Números enteros y polinomios

1. Para cada una de las siguientes parejas de números enteros, hallar el máximo común divisor, el mínimo común múltiplo y una identidad de Bezout.

   a) 10672, 4147; b) 12075, 4655; c) 2597, 1369; d) 2048, 1275.

2. Resolver las congruencias siguientes:

   a) $5x \equiv 17 \pmod{19}$; b) $5x \equiv 17 \pmod{15}$; c) $34x \equiv 60 \pmod{98}$;

   d) $35x \equiv 119 \pmod{139}$; e) $125x \equiv 27 \pmod{256}$; f) $211x \equiv 658 \pmod{900}$.

3. Determina las soluciones de las siguientes ecuaciones.

   a) $12x = 2$ en $\mathbb{Z}_{19}$; b) $7x = 2$ en $\mathbb{Z}_{24}$; c) $31x = 1$ en $\mathbb{Z}_{50}$;

   d) $15x = 9$ en $\mathbb{Z}_{18}$; e) $25x = 10$ en $\mathbb{Z}_{65}$; f) $35x = 2$ en $\mathbb{Z}_5$;

4. Resolver los siguientes sistemas de congruencias cuando tengan solución.

   a) $\left.\begin{array}{l} x \equiv 2 \pmod{4} \\ x \equiv 4 \pmod{5} \end{array}\right\}$ b) $\left.\begin{array}{l} x \equiv 1 \pmod{2} \\ x \equiv 2 \pmod{3} \\ x \equiv 3 \pmod{5} \end{array}\right\}$ c) $\left.\begin{array}{l} x \equiv 18 \pmod{7} \\ x \equiv 3 \pmod{12} \\ x \equiv 7 \pmod{5} \\ x \equiv 11 \pmod{28} \end{array}\right\}$

   d) $\left.\begin{array}{l} x \equiv 3 \pmod{17} \\ x \equiv 4 \pmod{18} \\ x \equiv 5 \pmod{19} \end{array}\right\}$ e) $\left.\begin{array}{l} 2x \equiv 4 \pmod{6} \\ x \equiv 3 \pmod{4} \\ x \equiv 4 \pmod{5} \end{array}\right\}$ f) $\left.\begin{array}{l} 2x \equiv 3 \pmod{7} \\ 5x \equiv 4 \pmod{9} \\ 3x \equiv 1 \pmod{10} \end{array}\right\}$

5. Calcular (i) $(a+b)^2$ en $\mathbb{Z}_2$, (i) $(a+b)^5$ en $\mathbb{Z}_5$. Deducir una formula para $(a+b)^p$ en $\mathbb{Z}_p$ con p un número primo. (Sugerencia: usa el binomio de Newton).

6. Hallar un número de tres cifras que dé restos 1, 2 y 3 cuando se divide por 7, 9 y 11 respectivamente.

7. a) Demostrar que sólo existe una terna de números primos consecutivos: 3, 5 y 7.

   b) Demostrar que si $3|a^2+b^2$ entonces $3|a$ y $3|b$.

   c) Probar que para $n \geq 1$, el entero $n(7n^2+5)$ es de la forma $6k$.

   d) Si n es un entero positivo impar, probar que n^4+4n^2+11 es divisible por 16.

   e) Probar que para cualquier entero a se verifica que $3|a(2a^2+7)$.

8. Calcular las soluciones positivas de las siguientes ecuaciones diofánticas lineales:

   a) $18x+5y = 48$; b) $54x+21y = 906$; c) $1588x-5y = 7$.

9. Probar que $\text{mcd}\,(n, n+1) = 1$, $\forall n \in \mathbb{Z}$. ¿Cuáles son los posibles valores de $\text{mcd}\,(n, n+2)$ y $\text{mcd}\,(n, n+6)$?

10. Sean $a, b, c \in \mathbb{Z}$ tales que $\text{mcd}\,(a,b) = \text{mcd}\,(a,c) = 1$. Decir si son verdaderas o falsas las siguientes afirmaciones y justificar las respuestas:

    a) $\text{mcd}\,(ab, a) = 1$, b) $\text{mcd}\,(b, c) = 1$,

    c) $\text{mcd}\,(bc, a) = 1$, d) $\text{mcd}\,(ab, c) = 1$.

11. Un empresario compró 100 unidades de material informático por 4000 euros. Los precios fueron los siguientes: discos duros a 120 euros, impresoras a 50 euros y dispositivos USB a 25 euros, cada uno. Sabiendo que el empresario compró al menos una unidad de cada tipo, determinar cuantas compró.

12. Estando en Estados Unidos el seÅor Herrera se quedó sin dinero en efectivo y fue a un banco a cambiar un cheque de viaje. El cajero al pagarle confundió el número de dólares con el número de centavos y viceversa. Sin darse cuenta de este hecho el seÅor Herrera gastó 68 centavos en sellos, y entonces vio para su sorpresa que la cantidad de dinero en efectivo que tenía era exactamente el doble del valor del cheque de viaje que había cambiado. Determinar el valor mínimo que podría tener dicho cheque.

13. Probar que para todo entero n los números $n^3 - 7n + 7$ y $n - 1$ son primos entre sí.

Grupos

1. Un subconjunto no vacío H de un grupo $(G, *)$ es un subgrupo si se verifica que

$$a, b \in H \Rightarrow a * b \in H \text{ y además } a \in H \Rightarrow a^{-1} \in H.$$

   Prueba que H es un subgrupo si y sólo si $a, b \in H \Rightarrow a * b^{-1} \in H$.

2. Prueba que si H es un subconjunto *finito* de un grupo $(G, *)$ tal que $a, b \in H \Rightarrow a * b \in H$ entonces H es un subgrupo.

3. Muestra que los siguientes conjuntos tienen estructura de grupo:

   (a) $G = \{x \in \mathbb{R} \mid x \neq 0\}$ con el producto.

   (b) $G = \{1, -1, i, -i\} \subset \mathbb{C}$ con el producto.

   (c) $G = \{x \in \mathbb{C} \mid x^n = 1\}$ con el producto, para $n \in \mathbb{N}$ fijo.

   (d) $S^1 = \{z \in \mathbb{C} \mid |z| = 1\}$ con el producto.

   (e) $\mathrm{O}(2, \mathbb{Z}_3) = \left\{ A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \mid a, b, c, d \in \mathbb{Z}_3, ad - bc \neq_3 0,\ A^t = A^{-1} \right\}$.

   (f) $\mathrm{GL}(2, \mathbb{Z}_3) = \left\{ A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \mid a, b, c, d \in \mathbb{Z}_3,\ ad - bc \neq_3 0 \right\}$.

4. Indica por qué no son grupos los siguientes conjuntos:

   (a) $G = \{x \in \mathbb{R} \mid x < 0\}$ con el producto.

   (b) $G = \{a \in \mathbb{Z} \mid a$ es un cuadrado perfecto $\}$ con la suma.

   (c) $G = \{a \in \mathbb{Z} \mid a$ es un cuadrado perfecto $\}$ con el producto.

   (d) $G = \{[0], [2], [3], [6]\} \subset \mathbb{Z}_8$

5. Indica los elementos de matrices invertibles con coeficientes en $\mathbb{Z}_2$,

$$\mathrm{GL}(2, \mathbb{Z}_2) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \mid a, b, c, d \in \mathbb{Z}_2, ad - bc \neq_2 0 \right\}$$

   y calcula la tabla del grupo. Indica los órdenes de sus elementos y si el grupo es cíclico o abeliano.

6. Comprueba que conjunto G formado por las siguientes matrices,

$$I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, A = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, B = \begin{pmatrix} 1 & -1 \\ 0 & -1 \end{pmatrix}, C = \begin{pmatrix} -1 & 0 \\ -1 & 1 \end{pmatrix}, D = \begin{pmatrix} 0 & -1 \\ 1 & -1 \end{pmatrix}, E = \begin{pmatrix} -1 & 1 \\ -1 & 0 \end{pmatrix},$$

   es un grupo con el producto de matrices. ¿Es G cíclico? ¿Es G abeliano? Encontrar si lo hubiera un subgrupo de G con k elementos, en los casos $k = 2, 3, 4$.

7. En el grupo diédrico D_4 consideramos la rotación r y la simetría axial s de manera que $\mathrm{ord}(r) = 4$, $\mathrm{ord}(s) = 2$ y $r \circ s = s \circ r^3$.

(a) Prueba que son subgrupos los siguientes subconjuntos de D_4:

$$H = \{1, r, r^2, r^3\},\ L = \{1, r^2, s, r^2 \circ s\},\ G = \{1, r^2, r \circ s, r^3 \circ s\}.$$

(b) Halla los subgrupos de D_4 que tengan orden dos.

(c) Indica cuáles de los subgrupos de los apartados anteriores son abelianos o cíclicos.

(d) Halla las clases de congruencia módulo M a la izquierda (es decir los conjuntos $a \circ M$, $a \in D_4$) y a la derecha (es decir los conjuntos $M \circ a$, $a \in D_4$) para $M = \{1, s\}$ y para $M = L$. ¿Es alguno de estos dos subgrupos normal?

8. Prueba que D_3 es isomorfo al grupo simétrico S_3. ¿Es D_4 isomorfo a S_4?

9. Demostrar que el orden de un grupo finito G es un número primo si y sólo si G no tiene ningun subgrupo propio (es decir, un subgrupo distinto de $\{e\}$ y de G).

10. Sean G un grupo y a, $b \in G$. Demostrar que:

(a) Si $\mathrm{ord}(a) = n \in \mathbb{N}$ y si $n = pq$ prueba que $\mathrm{ord}(a^p) = q$.

(b) $\mathrm{ord}(a^{-1}) = \mathrm{ord}(a)$ y $\mathrm{ord}(ab) = \mathrm{ord}(ba)$.

(c) Si a y b conmutan y tienen órdenes finitos y primos entre sí, entonces $\langle a \rangle \cap \langle b \rangle = \{e\}$ y $\mathrm{ord}(ab) = \mathrm{ord}(a)\,\mathrm{ord}(b)$. ¿Es cierta esta propiedad si $ab \neq ba$?.

11. Encuentra explícitamente un isomorfismo de grupos $f : \mathbb{Z}_{12} \times \mathbb{Z}_{11} \to \mathbb{Z}_{132}$.

12. Calcula el orden de los elementos de $\mathbb{Z}_n^*$ para $n = 6, 7, 8, 9, 10, 12$. Indica generadores para cada uno de estos grupos. ¿Cuáles son cíclicos?

13. En el grupo diédrico D_6 consideramos la rotación r y la simetría axial s de manera que $\mathrm{ord}(r) = 6$, $\mathrm{ord}(s) = 2$ y $r \circ s = s \circ r^5$.

(a) Calcula los órdenes de los elementos de D_6.

(b) ¿Puede tener D_6 un subgrupo de orden 5? ¿y de orden 4?

(c) Determina los elementos de los subgrupos

$$M = \langle r^2, r^3 \rangle,\ H = \langle r^3, s \rangle,\ G = \langle r^2, s \rangle \text{ y } L = \langle s, r^5 \rangle.$$

(d) Indica cuáles de los subgrupos anteriores son abelianos, ¿cuáles de estos son cíclicos?

(e) Halla los índices $[D_6 : M]$, $[D_6 : H]$, $[D_6 : G]$ y $[D_6 : L]$.

14. Considera las siguientes matrices complejas

$$\mathbf{1} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix},\quad \mathbf{i} = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix},\quad \mathbf{j} = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix},\quad \mathbf{k} = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}$$

Prueba que el conjunto $G = \{\mathbf{1}, -\mathbf{1}, \mathbf{i}, -\mathbf{i}, \mathbf{j}, -\mathbf{j}, \mathbf{k}, -\mathbf{k}\}$ es un grupo con la multiplicación de matrices (se llama *grupo de cuaterniones*). Da la tabla de multiplicación de G e indica el orden de G y el orden de cada uno de sus elementos. Estudia si G es isomorfo al grupo diédrico D_4 o al grupo S_4 de permutaciones de cuatro elementos.

15. Sea $f : \mathbb{R} \to \mathbb{C}^*$ la aplicación definida por $f(t) = \cos(2\pi t) + i\text{sen}(2\pi t)$. Consideramos $\mathbb{R}$ como grupo con la suma y $\mathbb{C}^*$ como grupo con la multiplicación.

    (a) Prueba que f es un homomorfismo de grupos.

    (b) Halla el núcleo y la imagen de f.

    (c) Deduce que el grupo cociente $\mathbb{R}/\mathbb{Z}$ es isomorfo al grupo S^1 del ejercicio 2 (d).

16. Sea $f : G \to G'$ un homomorfismo de grupos. Demostrar:

    a) Si $a \in G$ tiene orden finito, entonces $\text{ord}(f(a)) \,|\, \text{ord}(a)$.

    b) f es inyectivo si y sólo si para todo $a \in G$ se tiene que $\text{ord}(f(a)) = \text{ord}(a)$.

17. Halla todos los homomorfismos (indicando su imagen y núcleo) entre los pares de grupos siguientes:

    a) De $(\mathbb{Z}_3, +)$ en $(\mathbb{Z}_2, +)$.
    b) De $(\mathbb{Z}_n, +)$ en $(\mathbb{Z}, +)$.
    c) De $(\mathbb{Z}_6, +)$ en $(D_3, \circ)$.
    d) De $(D_3, \circ)$ en $(\mathbb{Z}_6, +)$.
    e) De $(D_3, \circ)$ en $(D_3, \circ)$.
    f) De $(\mathbb{Z}_3, +)$ en $(\mathbb{Z}_6, +)$.
    g) De $(\mathbb{Z}_6, +)$ en $(\mathbb{Z}_3, +)$.
    h) De $(\mathbb{Z}_8, +)$ en $(\mathbb{Z}_{12}, +)$.
    i) De $(\mathbb{Z}_{12}, +)$ en $(\mathbb{Z}_{18}, +)$.

18. Sea p un número primo. Consideramos los conjuntos de matrices siguientes:

$$\text{GL}(2, \mathbb{Z}_p) = \{A \in M_2(\mathbb{Z}_p) / \det A \neq_p 0\}, \quad \text{SL}(2, \mathbb{Z}_p) = \{A \in \text{GL}(2, \mathbb{Z}_p) / \det A =_p 1\}.$$

    (a) Probar que $\text{SL}(2, \mathbb{Z}_p)$ es un subgrupo del grupo lineal $\text{GL}(2, \mathbb{Z}_p)$.

    (b) Indicar un homomorfismo de grupos $\phi : \text{GL}(2, \mathbb{Z}_p) \longrightarrow \mathbb{Z}_p^*$, siendo $\mathbb{Z}_p^*$ el grupo de unidades de $\mathbb{Z}_p$.

    (c) Mostrar que $\text{SL}(2, \mathbb{Z}_p)$ es un subgrupo normal de $\text{GL}(2, \mathbb{Z}_p)$.

    (d) Prueba que el grupo cociente $\text{GL}(2, \mathbb{Z}_p)/\text{SL}(2, \mathbb{Z}_p)$ es isomorfo a $\mathbb{Z}_p^*$.

19. Calcula los órdenes de las siguientes permutaciones:

$$\text{(a)} \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 1 & 2 & 6 & 3 & 4 \end{pmatrix} \quad \text{(b)} \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 3 & 4 & 5 & 6 & 7 & 8 & 9 & 2 & 1 \end{pmatrix}$$

    Se pide descomponer las permutaciones anteriores en producto de ciclos disjuntos y hallar su signo.

20. (a) Sean G un grupo y $H \leq G$. Si $[G : H] = 2$, prueba que H es subgrupo normal.

    (b) Deduce que el subgrupo H de D_n formado por las rotaciones es normal.

21. Indica los ocho elementos del grupo ortogonal

$$\text{O}(2, \mathbb{Z}_3) = \left\{ A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \mid a, b, c, d \in \mathbb{Z}_3, ad - bc \neq_3 0, A^t = A^{-1} \right\}.$$

    y calcula la tabla de este grupo. Indica los órdenes de sus elementos y si el grupo es cíclico o abeliano.

22. a) Determina la última cifra de 2^{333} y de 3^{1313}.

    b) Calcula el resto de dividir $2^{37\cdot 73}$ por 37.

    c) Determina las dos últimas cifras de 2^{4927}.

23. Encontrar todos los ceros en $\mathbb{Z}_5$ de cada uno de los polinomios $f(x) = x^5+3x^3+x^2+2x \in \mathbb{Z}_5[x]$ y $g(x) = 2x^{219} + 3x^{74} + 2x^{57} + 3x^{44} \in \mathbb{Z}_5[x]$.

Grupos abelianos finitamente generados

1. Determinar todas las clases de isomorfía de grupos abelianos de orden 144. Escribir sus divisores elementales y factores invariantes. Estudiar en cuáles de las clases existen elementos de orden 12 ó 15, y en caso de que exista, dar un ejemplo.

2. Dado el grupo abeliano libre con base $\{g_1, g_2, g_3\}$, encontrar una base del subgrupo H generado por los elementos $x_1 = 2g_1 - g_2$, $x_2 = 2g_1 + g_2$, $x_3 = 2g_2$.

3. Hallar todas las clases de isomorfía de grupos abelianos de orden 1000. Escribir sus divisores elementales y factores invariantes. Estudiar en cuáles de las clases existe un elemento de orden 100, y en caso de que exista, dar un ejemplo.

4. Si $G = \mathbb{Z} \times \mathbb{Z} \times \mathbb{Z}$ y H es el subgrupo de G engendrado por los elementos $a = (2, 1, 0)$ y $b = (1, 5, 0)$, determinar el grupo cociente G/H por un conjunto de generadores y relaciones.

5. Calcular el rango y los coeficientes de torsión del grupo abeliano G que tiene los generadores x, y, z, t y el sistema completo de relaciones:

$$3x + 9y + 9z = 0, \quad 9x - 3y + 9z = 0, \quad 2x + 3y + 6t = 0.$$

6. Determinar los factores invariantes y los divisores elementales de los grupos:

   a) $\mathbb{Z}_5 \times \mathbb{Z}_{15} \times \mathbb{Z}_{25} \times \mathbb{Z}_{36}$ b) $\mathbb{Z}_2 \times \mathbb{Z}_9 \times \mathbb{Z}_{35}$ c) $\mathbb{Z}_{26} \times \mathbb{Z}_{42} \times \mathbb{Z}_{49} \times \mathbb{Z}_{200} \times \mathbb{Z}_{100}$

7. Clasificar los grupos abelianos generados por elementos a, b, c y d que verifican las relaciones:

   a) $\left.\begin{array}{rcl} 2b - 4c - 12d &=& 0 \\ 12a + 4b + 10c + 6d &=& 0 \end{array}\right\}$ b) $\left.\begin{array}{rcl} 6a + 12b - 12d &=& 0 \\ 12b + 16c + 32d &=& 0 \\ 8a + 4b + 8c + 16d &=& 0 \end{array}\right\}$

   c) $\left.\begin{array}{rcl} 2a - 4c &=& 0 \\ 12a + 24b + 8c + 8d &=& 0 \\ 4a + 8b + 8c + 16d &=& 0 \end{array}\right\}$ d) $\left.\begin{array}{rcl} 8b &=& 0 \\ 2a + 10c &=& 0 \\ 20a + 10d &=& 0 \\ 6b + 12d &=& 0 \end{array}\right\}$

8. Sean $G_1 = \mathbb{Z}_{24} \times \mathbb{Z}_{60}$ y $G_2 = \mathbb{Z}_2 \times \mathbb{Z}_6 \times \mathbb{Z}_6 \times \mathbb{Z}_{20}$.

   a) Demostrar que G_1 y G_2 no son isomorfos.

   b) Estudiar si existen homomorfismos (de grupos aditivos) sobreyectivos de G_1 sobre $\mathbb{Z}_{120}$ y de G_2 sobre $\mathbb{Z}_{120}$.

   c) Obtener cuatro grupos conmutativos de orden 1440 no isomorfos entre sí y que tampoco sean isomorfos ni a G_1 ni a G_2.

Anillos y cuerpos

1. Indicar si los siguientes conjuntos tienen estructura de anillo, indicando en su caso si son conmutativos, unitarios, íntegros o cuerpos:
   (a) Los enteros positivos
   (b) Los enteros múltiplos de 7.
   (c) $\{0, 1, -1, i, -i\}$.
   (d) $\mathcal{M}_{2\times 3}(\mathbb{R})$.
   (e) $\mathcal{M}_{2\times 2}(\mathbb{Z}_3)$.
   (f) $\mathbb{Z} \times \mathbb{Z}_3 \times 2\mathbb{Z}$.
   (g) $\mathbb{Z}[\sqrt{2}] = \{a + b\sqrt{2} \,|\, a, b \in \mathbb{Z}\}$.
   (h) $\mathbb{Z}[i] = \{a + bi \,|\, a, b \in \mathbb{Z}\}$.
   (i) El conjunto de polinomios $\{a + bx + cx^2 \mid a, b, c \in \mathbb{R}\}$ de $\mathbb{R}[x]$.

2. Recordemos que un subconjunto no vacío B de un anillo A es un *subanillo* si para todo $b, b' \in B$ se tiene que $b - b'$ y bb' pertenecen a B. Además, B es un *ideal* de A si para todo $b, b' \in B$ y $a \in A$ se verifica que $b - b'$, ab, y ba pertenecen a B.
   Da un ejemplo de un subanillo de $\mathbb{Z}[x]$ que no sea un ideal.

3. Probar que el conjunto $A = \{0, 2, 4, 6, 8\}$ es un subanillo de $\mathbb{Z}_{10}$. ¿Es A un ideal de Z_{10}?. Calcula la tabla de A para el producto y estudia si A tiene elemento neutro para el producto. ¿Es A un cuerpo?

4. Mostrar que el conjunto $B := \left\{ \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \mid a, b, c \in \mathbb{R} \right\}$ es un subanillo de $\mathcal{M}_2(\mathbb{R})$. Probar que el conjunto I de matrices de la forma $\begin{pmatrix} 0 & b \\ 0 & 0 \end{pmatrix}$ es un ideal de B. ¿Es I un ideal de $\mathcal{M}_2(\mathbb{R})$?

5. Un elemento b de un anillo B es *divisor de cero* si $b \neq 0$ y existe $0 \neq a \in B$ tal que $ab = 0$. Decimos que $a \in B$ es *nilpotente* si $a \neq 0$ y existe un entero $n > 1$ tal que $a^n = 0$. Prueba que si a es nilpotente entonces es divisor de cero.
   (a) Consideramos el anillo B del ejercicio 4. Prueba que todo elemento no nulo en el ideal I del ejercicio 4 es nilpotente. Halla dos divisores de cero en el anillo B que no estén en I.
   (b) Halla los elementos nilpotentes del anillo $\mathbb{Z}_{12}$.

6. Mostrar que el conjunto B de matrices de la forma $\begin{pmatrix} a & b \\ -b & a \end{pmatrix}$ con $a, b \in \mathbb{R}$ es un subanillo unitario de $\mathcal{M}_2(\mathbb{R})$. Sea $f : B \to \mathbb{C}$ la aplicación definida por $f\begin{pmatrix} a & b \\ -b & a \end{pmatrix} = a + bi$. Prueba que f es un isomorfismo de anillos. Deduce que B es un cuerpo.

7. Recordemos que un *dominio de integridad* es un anillo unitario, conmutativo e íntegro.
   (a) Sean A_1 y A_2 dominios de integridad, ¿es $A_1 \times A_2$ un dominio de integridad?
   (b) Sea A un dominio de integridad con n elementos. Prueba que si $a \in A$ entonces la aplicación $f : A \to A$, $f(b) = ab$ es biyectiva. Deduce que A es un cuerpo.
8. Prueba que $\mathbb{Q}[\sqrt{2}] := \{a + b\sqrt{2} \,|\, a, b \in \mathbb{Q}\}$ es un subcuerpo de $\mathbb{R}$.
9. Prueba que $\mathbb{Q}[i] = \{a + bi \,|\, a, b \in \mathbb{Q}\}$ es un subcuerpo de $\mathbb{C}$.
10. Sean I, J ideales de un anillo conmutativo con unidad A. Probar que la intersección $I \cap J$ y la suma $I + J = \{a + b \,|\, a \in I,\, b \in J\}$ son ideales de A.
11. Sean $f : A \to B$ un homomorfismo de anillos, I un ideal de A y J un ideal de B. Demostrar que $f^{-1}(J)$ es un ideal de A; en particular, $\ker f = \{a \in A \mid f(a) = 0\}$ es un ideal de A. Probar que $f(I)$ es un subanillo de B. Dar un ejemplo en el que $f(I)$ no sea un ideal de B.
12. (a) Demostrar que si un ideal contiene una unidad, entonces coincide con todo el anillo. Deducir que los únicos ideales de un cuerpo K son los triviales: $\{0\}$ y K.
    (b) Demostrar que todo homomorfismo no nulo de un cuerpo en un anillo es inyectivo.
13. Sea $f : R \to S$ un homomorfismo de anillos. Probar que si f es sobreyectivo, $S \neq \{0_S\}$ y R es unitario entonces S es unitario y $f(1_R) = 1_S$.
14. Si R y S son anillos unitarios un *homomorfismo de anillos unitarios* es un homomorfismo de anillos $f : R \to S$ tal que $f(1_R) = 1_S$.
15. Estudia si la aplicación inclusión de $A = \{0, 2, 4, 6, 8\}$ en $\mathbb{Z}_{10}$ es un homomorfismo de anillos unitarios (ver ejercicio 3).

Anillos de polinomios, anillos cociente y cuerpos finitos

1. Calcular el cociente y el resto de dividir:
   a) $x^4+3x^3+2x^2+x+4$ por $3x^2+2x$ en $\mathbb{Z}_5[x]$,
   b) x^{10} por x^2+1 en $\mathbb{Z}_2[x]$;
   d) $x^4+3x^3+2x^2+x+4$ por x^2+2x en $\mathbb{Z}[x]$;
   e) $x^4+3x^3+2x^2+x+4$ por $3x^2+2x$ en $\mathbb{Q}[x]$.

2. Calcular el máximo común divisor de cada uno de los siguientes pares de polinomios y expresarlo en la forma $a(x)f(x)+b(x)g(x)$:
   a) $f(x)=x^3-1, \quad g(x)=x^4-x^3+x^2+x-2$, en $\mathbb{Q}[x]$;
   b) $f(x)=x^2+1, \quad g(x)=x^3+2x-i$, en $\mathbb{C}[x]$;
   c) $f(x)=x^3+x+1, \quad g(x)=x+1$, en $\mathbb{Z}_3[x]$;
   d) $f(x)=x^3+x+1, \quad g(x)=x+1$, en $\mathbb{Z}_5[x]$;
   e) $f(x)=x^4+x^3-x^2+x-2, \quad g(x)=x^3+6x^2+x+6$, en $\mathbb{Q}[x]$;
   f) $f(x)=x^4+x^3+x^2+x, \quad g(x)=x^2+x-1$ en $\mathbb{Z}_3[x]$
   g) $f(x)=x^5+5x^4+3x^3+2x+1, \quad g(x)=x^4+3$, en $\mathbb{Z}_7[x]$.

3. El polinomio $f(x)\in\mathbb{R}[x]$ tiene resto -45 al dividirlo por $x+1$ y -165 al dividirlo por $x-3$. Se pide:
   a) el resto de la división de $f(x)$ por x^2-2x-3;
   b) el polinomio $f(x)$, sabiendo que es de grado 4 y que es divisible por $x(x^2-4)$;

4. Encontrar todos los ceros en $\mathbb{Z}_5$ de los polinomios $f(x)=x^5+3x^3+x^2+2x\in\mathbb{Z}_5[x]$ y $g(x)=x^5-x\in\mathbb{Z}_5[x]$.

5. (a) Encontrar todos los polinomios mónicos irreducibles de grados 2 y 3 en $\mathbb{Z}_2[x]$ y $\mathbb{Z}_3[x]$, y de grado 2 en $\mathbb{Z}_5[x]$.
   (b) Descomponer en producto de polinomios irreducibles el polinomio x^4+4 en $\mathbb{Z}_5[x]$.

6. Descomponer en factores irreducibles los polinomios $f=x^6-1$ y $g=x^6+1$ vistos en los anillos $\mathbb{R}[x]$ y $\mathbb{C}[x]$.

7. Factorizar $f=4x^2-4x+8$ como producto de irreducibles en $\mathbb{Z}[x]$, $\mathbb{Q}[x]$ y $\mathbb{Z}_{11}[x]$.

8. Descomponer en factores irreducibles el polinomio $f=x^4+1$ visto, sucesivamente, en los anillos $\mathbb{Z}[x]$, $\mathbb{R}[x]$, $\mathbb{Z}_2[x]$, $\mathbb{Z}_3[x]$ y $\mathbb{Z}_7[x]$.

9. Sea $f=a_nx^n+a_{n-1}x^{n-1}+\cdots+a_0\in\mathbb{Z}[x]$ un polinomio de grado n con $a_0\neq 0$. Mostrar que si p,q son dos enteros primos entre si, entonces $f(p/q)=0$ implica que $p|a_0$ y $q|a_n$. Empleando este resultado factorizar $f=3x^3+4x^2+2x-4$ en $\mathbb{Q}[x]$.

10. Estudiar la irreducibilidad en $\mathbb{Z}[x]$ y en $\mathbb{Q}[x]$ de los polinomios:
    a) $f_1=x^3+3x^2+3x+9$, b) $f_2=5x^{10}+10x^7+20x^3+10$, c) $f_3=x^3+5x^2+3x+35$,
    d) $f_4=-x^7+25x^2-15x+10$, e) $f_5=7x^3+6x^2+4x+6$, f) $f_6=9x^4+4x^3-3x+7$.

11. Sea f un polinomio irreducible en $\mathbb{Q}[x]$.

    (a) Para $a \in \mathbb{C}$ considera el *homomorfismo evaluación* $ev_a : \mathbb{Q}[x] \to \mathbb{C}$ definido por $h(x) \mapsto h(a)$. Probar que si $f(a) = 0$ entonces el núcleo de ev_a es el ideal principal generado por f.

    (b) Deduce que si además $g \in \mathbb{Q}[x]$ y $g(a) = 0$ entonces f divide a g en $\mathbb{Q}[x]$.

12. Consideramos el homomorfismo evaluación $ev_i : \mathbb{R}[x] \to \mathbb{C}$ definido por $ev_i(P(x)) = P(i)$. Calcula la imagen de ev_i. Prueba que el núcleo $\ker(ev_i)$ es el ideal generado por el polinomio $H(x) = x^2 + 1$. Deducir que $\mathbb{R}[x]/(H(x))$ es un cuerpo isomorfo a $\mathbb{C}$.

13. Descomponer en factores irreducibles el polinomio $f = 4x^2 - 12$ considerado, sucesivamente, como elemento de $\mathbb{Z}[x]$, $\mathbb{Q}[x]$ y $\mathbb{R}[x]$. ¿Es $\mathbb{Q}[x]/(f)$ cuerpo? ¿Y $\mathbb{R}[x]/(f)$? En caso afirmativo indica su característica y su dimensión como espacio vectorial sobre $\mathbb{Q}$ y $\mathbb{R}$ respectivamente.

14. ¿Es $\mathbb{Q}[x]/(x^2 - 5x + 6)$ un cuerpo? ¿Y $\mathbb{Q}[x]/(x^2 - 6x + 6)$? En caso afirmativo indica su característica y su dimensión como espacio vectorial sobre $\mathbb{Q}$.

15. Estudiar el anillo cociente $\mathbb{Z}_2[x]/(f)$, indicando el número de elementos y construyendo la tabla de adición y de multiplicación en los siguientes casos:

    (i) $f = x^2+1$, (ii) $f = x^2+x$ (iii) $f = x^2+x+1$ (iv) $f = x^3+x+1$ (v) $f = x^3+x^2+1$

    ¿Alguno de estos anillos es cuerpo? Indica en este caso su característica. ¿Cúal es la dimensión de estos anillos como espacios vectoriales sobre el cuerpo $\mathbb{Z}_2$?

16. Construir cuerpos con 4, 8, 9 y 25 elementos, indicando su característica.

17. Hallar un divisor de cero en el anillo cociente $A := \mathbb{Q}[x]/(x^3 - x^2 + x - 1)$. ¿ Es $\alpha = [x]$ (clase de x en el anillo A) una unidad en este anillo? En caso afirmativo encuentra su inverso.

18. Consideramos $\alpha = [x]$ como elemento de $\mathbb{Z}_3[x]/(x^2 + x - 1)$. Calcular, si existe, el inverso de $\alpha^4 + \alpha^3 + \alpha^2 + \alpha$.

19. Sea $f = x^3 + x + 1 \in \mathbb{F}[x]$ y se considera el cociente $L = \mathbb{F}[x]/(f)$.

    a) Estudiar si L es un cuerpo en los casos $\mathbb{F} = \mathbb{Z}_3$ y $\mathbb{F} = \mathbb{Z}_5$.

    b) Denotamos $\alpha = [x] \in L$. En cada caso, estudiar si $\alpha - 1$ tiene o no inverso en L, calculándolo si existe.

20. Consideramos un número primo $n \geq 2$ y el anillo cociente $A = \mathbb{Z}_n[x]/(x^2-x)$. Mostrar que es un isomorfismo de anillos la aplicación $f : A \to \mathbb{Z}_n \times \mathbb{Z}_n$ dada por $f(a+b\alpha) = (a+b, a)$ (siendo $\alpha = [x]$ en A).

21. Estudiar si hay isomorfismos entre los siguientes anillos

    $\mathbb{Z}_2 \times \mathbb{Z}_2$, $\mathbb{Z}_4$, $\mathbb{Z}_2[x]/(x^2+x+1)$, $\mathbb{Z}_2[x]/(x^3+x+1)$, $\mathbb{Z}_2[x]/(x^3+x^2+1)$, $\mathbb{Z}_2[x]/(x^2)$,

    justificando la respuesta en cada caso.

22. Sea K un cuerpo finito. Sea a un elemento del grupo multiplicativo $K^* = K \setminus \{0\}$ tal que $ord\,(a) = \max\{ord\,(b) \mid b \in K^*\}$.

    a) Prueba que para todo $b \in K^*$ se tiene que $ord\,(b) | ord\,(a)$.

    b) Comprueba que todos los elementos de K^* son raíces del polinomio $x^{ord\,(a)} - 1$.

    c) Deducir que K^* es el grupo cíclico generado por a.

23. Sea A el anillo $\mathbb{Z}_3[x]/(f)$, con $f = x^2 + x - 1$ y $\alpha = [x]$.

    a) Indica los órdenes posibles de los elementos del grupo multiplicativo de unidades de A.

    b) Calcula el orden de α y de $\alpha + 2$ en A^*.

24. Sea $f = x^3 + x^2 + x + 1 \in \mathbb{Z}_5[x]$. Denotamos $L := \mathbb{Z}_5[x]/(f)$ y $\alpha := [x] \in L$.

    a) Probar que L es un cuerpo indicando su característica, el número de elementos y una base de L como espacio vectorial sobre el cuerpo $\mathbb{Z}_5$.

    b) Indicar los ordenes posibles de los elementos del grupo multiplicativo L^*.

    c) Deduce que α^4 es de orden 31 (sin calcular las potencias de α^4) e indica el orden de $2\alpha^4$.

25. Sean $f = x^5 + x^2 + 1$ y $g = x^2 + x + 1$ en $\mathbb{Z}_2[x]$. Se pide:

    (a) Calcular el máximo común divisor de f y g, y una identidad de Bezout.

    (b) Indica los elementos del anillo cociente $K = \mathbb{Z}_2[x]/(f)$ en función de $\alpha = [x] \mod f$. Prueba que K es un cuerpo.

    (c) Halla un elemento $\beta \in K$ tal que $(\alpha^2 + \alpha + 1)\beta = 1 + \alpha$.

    (d) Indica los órdenes posibles de los elementos del grupo de unidades K^* de K. Determina, sin calcular las potencias, cúal es el orden de α en K^*.