0. Enteros

1. Para los números enteros a y b que se citan, halla su máximo común divisor y mínimo común múltiplo, así como enteros n y m tales que $na+mb$ sea el máximo común divisor.
   i) $a = 1761$, $b = 1567$.
   ii) $a = 507885$, $b = 60808$.

2. Dado un primo p, prueba que $\sqrt{p}$ no es un número racional.

3. Dado $a = a_n 10^n + a_{n-1}10^{n-1} + \cdots + a_1 10 + a_0$, con $0 \leq a_i < 10$ para todo $i = 0, \ldots, n$, demuestra que $a \equiv a_0 + a_1 + \cdots + a_n \pmod 9$. Deduce la regla del 9 para comprobar multiplicaciones.

4. Siendo a como en el ejercicio anterior, demuestra que $a \equiv a_0 - a_1 + \cdots \pm a_n \pmod{11}$.

5. Sean $a, b \in \mathbb{Z}$:
   i) prueba que $10a + b$ es múltiplo de 7 si y sólo si lo es $a - 2b$,
   ii) prueba que $10a + b$ es múltiplo de 13 si y sólo si lo es $a + 4b$.

6. Calcula el resto de dividir 37^{100} por 29.

7. Halla las dos últimas cifras de 9^{1500}.

8. Halla la última cifra de $99999^{9999^{999^{99^9}}}$.

9. Demuestra que no hay cuadrados terminados en 2, 3, 7 u 8.

10. Prueba que el cuadrado de todo número impar deja resto 1 al dividirlo por 8.

11. Demuestra que $\dfrac{7^{1968^{1978}} - 3^{68^{78}}}{1978 - 1968}$ es un número entero.

12. Con $a, b \in \mathbb{Z}$, prueba que al dividir $a^2 + b^2$ por 4 nunca da resto 3.

13. Prueba que no existen $a, b, c \in \mathbb{Z}$, no todos nulos, tales que $a^2 + b^2 = 3c^2$.

14. Para cada uno de los siguientes pares de enteros a y n, prueba que a y n son primos entre sí y encuentra el inverso de a módulo n (esto es, $1 \leq x < n$ tal que $ax \equiv 1 \pmod n$):
   i) $a = 13$, $n = 20$,
   ii) $a = 69$, $n = 89$.
   iii) $a = 1891$, $b = 3797$,
   iv) $a = 6003722857$, $n = 77695236973$.

15. Sea p un número primo, dado n tal que $1 \leq n \leq p-1$, demuestra que p divide a $\binom{p}{n}$. Deduce que si $x, y \in \mathbb{Z}$, $(x+y)^p \equiv x^p + y^p \pmod p$.

---

[13] Reduce módulo 4.

1. Anillos

16. Razona cuáles de los siguientes conjuntos son subanillos del anillo de las funciones del intervalo $[0,1]$ en $\mathbb{R}$:
    a) El conjunto de funciones $f(x)$ tal que $f(q)=0$ para todo $q \in \mathbb{Q} \cap [0,1]$.
    b) El conjunto de funciones polinómicas.
    c) El conjunto de funciones que tienen solamente un número finito de ceros junto con la función cero.
    d) El conjunto de funciones que tienen un número infinito de ceros.
    e) El conjunto de todas las combinaciones lineales con coeficientes racionales de las funciones $\cos(nx)$ y $\operatorname{sen}(mx)$ con $n, m \in \{0,1,2,\ldots\}$.

17. Sea $\overline{0} \neq \overline{n} \in \mathbb{Z}/m\mathbb{Z}$, prueba que $\overline{n}$ es divisor de cero si y sólo si $\operatorname{mcd}(n,m) \neq 1$.

18. Definimos el *centro* de un anillo R como el conjunto $Z(R) = \{z \in R \mid zx = xz \ \ \forall x \in R\}$. Prueba que el centro de un anillo es un subanillo. Si además R es un anillo de división, demuestra que $Z(R)$ es un cuerpo.

19. Dado un elemento a de un anillo R, definimos el conjunto $C(a) = \{x \in R \mid xa = ax\}$. Prueba que $C(a)$ es un subanillo de R. Demostrar que $Z(R) = \bigcap_{a \in R} C(a)$.

20. Halla el centro del anillo de cuaternios de Hamilton.

21. Sean R y S dos anillos. Demuestra que el producto cartesiano $R \times S$ es un anillo con las operaciones $(r,s)+(r',s') = (r+r', s+s')$ y $(r,s)\cdot(r',s') = (rr', ss')$. Observa que $R \times S$ es conmutativo si y sólo si R y S lo son y que $R \times S$ posee identidad si y sólo si R y S tienen identidades.

22. Un anillo R se dice *anillo booleano* si $a^2 = a \ \forall a \in R$. Demuestra que todo anillo booleano es conmutativo.

23. Sea X un conjunto no vacío y $\mathcal{P}(X)$ el conjunto de todos los subconjuntos de X. Definimos una suma y un producto en $\mathcal{P}(X)$ mediante

$$A + B = (A \setminus B) \cup (B \setminus A) \quad \text{y} \quad A \cdot B = A \cap B$$

    donde $A \setminus B = A \cap B^c$ y B^c denota el complementario de B. Demuestra que $\mathcal{P}(X)$ con estas operaciones es un anillo booleano con identidad.

24. Sea d un número entero que no es un cuadrado perfecto. Definimos el siguiente subconjunto de $\mathbb{C}$:

$$\mathbb{Z}[\sqrt{d}\,] = \{a + b\sqrt{d} \mid a, b \in \mathbb{Z}\}$$

    a) Prueba que $\mathbb{Z}[\sqrt{d}\,]$ es un subanillo de $\mathbb{C}$.
    b) Definimos la aplicación, que llamaremos *norma*, $N : \mathbb{Z}[\sqrt{d}\,] \to \mathbb{Z}$ mediante $N(a + b\sqrt{d}) = a^2 - db^2$. Demuestra que $N(xy) = N(x)N(y)$ para todo $x, y \in \mathbb{Z}[\sqrt{d}\,]$.
    c) Demuestra que el inverso en $\mathbb{C}$ de $a + b\sqrt{d} \neq 0$ es $\dfrac{a - b\sqrt{d}}{a^2 - db^2}$.
    d) Demuestra que u es una unidad en $\mathbb{Z}[\sqrt{d}\,]$ si y sólo si $N(u) = \pm 1$. Como consecuencia, si $d < -1$ entonces $\mathbb{Z}[\sqrt{d}\,]^\times = \{\pm 1\}$.

25. Prueba que las siguientes tablas definen un cuerpo

$+$	0	1	α	β
0	0	1	α	β
1	1	0	β	α
α	α	β	0	1
β	β	α	1	0

$\cdot$	0	1	α	β
0	0	0	0	0
1	0	1	α	β
α	0	α	β	1
β	0	β	1	α

¿Cuántos cuerpos hay, salvo isomorfismos, de 4 elementos?

26. Considera el conjunto

$$\mathcal{Q}_1 = \left\{ \begin{pmatrix} a+bi & c+di \\ -c+di & a-bi \end{pmatrix} \mid a,b,c,d \in \mathbb{R} \right\}$$

con la suma y producto usuales en $\mathrm{Mat}_2(\mathbb{C})$, así como el conjunto

$$\mathcal{Q}_2 = \left\{ \begin{pmatrix} \alpha & \beta & \gamma & \delta \\ -\beta & \alpha & -\delta & \gamma \\ -\gamma & \delta & \alpha & -\beta \\ -\delta & -\gamma & \beta & \alpha \end{pmatrix} \mid \alpha,\beta,\gamma,\delta \in \mathbb{R} \right\}$$

con la suma y producto usuales en $\mathrm{Mat}_4(\mathbb{R})$.
Prueba que tanto $\mathcal{Q}_1$ como $\mathcal{Q}_2$ son anillos isomorfos a $\mathbb{H}$.

27. Sean A y B anillos con identidad, $f : A \longrightarrow B$ un homomorfismo tal que $f(a)$ es una unidad de B para algún $a \in A$. Prueba que $f(1_A) = 1_B$ y que $f(u^{-1}) = [f(u)]^{-1}$ para toda unidad $u \in A$.

28. Comprueba si las siguientes aplicaciones son homomorfismos de anillos, ¿cuáles son isomorfismos?
    i) $\mathbb{Q}(\sqrt{2}) \longrightarrow \mathbb{Q}(\sqrt{2}) : x + y\sqrt{2} \mapsto x - y\sqrt{2}$,
    ii) $2\mathbb{Z} \longrightarrow 3\mathbb{Z} : 2n \mapsto 3n$,
    iii) $\mathbb{C} \longrightarrow \mathbb{C} : x + yi \mapsto x - yi$,
    iv) $\mathbb{Z}_{60} \longrightarrow \mathbb{Z}_6 \times \mathbb{Z}_{10} : m + 60\mathbb{Z} \mapsto (m + 6\mathbb{Z}, m + 10\mathbb{Z})$ $(0 \leq m < 60)$.

29. Sea d un número entero no cuadrado perfecto y $S = \left\{ \begin{pmatrix} a & b \\ db & a \end{pmatrix} \mid a,b \in \mathbb{Z} \right\}$. Prueba que:
    a) S es subanillo de $M_2(\mathbb{Z})$.
    b) La aplicación $\varphi\colon \mathbb{Z}[\sqrt{d}\,] \to S$ definida mediante $\varphi(a+b\sqrt{d}) = \begin{pmatrix} a & b \\ db & a \end{pmatrix}$ es un isomorfismo de anillos.

---

[28] $\mathbb{Q}(\sqrt{2}) = \{x + y\sqrt{2} \mid x,y \in \mathbb{Q}\}$ $(\subseteq \mathbb{R})$ es un cuerpo, $\mathbb{Z}_n := \mathbb{Z}/n\mathbb{Z}$.

30. Sea X un conjunto no vacío y $\mathcal{P}(X)$ el anillo booleano de los subconjuntos de X. Sea R el anillo de todas las funciones de X en $\mathbb{Z}_2$. A cada $A \in \mathcal{P}(X)$ le asociamos la función

$$\chi_A \colon X \to \mathbb{Z}_2 \quad \text{dada por} \quad \chi_A(x) = \begin{cases} 1 & x \in A \\ 0 & x \notin A \end{cases}$$

(χ_A se llama la función característica de A con valores en $\mathbb{Z}_2$). Demuestra que la aplicación $\mathcal{P}(X) \to R$ definida por $A \mapsto \chi_A$ es un isomorfismo de anillos.

31. Determina cuáles de los siguientes conjuntos son ideales de $\mathbb{Z}[X]$:
    a) El conjunto de polinomios cuyo término independiente es múltiplo de 3.
    b) El conjunto de polinomios cuyo coeficiente de X^2 es múltiplo de 3.
    c) El conjunto de polinomios cuyo término independiente y los coeficientes de X y X^2 son nulos.
    d) El conjunto de polinomios cuyos coeficientes suman cero.
    e) El conjunto de polinomios $p(X)$ tales que $p'(0) = 0$, donde $p'(X)$ denota la derivada de $p(X)$.

32. Sea a un elemento de un anillo R.
    a) Prueba que el conjunto $\{x \in R \mid xa = 0\}$ es un ideal a izquierda del anillo R, al que llamaremos anulador a izquierda en R del elemento a. Análogamente prueba que el conjunto $\{x \in R \mid ax = 0\}$ es un ideal a derecha, que llamaremos anulador a derecha en R de a.
    b) Demuestra que si L es un ideal a izquierda de R entonces el conjunto $\{x \in R \mid xa = 0 \ \forall a \in L\}$ es un ideal bilátero de R (este ideal se llama anulador en R de L).

33. Sea A un anillo conmutativo con identidad, un elemento $a \in A$ se dice *nilpotente* si existe $n \geq 1$ tal que $a^n = 0$. Demuestra que:
    i) A no tiene elementos nilpotentes no nulos si y sólo si 0 es el único elemento de A cuyo cuadrado es 0 .
    ii) El conjunto $\mathcal{N}(A)$ de todos los elementos nilpotentes de A es un ideal de A (llamado *nilradical* de A) y $\mathcal{N}\left(A/\mathcal{N}(A)\right) = 0$.
    iii) $\mathcal{N}(A)$ es la intersección de todos los ideales primos de A.

34. Sea A un anillo conmutativo con identidad, demuestra que la suma de una unidad con un elemento nilpotente es una unidad.

35. Sea A un anillo conmutativo con identidad, se define su *radical de Jacobson* $\mathcal{J} = \mathcal{J}(A)$ como la intersección de todos los ideales maximales de A. Demuestra que $a \in \mathcal{J}(A)$ si y sólo si $1 - ab$ es una unidad para todo $b \in A$. Demuestra también que $\mathcal{J}(A/\mathcal{J}(A)) = 0$ y que $\mathcal{N}(A) \subset \mathcal{J}(A)$.

---

[30] R es un anillo con las operaciones $(f+g)(x) = f(x) + g(x)$ y $(f \cdot g)(x) = f(x) \cdot g(x)$.

[33] Es fácil ver que $\mathcal{N}$ está contenido en todo ideal primo de A. Para el otro contenido, sea a no nilpotente y considera el conjunto de ideales I de A tales que $a^n \notin I$ para todo $n \in \mathbb{N}$. Aplica el lema de Zorn a este conjunto y comprueba que sus elementos maximales son ideales primos de A.

[34] Si $a^m = 0$, con m impar, se verifica $1 = 1 + a^m = (1+a)(1 - a + a^2 - \cdots + a^{m-1})$.

[35] Si M es ideal maximal de A y $a \notin M$, entonces $M + (a) = A$.

36. Sea A un anillo conmutativo con identidad, sea $\mathcal{Z} = \mathcal{Z}(A)$ el subconjunto de A formado por 0 y todos los divisores de cero de A. Demuestra que $\mathcal{Z}$ es unión de ideales primos.

37. Sea R un dominio de integridad y a, b elementos de R. Prueba que $(a) = (b)$ si y sólo si $a = ub$ para alguna unidad u en R.

38. Sea P un ideal propio del anillo A conmutativo con identidad. Prueba que P es primo si y sólo si para cualesquiera ideales I, J de A tales que $IJ \subseteq P$ se cumple $I \subseteq P$ ó $J \subseteq P$.

39. Prueba que en un anillo booleano todo ideal finitamente generado es principal.

40. Sea R un anillo con identidad. Un elemento $e \in R$ se dice idempotente si $e^2 = e$. Supongamos que e es un idempotente en R tal que $er = re\ \forall r \in R$. Demuestra que $(1-e), (e)$ son ideales de R tal que $R \cong (e) \times (1-e)$. Además $e, 1-e$ son identidades de los anillos (e) y $(1-e)$ respectivamente.

41. Sea R un anillo booleano finito con identidad. Demuestra que $R \cong \mathbb{Z}_2 \times \cdots \times \mathbb{Z}_2$.

42. Resuelve los siguientes sistemas de congruencias simultáneas:

[1] En $\mathbb{Z}$, $\begin{cases} x \equiv 1 \pmod 8 \\ x \equiv 3 \pmod 7 \\ x \equiv 9 \pmod{11} \end{cases}$

[2] En $\mathbb{Z}_3[X]$, $\begin{cases} f(X) \equiv 1 \pmod{X-1} \\ f(X) \equiv X \pmod{X^2+1} \\ f(X) \equiv X^3 \pmod{X+1} \end{cases}$

43. i) ¿Son $\mathbb{Z}[X]$ y $\mathbb{Q}[X]$ anillos isomorfos?
ii) ¿Son los cuerpos de cocientes de $\mathbb{Z}[X]$ y $\mathbb{Q}[X]$ isomorfos?

44. Sea A un dominio de integridad, $Q(A)$ su cuerpo de fracciones, B un anillo tal que $A \subseteq B \subseteq Q(A)$. Prueba que $Q(A)$ es el cuerpo de fracciones de B. En particular, comprueba que $\mathbb{Q}$ es el cuerpo de fracciones de $\{\frac{m}{2^n} \mid m \in \mathbb{Z}, n \in \mathbb{N}\}$.

45. Dado un cuerpo F, demuestra que:
i) La aplicación $\Gamma\colon \mathbb{Z} \to F$ dada por $\Gamma(0) = 0$, $\Gamma(n) = 1 + \cdots + 1$ (n sumandos) y $\Gamma(-n) = -\Gamma(n)$ ($n \in \mathbb{N}$) es un homomorfismo de anillos.
ii) $\ker \Gamma$ es un ideal primo de $\mathbb{Z}$.
iii) Si $\ker \Gamma = 0$, entonces F contiene una copia isomorfa de $\mathbb{Q}$. En particular todo subcuerpo de $\mathbb{R}$ contiene a $\mathbb{Q}$.
iv) Si $\ker \Gamma \neq 0$, entonces $\ker \Gamma$ es ideal maximal y así F contiene una copia isomorfa de $\mathbb{Z}/p\mathbb{Z}$ para algún primo p.

---

[36] Dado $x \in \mathcal{Z}(A)$, aplica el lema de Zorn al conjunto de todos los ideales de A que contienen a x y están contenidos en $\mathcal{Z}$. Prueba que sus elementos maximales son ideales primos de A. Prueba que $\mathcal{Z}$ es la unión de todos ellos.

[39] Observa que $(x, y) = (x + y + xy)$.

[41] Usa el ejercicio anterior.

[43] i) Si lo fueran, comprueba que se tendría que $1_{\mathbb{Z}} \to 1_{\mathbb{Q}}$, luego $n \to n, \forall n \in \mathbb{Z}$.

46. Sea R un dominio euclídeo con una norma N que satisface $N(a) \leq N(ab)\ \forall\ 0 \neq a, b \in R$. Demuestra que:
    i) $N(a) = N(ua)\ \forall u \in R^\times$,
    ii) $(a) = (b)$ si y sólo si $b \in (a)$ y $N(a) = N(b)$.

47. Prueba que $\mathbb{Z}[\sqrt{-2}]$, con la norma dada por $N(a + b\sqrt{-2}) = a^2 + 2b^2$ es un dominio euclídeo.

48. En el anillo euclídeo correspondiente A, halla el máximo común divisor d de los elementos a y b y encuentra r y s tales que $d = ra + sb$.
    i) $A = \mathbb{Z}_3[X], \quad a = 2X^2 + 2, \quad b = X^5 + 2$.
    ii) $A = \mathbb{Z}[i], \quad a = 7 - 3i, \quad b = 5 + 3i$.

49. Sea A un D.F.U., demuestra que:
    i) todo ideal primo no nulo contiene un elemento que es primo,
    ii) si $0 \neq a \in A$, entonces existe sólo un número finito de ideales principales de A que contienen al elemento a.

50. Recuerda que $\mathbb{Z}[\sqrt{-1}]$ es un D.E, en particular un D.F.U.
    i) Demuestra que las soluciones enteras de $x^2 + y^2 = z^2$ son, salvo permutación de x e y, $x = d(u^2 - v^2)$, $y = 2duv$, $z = d(u^2 + v^2)$, donde d, u, v son enteros con u y v primos entre sí.
    ii) Prueba que la ecuación $x^4 + y^4 = z^2$ no tiene soluciones enteras no triviales.
    iii) Prueba que la ecuación de Fermat $x^n + y^n = z^n$ no tiene soluciones enteras no triviales cuando n es múltiplo de 4.

A través de los siguientes ejercicios demostraremos que el anillo $R = \{a + b\frac{1+\sqrt{-19}}{2} \mid a, b \in \mathbb{Z}\}\ (\subseteq \mathbb{C})$ es un dominio de ideales principales pero no un dominio euclídeo.

51. Sea $F = \{a + b\sqrt{-19} \mid a, b \in \mathbb{Q}\} \subseteq \mathbb{C}$ y $R = \{a + b\frac{1+\sqrt{-19}}{2} \mid a, b \in \mathbb{Z}\} \subseteq F$.
    i) Prueba que F es el cuerpo de fracciones de R.
    ii) Dado $x = a + b\sqrt{-19} \in F$ y $\bar{x}$ su conjugado complejo, definimos $N(x) = x\bar{x}$. Demuestra que N es multiplicativa (i.e $N(xy) = N(x)N(y)\ \forall x, y \in F$). Comprueba también que si $0 \neq x \in R$ entonces $0 < N(x) \in \mathbb{Z}$.
    iii) Prueba que ± 1 son las únicas unidades de R.

52. **Criterio de Dedekind y Hasse.** Sea S un dominio de integridad y $N\colon S \to \mathbb{Z}$ tal que $N(x) > 0\ \forall 0 \neq x \in S$ y verificando que $\forall f, g \in S$ con $N(f) \geq N(g)$, o bien g divide a f en S, o bien existen $s, t \in S$ tal que $0 < N(sf - tg) < N(g)$. Demuestra que S es un dominio de ideales principales.

---

[50] i) Puede suponerse que si x, y, z es una solución, $x, y, z \geq 1$, estos elementos son primos dos a dos siendo x, z impares e y par. Factoriza la ecuación $(x + iy)(x - iy) = z^2$, prueba que $x + iy, x - iy$ son primos entre sí y deduce que son cuadrados.

ii) Si $x, y, z \geq 1$ es una solución tal que z es mínimo, aplica adecuadamente i) y llega a una contradicción.

[52] Si I es un ideal no nulo de S y $0 \neq b \in I$ con $N(b)$ mínima, demuestra que $I = (b)$.

53. Veamos que R con la función N definida anteriormente satisface el Criterio de Dedekind y Hasse, demostrando así que R es un D.I.P. Sean f, g elementos no nulos de R tal que $\frac{f}{g} \notin R$. Escribe $\frac{f}{g} = \frac{a+b\sqrt{-19}}{c} \in F$ con a, b, c números enteros sin ningún divisor común y $c > 1$ (pues g no divide a f en R).
    a) Observa que, como N es multiplicativa, la condición $0 < N(sf - tg) < N(g)$ es equivalente a
    $$0 < N\left(\frac{f}{g}s - t\right) < 1 \qquad (*)$$
    b) Como a, b, c no tienen divisores comunes entonces existen $x, y, z \in \mathbb{Z}$ tal que $ax + by + cz = 1$. Podemos encontrar $q, r \in \mathbb{Z}$ con $ay - 19bx = cq + r$ y $|r| \leq c/2$. Con estos q y r los elementos $s = y + x\sqrt{-19}$ y $t = q - z\sqrt{-19}$ satisfacen la ecuación $(*)$ si $c \geq 5$.
    c) Si $c = 2$, como $f/g \notin R$ entonces a, b tienen distinta paridad y así puedes comprobar que $s = 1$ y $t = \frac{(a-1)+b\sqrt{-19}}{2}$ son elementos de R que satisfacen $(*)$.
    d) Si $c = 3$, muestra que $a^2 + 19b^2$ no es un múltiplo de 3, luego podemos encontrar $q, r \in \mathbb{Z}$ tal que $a^2 + 19b^2 = 3q + r$ con $r = 1$ ó 2. Los elementos $s = a - b\sqrt{-19}$ y $t = q$ satisfacen $(*)$.
    e) Veamos, por último, el caso $c = 4$. Aquí a y b no son a la vez pares. Si sólo uno de ellos es impar entonces podemos encontrar $q, r \in \mathbb{Z}$ tal que $a^2 + 19b^2 = 4q + r$ y $0 < r < 4$. En este caso $s = a - b\sqrt{-19}$ y $t = q$ satisfacen $(*)$. Finalmente si a y b son impares entonces prueba que existe $q \in \mathbb{Z}$ verificando $a^2 + 19b^2 = 8q + 4$ por lo que $s = \frac{a-b\sqrt{-19}}{2}$ y $t = q$ son elementos de R que cumplen $(*)$.

54. En este ejercicio demostraremos que, aunque R es un D.I.P., sin embargo R no es un dominio euclídeo. Sea D un dominio de integridad y $\tilde{D}$ el conjunto de unidades de D junto con el 0. Un elemento $u \in D \setminus \tilde{D}$ se dice *divisor universal* si para todo $x \in D$ existe $z \in \tilde{D}$ tal que u divide a $x - z$ en D.
    a) Demuestra que si D no es un cuerpo y D no tiene divisores universales entonces D no es un dominio euclídeo.
    b) Prueba que el anillo R no tiene divisores universales y por lo tanto no puede ser un dominio euclídeo.

55. Prueba que $R = \{a + b\frac{1+\sqrt{-m}}{2} \mid a, b \in \mathbb{Z}\}$ es D.E. para $m = 3, 7, 11$.

---

[54] a) Si D es un dominio euclídeo, entonces cualquier elemento de $D \setminus \tilde{D}$ de norma mínima es un divisor universal.

b) Demuestra que los únicos divisores en R de 2 son $\{\pm 1, \pm 2\}$ y análogamente los divisores de 3 son $\{\pm 1, \pm 3\}$. Tomando $x = 2$ demuestra que si u es un divisor universal, u es un divisor, no unidad, de 2 o 3. En consecuencia $u = \pm 2$ o ± 3. Sin embargo, con $x = \frac{1+\sqrt{-19}}{2}$ podemos ver que ninguno de éstos son divisores universales.

[55] Para hallar el cociente de dos elementos, calcula su cociente en $\mathbb{C}$, que será de la forma $u + v\sqrt{-m}$ con $u, v \in \mathbb{Q}$, elige ahora $c, d \in \mathbb{Z}$ con $|c - 2u| \leq 1$, $|d - 2v| \leq \frac{1}{2}$ y de la misma paridad y considera como cociente el elemento $\frac{c+d\sqrt{m}}{2}$.

2. Polinomios

56. Sea A un anillo conmutativo y unitario e i, n enteros positivos con $i \leq n$. Demuestra que $A[X_{i+1}, \ldots, X_n]$ es isomorfo al anillo cociente $A[X_1, \ldots, X_n]/(X_1, \ldots X_i)$. Deduce que si A es un $D.I.$ entonces $(X_1, \ldots, X_i)$ es un ideal primo y que si A es un cuerpo, entonces $(X_1, \ldots, X_n)$ es un ideal maximal.

57. Sea I un ideal del anillo conmutativo y unitario A.
   i) Prueba que el conjunto $I[X]$ de todos los polinomios de $A[X]$ cuyos coeficientes están en I es un ideal de $A[X]$ y que es el menor ideal de $A[X]$ que contiene a I.
   ii) Demuestra que $I[X] \subseteq (I, X)$, $A[X]/I[X] \cong (A/I)[X]$ y $A[X]/(I, X) \cong A/I$.
   iii) Deduce que si P es un ideal primo de A, entonces $P[X]$ y (P, X) son ideales primos de $A[X]$ y si M es un ideal maximal de A, entonces (M, X) lo es de $A[X]$.

58. Demuestra que $\mathbb{Z}[X]/(X^2 + 2) \cong \mathbb{Z}[\sqrt{-2}]$. Prueba que $(X^2 + 2)$ es un ideal primo en $\mathbb{Z}[X]$ que no es maximal; encuentra un ideal maximal que lo contenga.

59. Prueba que (X, Y) no es un ideal principal de $\mathbb{Q}[X, Y]$.

60. i) Prueba que existe un monomorfismo de $\mathbb{Z}_2[X]$ en $\mathbb{Z}_2[X, Y]/(XY + 1) = B$ tal que la imagen de X es una unidad de B.
   ii) Demuestra que $\mathbb{Z}_2[X]$ y B no son isomorfos.
   iii) Demuestra que existe un monomorfismo de B en el cuerpo de fracciones de $\mathbb{Z}_2[X]$.
   iv) Deduce que los cuerpos de fracciones de $\mathbb{Z}_2[X]$ y $\mathbb{Z}_2[X, Y]/(XY + 1)$ son isomorfos.

61. Demuestra la siguiente variante del criterio de Eisenstein. Sea P un ideal primo en un dominio de factorización única R y $p(X) = a_0 + \cdots + a_n X^n$ un polinomio en $R[X]$ con $n \geq 1$. Supongamos que $a_n \notin P, a_{n-1}, \cdots, a_0 \in P$ y $a_0 \notin P^2$. Prueba que $p(X)$ es irreducible en $Q[X]$, donde Q denota el cuerpo de fracciones de R.

62. Sea p un primo impar en $\mathbb{Z}$ y n un entero positivo. Prueba que $X^n - p$ es irreducible sobre $\mathbb{Z}[i]$.

63. Comprueba que $X^3 - X$ tiene 6 raíces en $\mathbb{Z}_6 = \mathbb{Z}/6\mathbb{Z}$.

64. Comprueba que el polinomio $f(X) = X \in \mathbb{Z}_6[X]$ se factoriza como $f(X) = (3X+4)(4X+3)$, luego no es irreducible. Además:
   i) Las reducciones de $f(X)$ módulo los ideales (2) y (3) de $\mathbb{Z}_6$ sí son irreducibles.
   ii) Prueba que en toda factorización $f(X) = g(X)h(X)$ en $\mathbb{Z}_6[X]$, la reducción de $g(X)$ módulo (2) es 1 o X y la de $h(X)$ X o 1 respectivamente, y que algo parecido pasa módulo (3). Determina todas las factorizaciones de $f(X)$ en $\mathbb{Z}_6[X]$.

65. Describe las unidades, los elementos nilpotentes y los divisores de cero de los anillos $\mathbb{Z}_4[X]$ y $\mathbb{Z}_6[X]$.

---

[64] ii) Usa el Teorema Chino de los restos.

66. Sea F un cuerpo, $a_1, \ldots, a_n \in F$ distintos dos a dos, y $b_1, \ldots, b_n \in F$ arbitrarios. Sea $p_i(X) = \prod_{j \neq i}(X - a_j)$ $(i = 1, \ldots, n)$ y sea $f(X) = \sum_{i=1}^{n} b_i \frac{p_i(X)}{p_i(a_i)}$. Demuestra que $f(X)$ es el único polinomio sobre F de grado menor o igual que $n-1$ para el que $f(a_i) = b_i (i = 1, \ldots, n)$. *(Método de interpolación de Lagrange).*

67. Construye un polinomio $f(X) \in \mathbb{Q}[X]$ de grado a lo sumo 3 tal que:
i) $f(0) = f(1) = 1$; $f(2) = 3$; $f(3) = 4$,
ii) $f(-2) = 0$; $f(-1) = -2$; $f(1) = 3$; $f(2) = 4$.

68. Factoriza los siguientes polinomios en $\mathbb{Z}[X, Y]$:
$X^3 + YX^2 + (Y - 2Y^2)X - Y^2$,
$Y^2X^3 + Y^3X + Y^3X^2 - Y^4 - 2Y^4X - X^3 - YX^2 - YX + 2Y^2X + Y^2$.

69. Prueba que los siguientes polinomios son irreducibles en $\mathbb{Q}[X]$:
i) $\frac{2}{9}X^5 + \frac{5}{3}X^4 + X^3 + \frac{1}{3}$,
ii) $2X^5 - 6X^3 + 9X^2 - 15$,
iii) $X^3 + 6X^2 + 17X + 3$,
iv) $X^4 + 4X^3 + 6X^2 + 2X + 1$.

70. Factoriza los siguientes polinomios:
i) $X^2 + X + 1$ en $\mathbb{Z}_2[X]$,
ii) $X^4 + 1$ en $\mathbb{Z}_5[X]$,
iii) $X^4 + 10X^2 + 1$ en $\mathbb{Z}[X]$.

71. Demuestra que el polinomio $(X-1)(X-2)\cdots(X-n) - 1$ es irreducible en $\mathbb{Z}[X]$ para todo $n \geq 1$, y que ocurre lo mismo para $(X-1)(X-2)\cdots(X-n) + 1$ si $n \neq 4$.

72. Demuestra que $p(X) = X^3 + 9X + 6$ es irreducible sobre $\mathbb{Q}[X]$. Sea α una raíz de $p(X)$ en alguna extensión de $\mathbb{Q}$. Halla el inverso de $1 + \alpha$ en $\mathbb{Q}(\alpha)$.

73. Comprueba que $p(X) = X^3 + X + 1$ es irreducible sobre $\mathbb{Z}_2$. Sea α una raíz de $p(x)$. Calcula las potencias de α en $\mathbb{Z}_2(\alpha)$.

74. Sea $p(X) = X^3 - 2 \in \mathbb{Q}[x]$. Las raíces de $p(X)$ en $\mathbb{C}$ son $\alpha = \sqrt[3]{2}$, $\beta = \sqrt[3]{2}(\frac{-1+i\sqrt{3}}{2})$ y $\gamma = \sqrt[3]{2}(\frac{-1-i\sqrt{3}}{2})$. Demuestra, construyendo explícitamente los isomorfismos, que $\mathbb{Q}(\beta) \cong \mathbb{Q}(\alpha) \cong \mathbb{Q}(\gamma)$.

75. Calcula el discriminante de $f(X) = X^3 + pX + q$ y el de $X^n + a$.

76. Prueba las siguientes propiedades de la resultante y el discriminante:
i) $\mathrm{Res}_{n,m}(f, g) = (-1)^{nm} \mathrm{Res}_{m,n}(g, f)$.
ii) Si $f(X) = \sum_{i=0}^{n} a_i X^{n-i}$, entonces $\mathrm{Res}(f, X - 1) = (-1)^n \sum_{i=0}^{n} a_i$.
iii) $\mathrm{Res}(fg, h) = \mathrm{Res}(f, h)\,\mathrm{Res}(g, h)$.
iv) $\mathrm{D}(fg) = \mathrm{D}(f)\,\mathrm{D}(g)\,\mathrm{Res}(f, g)^2$.

77. Sea $p \in \mathbb{Z}$ un primo, $f(X) = \pm p + a_1X + a_2X^2 + \cdots + a_nX^n$ un polinomio con coeficientes en $\mathbb{Z}$ y tal que $\sum_{i=1}^{n} |a_i| < p$. Prueba que $f(X)$ es irreducible en $\mathbb{Q}[X]$.

---

[67] Usa el ejercicio anterior.

[76] iii) y iv) Factoriza $f(X)$ y $g(X)$ en alguna extensión.

[77] Prueba que tal polinomio no puede tener raíces complejas de módulo ≤ 1 y usa el Teorema Fundamental del Álgebra.

3. Cuerpos

78. Sea α una raíz de $X^3 - X + 1 \in \mathbb{Q}[X]$. Calcula los inversos y los polinomios mínimos de los elementos $\beta = 2 - 3\alpha + 2\alpha^2$ y $\gamma = 1 - 2\alpha + 3\alpha^2$ de $\mathbb{Q}(\alpha)$.

79. Sea α un elemento algebraico sobre un cuerpo F cuyo polinomio mínimo tiene grado impar. Prueba que $F(\alpha) = F(\alpha^2)$. Da un ejemplo mostrando que esto es falso si el grado es par.

80. Encuentra elementos α, β tales que $\mathbb{Q}(\sqrt{3}, i) = \mathbb{Q}(\alpha)$ y $\mathbb{Q}(\sqrt{3}, i, \omega) = \mathbb{Q}(\gamma)$, donde $\omega^3 = 1 \neq \omega$.

81. Prueba que existen extensiones finitas de $\mathbb{Q}$ de grado arbitrario. ¿Es esto cierto para $\mathbb{R}$?

82. Calcula el grado de la extensión $\mathbb{C}/\mathbb{Q}$.

83. Encuentra los polinomios mínimos sobre $\mathbb{Q}$ de los números reales $\sqrt{2} + 5$, $\sqrt[3]{2} + 5$, $\sqrt{-1 + \sqrt{2}}$ y $\sqrt{2} - \sqrt[3]{3}$.

84. Halla subcuerpos de $\mathbb{C}$ que sean cuerpos de descomposición sobre $\mathbb{Q}$ de los polinomios $X^3 - 1$, $X^4 + 5X^2 + 6$, $X^6 - 8$ y $(X^2 - 2)(X^3 - 2)$. Calcula el grado de tales extensiones sobre $\mathbb{Q}$.

85. Demuestra que $p(X) = X^3 + X + 1$ es irreducible en $\mathbb{F}_2[X]$ y que si ζ es una raíz del mismo (en alguna extensión), entonces $\mathbb{F}_2(\zeta)$ es un cuerpo de descomposición de $p(X)$. Halla todas las raíces de $p(X)$ y el grado $[\mathbb{F}_2(\zeta) : \mathbb{F}_2]$.

86. Halla todos los polinomios irreducibles de grados 2 y 3 sobre $\mathbb{F}_2$, $\mathbb{F}_3$ y $\mathbb{F}_5$.

87. Construye cuerpos con 8, 9 y 16 elementos.

88. Sean $p, n \in \mathbb{N}$ con p primo y K un cuerpo de descomposición de $f_n(X) = X^{p^n} - X$ sobre $\mathbb{F}_p$. Prueba que K coincide con el conjunto de raíces de $f_n(X)$. Deduce que $[K : \mathbb{F}_p] = n$.

89. Sea K un cuerpo finito.
    i) Prueba que existen $p, n \in \mathbb{N}$, con p primo, tales que K tiene p^n elementos.
    ii) Demuestra que todo elemento de K es raíz del polinomio $f_n(X)$ del ejercicio anterior.
    iii) Deduce que, salvo isomorfismos, los cuerpos finitos son precisamente los del ejercicio anterior.

90. Halla las raíces (complejas) del polinomio $X^3 + X^2 - 2X - 1 \in \mathbb{Q}[X]$.

---

[89] ii) Como en una de las prácticas, muestra que dado un elemento $0 \neq \alpha \in K$ existe un natural m tal que $\alpha^m = 1$ y que m divide a $p^n - 1$.