciones en el anillo $\mathbb{Z}_5[X]$

$$\begin{array}{l}(3+4X+X^2+2X^3)+(3+4X+4X^4+3X^3),\\(3+4X+X^2+2X^3)(3+4X+4X^4+3X^3),\\(2-4X+X^2-2X^3)+(3-4X+4X^2-3X^3),\\(2-4X+X^2-2X^3)(3-4X+4X^2-3X^3).\end{array}$$

4.10. Si $p(X) \in \mathbb{Z}_5[X]$ es cualquiera de los cuatro polinomios obtenidos al realizar el ejercicio anterior, calcular $p(1)$ y $p(-1)$ en cada caso.

4.11. Sea R un anillo y sea $a \in R$ un elemento invertible. Demostrar que la aplicación $f_a : R \to R$ dada por $f_a(x) = axa^{-1}$ es un automorfismo de R.

4.12. Dado un anillo R, demostrar que existe un único homomorfismo de anillos de $\mathbb{Z}$ en R.

4.13. Demostrar que si A es un anillo de característica n, entonces existe un único homomorfismo de anillos de $\mathbb{Z}_n$ en A que es inyectivo.

4.14. Dados dos números naturales n y m, dar condiciones para que exista un homomorfismo de anillos de $\mathbb{Z}_n$ en $\mathbb{Z}_m$.

4.15. Dado un morfismo de anillos $f : A \longrightarrow B$, ¿la imagen directa de un subanillo de A es subanillo de B? ¿la imagen inversa de un subanillo de B es subanillo de A?

4.16. Razonar si las siguientes afirmaciones son verdaderas o falsas:

i) Existe un único homomorfismo de anillos de $\mathbb{Z}$ en $\mathbb{Z}_2 \times \mathbb{Z}_7$ que es sobreyectivo.

ii)$\mathbb{Z}_{1457}$ es un cuerpo.

iii) De $\mathbb{Z}_7$ en $\mathbb{Z}_{14}$ hay exactamente 7 homomorfismos de anillos.

ÁLGEBRA 1

CURSO 20-21

DOBLE GRADO MATEMÁTICAS INFORMÁTICA

RELACIÓN DE EJERCICIOS 5

5.1. En el anillo $\mathbb{Z}[x]$ de los polinomios con coeficientes en $\mathbb{Z}$, estudiar si son ideales los subconjuntos:

I formado por todos los polinomios con término independiente cero,
J formado por los polinomios con término independiente par y
K formado por los polinomios que tienen todos sus coeficientes pares.

5.2. Determinar los ideales del cuerpo $\mathbb{R}$ de los números reales.

5.3. Dados I, J ideales de un anillo A tales que $I \subseteq J$, se denota $J/I = \{x + I \in A/I \mid x \in J\}$. Probar que todo ideal de A/I es de la forma J/I para algún ideal J de A tal que $I \subseteq J$.

5.4. Sean I, J ideales de un anillo A tales que $I \subseteq J$. Probar que existe un isomorfismo de anillos:

$$\frac{A/I}{J/I} \cong \frac{A}{I}.$$

5.5. Probar que todos los ideales de $\mathbb{Z}$ son principales. Dar condiciones para que se verifique que $n\mathbb{Z} \subseteq m\mathbb{Z}$.

5.6. Describir los ideales de $\mathbb{Z}_{14}$ enumerando los elementos de cada uno de ellos.

5.7. Estudiar qué ideales de los del ejercicio 5.1 son principales.

5.8. En el anillo $\mathbb{Z} \times \mathbb{Z}$ se considera el subconjunto $I = \{(x, y) \mid x, y \text{ son múltiplos de } 3\}$. Probar que I es un ideal de $\mathbb{Z} \times \mathbb{Z}$. ¿Es principal?

5.9. Sea A un anillo conmutativo no trivial e I un ideal de A, $I \neq A$. Decimos que I es *maximal* si no existe ningún ideal J de A verificando $I \subsetneq J \subsetneq A$. Probar que I es un ideal maximal si, y sólo si, A/I es un cuerpo. Determinar los ideales maximales de $\mathbb{Z}$

ÁLGEBRA 1 CURSO 20-21

DOBLE GRADO MATEMÁTICAS INFORMÁTICA RELACIÓN DE EJERCICIOS 6

6.1. Determinar las unidades y los divisores de cero de los anillos $\mathbb{Z}_5$ y $\mathbb{Z}_8$.

6.2. ¿Es el anillo definido por el conjunto $\mathbb{Z} \times \mathbb{Z}$ con las operaciones $(a, a') + (b, b') = (a + b, a' + b')$ y $(a, a')(b, b') = (ab, ab' + a'b)$ un Dominio de Integridad?

6.3. Estudiar si los siguientes anillos son, o no, Dominios de Integridad:

$$\mathbb{Z}_8, \ \ \mathbb{Z}[\sqrt{2}], \ \ \mathbb{Z}_3, \ \ \mathbb{Z}_6[X], \ \ \mathbb{Z}[i], \ \ \mathbb{Z}_5[X].$$

6.4. En un anillo R un elemento a es idempotente si $a^2 = a$. Demuestra que en un dominio de integridad los únicos idempotentes son 0 y 1. Dar un ejemplo de un anillo que tenga otros idempotentes.

6.5. ¿Es $3 - 2i$ un divisor de $8 - i$ en el anillo $\mathbb{Z}[i]$? ¿Cuáles son los divisores de 5 en $\mathbb{Z}[i]$?

6.6. Argumentar la veracidad o falsedad de las siguientes proposiciones referidas a elementos de un Dominio de Integridad

1. $a \mid b \wedge a \nmid c \Rightarrow a \nmid b + c$.
2. $a \nmid b \wedge a \nmid c \Rightarrow a \nmid b + c$.

6.7. Denotemos por $\mathbb{Q}(x)$ el cuerpo de fracciones de $\mathbb{Z}[X]$. Describir los elementos de $\mathbb{Q}(x)$ y sus operaciones. Probar que $\mathbb{Q}(x)$ es también el cuerpo de fracciones de $\mathbb{Q}[x]$

6.8. Dado el conjunto $A = \{\frac{m}{2^k} \mid m \in \mathbb{Z}, k \geq 0\}$, probar que A es un subanillo de $\mathbb{Q}$ que no contiene a $\mathbb{Z}$ y que el cuerpo de fracciones de A es $\mathbb{Q}$.

ÁLGEBRA 1 CURSO 20-21

DOBLE GRADO MATEMÁTICAS INFORMÁTICA **RELACIÓN DE EJERCICIOS 7**

7.1. En el anillo $\mathbb{Z}[i]$, calcular cociente y resto de dividir $1+15i$ entre $3+5i$.

7.2. En el anillo $\mathbb{Z}[\sqrt{-2}]$, calcular

$$mcd(2-3\sqrt{-2}, 1+\sqrt{-2}),\ mcm(2-3\sqrt{-2}, 1+\sqrt{-2}).$$

7.3. En $\mathbb{Z}[\sqrt{3}]$, calcular $mcd(3+\sqrt{3}, 2)$ y $mcm(3+\sqrt{3}, 2)$.

7.4. Determinar, si existe, un polinomio $p(X) \in \mathbb{Z}_3[X]$ tal que

$$(2X^2+X+2)p(X) = 2X^7 + X^6 + 2X^4 + 2.$$

7.5. Demostrar las reglas del 2,3,5 y 11 para la división.

7.6. Demuestra que si $3|a^2+b^2$, entonces $3|a$ y $3|b$.

7.7. Demuestra que para todo $n \in \mathbb{N}$:

a) $3^{2n} - 2^n$ es divisible por 7, b) $3^{2n+1} + 2^{n+2}$ es divisible por 7,

c) $3^{2n+2} + 2^{6n+1}$ es divisible por 11, d) $3 \cdot 5^{2n+1} + 2^{3n+1}$ es divisible por 17.

7.8. Resolver en $\mathbb{Z}$ las ecuaciones

$$60x + 36y = 12, \qquad 35x + 6y = 8, \qquad 12x + 18y = 11.$$

7.9. Calcular el máximo común divisor y el mínimo común múltiplo, en el anillo $\mathbb{R}[X]$, de los polinomios $X^3 - 2X^2 - 5X + 6$ y $X^3 - 3X^2 - X + 3$. Resolver la siguiente ecuación en el anillo $\mathbb{R}[x]$,

$$(X^3 - 2X^2 - 5X + 6)p(X) + (X^3 - 3X^2 - X + 3)g(X) = X^3 - 6X^2 + 11X - 6.$$

7.10. Calcular el máximo común divisor y el mínimo común múltiplo, en el anillo $\mathbb{Z}_3[X]$, de los polinomios $X^4 + X^3 - X - 1$ y $X^5 + X^4 - X - 1$. Encontrar todos los polinomios $p(X)$ y $g(X)$ en $\mathbb{Z}_3[X]$, con grado de $g(X)$ igual a 7, tales que

$$(X^4 + X^3 - X - 1)p(X) + (X^5 + X^4 - X - 1)g(X) = X^4 + X^2 + 1.$$

7.11. Resolver la siguiente ecuación en el anillo $\mathbb{Z}[i]$, se verifique la ecuación

$$(-2+3i)x + (1+i)y = 1+11i.$$

7.12. Resolver la siguiente ecuación en el anillo $\mathbb{Z}[\sqrt{2}]$:

$$(4+\sqrt{2})x + (6+4\sqrt{2})y = \sqrt{2}.$$

7.13. En el anillo $\mathbb{Z}[\sqrt{3}]$, resolver la congruencia

$$(1+\sqrt{3})x \equiv 9-4\sqrt{3} \bmod (2\sqrt{3})$$

7.14. Determinar todos los polinomios $f(X) \in \mathbb{Z}_5[X]$ tales que

$$(X^4+3X^3+2X^2+3X+1)f(X) \equiv X^4-2X^3-X+2 \mod (X^3+3X^2+4X+2).$$

7.15. Discutir y resolver los sistemas de congruencias:

$$\begin{cases} 5x & \equiv & 1 & \pmod{14} \\ 11x & \equiv & 10 & \pmod{16} \end{cases}$$

$$\begin{cases} 5x & \equiv & 1 & \pmod{14} \\ 11x & \equiv & 13 & \pmod{16} \end{cases}$$

7.16. Calcular la menor solución positiva del sistema de congruencias

$$\begin{cases} 3x & \equiv & 1 & \pmod{4} \\ 2x & \equiv & 2 & \pmod{5} \\ x & \equiv & -1 & \pmod{3} \end{cases}$$

7.17. Una banda de 13 piratas se reparten N monedas de oro, pero le sobran 8. Dos mueren, las vuelven a repartir y sobran 3. Luego 3 se ahogan y sobran 5. ¿Cuál es la mínima cantidad posible N de monedas?

7.18. En el anillo $\mathbb{Z}[i]$, resolver el siguiente sistema de congruencias

$$\begin{cases} x & \equiv & i & \mod(3) \\ x & \equiv & 1+i & \mod(3+2i) \\ x & \equiv & 3+2i & \mod(4+i) \end{cases}$$

7.19. Determinar los polinomios $f(X) \in \mathbb{Q}[X]$ de grado menor o igual que tres que satisfacen el sistema de congruencias

$$\begin{array}{lcll} f(X) & \equiv & X-1 & \mod(X^2+1) \\ f(X) & \equiv & X+1 & \mod(X^2+X+1) \end{array}$$

7.20. Probar el Teorema de Ruffini: *Si* $f(X) \in A[X]$, *para cualquier* $a \in A$, $f(a)$ *es igual al resto de dividir* $f(X)$ *entre* $(X-a)$.

7.21. Encontrar un polinomio $f(X) \in \mathbb{Q}[X]$ de grado 3 tal que: $f(0)=6,\ f(1)=12$ y $f(X) \equiv (3X+3) \bmod (X^2+X+1)$.

7.22. Determinar todos los polinomios $f(X) \in \mathbb{Z}_2[X]$ de grado menor o igual que 4, tales que: 1) el resto de dividir $f(X)$ entre X^2+1 es X, 2) el resto de dividir $Xf(X)$ entre X^2+X+1 es $X+1$, y 3) $f(1)=1$.

7.23. Calcular el resto de dividir 279^{323} entre 17.

7.24. Calcular las dos últimas cifras de $3^{3^{100}}$.

7.25. Resolver, si es posible, la congruencia $43^{51}\,x \equiv 2 \pmod{36}$.

7.26. Estudiar si $[5]^{10077}$ es una unidad de $\mathbb{Z}_{38808}$. Calcular su inverso en caso de que lo tenga.

ÁLGEBRA 1 CURSO 20-21

DOBLE GRADO MATEMÁTICAS INFORMÁTICA — RELACIÓN DE EJERCICIOS 8

8.1. En el anillo $\mathbb{Z}[i]$, factorizar -300 y $66+12i$ como producto de una unidad por irreducibles no asociados entre sí.

8.2. Sea K un cuerpo. Dado un polinomio $f \in K[X]$ cuyo grado es 2 o 3, demostrar que f es irreducible si, y sólo si, f tiene una raíz en K.

8.3. Determinar los elementos de los anillos cociente $\frac{\mathbb{Z}_2[x]}{<x^2+1>}$ y $\frac{\mathbb{Z}_2[x]}{<x^2+x+1>}$ y las tablas de suma y producto.

8.4. Sea I el ideal de $\mathbb{Z}_3[x]$ generado por x^2+2x+2. Demostrar que el anillo cociente $\mathbb{Z}_3[x]/I$ es un cuerpo y hallar el inverso de cada elemento no nulo.

8.5. Calcular las unidades de los anillos cociente $\frac{\mathbb{Z}_5[x]}{<x^2+x+1>}$, $\frac{\mathbb{Z}_5[x]}{<x^2+1>}$ y $\frac{\mathbb{Z}_3[x]}{<x^2+2>}$.

8.6. Calcular el inverso de la clase del polinomio $2x+1$ en el anillo cociente $\frac{\mathbb{Q}[x]}{<x^3+2x^2+4x-2>}$

8.7. Construir cuerpos con 4, 8 y 9 elementos.

8.8. Determinar los elementos de los anillos cociente $\frac{\mathbb{Z}[i]}{<2>}$ y $\frac{\mathbb{Z}[i]}{<2+i>}$ y las tablas de suma y producto.

ÁLGEBRA 1

CURSO 20-21

DOBLE GRADO MATEMÁTICAS INFORMÁTICA

RELACIÓN DE EJERCICIOS 9

Estudiar si los siguientes polinomios son reducibles ó irreducibles en $\mathbb{Z}[x]$ y en $\mathbb{Q}[x]$:

1. $2x^5 - 6x^3 + 9x^2 - 15$

2. $x^4 + 15x^3 + 7$

3. $2x^4 + 2x^3 + 6x^2 + 4$

4. $2x^4 + 3x^3 + 3x^2 + 3x + 1$

5. $x^4 - 22x^2 + 1$

6. $x^3 + 17x + 36$

7. $x^5 - x^2 + 1$

8. $x^4 + 10x^3 + 5x^2 - 2x - 3$

9. $x^4 + 6x^3 + 4x^2 - 15x + 1$

10. $x^4 - x^2 - 2x - 1$

11. $x^5 + 5x^4 + 7x^3 + x^2 - 3x - 11$

12. $3x^4 + 3x^3 + 9x^2 + 6$

13. $2x^5 - 2x^2 - 4x - 2$

14. $x^6 - 2x^5 - x^4 - 2x^3 - 2x^2 - 2x - 1$