Anillos, dominios enteros, anillos ordenados y campos

1. Sea $A = \mathbb{Z}$ con las operaciones $\oplus$ y $\odot$ definidas como:

$$a \oplus b = a + b - 1 \text{ y } a \odot b = a + b - ab$$

   $(A, \oplus, \odot)$ ¿es un anillo? ¿es conmutativo? ¿tiene unitario? ¿es un dominio entero? ¿quiénes son el cero y el uno? ¿cuáles son las unidades?

2. Sea X un conjunto arbitrario pero fijo, y sea $A = \mathcal{P}(X)$ el conjunto potencia de X con las operaciones $\oplus$ y $\odot$ definidas como:

$$V \oplus W = V \cup W - V \cap W \text{ y } V \odot W = V \cap W$$

   $(A, \oplus, \odot)$ ¿es un anillo? ¿es conmutativo? ¿tiene unitario? ¿es un dominio entero? ¿quiénes son el cero y el uno? ¿cuáles son las unidades?

3. Sea $A = \mathbb{Z}$ con las operaciones $\oplus$ y $\odot$ definidas como:

$$a \oplus b = a + b - 7 \text{ y } a \odot b = a + b - 3ab$$

   $(A, \oplus, \odot)$ ¿es un anillo? ¿es conmutativo? ¿tiene unitario? ¿es un dominio entero? ¿quiénes son el cero y el uno? ¿cuáles son las unidades?

4. Considera el conjunto de matrices $M_{2\times 2}(\mathbb{R})$ con la suma y producto usuales. ¿Es anillo? ¿es conmutativo?¿tiene unitario? ¿es un dominio entero? ¿quiénes son las unidades?

5. Sea A un anillo con unitario. Demuestra que si a, b son unidades en A, entonces ab también es una unidad en A.

6. Si A es un anillo con unitario 1, el producto cumple las leyes de los exponentes, considerando que $\forall a \in A$, $a^0 = 1$. Demuestra usando inducción matemática, que efectivamente las leyes se cumplen.

7. Demuestra que todo dominio entero finito es un campo.

8. Sean A un anillo ordenado con clase positiva P y $a, b, c \in A$, demuestra que:

   a) $a < b \Rightarrow a + c < b + c$
   b) $a < b$ y $c \in P \Rightarrow ac < bc$
   c) Se cumple una y solamente una de las siguientes: $a < b$ ó $a = b$ ó $b < a$
   d) Si $a < b$ y $b < c \Rightarrow a < c$
   e) Si $a \neq 0 \Rightarrow a^2 \in P$
   f) Se cumple una y solamente una de las siguientes: $0 < a$ ó $a = 0$ ó $a < 0$
   g) Si $a < b$ y $c < 0 \Rightarrow bc < ac$
   h) Si $a < 0$ y $b < 0 \Rightarrow 0 < ab$

Enteros y divisibilidad

1. Demuestra que si $a|b$ y $c|d$ entonces $ac|bd$

2. Demuestra que si $a|b$ y $a|c$, entonces $a|bx + cy$, para calquier par de enteros x, y.

3. Sea $p \in \mathbb{Z}$, $p > 1$, tal que para cualesquiera $a, b \in \mathbb{Z}$, si $p \mid ab$, entonces $p \mid a$ ó $p \mid b$. Demuestra que p es primo.

4. Demuestra que si $a, b, c \in \mathbb{Z} \setminus \{0\}$ entonces $mcd(a, b) = mcd(ac + b)$.

5. Sea $d = mcd(a, b)$ demuestra que $mcd(\frac{a}{d}, \frac{b}{d}) = 1$

6. Demuestra que $mcd(n, n + 1) = 1$ para todo $n \in \mathbb{Z}$.

7. Demuestra que $mcd(a, b) = mcd(a, ac + b)$.

8. Demuestra que si $mcd(a, a) = 1$, entonces $mcd(a + b, a - b)$ es 1 ó 2.
9. Demuestra que si $mcd(a, b) = 1$, entonces $mcd(a + 2b, 2a + b)$ es 1 ó 3.
10. Demuestra que si p es primo y $p \mid a^n$, entonces $p^n \mid a^n$.
11. ¿Para qué enteros positivos m es cierto que $31 \equiv 3 \pmod{m}$?
12. ¿Para qué enteros positivos m es cierto que $215 \equiv 172 \pmod{m}$?
13. Calcular el residuo al dividir 17^{52} entre 5.
14. Calcular el residuo al dividir 15^{63} entre 8.
15. Demuestra que si $a \equiv b \pmod{m}$ y $n \mid m$ entonces $a \equiv b \pmod{n}$.
16. Demuestra que si $a \equiv b \pmod{m_1}$ y $a \equiv b \pmod{m_2}$ entonces $a \equiv b \pmod{M}$, donde $M = mcm(m_1, m_2)$.
17. Demuestra que si $n = abcddcba$ (en base 10), entonces n es divisible entre once
18. Demostrar que si $2^m - 1$ es primo, donde $m > 1$ es un entero, entonces el número
$$n = 2^{m-1}(2^m - 1)$$
es perfecto.
19. Demuestra que
    a) Si a es un entero par, entonces $a^2 \equiv 0 \pmod{4}$.
    b) Si a es un entero impar, entonces $a^2 \equiv 1 \pmod{4}$
20. Demuestra que si a es un entero impar, entonces $a^2 \equiv 1 \pmod{8}$.
21. Demuestra que $a^3 = a \pmod{3}$, para todo entero a (obviamente sin usar el pequeño teorema de Fermat).
22. Resolver el siguiente sistema de congruencias lineales:
$$x \equiv 4 \pmod{7}$$
$$x \equiv 3 \pmod{13}$$
23. Resolver el siguiente sistema de congruencias lineales:
$$x \equiv 4 \pmod{6}$$
$$x \equiv 3 \pmod{11}$$
24. Resolver el siguiente sistema de congruencias lineales:
$$x \equiv 3 \pmod{5}$$
$$x \equiv 1 \pmod{2}$$
$$x \equiv 2 \pmod{7}$$
25. Resolver el siguiente sistema de congruencias lineales:
$$x \equiv 5 \pmod{11}$$
$$x \equiv 4 \pmod{8}$$
$$x \equiv 1 \pmod{3}$$
26. Demuestra que el producto definido en $\mathbb{Z}_m$ como $[a][b] = [ab]$ está bien definido.
27. Demuestra que $m\mathbb{Z}$ es un subanillo de $\mathbb{Z}$ para cualquier entero m.
28. Demuestra que $\mathbb{Z}_m$ es un anillo conmutativo con uno para cualquier número natural m.
29. Sea $m \in \mathbb{Z}$ y sea $f : \mathbb{Z} \to \mathbb{Z}_m$ definida como $f(z) = [z]$. Demuestra que f es un morfismo de anillos.
30. Demuestra que $\mathbb{Z}_0$ es isomorfo a $\mathbb{Z}$. *Hint: Usa el ejercicio anterior.*