NOTAS DEL CURSO

MATEMÁTICA DISCRETA

(Ejercicios y problemas)

Pascual Jara Martínez

Departamento de Álgebra. Universidad de Granada

Granada, 2005

Primera redacción: Agosto 2005–Enero 2006

Revisión: Octubre 2006

Introducción

Índice general

Capítulo I

Nociones básicas

1. Introducción intuitiva a la teoría de conjuntos

Ejercicio. 1.1.
Preparación para probar la fórmula del binomio de Newton:
Se define el número combinatorio $\binom{n}{i} = \frac{n(n-1)\cdots(n-i+1)}{i(i-1)\cdots 2\cdot 1} = \frac{n!}{i!\,(n-i)!}$, *para* $1 \leq i \leq n$ *y* $\binom{n}{0} = 1$.
Probar que se verifica la igualdad siguiente:

$$\binom{n}{i} + \binom{n}{i+1} = \binom{n+1}{i+1}.$$

SOLUCIÓN.

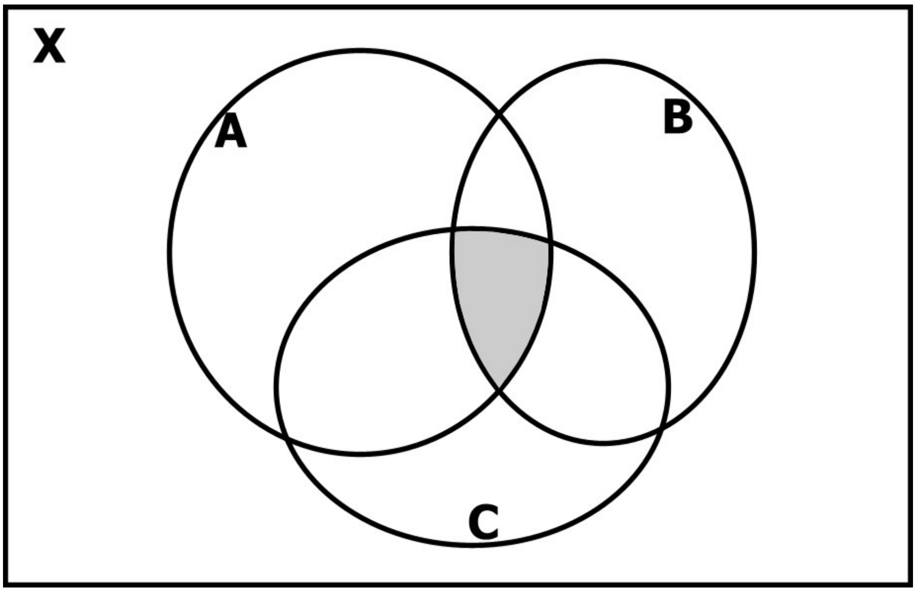
$$\begin{aligned}\binom{n}{i}+\binom{n}{i+1} &= \frac{n!}{i!\,(n-i)!}+\frac{n!}{(i+1)!\,(n-(i+1))!}\\ &= \frac{n!(i+1)}{(i+1)!\,(n-i)!}+\frac{n!(n-i)}{(i+1)!\,(n-i))!}\\ &= \frac{n!(i+1)+n!(n-i)}{(i+1)!\,(n-i)!}\\ &= \frac{n!(n+1)}{(i+1)!\,(n-i)!}\\ &= \frac{(n+1)!}{(i+1)!\,((n+1)-(i+1))!}\\ &= \binom{n+1}{i+1}.\end{aligned}$$

□

Ejercicio. 1.2.
¿Cuántos elementos tiene el conjunto $\{1,2,\{1,2\}\}$.

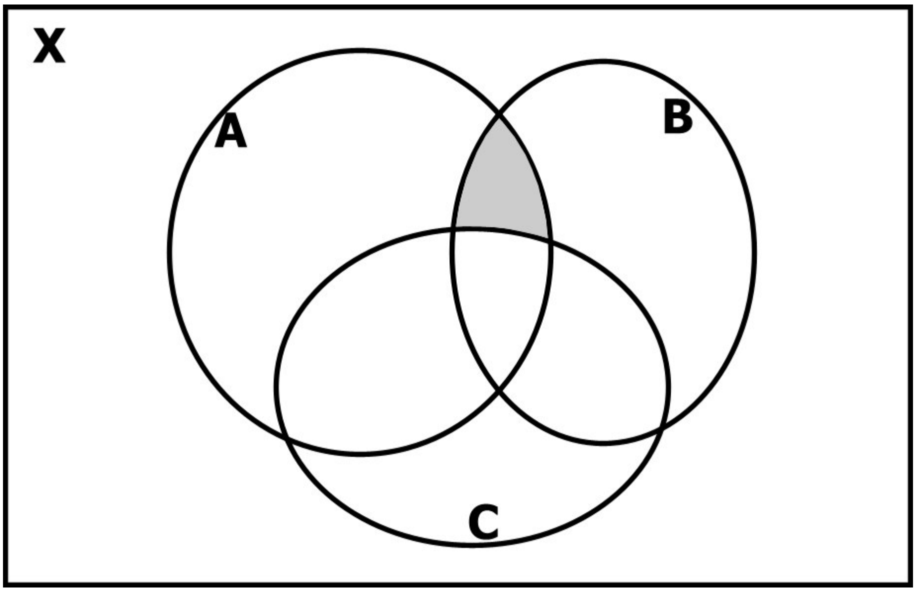
SOLUCIÓN. Tiene tres elementos; estos son: 1, 2 y $\{1,2\}$. □

Ejercicio. 1.3.
Dada la figura siguiente:

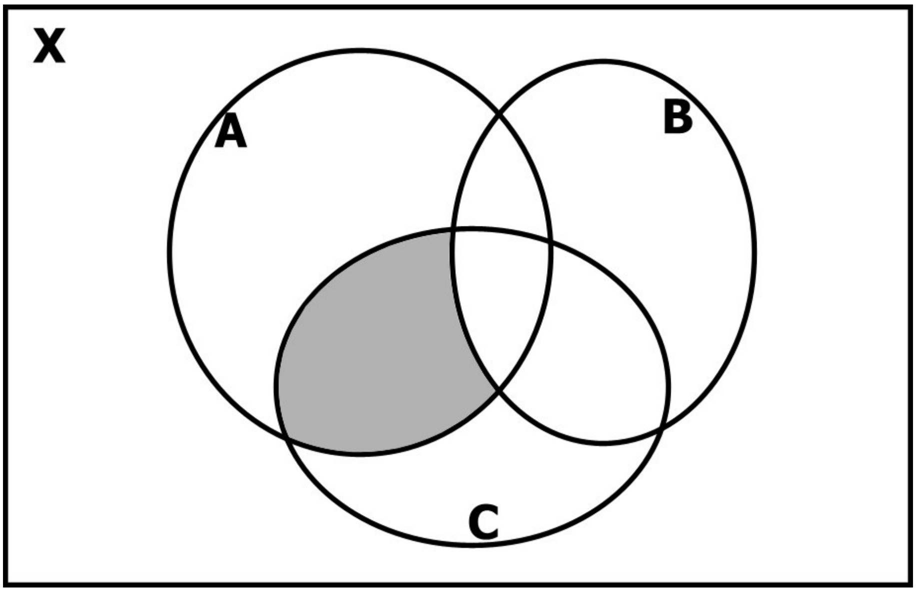


describir mediante una fórmula, cada una de las regiones del dibujo. Por ejemplo la parte coloreada es $A\cap B\cap C$.

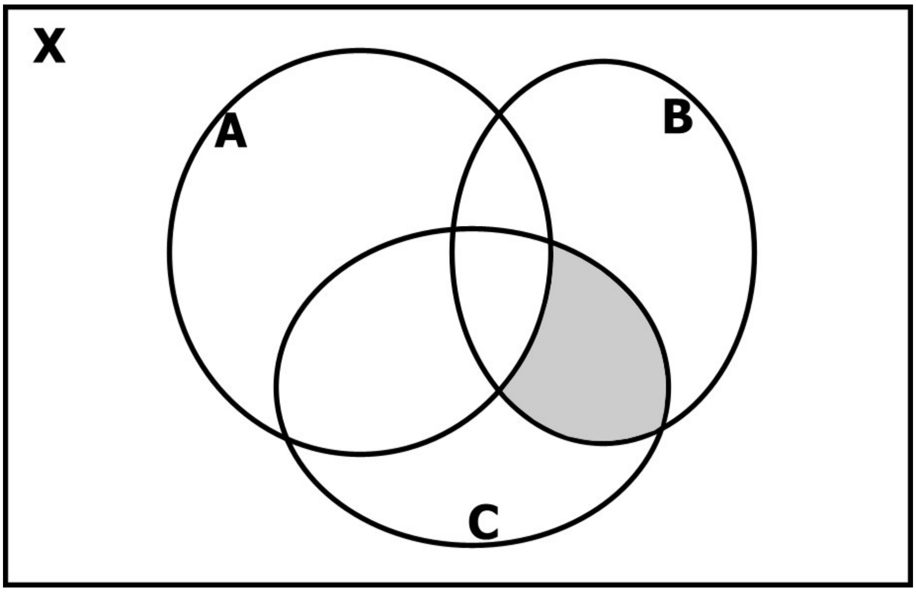
SOLUCIÓN. Veamos diferentes regiones:



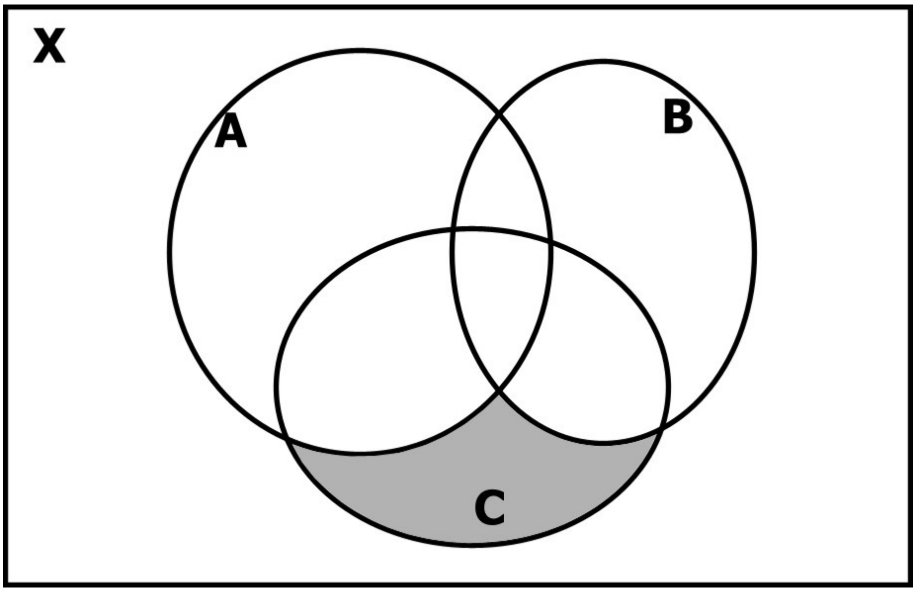
es $A \cap B \setminus C = A \cap B \cap \overline{C}$.



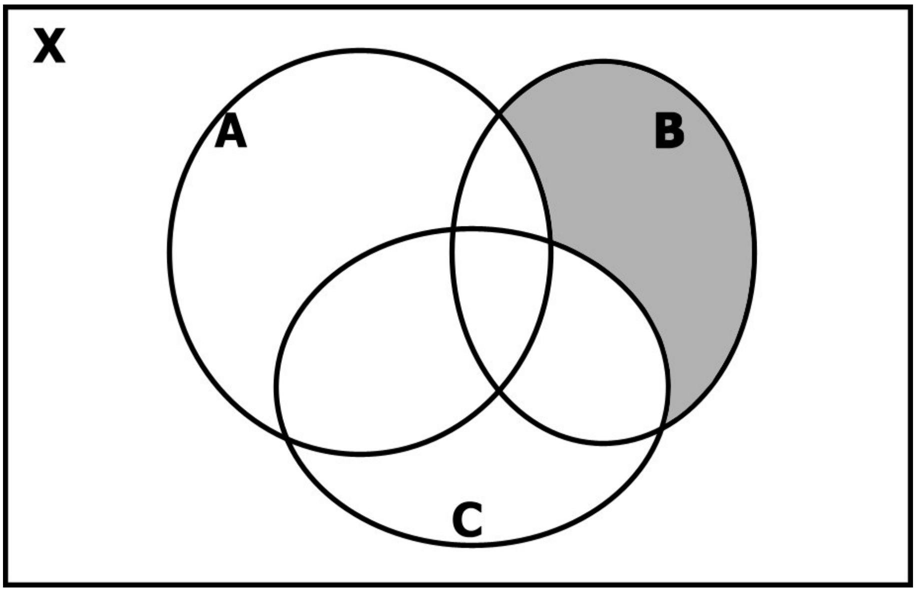
es $A \cap C \setminus B = A \cap \overline{B} \cap C$.



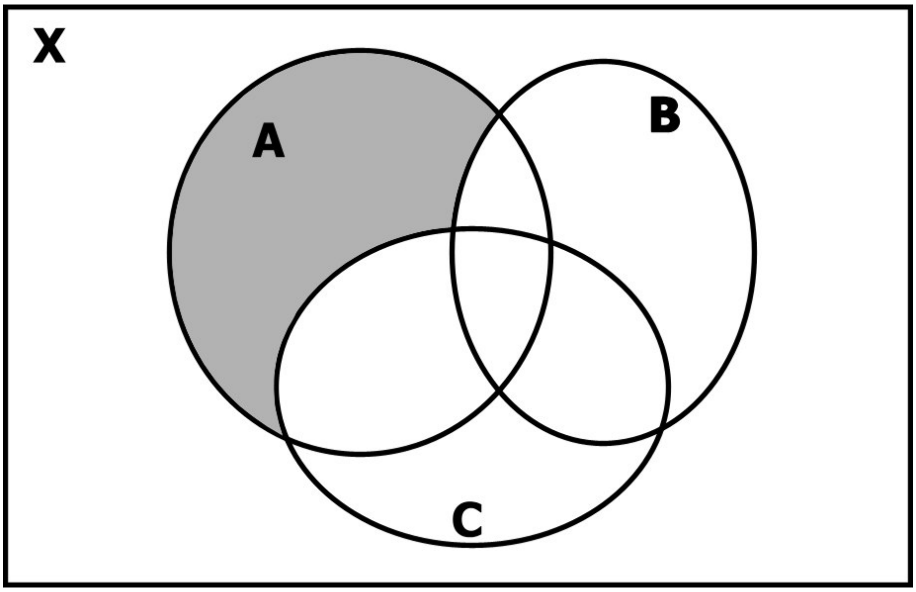
es $B \cap C \setminus A = \overline{A} \cap B \cap C$.



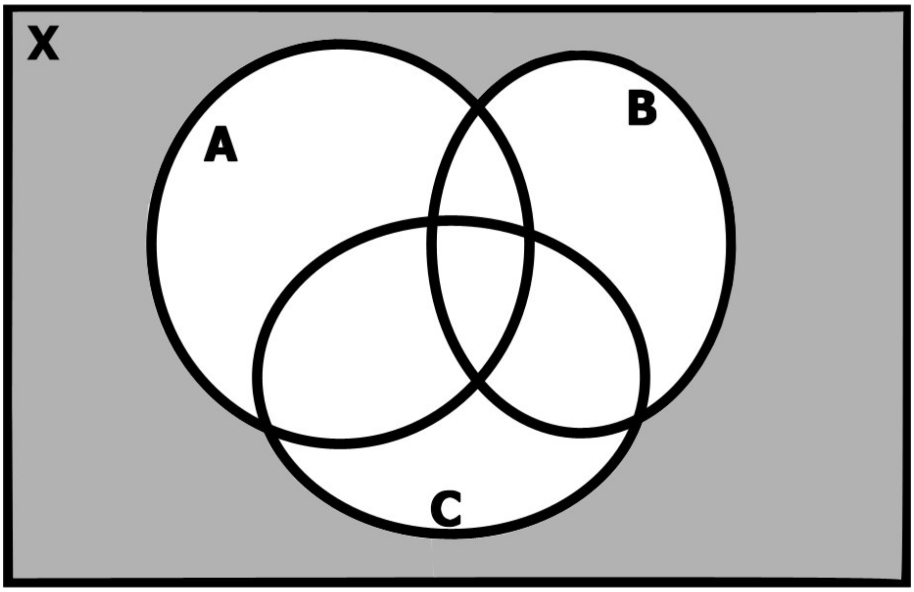
es $C \setminus (A \cup B) = \overline{A} \cap \overline{B} \cap C$.



es $B \setminus (A \cup C) = \overline{A} \cap B \cap \overline{C}$.



es $A \setminus (B \cup C) = A \cap \overline{B} \cap \overline{C}$.



es $\overline{A \cup B \cup C} = \overline{A} \cap \overline{B} \cap \overline{C}$. $\square$

2. Álgebra de proposiciones

Ejercicio. 2.1.
Probar que las proposiciones $(\mathbf{A} \wedge \mathbf{B}) \vee \mathbf{C}$ *y* $(\mathbf{A} \vee \mathbf{C}) \wedge (\mathbf{B} \vee \mathbf{C})$ *son equivalentes, y que como consecuencia para tres subconjuntos* X_1, X_2 *y* X_3 *de un conjunto dado se tiene la igualdad:* $(X_1 \cap X_2) \cup X_3 = (X_1 \cup X_3) \cap (X_2 \cup X_3)$.

SOLUCIÓN.

$(\mathbf{A}$	$\wedge$	$\mathbf{B})$	$\vee$	$\mathbf{C}$	$\Leftrightarrow$	$(\mathbf{A}$	$\vee$	$\mathbf{C})$	$\wedge$	$(\mathbf{B}$	$\vee$	$\mathbf{C})$
V	V	V	V	V	V	V	V	V	V	V	V	V
F	F	V	V	V	V	F	V	V	V	V	V	V
V	F	F	V	V	V	V	V	V	V	F	V	V
F	F	F	V	V	V	F	V	V	V	F	V	V
V	V	V	V	F	V	V	V	F	V	V	V	F
F	F	V	F	F	V	F	F	F	F	V	V	F
V	F	F	F	F	V	V	V	F	F	F	F	F
F	F	F	F	F	V	F	F	F	F	F	F	F
1	2	1	3	1	4	1	2	1	3	1	2	1

Dado $x \in (X_1 \cap X_2) \cup X_3$, tenemos:

$$\begin{aligned}
x \in (X_1 \cap X_2) \cup X_3 &\Leftrightarrow (x \in X_1 \cap X_2) \vee (x \in X_3)\\
&\Leftrightarrow [(x \in X_1) \wedge (x \in X_2)] \vee (x \in X_3)\\
&\Leftrightarrow [(x \in X_1) \vee (x \in X_3)] \wedge [(x \in X_2) \vee (x \in X_3)]\\
&\Leftrightarrow (x \in X_1 \cup X_3) \wedge (x \in X_2 \cup X_3)\\
&\Leftrightarrow x \in (X_1 \cup X_3) \cap (X_2 \cup X_3)
\end{aligned}$$

□

Ejercicio. 2.2.
Probar que para dos subconjuntos X_1 *y* X_2 *de un conjunto dado* X *se verifica:*

$$(X_1 \cap X_2) \cup X_1 = X_1.$$

SOLUCIÓN. Podemos proceder probando la equivalencia $(A \wedge B) \vee A \Leftrightarrow A$, y a partir de aquí, el resultado se sigue fácilmente.

$(A$	$\wedge$	$B)$	$\vee$	A	$\Leftrightarrow$	A
V	V	V	V	V	V	V
F	F	V	F	F	V	F
V	F	F	V	V	V	V
F	F	F	F	F	V	F
1	2	1	3	1	=	1

□

Ejercicio. 2.3.
Probar que para dos subconjuntos X_1 y X_2 de un conjunto dado X se verifica:

$$(X_1 \cup X_2) \cap X_1 = X_1.$$

SOLUCIÓN. Procedemos como sigue:

$$\begin{aligned}(X_1 \cup X_2) \cap X_1 &= (X_1 \cap X_1) \cup (X_2 \cap X_1) \\ &= X_1 \cup (X_2 \cap X_1 \\ &= X_1.\end{aligned}$$

Observar que hemos utilizado el resultado contenido en el (Ejercicio 2.2.). □

Ejercicio. 2.4.
Si A, B y C son proposiciones, ¿son equivalentes las siguientes proposiciones?:

(1) $A \Rightarrow B$ y $B \Rightarrow A$,

(2) $(A \Rightarrow B) \Rightarrow C$ y $A \Rightarrow (B \Rightarrow C)$,

(3) $\neg(A \Rightarrow B)$ y $B \Rightarrow A$,

(4) $\neq A \Rightarrow \neq B$ y $B \Rightarrow A$,

(5) $\neq (A \Rightarrow B)$ y $\neq A \Rightarrow \neq B$.

SOLUCIÓN. Hacer □

Ejercicio. 2.5.
Si A, B y C son proposiciones, ¿son tautologías las siguientes proposiciones?:

(1) $A \wedge B \Rightarrow A \vee C$,

(2) $A \vee B \Rightarrow A \wedge C$.

SOLUCIÓN. Hacer □

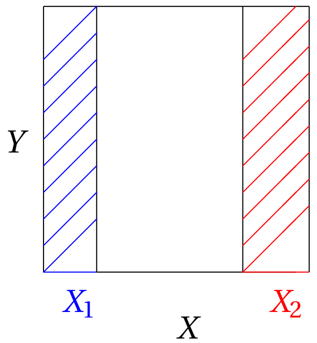
3. Aplicaciones

Ejercicio. 3.1.
Sean X e Y conjuntos y X_1, X_2 subconjuntos del conjunto X. Demostrar que se verifica

$$\begin{array}{l} X_1 \times Y \cup X_2 \times Y = (X_1 \cup X_2) \times Y \\ X_1 \times Y \cap X_2 \times Y = (X_1 \cap X_2) \times Y \end{array}$$

Nota: hacer previamente una representación gráfica.

SOLUCIÓN. Primera igualdad. Una representación gráfica podría ser la siguiente:



en donde el subconjunto $X_1 \subseteq X$ está señalado en azul y el subconjunto $X_2 \subseteq X$ está señalado en rojo. Tenemos $X_1 \times Y$ es la parte rayada en azul y $X_2 \times Y$ es la rayada en rojo. Por otro lado la parte rayada, tanto en azul como en rojo es el subconjunto $(X_1 \cap X_2) \times Y$.

Una demostración por elementos sería la siguiente:

$$\begin{array}{rl} & (x,y) \in X_1 \times Y \cup X_2 \times Y \\ \Leftrightarrow & ((x,y) \in X_1 \times Y) \vee ((x,y) \in X_2 \times Y) \\ \Leftrightarrow & ((x \in X_1) \wedge (y \in Y)) \vee ((x \in X_2) \wedge (y \in Y)) \\ \Leftrightarrow & ((x \in X_1) \vee (x \in X_2)) \wedge ((x \in X_1) \vee (y \in Y)) \wedge \\ & ((y \in Y) \vee (x \in X_2)) \wedge ((y \in Y) \vee (y \in Y)) \\ \Leftrightarrow & ((x \in X_1) \vee (x \in X_2)) \wedge (y \in Y) \\ \Leftrightarrow & (x \in X_1 \cup X_2) \wedge (y \in Y) \\ \Leftrightarrow & (x,y) \in (X_1 \cup X_2) \times Y. \end{array}$$

Se puede observar que hemos hecho uso de las siguientes propiedades para proposiciones:

$$\mathbf{A} \vee (\mathbf{B} \wedge \mathbf{C}) \Leftrightarrow (\mathbf{A} \vee \mathbf{B}) \wedge (\mathbf{A} \vee \mathbf{C}),$$

$$\mathbf{B} \wedge \mathbf{B} \Leftrightarrow \mathbf{B}$$

y

$$(\mathbf{A} \vee \mathbf{B}) \wedge \mathbf{B} \Leftrightarrow \mathbf{B},$$

las cuales las podéis probar mediante el uso de tablas de verdad.

Primera igualdad. Hacer una representación gráficas para esta igualdad.

Para una demostración por elementos podemos proceder como sigue:

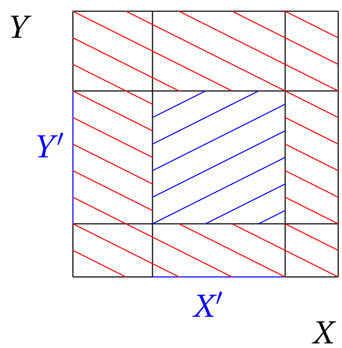
$$
\begin{aligned}
& (x,y) \in X_1 \times Y \cap X_2 \times Y \\
\Leftrightarrow\ & ((x,y) \in X_1 \times Y) \wedge ((x,y) \in X_2 \times Y) \\
\Leftrightarrow\ & ((x \in X_1) \wedge (y \in Y)) \wedge ((x \in X_2) \wedge (y \in Y)) \\
\Leftrightarrow\ & (x \in X_1) \wedge (x \in X_2) \wedge (y \in Y) \\
\Leftrightarrow\ & ((x \in X_1) \wedge (x \in X_2)) \wedge (y \in Y) \\
\Leftrightarrow\ & (x \in X_1 \cap X_2) \wedge (y \in Y) \\
\Leftrightarrow\ & (x,y) \in (X_1 \cap X_2) \times Y.
\end{aligned}
$$

□

Ejercicio. 3.2.
Sean X e Y dos conjuntos y X', Y' subconjuntos de X e Y respectivamente. Demostrar que se verifica $\overline{X' \times Y'} = (\overline{X'} \times Y) \cup (X \times \overline{Y'})$

Nota: hacer previamente una representación gráfica.

SOLUCIÓN. La representación gráfica es la siguiente:



Hemos representado en color azul el subconjunto $X' \times Y'$ y su complemento lo hemos pintado en rojo. Es claro que esta región es la unión $(\overline{X'} \times Y) \cup (X \times \overline{Y'})$.

Una demostración por elementos es la siguiente, en la que recordemos, que si $(x,y) \in X' \times Y'$, entonces $(x, y) \in X \times Y$.

$$\begin{aligned}
&(x, y) \in \overline{X' \times Y'} \\
\Leftrightarrow\ &(x, y) \notin X' \times Y' \\
\Leftrightarrow\ &\neg((x, y) \in X' \times Y') \\
\Leftrightarrow\ &\neg((x \in X') \wedge (y \in Y')) \\
\Leftrightarrow\ &(\neg(x \in X')) \vee (\neg(y \in Y')) \\
\Leftrightarrow\ &(x \notin X') \vee (y \notin Y') \\
\Leftrightarrow\ &(x \in \overline{X'}) \vee (y \in \overline{Y'}) \\
\Leftrightarrow\ &((x \in \overline{X'}) \wedge (y \in Y)) \vee ((x \in X) \wedge (y \in \overline{Y'})) \\
\Leftrightarrow\ &((x, y) \in \overline{X'} \times Y) \vee ((x, y) \in X \times \overline{Y'}) \\
\Leftrightarrow\ &(x, y) \in (\overline{X'} \times Y) \cup (X \times \overline{Y'})
\end{aligned}$$

□

Ejercicio. 3.3.
Sea $f : X \longrightarrow Y$ una aplicación y sean $A, B \subseteq X$ subconjuntos de X.
(1). Probar que $f(A \cup B) = f(A) \cup f(B)$.
(2). ¿Qué relación existe entre $f(A \cap B)$ y $f(A) \cap f(B)$?

SOLUCIÓN. Parte 1. Tenemos las siguientes equivalencias:

$$\begin{aligned}
y \in f(A \cup B) &\Leftrightarrow \exists x \in A \cup B, f(x) = y \\
&\Leftrightarrow (\exists x \in A, f(x) = y) \vee (\exists x \in B, f(x) = y) \\
&\Leftrightarrow (y \in f(A)) \vee (y \in f(B)) \\
&\Leftrightarrow y \in f(A) \cup f(B).
\end{aligned}$$

Parte 2. Es claro que se puede probar la inclusión $f(A \cap B) \subseteq f(A) \cap f(B)$ siguiendo las siguientes implicaciones:

$$\begin{aligned}
y \in f(A \cap B) &\Leftrightarrow \exists x \in A \cap B, f(x) = y \\
&\Leftarrow (\exists x \in A, f(x) = y) \wedge (\exists x \in B, f(x) = y) \\
&\Leftrightarrow (y \in f(A)) \wedge (y \in f(B)) \\
&\Leftrightarrow y \in f(A) \cap f(B).
\end{aligned}$$

En cambio la otra inclusión no es cierta; basta considerar el siguiente ejemplo:

$$\begin{aligned}
&X = \{a, b\}, \\
&Y = \{1\}, \\
&f : X \longrightarrow Y,\ f(a) = 1 = f(b)
\end{aligned}$$

Es claro que si $A = \{a\}$ y $B = \{b\}$, entonces se verifica:

$$f(A \cap B) = f(\varnothing) = \varnothing \neq \{1\} = f(A) \cap f(B).$$

□

Ejercicio. 3.4.
Sea $f : X \longrightarrow Y$ una aplicación y sean $C, D \subseteq Y$ subconjuntos de Y.
(1). Probar que $f^{-1}(C \cup D) = f^{-1}(C) \cup f^{-1}(D)$.
(2). ¿Qué relación existe entre $f^{-1}(C \cap D)$ y $f^{-1}(C) \cap f^{-1}(D)$?

SOLUCIÓN. Parte 1. Tenemos las siguientes equivalencias:

$$\begin{aligned} x \in f^{-1}(C \cup D) &\Leftrightarrow f(x) \in C \cup D \\ &\Leftrightarrow (f(x) \in C) \vee (f(x) \in D) \\ &\Leftrightarrow (x \in f^{-1}(C)) \vee (x \in f^{-1}(D)) \\ &\Leftrightarrow x \in f^{-1}(C) \cup f^{-1}(D). \end{aligned}$$

Parte 2. Se puede probar la igualdad también en este caso:

$$\begin{aligned} x \in f^{-1}(C \cap D) &\Leftrightarrow f(x) \in C \cap D \\ &\Leftrightarrow (f(x) \in C) \wedge (f(x) \in D) \\ &\Leftrightarrow (x \in f^{-1}(C)) \wedge (x \in f^{-}(D)) \\ &\Leftrightarrow x \in f^{-1}(C) \cap f^{-1}(D). \end{aligned}$$

$\square$

Ejercicio. 3.5.
Observar que al decir que una aplicación $f : X \longrightarrow Y$ tiene una inversa hemos dicho que existe una aplicación $g : Y \longrightarrow X$ verificando $fg = 1_Y$ y $gf = 1_X$.

No basta con solo una de las igualdades, ya que dada la aplicación $f : \{1, 2\} \longrightarrow \{a\}$ existe una aplicación $g : \{a\} \longrightarrow \{1, 2\}$ verificando $fg = 1_{\{a\}}$, pero no es biyectiva. En efecto, es fácil ver que no es una aplicación inyectiva.

SOLUCIÓN. ¡Estudiar bien el enunciado! $\square$

4. Relaciones de equivalencia y de orden

Ejercicio. 4.1.
Se considera el conjunto $\mathbb{N} \setminus \{0\}$ *y la relación aRb si* $\lfloor \log(a) \rfloor = \lfloor \log(b) \rfloor$.

(1) Demuestra que R es una relación de equivalencia en $\mathbb{N} \setminus \{0\}$.

(2) Describe el conjunto cociente.

SOLUCIÓN. Tenemos que $\lfloor \log(a) \rfloor$ es la parte entera del número $\log(a)$, utilizando la base decimal.

(1) Es claro.

(2) Cada clase está determinada por un número natural, así la clase determinada por 0 es: $\{1, 2, 3, 4, 5, 6, 7, 8, 9\}$, la determinada por 1 es: $\{10, 11, \ldots, 98, 99\}$, etc.

□

Ejercicio. 4.2.
Se considera el conjunto $\mathbb{N} \setminus \{0\}$ *y la relación aRb si* $\lfloor \log_2(a) \rfloor = \lfloor \log_2(b) \rfloor$.

(1) Demuestra que R es una relación de equivalencia en $\mathbb{N} \setminus \{0\}$.

(2) Describe el conjunto cociente.

SOLUCIÓN. Tenemos que $\lfloor \log(a) \rfloor$ es la parte entera del número $\log(a)$, utilizando la base decimal.

(1) Es claro.

(2) Cada clase está determinada por un número natural, así la clase determinada por 0 es: $\{1\}$, la determinada por 1 es: $\{2, 3\}$, la determinad por 2 es: $\{4, 5, 6, 7\}$, etc.

□

Ejercicio. 4.3.
Se considera el conjunto $\mathbb{N} \setminus \{0\}$ *y la relación aRb si* $\lfloor \log(a) \rfloor \leq \lfloor \log(b) \rfloor$. *Demuestra que R no es una relación de orden al no verifica la propiedad antisimétrica.*

SOLUCIÓN. Es claro que $\lfloor \log(1) \rfloor = \lfloor \log(2) \rfloor$, luego $1R2$ y $2R1$, pero como $1 \neq 2$, resulta que R no verifica la propiedad antisimétrica. □

Ejercicio. 4.4.
Dada una relación R en un conjunto X decimos que R verifica la ***propiedad circular*** *si*

$$\text{si } aRb \text{ y } bRc, \text{ entonces } cRa, \text{ para cada } a, b, c \in X.$$

Demuestra que R es una relación de equivalencia en X si y solo si R verifica las propiedades reflexiva y circular.

SOLUCIÓN. Hacer. □

Ejercicio. 4.5.
Dado un conjunto X y un subconjunto $A \subseteq X$, se define una relación en $\mathcal{P}(X)$ mediante:

$$BRC \text{ si } B \cap A = C \cap A, \text{ para cada } B, C \in \mathcal{P}(X).$$

(1) *Demuestra que R es una relación de equivalencia en $\mathcal{P}(X)$;*

(2) *Demuestra que existe una biyección entre $\mathcal{P}(X)/R$ y $\mathcal{P}(A)$.*

SOLUCIÓN. Hacer □

Ejercicio. 4.6.
En el conjunto $\mathbb{Z}$ se define la relación

$$aRb \text{ si } a^2 - b^2 = a - b, \text{ para cada } a, b \in \mathbb{Z}.$$

(1) *Demuestra que R es una relación de equivalencia,*

(2) *Determina la clase de equivalencia de cada elemento $a \in \mathbb{Z}$,*

(3) *Describe el conjunto cociente.*

SOLUCIÓN. Hacer □

Ejercicio. 4.7.
Dado un conjunto X y dos relaciones R y S en X, se define una nueva relación en X mediante:

$$a(R \circ S)b \text{ si existe } x \in X \text{ tal que } aRx \text{ y } xSb.$$

(1) *Demuestra que una relación R verifica la propiedad transitiva si y solo si $R \circ R \subseteq R$,*

(2) Demuestra que si R verifica la propiedad reflexiva, entonces $R \subseteq R \circ R$,

SOLUCIÓN.

(1) Si R verifica la propiedad transitiva y $a(R \circ R)b$, entonces existe $x \in X$ tal que aRx y xRb, luego aRb. Recíprocamente, si aRb y bRc, entonces $a(R \circ R)c$, y por tanto aRc, luego R verifica la propiedad transitiva.

(2) Dados $a, b \in X$ tales que aRb, como bRb, entonces $a(R \circ R)b$.

$\square$

Ejercicio. 4.8.
Dado un conjunto X y dos relaciones de equivalencia R y S en X, demuestra que $R \circ S$ es de equivalencia si y solo si $R \circ S = S \circ R$.

SOLUCIÓN. Hacer $\square$

Ejercicio. 4.9.
Dado un conjunto X y dos relaciones de equivalencia R y S en X, demuestra que $R \cup S$ es de equivalencia si y solo si $R \circ S \subseteq R \cup S$ y $S \circ R \subseteq R \cup S$.

SOLUCIÓN. Hacer $\square$

5. Cuantificadores

Ejercicio. 5.1.
Sea $X = \{1, a, z, 2\}$. Determinar el conjunto de partes de X.

SOLUCIÓN. Los subconjuntos de X son:

$$\begin{array}{l}
\varnothing, \\
\{1\}, \{2\}, \{a\}, \{z\}, \\
\{1,2\}, \{1,a\}, \{1,z\}, \{2,a\}, \{2,z\}, \{a,z\} \\
\{1,2,a\}, \{1,2,z\}, \{1,a,z\}, \{2,a,z\} \\
\{1,2,a,z\}
\end{array}$$

Observar que en total hay 16 subconjuntos. □

Ejercicio. 5.2.
Dado un conjunto X y subconjuntos A, B, $C \subseteq X$, demuestra que se verifican las siguientes propiedades:

(1) Si $A \vartriangle B = C$, entonces $A \vartriangle C = B$.

(2) $A \cup B = B \cup C$ si y solo si $A \vartriangle B \subseteq C$.

(3) Si $\left.\begin{array}{l} A \cup B = A \cup C \\ A \cap B = A \cap C \end{array}\right\}$, entonces $B = C$.

SOLUCIÓN. Hacer □

6. Métodos de demostración

Ejercicio. 6.1.
Demuestra que para cada número primo p el número real $\sqrt{p}$ no es un número racional.

SOLUCIÓN. Es claro. $\square$

Ejercicio. 6.2.
Demuestra que para cada par de números primos, distintos, p y q, el número real $\sqrt{pq}$ no es un número racional.

SOLUCIÓN. Es claro. $\square$

Ejercicio. 6.3.
Se tiene una lámina metálica cuadrada de 70 cm. de lado y se golpea 50 veces con una martillo. Demuestra que al menos dos de los golpes deben estar a una distancia de 15 cm.

SOLUCIÓN. Dibujamos en la lámina ua trama formada por 49 celdas cuadradas de 10 cm. de lados. Como hay 49 celdas y hemos golpeada la lámina metálica 50 veces, al menos dos de los golpes se han dado en la misma celda (¡los bordes son parte de la celda!).

Tenemos pues dos puntos en un cuadrado de 10 cm. de lado. Vamos a ver que estos puntos distan menos de 15 cm.

Dados dos puntos A y B en un cuadrado de 10 cm. de lado, unimos estos por una línea que cortaría al borde en dos puntos A' y B'. Si A' y B' están en lados contiguos, entonces la distancia $\overline{A'B'}$ es menor que la diagonal del cuadrado, y lo mismo ocurre se están en lados opuestos.

Por lo tanto la mayor distancia entre $\overline{A'B'}$ se produce cuando A' y B' son vértices opuestos. Esta distancia máxima es:

$$\sqrt{10^+10^2} = \sqrt{200} = 14,1cm.$$

$\square$

Capítulo II

Números naturales y números enteros

7. Números naturales

Ejercicio. 7.1.
Determinar el número de soluciones en $\mathbb{N}$ de la siguiente ecuación

$$X + 2Y = n, \quad \text{con } n \in \mathbb{N}.$$

SOLUCIÓN. Estudiemos el número de soluciones según valores particulares de n. Para $n = 0$ existe únicamente una solución, el par $(0, 0)$; para $n = 1$ existe también una única solución, el par $(1, 0)$. Para $n = 2$ y $n = 3$ existen dos soluciones, estas son: $(2, 0), (0, 1)$ y $(3, 0), (1, 1)$ respectivamente. Estudiemos ahora el caso general, para n par tenemos

$$X + 2Y = 2h, \quad \text{donde } h \in \mathbb{N}$$

entonces estudiando el problema en $\mathbb{Z}$ tenemos

$$X = 2h - 2Y = 2(h - Y),$$

para cada valor de Y obtenemos uno de X, tenemos que restringir únicamente para que siempre obtengamos valores positivos ó nulos, entonces tenemos exactamente $h + 1$ soluciones, estas corresponden a los siguientes valores de Y, $0, 1, \ldots, h$, y son: $(2h, 0), (2(h - 1), 1), \ldots, (0, h)$. Si n es impar entonces tenemos la siguiente igualdad

$$X + 2Y = 2h + 1, \quad \text{donde } h \in \mathbb{N}$$

o equivalentemente

$$X = 2(h - Y) + 1,$$

al igual que antes las $h+1$ soluciones están determinadas por valores de Y, y son $(2h+1, 0), (2(h-1)+1, 1), \ldots, (1, h)$. $\square$

Ejercicio. 7.2.
Probar que para $n \geq 1$ se verifica:

$$\sum_{i=1}^{n} i(i+1) = \frac{n(n+1)(n+2)}{3}.$$

SOLUCIÓN. Para $n = 1$ es cierto. Suponemos que es cierto para $n \geq 1$ y vamos a probarlo para $n+1$.

$$\begin{aligned} \textstyle\sum_{i=1}^{n+1} i(i+1) &= \textstyle\sum_{i=1}^{n} +(n+1)(n+2) \\ &= \tfrac{n(n+1)(n+2)}{3} + (n+1)(n+2) \\ &= (n+1)(n+2)\tfrac{n+3}{3}. \end{aligned}$$

$\square$

Ejercicio. 7.3.
Probar que para $n \geq 3$ se verifica $n^2 > 2n$.

SOLUCIÓN. $\square$

Ejercicio. 7.4.
Probar que para $n \geq 6$ se verifica $n! > n^3$.

SOLUCIÓN. Para $n = 6$ es cierto.

$$\begin{aligned} &6! = 6 \times 5 \times 4 \times 3 \times 2 \times 1 = 720; \\ &6^3 = 216. \end{aligned}$$

Supongamos que es cierto para $n \geq 6$ y vamos a probarlo para $n+1$.

$$\begin{aligned} &(n+1)! = n!(n+1) > n^4 + n^3; \\ &(n+1)^3 = n^3 + 3n^2 + 3n + 1. \end{aligned}$$

Basta ver que $n^4 \geq 3n^2 + 3n + 1$ si $n \geq 6$. Pero $3n^2 + 3n + 1 < n^2(3+3+1) < n^2$ si $n \geq 4$, luego tenemos el resultado. $\square$

Ejercicio. 7.5.
Probar que para $n \geq 2$ se verifica:

$$\left(1 - \frac{1}{4}\right)\left(1 - \frac{1}{9}\right)\left(1 - \frac{1}{16}\right)\cdots\left(1 - \frac{1}{n^2}\right) = \frac{n+1}{2n}.$$

SOLUCIÓN. Para $n = 2$ es cierto, suponemos que es cierto para $n \geq 2$, y probamos que también es cierto para $n+1$.

$$\begin{aligned}
\prod i = 1^{n+1}\left(1-\tfrac{1}{i^2}\right) = \prod i = 1^{n}\left(1-\tfrac{1}{i^2}\right)\left(1-\tfrac{1}{(n+1)^2}\right) \\
&= \tfrac{n+1}{2n}\left(1-\tfrac{1}{(n+1)^2}\right) \\
&= \tfrac{(n+1)(n+1)^2-1}{2n(n+1)^2} \\
&= \tfrac{(n+1)(n^2+2n)}{2n(n+1)^2} \\
&= \tfrac{n+2}{2(n+1)}.
\end{aligned}$$

□

Ejercicio. 7.6.
Usa el principio de inducción para probar la siguiente afirmación:

$$1+2+3+\cdots+n = \frac{n(n+1)}{2}\ \forall n \in \mathbb{N}.$$

SOLUCIÓN. Suponemos que la expresión $1+2+3+\cdots+n = \frac{n(n+1)}{2}$ tiene sentido para 0, siendo en este caso la suma de la izquierda igual a cero. Para los restantes números naturales es claro el significado. Así pues la expresión es cierta para $n = 0, 1$. Supongamos que sea cierta para un cierto $n \geq 1$, esto es, que se verifica la igualdad $1+2+3+\cdots+n = \frac{n(n+1)}{2}$, y vamos a ver qué ocurre para $n+1$. En este caso resulta que:

$$\begin{aligned}
1+2+3+\cdots+n+(n+1) &= \tfrac{n(n+1)}{2}+(n+1) \\
&= \tfrac{n(n+1)+2(n+1)}{2} \\
&= \tfrac{(n+1)(n+2)}{2},
\end{aligned}$$

y por tanto el resultado es cierto para todo número natural. □

Ejercicio. 7.7.
Usa el principio de inducción para probar la siguiente afirmación:

$$1+2^2+3^2+\cdots+n^2 = \frac{n(n+1)(2n+1)}{6}\ \forall n \in \mathbb{N}.$$

SOLUCIÓN. Al igual que antes la expresión tiene sentido para $n = 0$ si suponemos que la suma de la izquierda es igual a cero. Entonces el resultado es cierto para $n = 0, 1$. Supongamos que sea cierto para un cierto $n \geq 1$, y vamos a ver qué ocurre para $n+1$. En este caso tenemos:

$$\begin{aligned}
1 + 2^2 + 3^2 + \cdots + n^2 + (n+1)^2 &= \tfrac{n(n+1)(2n+1)}{6} + (n+1)^2 \\
&= (n+1)\left(\tfrac{n(2n+1)}{6} + (n+1)\right) \\
&= \tfrac{(n+1)(2n^2+7n+6)}{6} \\
&= \tfrac{(n+1)(n+2)(2n+3)}{6},
\end{aligned}$$

y por tanto el resultado es cierto para todo número natural. □

Ejercicio. 7.8.
Usa el principio de inducción para probar la siguiente afirmación:

$$\frac{1}{1\times 3} + \frac{1}{3\times 5} + \cdots + \frac{1}{(2n+1)(2n-1)} = \frac{n}{2n+1} \quad \forall n \in \mathbb{N}^*.$$

SOLUCIÓN. Es claro que la expresión no es cierta para el valor $n = 0$, por esto añadiremos este número al conjunto de números para los que esta expresión es cierta. Para $n = 1$ la expresión es cierta. Supongamos que sea cierta para un cierto número natural $n \geq 1$, entonces para ver qué ocurre con $n+1$, procedemos como sigue:

$$\begin{aligned}
&\tfrac{1}{1\times 3} + \tfrac{1}{3\times 5} + \cdots + \tfrac{1}{(2n-1)(2n+1)} + \tfrac{1}{(2(n+1)-1)(2(n+1)+1)} \\
&= \tfrac{n}{2n+1} + \tfrac{1}{(2n+1)(2n+3)} \\
&= \tfrac{n(2n+3)}{(2n+1)(2n+3)} + \tfrac{1}{(2n+1)(2n+3)} \\
&= \tfrac{n(2n+3)+1}{(2n+1)(2n+3)} \\
&= \tfrac{(2n+1)(n+1)}{(2n+1)(2n+3)} \\
&= \tfrac{n+1}{2n+3}
\end{aligned}$$

y por tanto el resultado es cierto para todo número natural mayor o igual que 1. □

Ejercicio. 7.9.
Usa el principio de inducción para probar la siguiente afirmación:

$$7^n - 1 \textit{ es un múltiplo de } 6\, \forall n \in \mathbb{N}^*.$$

SOLUCIÓN. Para $n = 0$, el resultado no es cierto. Supongamos que es cierto para un cierto $n \geq 0$. Estudiamos el caso $n+1$, para esto procedemos como sigue:

$$7^{n+1} - 1 = 7^n \cdot 7 - 1 = 7^{n+1} - 7^n + 7^n - 1 = 7^n(7-1) + (7^n - 1),$$

y por tanto tenemos que $7^{n+1} - 1$ es también un múltiplo de 6, luego el resultado es cierto para todo número natural. □

Ejercicio. 7.10.
Usa el principio de inducción para probar la siguiente afirmación:

$$7^{2n} + 16n - 1 \textit{ es un múltiplo de 64 } \forall n \in \mathbb{N}.$$

SOLUCIÓN. Para $n = 0$ el resultado es cierto. Supongamos que es cierto para cierto $n \geq 0$. Estudiamos el caso $n+1$, y procedemos como sigue:

$$\begin{aligned}
&7^{2(n+1)} + 16(n+1) - 1 \\
&= 7^{2n} \times 7^2 + 16(n+1) - 1 \\
&= 7^2(7^{2n} + 16n - 1) - 7^2 \times 16n + 7^2 + 16(n+1) - 1 \\
&= 7^2(7^{2n} + 16n - 1) - 7^2(16n - 1) + 16n - 1 + 16 \\
&= 7^2(7^{2n} + 16n - 1) - (7^2 - 1)(16n - 1) + 16 \\
&= 7^2(7^{2n} + 16n - 1) - (3 \times 16)(16n - 1) + 16 \\
&= 7^2(7^{2n} + 16n - 1) - (3(16n - 1) - 1)16 \\
&= 7^2(7^{2n} + 16n - 1) - (48n - 3 - 1)16 \\
&= 7^2(7^{2n} + 16n - 1) - (48n - 4)16 \\
&= 7^2(7^{2n} + 16n - 1) - (12n - 1) \times 4 \times 16 \\
&= 7^2(7^{2n} + 16n - 1) - (12n - 1) \times 64.
\end{aligned}$$

luego el resultado es cierto para todo número natural. □

Ejercicio. 7.11.
Usa el principio de inducción para probar la siguiente afirmación:

$$a^{2n} - b^{2n} \textit{ es divisible por } a + b \quad \forall n \in \mathbb{N}.$$

SOLUCIÓN. Para $n = 0$ el resultado es cierto. Comprobamos que el resultado es también cierto para $n = 1$ y $n = 2$. Suponemos que es cierto para un $n \geq 2$ y vamos a ver qué ocurre para $n+1$. Procedemos como sigue:

$$\begin{aligned}
a^{2(n+1)} - b^{2(n+1)} &= a^{2n+2} - b^{2n+2} \\
&= a^{2n+2} - a^{2n}b^2 + a^{2n}b^2 - b^{2n+2} \\
&= a^{2n}(a^2 - b^2) + (a^{2n} - b^{2n})b^2,
\end{aligned}$$

luego el resultado es cierto para todo número natural. □

Ejercicio. 7.12.
Usa el principio de inducción para probar la siguiente afirmación:

$$\frac{1}{2n} \leq \frac{1 \times 3 \times 5 \times \cdots \times (2n-1)}{2 \times 4 \times 6 \times \cdots \times (2n)} \text{ para } n \geq 1.$$

SOLUCIÓN. Para $n = 0$ no tiene sentido la expresión, por lo que añadiremos este valor al conjunto de los números naturales que satisfacen esta relación. Para $n = 1$ el resultado es cierto. Supongamos que $n \geq 1$ también satisface esta relación y veamos qué ocurre con $n+1$. En este caso tenemos:

$$\begin{aligned} \frac{1\times3\times5\times\cdots\times(2n-1)\times(2n+1)}{2\times4\times6\times\cdots\times(2n)\times(2n+2)} &= \frac{1\times3\times5\times\cdots\times(2n-1)}{2\times4\times6\times\cdots\times(2n)} \frac{2n+1}{2n+2} \\ &\geq \frac{1}{2n} \frac{2n+1}{2n+2} \\ &= \frac{1}{2n+2} \frac{2n+1}{2n} \\ &\geq \frac{1}{2n+2}, \end{aligned}$$

luego el resultado es cierto para todo número natural mayor o igual que 1. □

Ejercicio. 7.13.
Usa el principio de inducción para probar la siguiente afirmación:

$$\frac{1}{\sqrt{1}} + \frac{1}{\sqrt{2}} + \cdots + \frac{1}{\sqrt{n}} > \sqrt{n} \text{ para } n \geq 2.$$

SOLUCIÓN. Para $n = 0, 1$ el resultado no es cierto, por lo que añadiremos estos valores al conjunto de los números naturales que verifican la relación. Para $n = 2$ el resultado es cierto. Supongamos que $n \geq 2$ satisface esa condición, y estudiemos el caso de $n + 1$. Procedemos como sigue:

$$\begin{aligned} \frac{1}{\sqrt{1}} + \frac{1}{\sqrt{2}} + \cdots + \frac{1}{\sqrt{n}} + \frac{1}{\sqrt{n+1}} &> \sqrt{n} + \frac{1}{\sqrt{n+1}} \\ &= \frac{n}{\sqrt{n}} + \frac{1}{\sqrt{n+1}} \\ &= \frac{n\sqrt{n+1}+\sqrt{n}}{\sqrt{n}\sqrt{n+1}} \\ &> \frac{n\sqrt{n}+\sqrt{n}}{\sqrt{n}\sqrt{n+1}} \\ &= \frac{\sqrt{n}(n+1)}{\sqrt{n}\sqrt{n+1}} \\ &= \frac{n+1}{\sqrt{n+1}} \\ &= \sqrt{n+1}, \end{aligned}$$

luego el resultado es cierto para todo número natural mayor o igual que 2. □

Ejercicio. 7.14.
Usa el principio de inducción para probar la siguiente afirmación:

$$2^n \geq 2n + 1 \text{ para } n \geq 3.$$

SOLUCIÓN. Para $n = 0, 1, 2$ el resultado no es cierto, por lo que añadiremos estos valores al conjunto de los números naturales que verifican esta relación. Para $n = 3$ el resultado es cierto. Supongamos que $n \geq 3$ satisface esta condición, y estudiemos el caso de $n + 1$. Procedemos como sigue:

$$\begin{aligned} 2^{n+1} &= 2^n \cdot 2 \geq (2n+1)2 = 4n+2 \\ &= 2n+3+(2n-1) \geq 2(n+1)+1. \end{aligned}$$

luego el resultado es cierto para todo número natural mayor o igual que 3. □

Ejercicio. 7.15.
Usa el principio de inducción para probar la siguiente afirmación:

$$2^n \geq n^2 \text{ para } n \geq 4.$$

SOLUCIÓN. Para $n = 0, 1, 2, 3$ el resultado no es cierto, por lo que añadiremos estos valores al conjunto de los números naturales que verifican esta relación. Para $n = 4$ el resultado es cierto. Supongamos que $n \geq 4$ satisface esta condición, y estudiemos el caso de $n + 1$. Procedemos como sigue:

$$\begin{aligned} 2^{n+1} &= 2^n \cdot 2 \geq n^2 \cdot 2 = n^2 + 2n + 1 + n^2 - 2n - 2 \\ &= (n+1)^2 + (n^2 - 2n - 2) \geq (n+1)^2. \end{aligned}$$

luego el resultado es cierto para todo número natural mayor o igual que 4. □

Ejercicio. 7.16.
Encuentra una definición recursiva verificada por cada una de las siguientes secuencias de números:

(1) $8, 15, 22, 29, 36, 43, \ldots$

(2) $6, 12, 24, 48, 96, \ldots$

(3) $1, 3, 7, 15, 31, 63, \ldots$

SOLUCIÓN.

(1) Llamamos $a_0 = 8$, $a_1 = 15$, $a_2 = 22$, $a_3 = 29$, $a_4 = 36$, $a_5 = 43$, entonces las diferencias son:

$$\begin{aligned} \Delta a_0 &= a_1 - a_0 = 15 - 8 = 7 \\ \Delta a_1 &= a_2 - a_1 = 22 - 15 = 7 \\ \Delta a_2 &= a_3 - a_2 = 29 - 22 = 7 \\ \Delta a_3 &= a_4 - a_3 = 36 - 29 = 7 \\ \Delta a_4 &= a_5 - a_4 = 43 - 36 = 7 \ldots \end{aligned}$$

Así pues tenemos una sucesión aritmética de diferencia 7, el término general es $a_n = a_0 + n \times 7 = 8 + n \times 7$.

(2) Llamamos $a_0 = 6$, $a_1 = 12$, $a_2 = 24$, $a_3 = 48$, $a_4 = 96$, es claro que $a_{n+1} = 2a_n$. Suponemos que el término general verifica la fórmula $a_n = 2^n 6$. Para probar este resultado hacemos inducción sobre n. Para $n = 0$ es resultado es cierto; suponemos que es cierto para un $n \geq 0$, y vamos a probarlo para $n + 1$. Procedemos como sigue:

$$a_{n+1} = 2a_n = 2 \times (2^n 6) = 2^{n+1} 6.$$

(3) Llamamos $a_0 = 1$, $a_1 = 3$, $a_2 = 7$, $a_3 = 15$, $a_4 = 31$, $a_5 = 63$, entonces las diferencias son:

$$\begin{aligned}
\Delta a_0 &= a_1 - a_0 = 3 - 1 = 2 = 2^1 \\
\Delta a_1 &= a_2 - a_1 = 7 - 3 = 4 = 2^2 \\
\Delta a_2 &= a_3 - a_2 = 15 - 7 = 8 = 2^3 \\
\Delta a_3 &= a_4 - a_3 = 31 - 15 = 16 = 2^4 \\
\Delta a_4 &= a_5 - a_4 = 63 - 31 = 32 = 2^5 \ldots
\end{aligned}$$

Así pues tenemos

$$\begin{aligned}
a_0 &= 1 = 2^1 - 1 \\
a_1 &= a_0 + 2^1 = 1 + 2^1 = \tfrac{2^2-1}{2-1} = 2^2 - 1, \\
a_2 &= a_1 + 2^2 = 1 + 2^1 + 2^2 = \tfrac{2^3-1}{2-1} = 2^3 - 1, \\
a_3 &= a_2 + 2^3 = 1 + 2^1 + 2^2 + 2^3 = \tfrac{2^4-1}{2-1} = 2^4 - 1, \\
a_4 &= a_3 + 2^4 = 1 + 2^1 + 2^2 + 2^3 + 2^4 = \tfrac{2^5-1}{2-1} = 2^5 - 1, \\
a_5 &= a_4 + 2^5 = 1 + 2^1 + 2^2 + 2^3 + 2^4 + 2^5 = \tfrac{2^6-1}{2-1} = 2^6 - 1.
\end{aligned}$$

Entonces el término general es $a_n = 2^{n+1} - 1$.

Hacer la demostración por inducción sobre n.

□

Ejercicio. 7.17.
Demostrar que

$$1 \cdot 1! + 2 \cdot 2! + 3 \cdot 3! + \cdots + n \cdot n! = (n+1)! - 1.$$

SOLUCIÓN. Para $n = 1$ el resultado es cierto, ya que

$$1 \cdot 1! = 1 = 2! - 1.$$

Suponemos que el resultado es cierto para n y vamos a probarlo para $n + 1$.

$$\begin{aligned}
&1 \cdot 1! + 2 \cdot 2! + 3 \cdot 3! + \cdots + n \cdot n! + (n+1) \cdot (n+1)! \\
&= (n+1)! - 1 + (n+1) \cdot (n+1)! \\
&= (n+1)![1 + n + 1] - 1 \\
&= (n+1)!(n+2) - 1 = (n+2)! - 1.
\end{aligned}$$

□

Ejercicio. 7.18.
Demostrar que:

$$\frac{1}{1\cdot 3}+\frac{1}{3\cdot 5}+\cdots+\frac{1}{(2n-1)(2n+1)}=\frac{n}{2n+1}.$$

SOLUCIÓN. Para $n=1$ el resultado es cierto, ya que:

$$\frac{1}{1\cdot 3}=\frac{1}{3}=\frac{1}{2+1}.$$

Supongamos que el resultado es cierto para n y vamos a probarlo para $n+1$.

$$\begin{aligned}
&\tfrac{1}{1\cdot 3}+\tfrac{1}{3\cdot 5}+\cdots+\tfrac{1}{(2n-1)(2n+1)}+\tfrac{1}{(2n+1)(2n+3)}\\
&=\tfrac{n}{2n+1}+\tfrac{1}{(2n+1)(2n+3)}\\
&=\tfrac{n(2n+3)+1}{(2n+1)(2n+3)}\\
&=\tfrac{2n^2+3n+1}{(2n+1)(2n+3)}\\
&=\tfrac{(2n+1)(n+1)}{(2n+1)(2n+3)}\\
&=\tfrac{2n+1}{2n+3}.
\end{aligned}$$

□

Ejercicio. 7.19.
Demostrar que:

$$4\left(\frac{1}{2\cdot 3}\right)+8\left(\frac{2}{3\cdot 4}\right)+\cdots+2^{n+1}\left(\frac{n}{(n+1)(n+2)}\right)=\frac{2^{n+2}}{n+2}-2.$$

SOLUCIÓN. Para $n=1$ el resultado es cierto, ya que

$$4\frac{1}{2\cdot 3}=\frac{2}{3}=\frac{2^3}{3}-2.$$

Supongamos que el resultado es cierto para n y vamos a probarlo para $n+1$.

$$\begin{aligned}
&4\left(\tfrac{1}{2\cdot 3}\right)+8\left(\tfrac{2}{3\cdot 4}\right)+\cdots+2^{n+1}\left(\tfrac{n}{(n+1)(n+2)}\right)+2^{n+2}\left(\tfrac{n+1}{(n+2)(n+3)}\right)\\
&=\tfrac{2^{n+2}}{n+2}-2+2^{n+2}\left(\tfrac{n+1}{(n+2)(n+3)}\right)\\
&=2^{n+2}\left(\tfrac{1}{n+2}+\tfrac{n+1}{(n+2)(n+3)}\right)-2\\
&=2^{n+2}\left(\tfrac{2(n+2)}{(n+2)(n+3)}\right)-2\\
&=2^{n+3}\tfrac{1}{n+3}-2.
\end{aligned}$$

□

Ejercicio. 7.20.
Demostrar que para número natural $n \geq 1$ el número $11^n - 1$ es un múltiplo de 5.

SOLUCIÓN. Hacer □

Ejercicio. 7.21.
Demostrar que para número natural $n \geq 0$ el número $3^n + 7^n - 2$ es un múltiplo de 8.

SOLUCIÓN. Hacer □

Ejercicio. 7.22.
Dar una fórmula simple para la siguiente expresión:

$$\frac{1}{1\cdot 2} + \frac{1}{2\cdot 3} + \frac{1}{3\cdot 4} + \cdots + \frac{1}{n(n+1)}.$$

SOLUCIÓN. Calculamos las siguientes sumas:
Para $n = 1$:

$$\frac{1}{2}.$$

Para $n = 2$:

$$\frac{1}{2} + \frac{1}{2\cdot 3} = \frac{1}{2} + \frac{1}{6} = \frac{2}{3}.$$

Para $n = 3$:

$$\frac{1}{2} + \frac{1}{2\cdot 3} + \frac{1}{3\cdot 4} = \frac{1}{2} + \frac{1}{6} + \frac{1}{12} = \frac{3}{4}.$$

Podemos entonces hacer la siguiente hipótesis:

$$\frac{1}{1\cdot 2} + \frac{1}{2\cdot 3} + \frac{1}{3\cdot 4} + \cdots + \frac{1}{n(n+1)} = \frac{n}{n+1}.$$

Se prueba por inducción sobre n. □

Ejercicio. 7.23.
Sea x un número real, $x > -1$. Demostrar que se verifica $(1+x)^n \geq 1 + nx$ para todo número natural n.

SOLUCIÓN. Si $n = 0$, entonces $(1+x)^0 = 1 = 1 + 0x$. Supongamos que el resultado es cierto para n y vamos a probarlo para $n+1$.

$$(1+x)^{n+1} = (1+x)^n(1+x) \geq (1+nx)(1+x) = 1+nx+x+nx^2 = 1+(n+1)x+nx^2 \geq 1+(n+1)x.$$

□

8. Sistemas de numeración

Ejercicio. 8.1.
Encuentra los sistemas de numeración, si existe alguno, para los que se verifica la siguiente igualdad:

$$3 \times 4 = 22.$$

SOLUCIÓN. Llamamos β a la base del sistema de numeración, se tiene entonces la siguiente igualdad:

$$3 \times 4 = 2\beta + 2,$$

entonces resulta: $12 = 2(\beta + 1)$, esto es, $6 = \beta + 1$ y resulta $\beta = 5$. □

Ejercicio. 8.2.
Encuentra los sistemas de numeración, si existe alguno, para los que se verifica la siguiente igualdad:

$$41 \times 14 = 1224.$$

SOLUCIÓN. Llamamos β a la base del sistema de numeración, se tiene entonces la siguiente igualdad:

$$(4\beta + 1)(1\beta + 4) = 1\beta^3 + 2\beta^2 + 2\beta + 4,$$

entonces resulta:

$$4\beta^2 + (16 + 1)\beta + 4 = \beta^3 + 2\beta^2 + 2\beta + 4,$$

$$\beta^3 - 2\beta^2 - 15\beta = 0.$$

Por lo tanto, como esta ecuación es: $\beta(\beta^2 - 2\beta - 15) = 0$, y como las raíces son $\beta = 0$, $\beta = 5$ y $\beta = -3$, la única posible base es $\beta = 5$. □

Ejercicio. 8.3.
Encuentra los sistemas de numeración, si existe alguno, para los que se verifica la siguiente igualdad:

$$52 \times 25 = 1693.$$

SOLUCIÓN. Llamamos β a la base del sistema de numeración, se tiene entonces la siguiente igualdad:

$$(5\beta + 2)(2\beta + 5) = 1\beta^3 + 6\beta^2 + 9\beta + 3,$$

entonces resulta:

$$10\beta^2 + (25 + 4)\beta + 10 = \beta^3 + 6\beta^2 + 9\beta + 3,$$

$$\beta^3 - 4\beta^2 - 20\beta - 7 = 0.$$

Una raíz es $\beta = 7$, entonces tenemos $(\beta - 7)(\beta^2 + 3\beta + 1) = 0$, siendo $\beta = 7$ la única raíz entera, luego la base sería $\beta = 7$.

9 no es una cifra al considerar la base 7, luego no existe una base para la que se verifique la igualdad. □

Ejercicio. 8.4.
Encuentra los sistemas de numeración, si existe alguno, para los que se verifica la siguiente igualdad:

$$25 \times 13 = 51.$$

SOLUCIÓN. Llamamos β a la base del sistema de numeración, se tiene entonces la siguiente igualdad:

$$(2\beta + 5)(1\beta + 3) = 5\beta + 1,$$

entonces resulta:

$$2\beta^2 + (6 + 5)\beta + 15 = 5\beta + 1,$$

$$2\beta^2 + 6\beta + 14 = 0,$$

$$\beta^2 + 3\beta + 7 = 0.$$

Esta ecuación no tiene raíces enteras, luego no hay ninguna base para la que esta igualdad sea cierta. □

Ejercicio. 8.5.
Encuentra los sistemas de numeración, si existe alguno, para los que se verifica la siguiente igualdad:

$$13^4 = 14641.$$

SOLUCIÓN. Llamamos β a la base del sistema de numeración, se tiene entonces la siguiente igualdad:

$$(1\beta + 3)^4 = 1\beta^4 + 4 \times 3\beta^3 + 6 \times 3^2\beta^2 + 4 \times 3^3\beta + 3^4,$$

entonces resulta:

$$\beta^4 + 12\beta^3 + 54\beta^2 + 108\beta + 81 = \beta^4 + 4\beta^3 + 6\beta^2 + 4\beta + 1,$$

$$8\beta^3 + 48\beta^2 + 104\beta + 80 = 0.$$

Como consecuencia, al no tener raíces enteras, resulta que no existe una tal base del sistema de numeración. □

Ejercicio. 8.6.
Da la expresión en base 8 *de los naturales que en base* 2 *se escriben:*

(1) 101101100010011010111,

(2) 10001000000100110,

(3) 1011101111011111.

SOLUCIÓN.

(1) 101101100010011010111 en base binaria cuando lo escribimos en base decimal es: 1492183 Este número en base 8 es: 5542327_8.

(2) 10001000000100110, en base binaria cuando lo escribimos en base decimal es: 69670 Este número en base 8 es: 210046_8.

(3) 1011101111011111, en base binaria cuando lo escribimos en base decimal es: 48095 Este número en base 8 es: 135737_8.

□

Ejercicio. 8.7.
Demuestra que para $B \geq 3$, los números $(B-1)^2$ y $2(B-1)$ se escriben en base B como ab y ba respectivamente.

SOLUCIÓN. Tenemos las igualdades:

$$\begin{array}{l} (B-1)^2 = B^2 - 2B + 1 = (B-2)B + 1 \quad \text{y} \\ 2(B-1) = B + (B-2). \end{array}$$

□

Ejercicio. 8.8.
Demuestra que un número escrito en base 10 es par si y sólo si su última cifra es par.

SOLUCIÓN. El número se escribe $\sum_{i=0}^{t} a_i 10^i$. Esta expresión también se puede escribir como la suma de dos sumandos

$$10 \sum_{i=1}^{t} a_i 10^{i-1} + a_0,$$

y como el primer sumando es múltiplo de dos, resulta que el número es múltiplo de dos si y solo si lo es el segundo sumando, esto es, la cifra de las unidades. □

Ejercicio. 8.9.
Demuestra que un número escrito en base 10 es un múltiplo de 3 si y sólo si la suma de sus cifras es un múltiplo de 3.

SOLUCIÓN. El número se escribe $\sum_{i=0}^{t} a_i 10^i$. Al hacer la reducción módulo 3, como $10 \equiv 1 \pmod{3}$, resulta que módulo 3 el número se escribirá:

$$\sum_{i=0}^{t} \overline{a_i}.$$

El número es múltiplo de 3 si y solo si al reducirlo módulo 3 el resultado es la clase de cero, y basta observar que $\sum_{i=0}^{t} \overline{a_i}$ es la clase de cero si y solo si la suma $\sum_{i=0}^{t} a_i$ es múltiplo de 3. □

Ejercicio. 8.10.
Demuestra que un número escrito en base 10 es un múltiplo de 9 si y sólo si la suma de sus cifras es un múltiplo de 9.

SOLUCIÓN. Igual al ejercicio 8.9.. □

Ejercicio. 8.11.
Demuestra que un número escrito en base 10 es un múltiplo de 5 si acaba en 0 o en 5.

SOLUCIÓN. Igual al ejercicio 8.8.. □

Ejercicio. 8.12.
Demuestra que un número escrito en base 10 es múltiplo de 11 si y sólo si la suma de las cifras que ocupan un lugar par menos la suma de las cifras que ocupan posiciones impares es un múltiplo de 11.

SOLUCIÓN. El número se escribe $\sum_{i=0}^{t} a_i 10^i$. Observamos que $10 \equiv -1 \pmod{11}$ y que $10^2 \equiv 1 \pmod{11}$. Entonces es fácil probar que

$$10^i \equiv \begin{cases} 1 \pmod{11} & \text{si } i \text{ es par y} \\ -1 \pmod{11} & \text{si } i \text{ es impar.} \end{cases}$$

Al reducir módulo 11 la clase del número es $\sum_{i=0}^{t}(-1)^i \overline{a_i}$. El número es múltiplo de 11 si ésta es la clase del cero y es la clase del cero si y solo si el número $\sum_{i=0}^{t}(-1)^i a_i$ es múltiplo de 11, esto es, si la suma de las cifras que ocupan lugares pares se diferencia de la suma de las cifras que ocupan lugares impares en un múltiplo de 11. □

Ejercicio. 8.13.
Demuestra que un número escrito en base 8 es un múltiplo de 7 si y sólo si la suma de sus cifras es un múltiplo de 7.

SOLUCIÓN. El número se escribe $\sum_{i=0}^{t} a_i 8^i$. Como $8 \equiv 1 \pmod{7}$, al reducir este número módulo 7 obtenemos $\sum_{i=0}^{t} \overline{a_i}$. El número es múltiplo de 7 si y solo si al reducir módulo 7 obtenemos la clase del cero, y esto ocurre si y solo si la suma $\sum_{i=0}^{t} a_i$ es un múltiplo de 7. □

Ejercicio. 8.14.
Dar un criterio para determinar cuando un número entero positivo escrito en base 10 es múltiplo de 7.

SOLUCIÓN. Realizamos la división de potencias de 10 por 7 hasta que repitamos un resto. En este caso tenemos:

$$\begin{aligned}
&1 = 7 \times 0 + 1\\
&10 = 7 \times 1 + 3\\
&10^2 = 7 \times 14 + 2\\
&10^3 = 7 \times 142 + 6\\
&10^4 = 7 \times 1428 + 4\\
&10^5 = 7 \times 14285 + 5\\
&10^6 = 7 \times 142857 + 1
\end{aligned}$$

A partir de este punto repetimos los restos en el mismo orden. Como consecuencia, dado un número entero positivo escrito en base 10, sea éste, por ejemplo

$$a_t a_{t-1} a_{t-2} \dots a_1 a_0,$$

se escribe como:

$$a_0 + 10a_1 + 10^2 a_2 + \cdots + 10^{t-1} a_{t-1} + 10^t a_t,$$

y por tanto como:

$$a_0+(7\times1+3)a_1+(7\times14+2)a_2+(7\times142+6)a_3+(7\times1428+4)a_4+(7\times14285+5)a_5+(7\times142857+1)a_6+\cdots,$$

esto es:

$$a_0 + 3a_1 + 2a_2 + 6a_3 + 4a_4 + 5a_5 + a_6 + 3a_7 + 2a_8 + 6a_9 + \cdots + \text{múltiplo de } 7,$$

que también se puede escribir como:

$$a_0 + 3a_1 + 2a_2 - a_3 - 3a_4 - 2a_5 + a_6 + 3a_7 + 2a_8 - a9 + \cdots + \text{múltiplo de } 7.$$

Por tanto el criterio es que la suma $a_0 + 3a_1 + 2a_2 - a_3 - 3a_4 - 2a_5 + a_6 + 3a_7 + 2a_8 - a9 + \cdots$ sea un múltiplo de 7. □

Ejercicio. 8.15.
Dar un criterio para determinar cuando un número entero positivo escrito en base 10 es múltiplo de 13.

SOLUCIÓN. Realizamos la división de potencias de 10 por 13 hasta que repitamos un resto. En este caso tenemos:

$$\begin{aligned}
&1 = 13 \times 0 + 1\\
&10 = 13 \times 0 + 10\\
&10^2 = 13 \times 7 + 9\\
&10^3 = 13 \times 76 + 12\\
&10^4 = 13 \times 769 + 3\\
&10^5 = 13 \times 7692 + 4\\
&10^6 = 13 \times 76923 + 1
\end{aligned}$$

A partir de este punto repetimos los restos en el mismo orden. Como consecuencia, dado un número entero positivo escrito en base 10, sea éste, por ejemplo

$$a_t a_{t-1} a_{t-2} \ldots a_1 a_0,$$

se escribe como:

$$a_0 + 10a_1 + 10^2 a_2 + \cdots + 10^{t-1} a_{t-1} + 10^t a_t,$$

y por tanto como:

$$a_0+10a_1+(13\times7+9)a_2+(13\times76+12)a_3+(13\times769+3)a_4+(13\times7692+4)a_5+(13\times76923+1)a_6+\cdots,$$

esto es:

$$a_0 + 10a_1 + 9a_2 + 12a_3 + 3a_4 + 4a_5 + a_6 + 10a_7 + 9a_8 + 12a_9 + \cdots + \text{múltiplo de } 13,$$

que también se puede escribir como:

$$a_0 - 3a_1 - 4a_2 - a_3 + 3a_4 + 2a_5 + a_6 - 3a_7 - 4a_8 - a9 + \cdots + \text{múltiplo de } 13.$$

Por tanto el criterio es que la suma $a_0 - 3a_1 - 4a_2 - a_3 + 3a_4 + 2a_5 + a_6 - 3a_7 - 4a_8 - a9 + \cdots$ sea un múltiplo de 13. □

9. Números enteros

Ejercicio. 9.1.
Calcular el mcd y la Identidad de Bezout de 92 *y* 108*.*

SOLUCIÓN. Hacemos la divisiones sucesivas obteniendo:

	1	5	1	3
108	92	16	12	4
16	12	4	0	

Luego el mcd es 4, y para obtener la Identidad de Bezout procedemos como sigue:

$$4 = 16 - 12 \cdot 1 = 16 - (92 - 16 \cdot 5) \cdot 1 = 92 \cdot (-1) + 16 \cdot (6) =$$
$$92 \cdot (-1) + (108 - 92) \cdot (6) = 108 \cdot (6) + 92(-7).$$

□

Con la definición de mcd y mcm dada por la relación de división, resolver los siguientes ejercicios.

Ejercicio. 9.2.
Probar que dados dos enteros primos relativos no nulos a y b se verifica $(a+b, ab) = 1 = (a-b, ab)$.

SOLUCIÓN. Supongamos que $d = (a+b, ab)$ y que p es un entero primo que divide a d, entonces $p \mid (a+b)$ y $p \mid ab$, de la segunda relación y del hecho de ser a y b primos relativos obtenemos que ó $p \mid a$ ó $p \mid b$, pero no se verifican las dos posibilidades a la vez; si suponemos que $p \mid a$, entonces de la relación $p \mid (a+b)$ deducimos que $p \mid b$, lo que es una contradicción. Como consecuencia d no tiene divisores primos, esto es; $d = 1$. El otro caso es análogo. □

Ejercicio. 9.3.
Probar que si a, b, c son enteros y a es positivo, entonces $(ab, ac) = a(b, c)$.

SOLUCIÓN. Supongamos que $d = (b, c)$, entonces ad divide a ab y a ac, además tenemos la Identidad de Bezout $d = \alpha b + \beta c$, entonces $ad = \alpha ab + \beta ac$, y por tanto si e es un divisor común de ab y de ac, entonces también es un divisor de ad, luego $ad = (ab, ac)$. □

Ejercicio. 9.4.
Probar que si a, b, c son enteros tales que $(a, c) = 1$ y $(b, c) = 1$, entonces $(ab, c) = 1$.

SOLUCIÓN. Vamos a aplicar las Identidades de Bezout, tenemos

$$1 = \alpha a + \beta c, \qquad 1 = \gamma b + \delta c,$$

multiplicando ambas expresiones y agrupando los términos convenientemente tenemos

$$1 = \alpha\gamma ab + (\alpha\delta a + \beta\gamma b + \beta\delta c)c,$$

y por tanto $(ab, c) = 1$. □

Ejercicio. 9.5.
Sean a, b enteros y $d = (a, b)$, probar que si $x \in \mathbb{Z}$ verifica $a \mid x$ y $b \mid x$, entonces $ab \mid dx$.

SOLUCIÓN. Es claro que si $a \mid x$ y $b \mid x$, entonces $M \mid x$, donde M es el mcm de a y b, entonces $dM \mid dx$, pero ya que se verifica $ab = dM$, tenemos el resultado. □

Ejercicio. 9.6.
Sean a, b enteros no nulos y $d = (a, b)$, probar que a/d y b/d son primos relativos.

SOLUCIÓN. En este ejercicio a/d representa al número entero z que verifica $a = dz$. Por la Identidad de Bezout se verifica $d = \alpha a + \beta b$, para $\alpha, \beta \in \mathbb{Z}$, esta expresión sustituimos a y b por sus expresiones en función de d, esto es;

$$d = \alpha d(a/d) + \beta d(b/d),$$

simplificando por d, que es no nulo ya que a y b lo son, tenemos

$$1 = \alpha(a/d) + \beta(b/d),$$

y por tanto a/d y b/d son primos relativos. □

Ejercicio. 9.7.
Sean a, b, c enteros, probar que $(a, (b, c)) = ((a, b), c)$.

SOLUCIÓN. Llamemos $d_1 = (b, c)$ y $d_2 = (a, (b, c))$, entonces tenemos las siguientes relaciones de divisibilidad:

$$d_2 \mid d_1;\ d_2 \mid a;\ d_2 \mid b;\ d_2 \mid c.$$

Como consecuencia se verifica $d_2 \mid (a, b)$, y entonces $d_2 \mid ((a, b), c)$. Si llamamos $d_3 = (a, b)$ y $d_4 = ((a, b, c)$, entonces hemos probado que $d_2 \mid d_4$. De forma análoga podemos probar que $d_4 \mid d_2$, y como ambos son positivos ó nulos, entonces son iguales. □

Ejercicio. 9.8.
Probar que para todo número entero $n \in \mathbb{Z}$ se verifica: $n^2 \geq n$.
En particular $n^2 \geq 0$ para todo $n \in \mathbb{Z}$.

SOLUCIÓN. Hacemos una disyunción de casos:

(1) Si $n = 0$, entonces $n^2 = 0 = n$.

(2) Si $n > 0$, entonces $n > 1$, y por tanto $n^2 = n \cdot n > 1 \cdot n = n$.

(3) Si $n < 0$, entonces $n^2 = n \cdot n > 0 \cdot n = 0 > n$.

□

Ejercicio. 9.9.
Probar que para cualesquiera n, $m \in \mathbb{Z}$ se verifica $n^2 + m^2 \geq 2nm$.

SOLUCIÓN. Como tenemos $(n-m)^2 \geq 0$, basta desarrollar para obtener $n^2 - 2nm + m^2 \geq 0$, entonces resulta $n^2 + m^2 \geq 2nm$. □

Ejercicio. 9.10.
Probar que para cada entero $n \geq 1$ se verifica:

$$1 + 2^3 + 3^3 + 4^3 + \cdots + n^3 = \frac{n^2(n+1)^2}{4}.$$

SOLUCIÓN. Para $n = 1$ el resultado es cierto. Suponemos que se verifica para $n \geq 1$ y vamos a veer si también se verifica para $n + 1$.

$$\begin{aligned} 1 + 2^3 + 3^3 + \cdots + n^3 + (n+1)^3 &= \tfrac{n^2(n+1)^2}{4} + (n+1)^3 \\ &= \tfrac{n^2(n+1)^2 + 4(n+1)^3}{4} \\ &= \tfrac{(n+1)^2[n^2+4n+4]}{4} \\ &= \tfrac{(n+1)^2(n+2)^2}{4}. \end{aligned}$$

□

Ejercicio. 9.11.
Calcular el mcd d de 24230 y 586, y encontrar números enteros a y b tales que $d = 24230a + 586b$.

SOLUCIÓN. Hacemos la divisiones sucesivas de 24230 por 586, obtenemos:

	41	2	1	6	1	5	2
24230	586	204	178	26	22	4	2
0790	178	026	022	04	02	0	
204							

Resulta entonces que el mcd es 2, ya que es el último resto no nulo, para hallar los coeficientes en la Identidad de Bezout tenemos que resolver las distintas igualdades que hemos obtenido con los restos, hagamos una lista con ellas:

$$\begin{aligned}
2 &= 22 - 4 \cdot 5 \\
4 &= 26 - 22 \cdot 1 \\
22 &= 178 - 26 \cdot 6 \\
26 &= 204 - 178 \cdot 1 \\
178 &= 586 - 204 \cdot 2 \\
204 &= 24230 - 586 \cdot 41
\end{aligned}$$

Ahora sustituyendo tenemos

$$\begin{gathered}
2 = 22 - 4 \cdot 5 = \\
22 - (26 - 22 \cdot 1) \cdot 5 = 26 \cdot (-5) + 22 \cdot (6) = \\
26 \cdot (-5) + (178 - 26 \cdot 6) \cdot (6) = 178 \cdot (6) + 26 \cdot (-41) = \\
178 \cdot (6) + (204 - 178 \cdot 1) \cdot (-41) = 204 \cdot (-41) + 178 \cdot (47) = \\
204 \cdot (-41) + (586 - 204 \cdot 2) \cdot (47) = 586 \cdot (47) + 204 \cdot (-135) = \\
586 \cdot (47) + (24230 - 586 \cdot 41) \cdot (-135) = 24230 \cdot (-135) + 586 \cdot (5582)
\end{gathered}$$

□

Ejercicio. 9.12.
Hasta ahora hemos realizado la división por números enteros positivos y hemos estudiado el mcd y el mcm para números enteros positivos, hacer las definiciones necesarias para extender la teoría a todos los números enteros (no nulos).

SOLUCIÓN. □

Ejercicio. 9.13.
Aplicar el Algoritmo de la división a los enteros 48 *y* -7*.*

SOLUCIÓN. Tenemos $48 = (-7) \cdot (-6) + 6$. □

Ejercicio. 9.14.
Probar que para $n \geq 8$ *se* n *se puede escribir como* $n = 3k + 5h$ *para* $k, h \in \mathbb{Z}$*.*

SOLUCIÓN. Para $n = 8$ tenemos $8 = 3 + 5$; para $n = 9$ tenemos $9 = 3 \times 3 + 5 \times 0$; para $n = 10$ tenemos $10 = 3 \times 0 + 5 \times 2$. Suponemos que es cierto para $n \geq 10$, y vamos a probarlo para $n + 1$.

Tenemos que $(n + 1) - 3 = n - 2$ es mayor o igual que 8, y menos que n, por tanto se puede escribir $n - 2 = 3k + 5h$, luego $n = (n - 2) + 3 = 3k + 5h + 3 = 3(k + 1) + 5h$. □

Ejercicio. 9.15.
Se p *y* q *son enteros primos positivos mayores que 5, entonces* $p + q$ *ó* $p - q$ *es un múltiplo de 3.*

SOLUCIÓN. Consideramos $p+2$ y $p-2$, como p es impar, podemos suponer que $p=2k+1$, entonces se tiene:

$$(p-2)(p-2)=p^2-4=4k^2+4k+1-4=4(k^2+k)-4$$

Vamos a ver que en los casos que nos interesan k^2-k es siempre un múltiplo de 3.

Caso $k\equiv 0 \pmod 3$, entonces k^2-k es múltiplo de 3.

Caso $k\equiv 1 \pmod 3$, entonces $p=2k+1=2(3h+1)+1=6h+3$ es múltiplo de 3, luego p no sería primo, ya que $p>3$.

Caso $k\equiv 2 \pmod 3$, entonces $k^2+k=(3h+2)^2+(3h+2)=(3h+2)[3h+2+1]$ es un múltiplo de 3.

En consecuencia, si $p=2k+1$ es primo, resulta que k^2+k es múltiplo de 3.

Al considerar $p+q$ y $p-q$, resulta que podemos escribirlos como:

$$\begin{array}{l} p+q=(p-2)+(q+2)=(p+2)+(q-2), \\ p-q=(p-2)-(q-2)=(p+2)-(q+2(. \end{array}$$

y alguno de ellos es un múltiplo de 3. □

Ejercicio. 9.16.
Se p y q son enteros primos positivos mayores que 5, entonces p^2-q^2 es un múltiplo de 24.

SOLUCIÓN. Por el Ejercicio 9.15. resulta que $p+q$ ó $p-q$ es un múltiplo de 3. Tenemos que ver que p^2-q^2 es un múltiplo de 8.

Es claro que $p+q$ y $p-q$ son múltiplos de 2, luego $p^2-q^2=(p+q)(p-q)$ es múltiplo de 4. Analicemos los posibles casos:

Caso 1. $p\equiv 1 \pmod 4$ y $q\equiv 1 \pmod 4$, entonces $p-q\equiv 0 \pmod 4$ y tenemos el resultado.

Caso 2. $p\equiv 1 \pmod 4$ y $q\equiv 3 \pmod 4$, entonces $p+q\equiv 0 \pmod 4$ y tenemos el resultado.

Caso 3. $p\equiv 3 \pmod 4$ y $q\equiv 1 \pmod 4$, entonces $p+q\equiv 0 \pmod 4$ y tenemos el resultado.

Caso 4. $p\equiv 3 \pmod 4$ y $q\equiv 3 \pmod 4$, entonces $p-q\equiv 0 \pmod 4$ y tenemos el resultado. □

Ejercicio. 9.17.
Probar que si $a^2\equiv b^2 \pmod n$, no necesariamente se verifica $a\equiv b \pmod n$

SOLUCIÓN. Basta tomar $n=4$, $a=1$ y $b=3$. □

Ejercicio. 9.18.
Probar que si $a \equiv b \pmod{nm}$*, entonces* $a \equiv b \pmod{n}$ *y* $a \equiv b \pmod{m}$*.*
Observar que el recíproco no es cierto, en general, si n y m no son primos relativos

SOLUCIÓN. Si $a - b = k(nm)$, entonces $a - b = (kn)m = (km)n$.
Para la segunda parte basta considerar el siguiente ejemplo: $n = 2$, $m = 4$ y $a = 3$, $b = 7$. □

Ejercicio. 9.19.
Sean a, b $\in \mathbb{Z}$ *tales que* $\mathrm{m.c.d.}\{a, b\} = 1$*. Demuestra que:*

(1) $\mathrm{m.c.d.}\{a + b, ab\} = 1$,

(2) $\mathrm{m.c.d.}\{a - b, ab\} = 1$.

SOLUCIÓN.

(1) Si un entero primo p divide a $\mathrm{m.c.d.}\{a + b, ab\}$, entonces p divide a ab, y por tanto $p \mid a$ ó $p \mid b$. En el primer caso, se tiene, como $p \mid a + b$, que $p \mid b$; y por tanto $p \mid \mathrm{m.c.d.}\{a + b, ab\} = 1$, lo que es una contradicción.

(2) Es análogo.

□

Ejercicio. 9.20.
Sean a, b, c $\in \mathbb{Z}$*. Demuestra que* $\mathrm{m.c.d.}\{\mathrm{m.c.d.}\{a, b\}, c\} = \mathrm{m.c.d.}\{a, \mathrm{m.c.d.}\{b, c\}\}$.

SOLUCIÓN. Si p es un entero primo que divide a

$$\mathrm{m.c.d.}\{\mathrm{m.c.d.}\{a, b\}, c\},$$

entonces $p \mid \mathrm{m.c.d.}\{a, b\}$ y $p \mid c$, y por tanto $p \mid a$, b y c, luego podemos reorganizar estos elementos y probar que $p \mid \mathrm{m.c.d.}\{b, c\}$, y por tanto $p \mid \mathrm{m.c.d.}\{a, \mathrm{m.c.d.}\{b, c\}\}$. □

Ejercicio. 9.21.
Prueba que dado un número entero cualquiera m se verifica una de las siguientes posibilidades:

(1) $m^2 \equiv 0 \pmod{8}$,

(2) $m^2 \equiv 1 \pmod{8}$,

(3) $m^2 \equiv 4 \pmod{8}$.

SOLUCIÓN. Si escribimos el número m en la base 8, la cifra de sus unidades es una de las siguientes: 0, 1, 2, 3, 4, 5, 6, 7. El cuadrado de m_8 tiene como cifra de las unidades justamente la cifra de las unidades del cuadrado de la cifra de las unidades de m_8, entonces basta con analizar qué les ocurre a estos números. Tenemos:

c_8	c_8^2
0_8	0_8^2
1_8	1_8^2
2_8	4_8^2
3_8	11_8^2
4_8	20_8^2
5_8	31_8^2
6_8	44_8^2
7_8	61_8^2

□

Ejercicio. 9.22.
Prueba que si x es un número entero e impar no divisible por 3 entonces $x^2 \equiv 1 \pmod{24}$.

SOLUCIÓN. Escribimos el número x en la base 6, entonces la cifra de las unidades es 1, 3 ó 5 por ser impar. Por no ser divisible por 3 resulta que de estas tres posibilidades únicamente 1 y 5 son válidas. Así pues el número x se escribe en la forma $6y+1$ ó $6y+5$. Sus cuadrados son:

<u>Caso 1</u>.
$$(6y+1)^2 = 36y^2 + 12y + 1 = 12y(3y+1) + 1$$
si y es par, entonces $12y$ es múltiplo de 24, y si y es impar, entonces $3y+1$ es par y por tanto $12y(3y+1)$ es múltiplo de 24, luego siempre se verifica $x^2 \equiv 1 \pmod{24}$.

<u>Caso 2</u>.
$$(6y+5)^2 = 36y^2 + 60y + 1 = 12y(3y+5) + 1$$
hacemos el mismo razonamiento sobre la paridad de y. □

Ejercicio. 9.23.
Resuelve la siguiente congruencia:

$$3x \equiv 2 \pmod{5}.$$

SOLUCIÓN. Basta tener en cuenta que $2 \cdot 3 \equiv 1 \pmod{5}$, entonces resulta:

$$\begin{array}{l} 3x \equiv 2 \pmod{5}, \\ 2 \cdot 3x \equiv 2 \cdot 2 \pmod{5}, \\ x \equiv 4 \pmod{5}. \end{array}$$

□

Ejercicio. 9.24.
Resuelve la siguiente congruencia:

$$7x \equiv 4 \pmod{10}.$$

SOLUCIÓN. Basta tener en cuenta que $3 \cdot 7 \equiv 1 \pmod{10}$, entonces resulta:

$$7x \equiv 4 \pmod{10}, 3 \cdot 7x \equiv 3 \cdot 4 \pmod{10}, x \equiv 2 \pmod{10},$$

□

Ejercicio. 9.25.
Resuelve la siguiente congruencia:

$$6x \equiv 3 \pmod{4}.$$

SOLUCIÓN. La ecuación $6x \equiv 3 \pmod{4}$ no tiene solución, ya que para cualquier valor de x el producto $6x$ es un número par y al reducir módulo 4 su clase es 0 ó 2 y nunca 3. □

Ejercicio. 9.26.
Resuelve el siguiente sistema de ecuaciones en congruencias:

$$\left.\begin{array}{r} x \equiv 1 \pmod{2} \\ 6x \equiv 3 \pmod{9} \\ 3x \equiv 3 \pmod{5} \end{array}\right\}$$

SOLUCIÓN.

$$\left.\begin{array}{r} x \equiv 1 \pmod{2} \\ 6x \equiv 3 \pmod{9} \\ 3x \equiv 3 \pmod{5} \end{array}\right\}$$

Resolvemos el sistema $\left.\begin{array}{r} x \equiv 1 \pmod{2} \\ 3x \equiv 3 \pmod{5} \end{array}\right\}$, o equivalentemente el sistema $\left.\begin{array}{r} x \equiv 1 \pmod{2} \\ x \equiv 1 \pmod{5} \end{array}\right\}$.
Tenemos que $2 \times (-2) + 5 \times 1 = 1$, entonces se verifica:

$$\begin{array}{l} 1 = 2 \times (-2) + 5 \times 1 \equiv 5 \times 1 \pmod{2} \\ 1 = 2 \times (-2) + 5 \times 1 \equiv 2 \times (-2) \pmod{5} \end{array}$$

una solución es: $5+2\times(-2)\equiv 1 \pmod{10}$. Estudiamos ahora el sistema $\left.\begin{array}{r}x\equiv 1 \pmod{10}\\ 6x\equiv 3 \pmod{9}\end{array}\right\}$,
o equivalentemente los sistemas $\left.\begin{array}{r}x\equiv 1 \pmod{10}\\ x\equiv 2 \pmod{9}\end{array}\right\}$, $\left.\begin{array}{r}x\equiv 1 \pmod{10}\\ x\equiv 5 \pmod{9}\end{array}\right\}$, $\left.\begin{array}{r}x\equiv 1 \pmod{10}\\ x\equiv 8 \pmod{9}\end{array}\right\}$.

Como la resolución de todos ellos es similar vamos a ver como resolver el primero.

En el sistema $\left.\begin{array}{r}x\equiv 1 \pmod{10}\\ x\equiv 2 \pmod{9}\end{array}\right\}$ tenemos en cuenta que $9\times(-1)+10=1$, entonces se verifica:

$$\begin{array}{l}1=9\times(-1)+10\equiv 9\times(-1) \pmod{10}\\ 2=2\times 9\times(-1)+2\times 10\equiv 2\times 10 \pmod{9}\end{array}$$

una solución es: $9\times(-1)+2\times 10\equiv 11 \pmod{90}$.

La solución de $\left.\begin{array}{r}x\equiv 1 \pmod{10}\\ x\equiv 5 \pmod{9}\end{array}\right\}$ es: $9\times(-1)+5\times 10\equiv 41 \pmod{90}$.

La solución de $\left.\begin{array}{r}x\equiv 1 \pmod{10}\\ x\equiv 8 \pmod{9}\end{array}\right\}$ es: $9\times(-1)+8\times 10\equiv 71 \pmod{90}$.

La solución del sistema es: $x\equiv 11, 41$ ó $71 \pmod{90}$. □

Ejercicio. 9.27.
Resuelve el siguiente sistema de ecuaciones en congruencias:

$$\left.\begin{array}{r}x\equiv 1 \pmod{2}\\ x\equiv 2 \pmod{4}\end{array}\right\}$$

SOLUCIÓN.

$$\left.\begin{array}{r}x\equiv 1 \pmod{2}\\ x\equiv 2 \pmod{4}\end{array}\right\}$$

En este caso los módulos no son primos relativos. De la primera ecuación se obtiene que x es un número impar y de la segunda que es un número par, luego el sistema no tiene solución. □

Ejercicio. 9.28.
Resuelve el siguiente sistema de ecuaciones en congruencias:

$$\left.\begin{array}{r}x\equiv 3 \pmod{6}\\ x\equiv 1 \pmod{4}\\ 2x\equiv 1 \pmod{5}\end{array}\right\}$$

SOLUCIÓN.

$$\left.\begin{array}{r} x \equiv 3 \pmod 6 \\ x \equiv 1 \pmod 4 \\ 2x \equiv 1 \pmod 5 \end{array}\right\}$$

Intentamos resolver el sistema $\left.\begin{array}{r} x \equiv 3 \pmod 6 \\ x \equiv 1 \pmod 4 \end{array}\right\}$. Para ello observamos que toda solución a la primera ecuación es de la forma $x = 6k + 3$ luego se puede escribir como $x = 3(2k + 1)$, y como esto es para cualquier valor de k. Si introducimos este valor en la segunda ecuación resulta:

$$\begin{array}{l} 3(2k+1) \equiv 1 \pmod 4 \\ 2k+1 \equiv 3 \pmod 4 \\ 2k \equiv 2 \pmod 4 \end{array}$$

Luego k es un número impar, esto es, de la forma $k = 2h + 1$, para cualquier valor de h. Las soluciones al sistema son de la forma $x = 3(2k + 1) = 3(2(2h + 1) + 1) = 12h + 9$, esto es: $x \equiv 9 \pmod{12}$.

Ahora abordamos la resolución del sistema $\left.\begin{array}{r} x \equiv 9 \pmod{12} \\ 2x \equiv 1 \pmod 5 \end{array}\right\}$, o equivalentemente $\left.\begin{array}{r} x \equiv 9 \pmod{12} \\ x \equiv 3 \pmod 5 \end{array}\right\}$ y como 12 y 5 son primos relativos, la solución es:

$$\begin{array}{l} 9 = 9(12 \times (-2) + 5 \times 5) \equiv 9 \times 5 \times 5 \pmod{12} \\ 3 = 3(12 \times (-2) + 5 \times 5) \equiv 3 \times 12 \times (-2) \pmod 5 \\ x = 9 \times 5 \times 5 + 3 \times 12 \times (-2) \equiv 225 - 72 \equiv 153 \equiv 33 \pmod{60} \end{array}$$

La solución es $x \equiv 33 \pmod{60}$. □

Ejercicio. 9.29.
Tres granjeros dividen en partes iguales el arroz que han cultivado en común. Fueron a mercados diferentes en los que se usaban medidas de peso diferentes: en un lugar era de 7 kilos, en otro de 15 kilos y en el último de 19 kilos. Cada uno vendió todo lo que pudo en medidas enteras en sus respectivos mercados y a la vuelta al primer granjero le sobraban 6 kilos, al segundo 11 y al tercero 14. ¿Cuánto arroz habían cultivado?

SOLUCIÓN. Si llamamos X al número de kilos que arroz que corresponde a cada granjero resulta que tenemos las siguientes relaciones:

$$\left.\begin{array}{l} X \equiv 6 \pmod 7 \\ X \equiv 11 \pmod{15} \\ X \equiv 14 \pmod{19} \end{array}\right\}$$

Luego la cantidad de arroz que han cultivado es $3X$. Para calcular el valor de X basta resolver el sistema anterior.

El sistema $\left.\begin{array}{l} X \equiv 6 \pmod 7 \\ X \equiv 11 \pmod{15} \end{array}\right\}$ tiene como solución

$$X \equiv (6 \times 15 + 11 \times 7 \times (-2)) \equiv -64 \equiv 41 \pmod{105}.$$

Entonces resolvemos el sistema $\left.\begin{array}{ll} X \equiv 41 & \pmod{105} \\ X \equiv 14 & \pmod{19} \end{array}\right\}$, como se tiene la identidad de Bezout $1 = 2 \times 105 - 11 \times 19$, la solución es:

$$X \equiv (41 \times (-11) \times 19 + 14 \times 2 \times 105) \equiv -5629 \equiv 356 \pmod{1995}.$$

Entonces $X = 356 + 1995\lambda$ y por tanto la cantidad de arroz es: $1068 + 5985\lambda$ □

Ejercicio. 9.30.
Calcula el resto de dividir 4225^{1000} *entre* 7.

SOLUCIÓN. Se verifica $x^6 \equiv 1 \pmod{7}$ para cada número entero x, entonces podemos proceder como sigue:

$$\begin{array}{l} 1000 = 6 \times 166 + 4, \\ 4225 = 7 \times 603 + 4 \end{array}$$

$$\begin{array}{lll} 4225^{1000} & \equiv 4225^{6\times166+4} & \equiv 4225^{6\times166}4225^4 \\ & \equiv (4225^6)^{166}4225^4 & \equiv 4225^4 \\ & \equiv 4^4 & \equiv (4^2)^2 \\ & \equiv 2^2 & \equiv 4 \pmod{7} \end{array}$$

□

Ejercicio. 9.31.
Calcula el número de divisores positivos de 120.

SOLUCIÓN. Escribimos la factorización en primos de 120:

$$\begin{array}{l|l} 120 & 2 \\ 60 & 2 \\ 30 & 2 \\ 15 & 3 \\ 5 & 5 \\ 1 & \end{array}$$

$$120 = 2^3 \cdot 3 \cdot 5$$

Entonces cada divisor positivo de 120 se escribe en la forma $2^a \cdot 3^b \cdot 5^c$, siendo $0 \leq a \leq 3$, $0 \leq b \leq 1$ y $0 \leq c \leq 1$. Por tanto tenemos en total $4 \times 2 \times 2 = 16$ divisores positivos de 120. □

Ejercicio. 9.32.
Demuestra que si p es un número primo, entonces $\sqrt{p}$ *es irracional. Como aplicación, demuestra que* $\sqrt{75}$ *es irracional.*

SOLUCIÓN. Supongamos que $\sqrt{p}$ es un número racional, esto es, una fracción de dos números enteros, sean estos a y b. Podemos suponer que la fracción $\frac{a}{b}$ es irreducible, esto es, a y b son primos relativos. Entonces tenemos:

$$\sqrt{p} = \frac{a}{b}.$$

Elevando al cuadrado se tiene $p = \frac{a^2}{b^2}$, y por tanto

$$pb^2 = a^2.$$

Este número entero tiene una factorización única en enteros primos positivos, pero si contamos estos números primos vemos que en la derecha tenemos un número par y en la izquierda un número impar, lo cual es una contradicción. Por lo tanto la suposición hecha no es cierta, esto es, $\sqrt{p}$ no puede ser un número racional. □

Ejercicio. 9.33.
Calcula las soluciones en $\mathbb{Z}$ de la ecuación

$$2X + 3Y = 7.$$

SOLUCIÓN. La identidad de Bezout para 2 y 3 se puede escribir: $(-1) \times 2 + 3 = 1$, y como el máximo común divisor de 2 y 3 es 1, entonces la ecuación tiene solución. Una solución se calcula a partir de la identidad de Bezout.

$$7 = 7((-1) \times 2 + 3) = (-7) \times 2 + 7 \times 3,$$

por tanto una solución es: $X = -7$, $Y = 7$. Para determinar el resto de las raíces recordemos que si el par a, b es otra raíz, entonces $2 \times (-7) + 3 \times 7 = 2a + 3b$, y se tiene

$$2(a + 7) = 3(7 - b).$$

Por tanto $3 \mid a + 7$, luego $a = -7 + 3\lambda$ y $2 \mid 7 - b$, luego $b = 7 + 2\mu$, que al sustituirlos en la ecuación nos da:

$$7 = 2(-7 + 3\lambda) + 3(7 + 2\mu) =$$
$$2 \times (-7) + 2 \times 3\lambda + 3 \times 7 + 3 \times 2\mu = 7 + 2 \times 3(\lambda + \mu),$$

de donde $\lambda + \mu = 0$ y la solución general es:

$$a = -7 + 3\lambda, \qquad b = 7 - 2\lambda.$$

□

Ejercicio. 9.34.
Calcula las soluciones en $\mathbb{Z}$ de la ecuación

$$6X + 10Y = 16.$$

SOLUCIÓN. Como la identidad de Bezout de 6 y 10 es: $2 = 2\times 6-10$, resulta que 2 divide a 16 y la ecuación tiene solución. Al dividir por el máximo común divisor obtenemos una ecuación que tiene las mismas soluciones que la original: $3X + 5Y = 8$. Una solución es $X = 1$ e $Y = 1$, entonces el resto de las soluciones se obtienen como los pares: $X = 1 - 5t$, $Y = 1 + 3t$. □

Ejercicio. 9.35.
Demuestra que el conjunto de los números primos es infinito.

SOLUCIÓN. Ver las notas de clase. □

Ejercicio. 9.36.
Encuentra un número entero cuyo resto al dividirlo entre 5 sea 3 y que al multiplicarlo por 3 y dividirlo entre 4 dé resto 1.

SOLUCIÓN. Llamamos X a este número entero, entonces verifica: $X \equiv 3 \pmod{5}$ por la condición "*el resto al dividirlo entre 5 es 3z* se verifica: $3X \equiv 1 \pmod{4}$ por la condición "*al multiplicarlo por 3 y dividirlo entre 4 da de resto 1*"Tenemos pues que resolver el sistema de congruencias:

$$\left.\begin{array}{l} X \equiv 3 \pmod{5} \\ 3X \equiv 1 \pmod{4} \end{array}\right\}$$

que es equivalente a este otro:

$$\left.\begin{array}{l} X \equiv 3 \pmod{5} \\ X \equiv 3 \pmod{4} \end{array}\right\}$$

Una solución es $X = 3$, y el resto de las soluciones son de la forma $3 + 20\lambda$. □

Ejercicio. 9.37.
Un cocinero de un barco pirata relató cómo había conseguido las dieciocho monedas de oro que llevaba: Quince piratas atacaron un barco francés. Consiguieron un cofre lleno de monedas de oro. Las repartieron en partes iguales y me dieron las cinco que sobraban. Sin embargo, tras una tormenta murieron dos de ellos, por lo que los piratas juntaron todas sus monedas y las volvieron a repartir. A mí me dieron las diez que sobraban. Por último, tras una epidemia de peste murieron cinco de los piratas que aún quedaban en pie, por lo que los supervivientes repitieron la misma operación.

Sabiendo que en el cofre no caben más de dos mil quinientas monedas, ¿cuántas monedas contenía el cofre?

SOLUCIÓN. Está claro que el grupo de facinerosos le dio las 18 monedas en tres momentos distintos, siendo las cantidades 5, 10 y 3 respectivamente. Si llamamos X a la cantidad de monedas que había en el cofre, se verifican las siguientes relaciones:

(1) $X \equiv 5 \mod 15$, ya que al repartir entre dieciocho sobraron cinco monedas.

(2) $X - 5 \equiv 10 \pmod{13}$, ya que desaparecieron dos piratas y el cocinero tenía cinco monedas en su bolsillo que evidentemente no compartía con los facinerosos.

(3) $X - 15 \equiv 3 \mod 8$, ya que desaparecieron cinco piratas más y el cocinero ya tenía en su poder quince monedas.

Si escribimos estas ecuaciones en un sistema tenemos:

$$\left.\begin{array}{l} X \equiv 5 \mod 15 \\ X - 5 \equiv 10 \pmod{13} \\ X - 15 \equiv 3 \mod 8 \end{array}\right\}$$

que podemos escribir como:

$$\left.\begin{array}{l} X \equiv 5 \mod 15 \\ X \equiv 2 \pmod{13} \\ X \equiv 2 \mod 8 \end{array}\right\}$$

La solución de las dos últimas ecuaciones es: $X \equiv 2 \pmod{104}$, entonces tenemos que resolver el sistema

$$\left.\begin{array}{l} X \equiv 5 \mod 15 \\ X \equiv 2 \pmod{104} \end{array}\right\}$$

La identidad de Bezout para 15 y 104 es: $1 = 7 \times 15 - 104$, entonces una solución es: $5 \times (-104) + 2 \times 7 \times 15 \equiv -310 \equiv 1250 \pmod{1560}$.

El número de monedas del cofre era: 1250. □

Ejercicio. 9.38.
Resuelve la ecuación en congruencias

$$x^2 - 3x + 3 \equiv 0 \pmod{7}$$

SOLUCIÓN. Damos a x todos los valores posibles:

x	$x^2 - 3x + 3 \equiv 0 \pmod{7}$
0	3
1	1
2	1
3	3
4	0
5	6
6	0

Por tanto las raíces son: $x = 4$ y $x = 6$. □

Ejercicio. 9.39.
Resuelve el sistema de ecuaciones en congruencias

$$\left.\begin{array}{r} 5x-7y\equiv 9 \pmod{12} \\ 2x+3y\equiv 10 \pmod{12} \end{array}\right\}$$

SOLUCIÓN. Planteamos el sistema y hacemos las transformaciones necesarias para reducirlo:

$$\left.\begin{array}{r} 5x-7y\equiv 9 \pmod{12} \\ 2x+3y\equiv 10 \pmod{12} \end{array}\right\} \qquad \left.\begin{array}{l} x-5\times 7y\equiv 5\times 9 \pmod{12} \\ 2x+3y\equiv 10 \pmod{12} \end{array}\right\}$$

$$\left.\begin{array}{l} x+y\equiv 9 \pmod{12} \\ 2x+3y\equiv 10 \pmod{12} \end{array}\right\} \qquad 2(9-y)+3y\equiv 10 \pmod{12}\}$$

$$6-2y+3y\equiv 10 \pmod{12}\} \qquad y\equiv 4 \pmod{12}\}$$

Entonces $x\equiv 9-y\equiv 9-4\equiv 5 \pmod{12}$. □

Ejercicio. 9.40.
Calcula todas las soluciones en $\mathbb{Z}$ de la ecuación

$$35x+45y+55z=60.$$

SOLUCIÓN. Es claro que podemos dividir todos los coeficientes por 5 y obtener una ecuación que tiene las mismas soluciones que la original, así que nuestra ecuación de partida va a ser $7x+9y+11z=12$.

Suponemos que $11z$ es un valor constante, entonces podemos considerar la ecuación en las indeterminadas x e y siguiente: $7x+9y = 12-11z$. Esta ecuación la sabemos resolver; si consideramos la identidad de Bezout de 7 y 9: $1=4\times 7-3\times 9$, entonces se verifica:

$$(12-11z)4\times 7-(12-11z)3\times 9=12-11z,$$

y por tanto una solución es: $x=(12-11z)4=48-44z$ e $y=-(12-11z)3=-36+33z$. Para obtener el resto de las soluciones tenemos que utilizar un nuevo parámetro t, así que éstas serán:

$$x=48-44z-9t \quad \text{e} \quad y=-36+33z+7t.$$

Observar que entonces las soluciones de la ecuación original dependen de dos parámetros, y que éstas son:

$$x=48-44s-9t, \qquad y=-36+33s+7t \quad \text{y} \quad z=s.$$

□

Ejercicio. 9.41.
Calcula las soluciones en $\mathbb{Z}$ de la ecuación

$$6x + 9y + 15z = 7.$$

SOLUCIÓN. No tiene solución ya que el miembro de la izquierda es siempre múltiplo de 3 y el de la derecha es siempre 7 que no es múltiplo de 3. □

Ejercicio. 9.42.
Calcula las soluciones en $\mathbb{Z}$ de la ecuación

$$6x + 10y + 15z = 7.$$

SOLUCIÓN. La ecuación $6x + 10y + 15z = 7$ la podemos escribir como $6x + 10y = 7 - 15$. Observar que el miembro de la derecha es siempre par, y que para que el miembro de la izquierda sea par es necesario y suficiente que z sea impar. Suponemos entonces que $z = 2h + 1$ para $h \in \mathbb{Z}$, entonces la ecuación se escribe:

$$6x + 10y = 7 - 15(2h + 1) = -2(15h + 4).$$

la identidad de Bezout para 6 y 10 es: $2 = 2 \times 6 - 10$, entonces una solución de la ecuación se puede obtener de la igualdad:

$$-2(15h + 4) = -(15h + 4)2 \times 6 + (15h + 4)10,$$

esto es, una solución de la ecuación en x e y es: $x = -(15h + 4)2 = -30h - 8$ e $y = 15h + 4$. El resto de las soluciones de esta ecuación en x e y son: $x = -30h - 8 - 9t$ e $y = 15h + 4 + 6t$.

Si introducimos ahora el valor de z resulta que tenemos todas las soluciones de la ecuación original:

$$x = -30h - 8 - 9t, \qquad y = 15h + 4 + 6t, \quad \text{y} \quad z = 2h + 1.$$

□

Capítulo III

El anillo de polinomios

10. Introducción

Ejercicio. 10.1.
Demuestra que los ideales del anillo $\mathbb{Z}$ son todos del tipo $n\mathbb{Z} = \{nx \mid x \in \mathbb{Z}\}$, para $n \in \mathbb{Z}$ entero no negativo.

SOLUCIÓN. Es claro que para cada $n \in \mathbb{Z}$ se verifica $n\mathbb{Z} = (-n)\mathbb{Z}$ es un ideal de $\mathbb{Z}$.

Recíprocamente, sea $I \subseteq \mathbb{Z}$ un ideal. Si $I \cap \mathbb{N} = \{0\}$, entonces $I = \{0\} = 0\mathbb{Z}$. Si $I \cap \mathbb{N} \neq \{0\}$, sea $n \in (I \cap \mathbb{N}) \setminus \{0\}$ mínimo, entonces $n\mathbb{Z} \subseteq I$, y si $s \in I$, al dividir s por n sea $s = nq + r$, se tiene $r = s - nq \in I$, y por la minimalidad de n se tiene $r = 0$. En consecuencia cada elemento $s \in I$ se escribe como nq, esto es, $I \subseteq n\mathbb{Z}$. □

Ejercicio. 10.2.
Demuestre que $\mathbb{Z}$ es el único subanillo de $\mathbb{Z}$.

SOLUCIÓN. Es fácil; como cada subanillo ha de contener al 1, resulta que debe contener a todo elemento de $\mathbb{Z}$. □

Ejercicio. 10.3.
Dado $n \in \mathbb{N} \setminus \{0, 1\}$, el anillo $\mathbb{Z}_n = \mathbb{Z}/n\mathbb{Z}$ tiene exactamente n elementos, cada uno de los

cuales tiene un único representante x verificando $0 \leq x < n$.

SOLUCIÓN. Dado un elemento $[a]$ de $\mathbb{Z}_n$, si se divide a por n, sea por ejemplo $a = nq + r$, entonces $[a] = [r]$, y por tanto cada elemento de $\mathbb{Z}_n$ tiene un representante x tal que $0 \leq x < n$. Si $[x_1] = [x_2]$ y $0 \leq x_1, x_2 < n$, entonces $x_1 - x_2$ es un múltiplo de n. Se tiene $0 \leq x_2 < n$, luego $-n < -x_2 \leq 0$ y sumando con $0 \leq x_1 < n$ se tiene $-n < x_1 - x_2 < n$. Pero el único múltiplo de n que verifica esta condición es 0. Entonces $x_1 - x_2 = 0$ y resulta $x_1 = x_2$. □

Ejercicio. 10.4.
En el anillo $\mathbb{Z}_8$ determina los elementos que tienen inverso, comprueba que son aquellos que tienen un representante primo relativo con 8, y los que son divisores de cero, comprueba que son aquellos que no son primos relativos con 8.

Utilizando la identidad de Bezout para números enteros generaliza este resultado al anillo $\mathbb{Z}_n$, $n \in \mathbb{N} \setminus \{0, 1\}$.

SOLUCIÓN. Los elementos que tienen inverso son: $1, 3, 5, 7$. Cada uno es inverso de sí mismo.

Los divisores de cero son: 0, 2, 4, 6.

Dado $[a] \in \mathbb{Z}_n$, consideramos la identidad de Bezout para a y n, sea: $d = a\alpha + n\beta$. Si $d = 1$, al tomar clases se tiene:

$$[1] = [a\alpha + n\beta] = [a][\alpha] + 0 = [a][\alpha],$$

luego $[a]$ tiene inverso. Recíprocamente, si $[a]$ tiene inverso, existe $[b]$ tal que $[a][b] = [1]$, y por tanto $1 - ab$ es u múltiplo de n, sea $1 - ab = n\lambda$. Se tiene: $1 = ab + n\lambda$, y por tanto a y n son primos relativos ya que en este caso d divide a 1.

Hemos probado que un elemento $[a]$ tiene inverso si y solo si a y n con primos relativos.

Si $[a]$ no tiene inverso, entonces a y n no son primos relativos, luego $d \neq 1$. Se verifica $a = d\lambda_1$ y $n = d\lambda_2$ para λ_1, $\lambda_2 \in \mathbb{Z}$. Entonces se verifica: $[a][\lambda_2] = [d\lambda_1\lambda_2] = [n\lambda_1] = 0$, y además $[\lambda_2] \neq 0$, ya que λ_2 es un divisor propio de n. □

11. Anillos de polinomios

Ejercicio. 11.1.
Tomamos $A = \mathbb{Z}_6$ y $p(X) = X^2 + 5X$, tenemos $p(X) = (X+3)(X+2) = X(X+5)$, entonces raíces de $p(X)$ son 0, 1, 2 y 3, sin embargo $X(X+5)(X+3)(X+2)$ no divide a $p(X)$.

SOLUCIÓN. Es inmediato. □

Ejercicio. 11.2.
Se considera el polinomio $p(X) = X^4 + X^3 - X^2 - 4X - 1 \in \mathbb{Z}[X]$. Si llamamos $Y = X - 1$, escribir el polinomio $p(X)$ en función de la indeterminada Y.

SOLUCIÓN. Hacemos el desarrollo de Taylor para $a = 1$ y obtenemos:

$$\begin{aligned} p(X) &= \sum_{i=0}^{4} \frac{D^i p(a)}{i!}(X-a)^i \\ &= p(1) + \frac{Dp(1)}{1}(X-1) + \frac{D^2p(1)}{2!}(X-1)^2 + \frac{D^3p(1)}{3!}(X-1)^3 + \frac{D^4p(1)}{4!}(X-1)^4 \\ &= -4 + \frac{1}{1}(X-1) + \frac{16}{2}(X-1)^2 + \frac{30}{6}(X-1)^3 + \frac{24}{24}(X-1)^4 \end{aligned}$$

Tenemos entonces que $p(X) =$ es igual a $q(Y) = 24Y^4 + 5Y^3 + 8Y^2 + Y - 4$. □

Ejercicio. 11.3.
Sea $\mathbb{Z}[\sqrt{2}] = \{a + b\sqrt{2} \mid a, b \in \mathbb{Z}\}$. Demuestra que $\mathbb{Z}[\sqrt{2}]$ es un dominio de integridad y que $1 + \sqrt{2}$ es una unidad en $\mathbb{Z}[\sqrt{2}]$.

SOLUCIÓN. Para ver que es un dominio basta ver cuando al multiplicar dos elementos el resultado es cero:

$$(a + b\sqrt{2})(c + d\sqrt{2}) = (ac + 2bd) + (ad + bc)\sqrt{2}$$

Si multiplicamos ahora por $c - d\sqrt{2}$, entonces tenemos:

$$\begin{aligned} (a + b\sqrt{2})(c + d\sqrt{2})(c - d\sqrt{2}) &= (a + b\sqrt{2})[(c^2 - 2d^2) + (cd - dc)\sqrt{2}] \\ &= (a + b\sqrt{2})[c^2 - 2d^2]. \end{aligned}$$

Como $c^2 - 2d^2 \neq 0$ si $c + d\sqrt{2} \neq 0$, entonces si $a + b\sqrt{2}$ y $c + d\sqrt{2}$ son no nulos, también su producto lo es.
Para ver que $1 + \sqrt{2}$ es una unidad (=invertible), supongamos que $x + y\sqrt{2}$ es su inverso, entonces se tiene:

$$(1 + \sqrt{2})(x + y\sqrt{2}) = (x + 2y) + (y + x)\sqrt{2} = 1,$$

luego $x + 2y = 1$ e $y + x = 0$. La única solución es $x = -1$, $y = 1$. Para comprobarlo hacemos el producto:

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

□

Ejercicio. 11.4.
Determina los divisores de cero y las unidades de $\mathbb{Z}_{12}$.

SOLUCIÓN. Los elementos de $\mathbb{Z}_{12}$ son: $\overline{0}$, $\overline{1}$, $\overline{2}$, $\overline{3}$, $\overline{4}$, $\overline{5}$, $\overline{6}$, $\overline{7}$, $\overline{8}$, $\overline{9}$, $\overline{10}$ y $\overline{11}$. Los divisores de cero son aquellos que tienen un representante que no es primo relativo con 12, en este caso:

$\overline{0}$, $\overline{2}$, $\overline{3}$, $\overline{4}$, $\overline{6}$, $\overline{8}$, $\overline{9}$ y $\overline{10}$.

y las unidades o elementos invertibles son aquellos que tienen un representante que es primo relativo con 12, en este caso:

$\overline{1}$, $\overline{5}$, $\overline{7}$ y $\overline{11}$. □

Ejercicio. 11.5.
Demuestra que todo dominio de integridad con un número finito de elementos es un cuerpo.

SOLUCIÓN. Si D es un dominio de integridad; el producto de dos elementos no nulos es siempre no nulo, y es finito, para cada elemento no nulo $a \in D$ consideramos la aplicación:

$$\lambda_a : D \longrightarrow D; \qquad \lambda : a(x) = ax$$

para cada $x \in D$. Vamos a comprobar que λ_a es una aplicación inyectiva. Si $\lambda_a(x) = \lambda_a(y)$, entonces $ax = ay$, y como D es un dominio de integridad y $a \neq 0$, resulta que $x = y$.

Si λ_a es inyectiva, como D es finito, resulta que también es sobreyectiva, luego una biyección. Entonces existe un elemento $b \in D$ tal que $\lambda_a(b) = 1$, esto es, $ab = 1$ y por tanto a es invertible. □

Ejercicio. 11.6.
Calcula $(2X^3 + 3X^2 + 1)(X^2 + 2X + 3)$ *en* $\mathbb{Z}_6[X]$.

SOLUCIÓN. Hacemos el desarrollo del producto y luego reducimos módulo 6, esto es,

$$\begin{aligned} &(2X^3 + 3X^2 + 1)(X^2 + 2X + 3) \\ =& 2X^5 + 4X^4 + 6X^3 + 3X^4 + 6X^3 + 9X^2 + x^2 + 2X + 3 \\ =& 2X^5 + 7X^4 + 12X^3 + 10X^2 + 2X + 3 \end{aligned}$$

Ahora reducimos módulo 6 cada uno de los coeficientes y obtenemos:

$$2X^5 + X^4 + 4X^2 + 2X + 3,$$

que es la solución. □

Ejercicio. 11.7.
Calcula el cociente y el resto de dividir $2X^4 + 3X^3 + X^2 + 6X + 1$ *entre* $3X^2 + 1$ *en* $\mathbb{Z}_7[X]$.

SOLUCIÓN. Por simplicidad escribimos a en vez de $\overline{a}$, siendo $0 \leq a < 7$.
Hacemos la división en $\mathbb{Z}_7$ en la forma usual. Para esto tenemos que saber que $3^{-1} = 5$

$$
\begin{array}{ll}
2X^4 + 3X^3 + X^2 + 6X + 1 & |\, 3X^2 + 1 \\
 & |- - - - - - - - - - - - - - \\
-(2X^4 + 3X^2) & 5 \times 2X^2 + 5 \times 3X + 5 \times 5 \\
- - - - - - - - - - - - - - & \\
3X^3 + 5X^2 + 6X + 1 & 3X^2 + X + 4 \\
-(3X^3 + X) & \\
- - - - - - - - - - - - - - & \\
5X^2 + 5X + 6X + 1 & \\
-(5X^2 + 4) & \\
- - - - - - - - - - - - - - & \\
5X + 4 &
\end{array}
$$

La división euclídea es:

$$2X^4 + 3X^3 + X^2 + 6X + 1 = (3X^2 + 1)(3X^2 + X + 4) + 5X + 4.$$

□

Ejercicio. 11.8.
Calcula un máximo común divisor de $a(X)$ y $b(X)$ en los siguientes casos:

(1) $a(X) = X^4 + 2X^2 + 1, b(X) = X^4 - 1$ *en* $\mathbb{Q}[X]$.

(2) $a(X) = X^4 + 2X^2 + 1, b(X) = X^2 + 2$ *en* $\mathbb{Z}_3[X]$.

SOLUCIÓN.

(1) La divisiones euclídeas son:

$$
\begin{array}{l}
X^4 + 2X^2 + 1 = (X^4 - 1) \times 1 + 2(X^2 + 1); \\
X^4 - 1 = (X^2 + 1)(X - 1).
\end{array}
$$

Luego $\mathrm{m.c.d.}\{a(X), b(X)\} = X^2 + 1$, el último resto no nulo.

(2) Es igual.

□

Ejercicio. 11.9.
Demuestra que que la ecuación

$$(X^4 + 2X^2 + 1)\mathcal{X} + (X^4 - 1)\mathcal{Y} = 3X^3 + 3X$$

tiene solución en $\mathbb{Q}[X]$, y halla una solución.

SOLUCIÓN. Tenemos:

$$\begin{array}{l}(X^4+2X^2+1)\mathcal{X}+(X^4-1)\mathcal{Y}=3X^3+3X\\(X^2+1)^2\mathcal{X}+(X^2+1)(X^2-1)\mathcal{Y}=3X(X^2+1)\end{array}$$

y simplificando por X^2+1 tenemos:

$$(X^2+1)\mathcal{X}+(X^2-1)\mathcal{Y}=3X$$

La identidad de Bezout es: $(X^2+1)\frac{1}{2}-(X^2-1)\frac{1}{2}=1$, luego una solución se obtiene de la igualdad:

$$(X^2+1)\frac{3X}{2}-(X^2-1)\frac{3X}{2}=3X,$$

esto es, $\mathcal{X}=\frac{3X}{2}$ y $\mathcal{Y}=-\frac{3X}{2}$.

Para calcular la solución general, sea α, β otra solución.

Entonces se verifica:

$$(X^2+1)\left(\alpha-\tfrac{3X}{2}\right)+(X^2-1)\left(\beta+\tfrac{3X}{2}\right)=0,$$

$$(X^2+1)\left(\alpha-\tfrac{3X}{2}\right)=-(X^2-1)\left(\beta+\tfrac{3X}{2}\right)=0,$$

$$\frac{\alpha-\frac{3X}{2}}{X^2-1}=-\frac{\beta+\frac{3X}{2}}{X^2+1}=:p(X),$$

$$\alpha=\tfrac{3X}{2}+p(X)(X^2-1);$$

$$\beta=-\tfrac{3X}{2}-p(X)(X^2+1).$$

que es la solución general. □

12. Raíces de polinomios

Ejercicio. 12.1.
Considerar el polinomio $p(X) = X^5 + 1 \in \mathbb{Z}_5[X]$, probar que tiene una raíz de multiplicidad cinco pero que su derivada es igual a cero.

SOLUCIÓN. Es claro que $p(X) = (X+1)^5$, luego -1 es una raíz de multiplicidad cinco de $p(X)$. Sin embargo $Dp(X) = 0$, y el Teorema no es aplicable. □

Ejercicio. 12.2.
Calcula las raíces en $\mathbb{Z}_5$ del polinomio $X^2 + X + 4$.

SOLUCIÓN. Basta probar con cada uno de los elementos de $\mathbb{Z}_5$. Si llamamos $p(X) = X^2+X+4$, tenemos:

x;	$p(x)$
0;	$p(0) = 4 \neq 0$;
1;	$p(1) = 1 \neq 0$;
2;	$p(2) = 0$;
3;	$p(3) = 1$;
4;	$p(4) = 4 \neq 0$.

Entonces una raíz es $x = 2$; en este caso el polinomio $p(X)$ se escribe:

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

Luego las dos raíces son: $x = 2$ y $x = 2$, una raíz doble. □

Ejercicio. 12.3.
Calcula las raíces en $\mathbb{Z}$ del polinomio $X^4 - X^3 + X^2 - X - 10$.

SOLUCIÓN. Las posibles raíces son los divisores en $\mathbb{Z}$ de 10, esto es: 1, 2, 5, 10 y -1, -2, -5 y -10. Basta probar a ver si alguna de ellas es una raíz. Si llamamos $p(X) = X^4 - X^3 + X^2 - X - 10$, tenemos:

x;	$p(x)$
1;	$p(1) = -10 \neq 0$;
2;	$p(2) = 0$;
5;	$p(5) = 510 \neq 0$;
10;	$p(10) = 9080 \neq 0$;
-1;	$p(-1) = -6 \neq 0$;
-2;	$p(-2) = 20 \neq 0$;
-5;	$p(-5) = 770 \neq 0$;
-10;	$p(-10) = 11100 \neq 0$;

Una raíz es: $x = 2$. Esta raíz proporciona la factorización: $p(X) = (X-2)(X^3 + X^2 + 3X + 5)$, y el polinomio $X^3 + X^2 + 3X + 5$, que no tiene raíces en $\mathbb{Z}$, luego es irreducible. □

Ejercicio. 12.4.
Calcula en $\mathbb{Q}[X]$ *el resto de dividir*

(1) $X^7 + X^2 + 1$ *entre* $X - 1$,

(2) $X^n + 1$ *entre* $X - 1$.

SOLUCIÓN.

(1) El resto es: 3.

(2) El resto es: 2.

□

Ejercicio. 12.5.
Calcula en $\mathbb{Z}_5[X]$ *el resto de dividir* $X^n + 2$ *entre* $X + 4$.

SOLUCIÓN. Como 4 es igual a -1 en $\mathbb{Z}_5$, tenemos que el resto es igual a 3. □

Ejercicio. 12.6.
Demuestra que el polinomio $X^n + 1$ *no tiene raíces múltiples en* $\mathbb{R}$.

SOLUCIÓN. Para que tenga raíces múltiples, el polinomio y su derivada deben de tener una raíz común, si esta raíz es α, resulta que $X - \alpha$ divide a $X_n - 1$ y a nX^{n-1}, que es su derivada. Pero la única raíz del último polinomio es 0, que no es raíz de $X^n - 1$. Luego el polinomio no tiene raíces múltiples. □

Ejercicio. 12.7.
Determina cuáles de los siguientes polinomios tienen raíces múltiples en $\mathbb{C}$.

(1) $X^3 - 3X^2 + 3X - 1$,

(2) $X^3 + X^2 + 1$,

(3) $X^4 + X^3 + X^2 + X + 1$.

SOLUCIÓN.

(1) Llamamos $p(X) = X^3 - 3X^2 + 3X - 1$, su derivada es: $p'(X) = 3X^2 - 6X + 3$. Se tiene las factorizaciones: $p(X) = X^3 - 3X^2 + 3X - 1 = (X-1)(X^2 - 2X + 1)$ y $p'(X) = 3(X^2 - 2X + 1)$, resulta que $\mathrm{m.\,c.\,d.}\{p(X), p'(X)\} = X^2 - 2X + 1$, entonces cualquier raíz de $X^2 - 2X + 1$ es doble de $X^3 - 3X^2 + 3X - 1$. La única raíz de $X^2 - 2X + 1$ es $X = -1$, que es una raíz doble, luego $X = -1$ es una raíz triple de $X^3 - 3X^2 + 3X - 1$.

(2) Llamamos $p(X) = X^3 + X^2 + 1$, su derivada es: $p'(X) = 3X^2 + 2X$, y las raíces de $p'(X) = 3X(X + \frac{2}{3})$ son: $X = 0$, $X = -\frac{2}{3}$. Como ninguna es raíz de $p(X)$, resulta que $p(X)$ no tiene raíces múltiples.

(3) Llamamos $p(X) = X^4 + X^3 + X^2 + X + 1$, su derivada es: $p'(X) = 4X^3 + 3X^2 + 2X + 1$. Para ver si tiene raíces comunes con $p(X)$, calculamos el máximo común divisor de $p(X)$ y $p'(X)$.

$$\begin{aligned} & X^4 + X^3 + X^2 + X + 1 \\ = & (4X^3 + 3X^2 + 2X + 1)(\tfrac{1}{16} + \tfrac{X}{4}) + \tfrac{5X^2}{16} + \tfrac{5X}{8} + \tfrac{15}{16}; \\ & \\ & 4X^3 + 3X^2 + 2X + 1 \\ = & (\tfrac{5X^2}{16} + \tfrac{5X}{8} + \tfrac{15}{16})(-16 - \tfrac{64X}{5}) + 16. \end{aligned}$$

entonces $p(X)$ y $p'(X)$ no tienen raíces comunes, ya que son primos relativos, pues su máximo común divisor es 1. Por tanto $p(X)$ no tiene raíces múltiples.

□

Ejercicio. 12.8.
(*) Encuentra todas las raíces de $X^2 - 1$ en $\mathbb{Z}_8[X]$.

SOLUCIÓN. El mejor método es evaluar $X^2 - 1$ en todos los elementos de $\mathbb{Z}_8$:

x;	$p(x)$
0;	$p(0) = 7 \neq 0$;
1;	$p(1) = 0$;
2;	$p(2) = 3 \neq 0$;
3;	$p(3) = 0 \neq 0$;
4;	$p(4) = 7 \neq 0$;
5;	$p(5) = 0 \neq 0$;
6;	$p(6) = 3 \neq 0$;
7;	$p(7) = 0 \neq 0$;

entonces las raíces son: $X = 1, 3, 5, 7$. Observar que tiene cuatro raíces, y que se verifica la igualdad:

$$X^2 - 1 = (X - 1)(X - 7) = (X - 3)(X - 5).$$

□

Ejercicio. 12.9.
Calcula un polinomio $a(X)$ en $\mathbb{Q}[X]$ tal que $a(2) = 0$, $a(1) = -2$, $a(3) = 1$ y $a(-1) = 2$.

SOLUCIÓN. Basta aplicar la fórmula de interpolación de Lagrange:

$$\begin{aligned}
&a(X)\\
= \quad & \tfrac{(X-1)(X-3)(X+1)}{(2-1)(2-3)(2+1)}0 + \tfrac{(X-2)(X-3)(X+1)}{(1-2)(1-3)(1+1)}(-2) + \tfrac{(X-2)(X-1)(X+1)}{(3-2)(3-1)(3+1)}\\
& + \tfrac{(X-2)(X-1)(X-3)}{(-1-2)(-1-1)(-1-3)}\\
= \quad & \tfrac{(X^2-5X+6)(X+1)}{4}(-2) + \tfrac{(X-2)(X^2-1)}{(1)(2)(4)} + \tfrac{(X^2-5X+6)(X-1)}{(-3)(-2)(-4)}2\\
= \quad & -\tfrac{X^3-4X^2+X+6}{2} + \tfrac{X^3-2X^2-X+2}{8} + \tfrac{X^3-6X^2+11X-6}{-12}\\
= \quad & -(\tfrac{11X^3}{24} + \tfrac{9X^2}{4} + \tfrac{37X}{12} + \tfrac{9}{4})
\end{aligned}$$

□

Ejercicio. 12.10.
Calcula un polinomio $a(X)$ en $\mathbb{Z}_5[X]$ tal que $a(2) = 1$, $a(3) = 2$ y $a(4) = 1$.

SOLUCIÓN. Podemos hacerlo calculando un polinomio $p(X)$ en $\mathbb{Q}[X]$ tal que $p(2) = 1$, $p(3) = 2$ y $p(4) = 1$

El polinomio $p(X)$ es:

$$\begin{aligned}
p(X) &= \tfrac{(X-3)(X-4)}{(2-3)(2-4)} + \tfrac{(X-2)(X-4)}{(3-2)(3-4)}2 + \tfrac{(X-2)(X-3)}{(4-2)(4-3)}\\
&= \tfrac{X^2-7X+12}{2} + \tfrac{X^2-6X+8}{-1}2 + \tfrac{X^2-5X+6}{2}\\
&= -X^2 + 6X - 7.
\end{aligned}$$

Como $p(X)$ es un polinomio con coeficientes en $\mathbb{Z}$, podemos reducirlo módulo 5 y obtenemos el polinomio $a(X) = -X^2 + 6X - 7 = 4X^2 + X + 3$. Este polinomio satisface las condiciones que aparecen en el enunciado. □

Ejercicio. 12.11.
(*) Comprueba que los polinomios $X^3 + X^2 + X + 1$ y $X^2 + 2X + 1$ determinan la misma aplicación $f : \mathbb{Z}_3 \longrightarrow \mathbb{Z}_3$.

SOLUCIÓN. Vamos a calcular cual es la imagen de cada elemento de $\mathbb{Z}_3$ por cada uno de los polinomios. Llamamos $p(X) = X^3 + X^2 + X + 1$ y $q(X) = X^2 + 2X + 1$.

x	$p(x)$	$q(x)$
0	1	1
1	1	1
2	0	0

□

13. Polinomios con coeficientes en $\mathbb{Z}$

Ejercicio. 13.1.
Calcula todos los polinomios irreducibles de grado dos en $\mathbb{Z}_2[X]$

SOLUCIÓN. Un polinomio de grado dos en $\mathbb{Z}_2$ se escribe en la forma $aX^2 + bX + c$ con el coeficiente líder a no nulo. Podemos suponer que a es igual a 1. Entonces los polinomios, con sus posibles descomposiciones son:

Polinomio	Descomposición
X^2	$X\,X$
X^2+1	$(X+1)(X+1)$
X^2+X	$X(X+1)$
X^2+X+1	irreducible.

□

Ejercicio. 13.2.
Demuestra que el polinomio $X^4 + X + 1$ es irreducible en $\mathbb{Z}_2[X]$.

SOLUCIÓN. Es claro que no tiene raíces en $\mathbb{Z}_2$. Además, el único polinomio irreducible de grado dos en $\mathbb{Z}_2[X]$ es $X^2 + X + 1$ y éste no es un factor, luego tenemos el resultado. □

Ejercicio. 13.3.
Demuestra que los polinomios $X^2 + 1$, $X^3 + X + 1$ y $X^4 + 2$ son irreducibles en $\mathbb{Z}[X]$

SOLUCIÓN. $X^2 + 1$ no tiene raíces, luego es irreducible.
$X^3 + X + 1$ no tiene raíces, luego es irreducible.
$X^4 + 2$ no tiene raíces, pero esto no nos asegura que sea irreducible, pues podría ser un producto de dos polinomios irreducibles de grado dos. Las raíces en $\mathbb{C}$ son: $\sqrt[4]{2}$, $i\sqrt[4]{2}$, $-\sqrt[4]{2}$ y $-i\sqrt[4]{2}$. Como consecuencia en $\mathbb{C}$ el polinomio se escribe:

$$X^4 + 2 = (X - \sqrt[4]{2})(X - i\sqrt[4]{2})(X + \sqrt[4]{2})(X + i\sqrt[4]{2}).$$

Por lo tanto un factor de grado dos será el producto de dos de estos polinomios de grado uno, pero como ninguno de ellos pertenece a $\mathbb{Z}[X]$, tenemos que es irreducible.

$$\begin{aligned}
&(X - \sqrt[4]{2})(X - i\sqrt[4]{2}) = X^2 - (\sqrt[4]{2} + i\sqrt[4]{2})X + i\sqrt{2},\\
&(X - \sqrt[4]{2})(X + \sqrt[4]{2}) = X^2 - \sqrt{2},\\
&(X - \sqrt[4]{2})(X + i\sqrt[4]{2}) = X^2 - (\sqrt[4]{2} - i\sqrt[4]{2})X - i\sqrt{2}.
\end{aligned}$$

Otro método es aplicar el criterio de Eisenstein para el número primo 2 y utilizar que el polinomio es primitivo. □

14. Criterios de irreducibilidad de polinomios

Ejercicio. 14.1.
El polinomio $p(X) = X^3 + X^2 + 15$ *es irreducible en* $\mathbb{Z}[X]$.

SOLUCIÓN. Consideramos la proyección canónica $\mathbb{Z} \to \mathbb{Z}_2$ y el homomorfismo inducido entre los anillos de polinomios $f : \mathbb{Z}[X] \to \mathbb{Z}_2[X]$. Entonces $f(p(X)) = X^3 + X^2 + 1$, ya que $f(p(X))$ es irreducible en $\mathbb{Z}_2[X]$, resulta que $p(X)$ no puede descomponerse en $\mathbb{Z}[X]$. □

Ejercicio. 14.2.
El polinomio $p(X) = X^4 + 2X^3 + 7X^2 - 4X + 5$ *es irreducible en* $\mathbb{Z}[X]$.

SOLUCIÓN. Consideramos la proyección canónica $\mathbb{Z} \to \mathbb{Z}_2$ y el homomorfismo inducido entre los anillos de polinomios $f : \mathbb{Z}[X] \to \mathbb{Z}_2[X]$. Entonces $f(p(X)) = X^4 + X^2 + 1$, que admite la descomposición $(X^2 + X + 1)^2$, luego no es irreducible en $\mathbb{Z}_2[X]$. Consideramos la proyección canónica $\mathbb{Z} \to \mathbb{Z}_3$ y el homomorfismo inducido entre los anillos de polinomios $g : \mathbb{Z}[X] \to \mathbb{Z}_3[X]$. Entonces $g(p(X)) = X^4 + 2X^3 + X^2 + 2X + 2$, que admite la descomposición $(X + 1)(X^3 + X^2 + 2)$, luego no es irreducible en $\mathbb{Z}_3[X]$. Uniendo los dos resultados obtenidos tenemos que $p(X)$ es irreducible en $\mathbb{Z}[X]$. Ya que una posible descomposición en irreducibles en $\mathbb{Z}[X]$ induce una descomposición en $\mathbb{Z}_2[X]$, con lo cual la descomposición en $\mathbb{Z}[X]$ sería en producto de dos polinomios de grado dos. Y esa misma descomposición induce en $\mathbb{Z}_3[X]$ una descomposición en producto de polinomios de grado como máximo dos, lo que es una contradicción con la descomposición que hemos hallado en $\mathbb{Z}_3[X]$ como un producto de un polinomio de grado uno y un polinomio de grado tres. □

Ejercicio. 14.3.
Probar, utilizando el criterio de Eisenstein, que el polinomio $X^4 + 2X^3 + 2X^2 + 2X + 2$ *es irreducible.*

SOLUCIÓN. Es inmediato. □

Ejercicio. 14.4.
Estudiar si es reducible en $\mathbb{Z}[X]$ *el polinomio* $p(X) = X^7 - 2X^6 + 3X^5 - 2X^3 + 6X^2 - 4X + 4$ *y, si lo es, encontrar una descomposición en irreducibles.*

SOLUCIÓN. Ya que el grado es siete, resulta que $s = 3$. Consideramos esta vez tres elementos de $\mathbb{Z}$: $a_0 = -1$, $a_1 = 0$, $a_2 = 1$.

Valoramos $p(X)$ en a_i obteniendo: $p(a_0) = 10$, $p(a_1) = 4$, $p(a_2) = 6$.

Consideremos los divisores $d_0 = 2$, $d_1 = 1$, $d_2 = 2$.

Construimos el polinomio de interpolación de Lagrange

$$q(X) = 2\frac{X(X-1)}{(-1-0)(-1-1)} + 1\frac{(X+1)(X-1)}{(0+1)(0-1)} + 2\frac{(X+1)X}{(1+1)(1-0)} = X^2 + 1.$$

Y resulta que $X^2 + 1$ es irreducible y es un divisor de $p(X)$:

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

Estudiamos ahora el polinomio $p_2(X) = X^5 - 2X^4 + 2X^3 + 2X^2 - 4X + 4$. Ya que su grado es cinco, resulta que $s = 2$. Consideramos tres elementos de $\mathbb{Z}$: $a_0 = -1$, $a_1 = 0$, $a_2 = 1$.

Valoramos $p_2(X)$ en a_i obteniendo: $p_2(a_0) = 5$, $p_2(a_1) = 4$, $p_2(a_2) = 3$.

Consideremos los divisores $d_0 = 5$, $d_1 = 2$, $d_2 = 1$.

Construimos el polinomio de interpolación de Lagrange

$$\begin{aligned} q(X) &= 5\frac{X(X-1)}{(-1-0)(-1-1)} + 2\frac{(X+1)(X-1)}{(0+1)(0-1)} + 1\frac{(X+1)X}{(1+1)(1-0)} = \\ &= \frac{5}{2}X(X-1) - 2(x^2-1) + \frac{1}{2}(X^2+X) = \\ &= \frac{1}{2}(2X^2 - 4X + 4) = X^2 - 2X + 2. \end{aligned}$$

Y resulta que $X^2 - 2X + 2$ es irreducible y es un divisor de $p_2(X)$:

$$p_2(X) = (X^2 - 2X + 2)(X^3 + 2).$$

Ya que el otro factor es irreducible, resulta que hemos obtenido una descomposición en irreducibles de $p(X)$ en la siguiente forma:

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

□

Capítulo IV

Conjuntos ordenados. Retículos

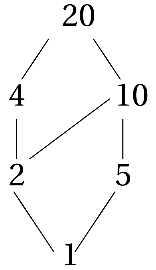
15. Relaciones de orden

Ejercicio. 15.1.
Dibuja el diagrama de Hasse de $(D(20), |)$.

(1) Dado $B = \{4, 10, 2\}$, *encuentra sus elementos notables.*

(2) Encuentra los elementos minimales de $C = D(20) \setminus \{1\}$. *(*$D(20) - \{1\}$*).*

SOLUCIÓN. Tenemos que $D(20)$ es el conjunto de todos los divisores de 20, esto es: $D(20) = \{1, 2, 4, 5, 10, 20\}$. El diagrama de Hasse de $D(20)$ es:



(1).
Dado $B = \{4, 10, 2\}$, tenemos:

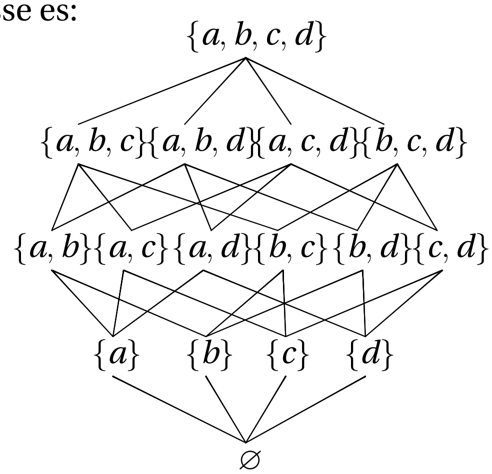
Elementos maximales: $\{4, 10\}$;
Máximo; no tiene;
Cotas superiores: $\{20\}$;
Supremo: 20.

Elementos minimales: $\{2\}$;
Mínimo: 2;
Cotas inferiores: $\{2, 1\}$;
Ínfimo: 2

(2). Los elementos minimales de $D(20) \setminus \{1\}$ son: $\{2, 5\}$. □

Ejercicio. 15.2.
Dibuja el diagrama de Hasse de $\mathcal{P}(\{a, b, c, d\})$. Encuentra los elementos minimales y maximales de $\mathcal{P}(\{a, b, c, d\}) \setminus \{\emptyset, \{a, b, c, d\}\}$.

SOLUCIÓN. El diagrama de Hasse es:



Los elementos minimales de $\mathcal{P}(\{a, b, c, d\}) \setminus \{\emptyset, \{a, b, c, d\}\}$ son: $\{a\}$, $\{b\}$, $\{c\}$ y $\{d\}$. Los elementos maximales son: $\{a, b, c\}$, $\{a, b, d\}$, $\{a, c, d\}$ y $\{b, c, d\}$. □

Ejercicio. 15.3.
Consideramos en $\mathbb{R}$ la siguiente relación binaria: $a \preceq_{lex} b$ si y sólo si $a \leq b$. Supuesto definido $\preceq_{lex}$ en $\mathbb{R}^{n-1}$, definimos $\preceq_{lex}$ en $\mathbb{R}^n$ de la siguiente forma: $(a_1, \ldots, a_n) \preceq_{lex} (b_1, \ldots, b_n)$ si y sólo si $a_1 < b_1$ ó ($a_1 = b_1$ y $(a_2, \ldots, a_n) \preceq_{lex} (b_2, \ldots, b_n)$).

*(1) Demuestra que para todo $n \in \mathbb{R}$, $(\mathbb{R}^n, \preceq_{lex})$ es un conjunto ordenado. A dicho orden se le denomina **orden!lexicográfico**.*

(2) Demuestra que si $(a_1, \ldots, a_n) \leq (b_1, \ldots, b_n)$ *(con el orden producto en* $\mathbb{R}^n$*), entonces también* $(a_1, \ldots, a_n) \preceq_{lex} (b_1, \ldots, b_n)$.

(3) Demuestra que $\preceq_{lex}$ *es un orden total.*

SOLUCIÓN.

(1) Es claro que verifica la propiedad reflexiva. Para comprobar la propiedad antisimétrica, sea $(a_1, \ldots, a_n) \preceq_{lex} (b_1, \ldots, b_n)$, entonces existe $i < n$ tal que $a_1 = b_1$, $\ldots$, $a_i = b_i$ y $a_{i+1} < b_{i+1}$ ó bien $a_j = b_j$ para todo $j = 1, \ldots, n$; en el segundo caso es claro que $(a_i)_i = (b_i)_i$; en el primer caso si además $(b_i)_i \preceq_{lex} (a_i)_i$, entonces se verifica también $b_{i+1} < a_{i+1}$, lo que es una contradicción. la propiedad transitiva se deja como trabajo al lector.

(2) Si $(a_i)_i \leq (b_i)_i$ con el orden producto, entonces $a_i \leq b_i$ para cada índice $i = 1, \ldots, n$; como consecuencia se tiene $(a_i)_i \preceq_{lex} (b_i)_i$.

(3) Dados dos elementos $(a_i)_i$, $(b_i)_i \in \mathbb{R}^n$, si no se verifica $(a_i)_i \not\preceq_{lex} (b_i)_i$, entonces para un cierto índice $i < n$ se verifica $a_1 = b_1, \ldots, a_i = b_i$ y $a_{i+1} > b_{i+1}$, por tanto $(b_i)_i \preceq_{lex} (a_i)_i$.

□

Ejercicio. 15.4.
Se define la relación binaria $\preceq_{tdeg}$ *en* $\mathbb{R}^n$ *de la siguiente forma:* $(a_1, \ldots, a_n) \preceq_{tdeg} (b_1, \ldots, b_n)$ *si y sólo si* $a_1 + \cdots + a_n < b_1 + \cdots + b_n$ *ó* ($a_1 + \cdots + a_n = b_1 + \cdots + b_n$ *y* $(a_1, \ldots, a_n) \preceq_{lex} (b_1, \ldots, b_n)$).

(1) Demuestra que para todo $n \in \mathbb{R}$, $(\mathbb{R}^n, \preceq_{tdeg})$ *es un conjunto ordenado. A dicho orden se le denomina* ***orden lexicográfico graduado****.*

(2) Demuestra que si $(a_1, \ldots, a_n) \leq (b_1, \ldots, b_n)$ *(con el orden producto en* $\mathbb{R}^n$*), entonces también* $(a_1, \ldots, a_n) \preceq_{tdeg} (b_1, \ldots, b_n)$.

(3) Demuestra que $\preceq_{tdeg}$ *es un orden total.*

SOLUCIÓN.

(1) La propiedad reflexiva se verifica. Para comprobar la propiedad antisimétrica, sean $(a_i)_i \preceq_{tdeg} (b_i)_i$ y $(b_i)_i \preceq_{tdeg} (a_i)_i$, entonces $\sum_i a_i < \sum_i b_i$ y $\sum_i b_i < \sum_i a_i$, lo que es una contradicción, ó $\sum_i a_i = \sum_i b_i$ y $(a_i)_i \preceq_{lex} (b_i)_i$ y $(b_i)_i \preceq_{lex} (a_i)_i$, lo que implica que $(a_i)_i = (b_i)_i$.

(2) Es inmediato.

(3) Es inmediato.

□

Ejercicio. 15.5.
Sea X un conjunto no vacío y $f : X \longrightarrow \mathbb{R}$ una aplicación. Definimos en X la siguiente relación binaria

$$x \leq_f y \text{ si y sólo si } f(x) \leq f(y).$$

(1) *¿Qué propiedad debe verificar f para que $\leq_f$ sea una relación de orden?*

(2) *En el caso particular de $X = \mathbb{R}^n$ y si $p_1, \ldots, p_n$ son los n primeros primos, demuestra que para la función*

$$f(a_1, \ldots, a_n) = p_1^{a_1} \times \cdots \times p_n^{a_n},$$

$\leq_f$ es un orden total.

SOLUCIÓN.

(1) Como $\leq_f$ tiene que verificar la propiedad antisimétrica, resulta que f tiene que ser inyectiva, pues si $x \neq y$ verifican $f(x) = f(y)$, entonces $x \leq_f y$ e $y \leq_f x$ y no se verifica la prop. antisimétrica. Esta condición que hemos visto que es necesaria es también suficiente.

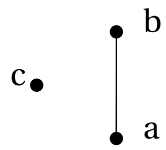
(2) Como la aplicación $f : \mathbb{R}^n \longrightarrow \mathbb{R}^n$ definida $f(a_1, \ldots, a_n) = p_1^{a_1} \times \cdots \times p_n^{a_n}$ es inyectiva, tenemos un orden parcial en $\mathbb{R}^n$. Para ver que es total, sean $(a_i)_i, (b_i)_i \in \mathbb{R}^n$, si $(a_i)_i \not\leq_f (b_i)_i)$ entonces $\prod_i p_i^{a_i} \not\leq \prod_i p_i^{b_i}$, y por tanto se verifica $\prod_i p_i^{b_i} \leq \prod_i p_i^{a_i}$, esto es, $(b_i)_i \leq_f (b_i)_i$.

□

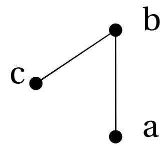
Ejercicio. 15.6.
Determinar todas las relaciones de orden que se pueden definir en el conjunto $X = \{a, b, c\}$ de manera que $a \leq b$.

SOLUCIÓN. Veamos las siguientes situaciones según el elemento c.

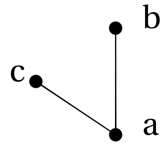
Caso 1. c no está relacionado con a ni con b.



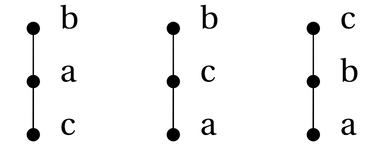
Caso 2. c no está relacionado con a pero sí con b.



Caso 3. c no está relacionado con b pero sí con a.



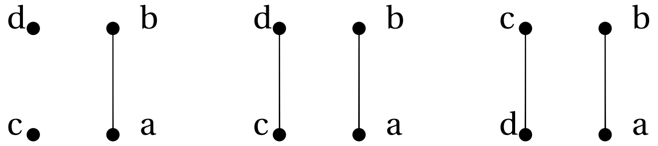
Caso 4. c está relacionado con a y b; tenemos tres posibilidades según las siguientes figuras.



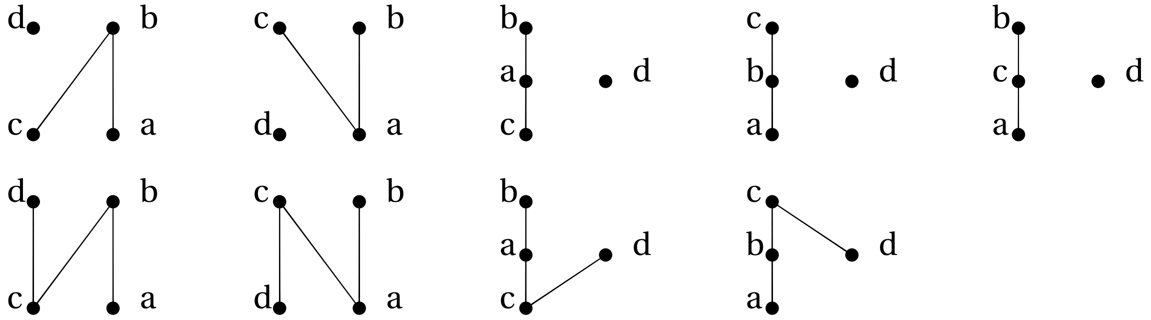
□

Ejercicio. 15.7.
Determinar todas las relaciones de orden que se pueden definir en el conjunto de cuatro elementos $X = \{a, b, c, d\}$ de manera que $a \leq b$.

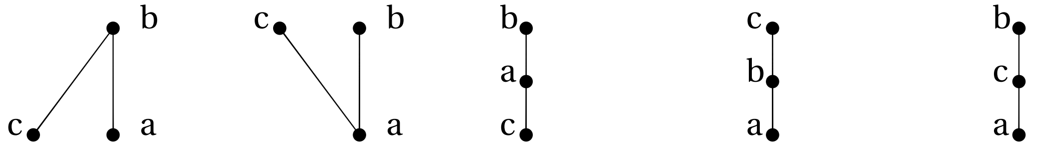
SOLUCIÓN. Si ninguno de los elementos c, d está relacionado con a ó b, tenemos tres posibles órdenes.



Si c está relacionado con a ó b y d no lo está tenemos nueve posibles órdenes, y otros cinco si suponemos que d está relacionado con a ó b y c no lo está.

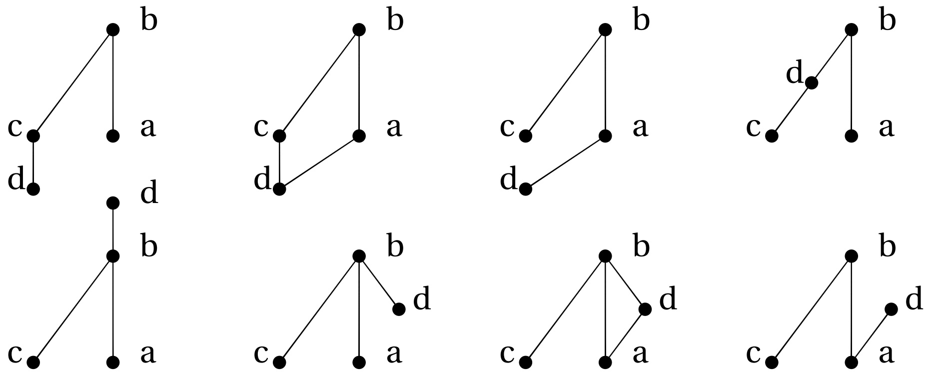


Si c y d están ambos relacionados con a ó b, tenemos, al considerar solo a, b y c, cinco posibles configuraciones:

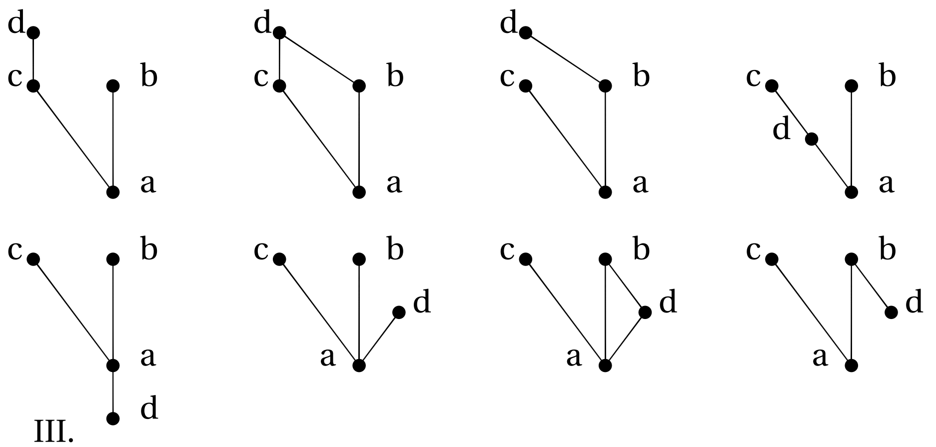


Para cada uno de éstas tenemos ocho posibles configuraciones:

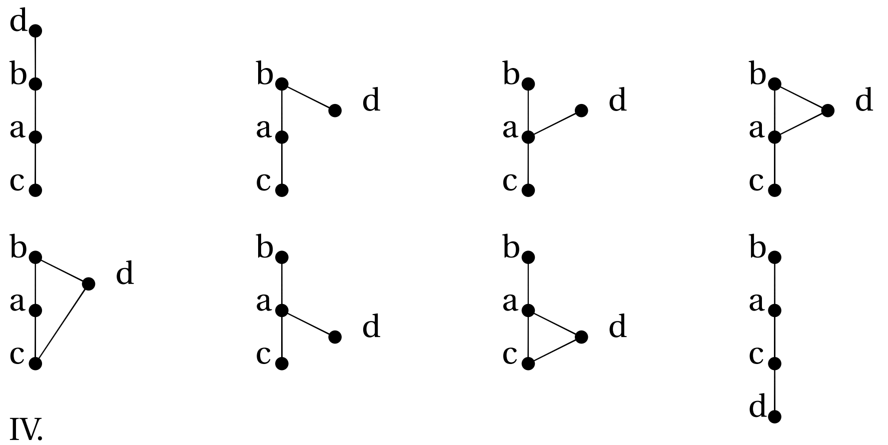
I.



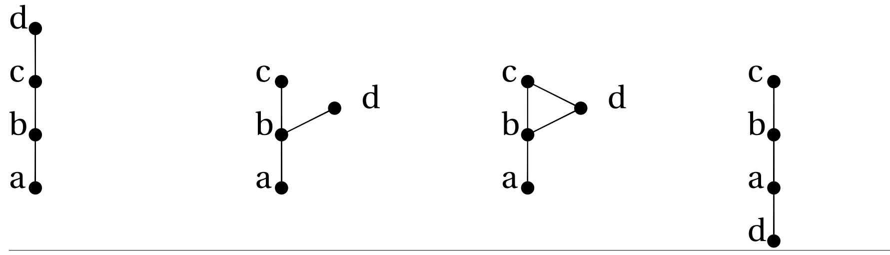
II.

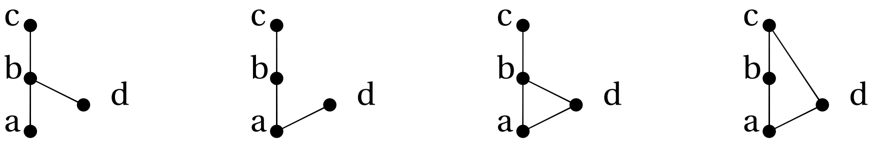


III.

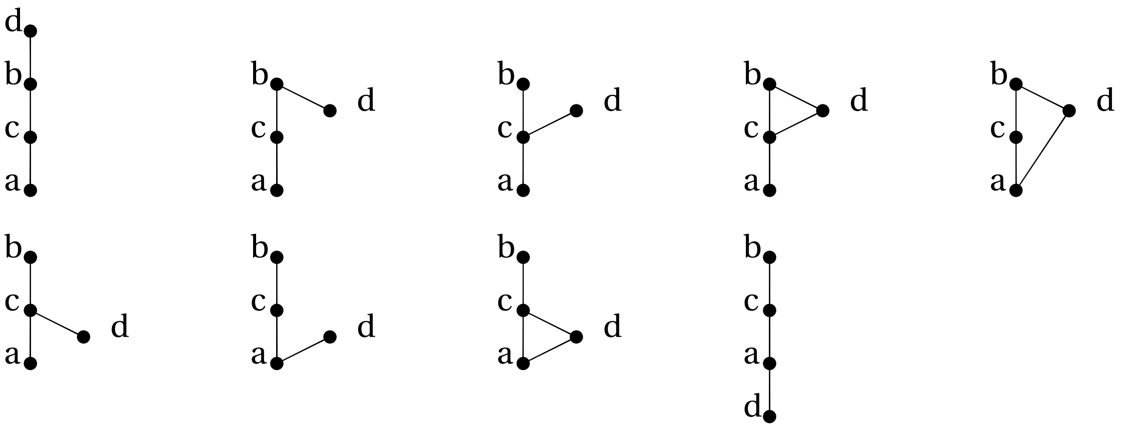


IV.





V.



□

Ejercicio. 15.8.
En $\mathbb{N} \times \mathbb{N}$ se define la relación:

$$(a, b) \preceq (c, d) \text{ si } (2a+1)2^d \leq (2c+1)2^b.$$

(1) *Demuestra que $\preceq$ es una relación de orden en $\mathbb{N} \times \mathbb{N}$.*

(2) *Demuestra que en $\mathbb{R} \times \mathbb{R}$ no es una relación de orden.*

SOLUCIÓN. Es claro que $\preceq$ verifica la propiedad reflexiva, tanto en $\mathbb{N} \times \mathbb{N}$ como en $\mathbb{R} \times \mathbb{R}$. También se verifica en ambos conjuntos la propiedad transitiva.

La propiedad antisimétrica se verifica en $\mathbb{N} \times \mathbb{N}$, ya que si $(a, b) \preceq (c, d)$ y $(c.d) \preceq (a, b)$, entonces se tiene:

$$(2a+1)2^d \leq (2c+1)2^b \text{ y}$$
$$(2c+1)2^b \leq (2a+1)2^d$$

De aquí se deduce que $(2a+1)2^d = (2c+1)2^b$, y por tanto, como un factor es par y el otro es impar, se tiene $2a+1 = 2c+1$ y $2^d = 2^b$, luego $a = c$ y $b = d$. En el caso de $\mathbb{R} \times \mathbb{R}$ esto no es cierto, ya que tenemos:

$$(1/2, 1) \preceq (0, 0) \text{ y } (0, 0) \preceq (1/2, 1), \text{ pero } (1/2, 1) \neq (0, 0).$$

□

Ejercicio. 15.9.
Sea R una relación en un conjunto X que verifica la propiedad transitiva y es irreflexiva ($\forall x \in X$ se tiene $x \not R x$.) Se define en X una nueva relación S mediante:

$$xSy \text{ si } x = y \text{ ó } xRy.$$

Demuestra que S es una relación de orden.

SOLUCIÓN. Es claro que S se verifica las propiedades reflexiva y transitiva. Para ver que también verifica la propiedad antisimétrica, supongamos que xSy y que ySx, si $x \neq y$, entonces xRy e yRx, y como R verifica la propiedad transitiva se tiene xRx, lo que es imposible al ser R irreflexiva. Como consecuencia se tiene $x = y$ y S verifica la propiedad antisimétrica. □

Ejercicio. 15.10.
Dada una relación R en un conjunto X, definimos la ***relación opuesta*** *R^t mediante:*

$$(x, y) \in R^t \text{ si } (y, x) \in R.$$

Dadas dos relaciones R y S en un conjunto X, definimos la ***composición*** *$R \circ S$ mediante:*

$$(x, y) \in R \circ S \text{ si } \exists z \in X \text{ tal que } (x, z) \in S \text{ y } (z, y) \in R.$$

La relación Diag es aquella que está definida por $Diag = \{(x, x) \mid x \in X\}$.

(1) *Demostrar que una relación R en un conjunto X es una relación de orden si y solo si $R \cap R^t = Diag$ y $R \circ R = R$.*

(2) *Demostrar que una relación R en un conjunto X es una relación de orden total si y sólo si $R \cap R^t = Diag$, $R \circ R = R$ y $R \cup R^t = X \times X$.*

SOLUCIÓN. HACER □

16. Retículos

Ejercicio. 16.1.
Demuestra que un retículo es un conjunto totalmente ordenado si y sólo si todos sus subconjuntos son subretículos

SOLUCIÓN. Sea X un retículo, entonces definimos una relación de orden en X mediante $a \leq b$ si $a \vee b = b$. Es claro que es una relación que verifica la prop. reflexiva, la prop. antisimétrica es también cierta, ya que si $a \leq b$ y $b \leq a$, entonces $a = a \vee b = b$. La prop. transitiva es también cierta.

Si verifica la condición del enunciado vamos a ver que es un orden total. Dados $a, b \in X$, si $a \nleq b$, entonces como $\{a, b\}$ es un retículo, existe el supremo de a y b, que no es igual a b, por tanto es igual a a y en consecuencia $b \leq a$. $\square$

Ejercicio. 16.2.
Sea $f : X \to Y$ una aplicación. Demuestra que el conjunto

$$\{f_*(S) \mid S \subseteq X\} \subseteq \mathcal{P}(Y)$$

es un subretículo.

SOLUCIÓN. Llamamos $R = \{f_*(S) \mid S \subseteq X\}$. Dados $A_1, A_2 \in R$, sean $A_i = f_*(S_i)$, para $i = 1, 2$. Como $S := S_1 \cup S_2$ verifica:

$$f_*(S) = f_*(S_1 \cup S_2) = f_*(S_1) \cup f_*(S_2) = A_1 \cup A_2.$$

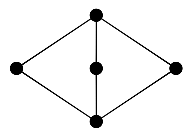
Podemos tomar el supremo de A_1 y A_2 igual a la unión.

Para el ínfimo no se puede utilizar el mismo razonamiento ya que solo tenemos: $f_*(S_1 \cap S_2) \subseteq f_*(S_1) \cap f_*(S_2)$. Sin embargo, dados $A_i = f_*(S_i)$, si tomamos $A_1 \cap A_2$, podemos definir $S_1' := \{s \in S_1 \mid f(s) \in A_1 \cap A_2\}$; es fácil comprobar que $f_*(S_1`) = A_1 \cap A_2$, y por tanto podemos tomar el ínfimo de A_1 y A_2 igual a la intersección. $\square$

Ejercicio. 16.3.
Demuestra que en un retículo distributivo $(L, \vee, \wedge)$ se verifica

$$(x \wedge y) \vee (y \wedge z) \vee (z \wedge x) = (x \vee y) \wedge (y \vee z) \wedge (z \vee x),$$

pero que esta igualdad no es cierta en el retículo de la figura.



SOLUCIÓN. Basta desarrollar una de las expresiones siguiendo las propiedades del supremo y el ínfimo.

$$\begin{aligned}
& (x \wedge y) \vee (y \wedge z) \vee (z \wedge x) \\
= & [(x \vee (y \wedge z)) \wedge (y \vee (y \wedge z))] \vee (z \wedge x) \\
= & [(x \vee y) \wedge (x \vee z) \wedge (y \vee y) \wedge (y \vee z)] \vee (z \wedge x) \\
= & (x \vee y \vee (z \wedge x)) \wedge (x \vee z \vee (z \wedge x)) \wedge (y \vee y \vee (z \wedge x)) \wedge (y \vee z \vee (z \wedge x)) \\
= & (x \vee y \vee z) \wedge (x \vee y \vee x) \wedge (x \vee z \vee z) \wedge (x \vee z \vee x) \\
& \wedge (y \vee y \vee z) \wedge (y \vee y \vee x) \wedge (y \vee z \vee z) \wedge (y \vee z \vee x) \\
= & (x \vee y \vee z) \wedge (x \vee y) \wedge (x \vee z) \wedge (y \vee z) \\
= & (x \vee y) \wedge (x \vee z) \wedge (y \vee z).
\end{aligned}$$

Para comprobar que esta propiedad no se verifica en el caso de la figura bata tomar x, y y z los puntos de la fila intermedia de la figura. □

Ejercicio. 16.4.
Demuestra que todo conjunto totalmente ordenado es un retículo distributivo.

SOLUCIÓN. Observamos que si tres elementos x, y y z pertenecen a un conjunto totalmente ordenado, entonces estos tres elementos forman una cadena, por ejemplo $x \leq y \leq z$. Esta o cualquier otra que se pueda obtener con una permutación de los elementos x, y, x.

Falta ver que cada cadena $x \leq y \leq z$ es un retículo distributivo. Probar esto es equivalente a probar que para cada ordenación de los elementos x, y, z se verifica la relación $x \wedge (y \vee z) = (x \wedge y) \vee (x \wedge z)$.

<u>Caso 1</u>. $x \leq y \leq z$.

$$\begin{aligned} x \wedge (y \vee z) &= x \wedge z = x \\ (x \wedge y) \vee (x \wedge z) &= x \vee x = x \end{aligned}$$

<u>Caso 2</u>. $x \leq z \leq y$.

$$\begin{aligned} x \wedge (y \vee z) &= x \wedge y = x \\ (x \wedge y) \vee (x \wedge z) &= x \vee x = x \end{aligned}$$

<u>Caso 3</u>. $y \leq x \leq z$.

$$\begin{aligned} x \wedge (y \vee z) &= x \wedge z = x \\ (x \wedge y) \vee (x \wedge z) &= y \vee x = x \end{aligned}$$

<u>Caso 4</u>. $y \leq z \leq x$.

$$\begin{aligned} x \wedge (y \vee z) &= x \wedge z = z \\ (x \wedge y) \vee (x \wedge z) &= y \vee z = z \end{aligned}$$

<u>Caso 5</u>. $z \leq x \leq y$.

$$\begin{aligned} x \wedge (y \vee z) &= x \wedge y = x \\ (x \wedge y) \vee (x \wedge z) &= x \vee z = x \end{aligned}$$

Caso 6. $z \leq y \leq x$.

$$\begin{aligned} x \wedge (y \vee z) = x \wedge y = y \\ (x \wedge y) \vee (x \wedge z) = y \vee z = y \end{aligned}$$

□

Ejercicio. 16.5.
Sea L un retículo complementado. Prueba que si L tiene tres o más elementos, entonces L no es totalmente ordenado.

SOLUCIÓN. Si un retículo es complementado y tiene tres o más elementos, entonces consideramos el subconjunto que contiene a 1, 0 y un tercer elemento, sea a. Com es complementado, existe $\overline{a}$ y es distinto de a, 1 y 0. Por tanto tenemos en L al menos cuatro elementos: 1, 0, a y $\overline{a}$. Es claro que a y $\overline{a}$ no son comparables, luego L no es un conjunto totalmente ordenado. □

Ejercicio. 16.6.
Demuestra que el producto cartesiano de retículos distributivos es un retículo distributivo.

SOLUCIÓN. Consideramos el orden producto cartesiano, esto es, si L_1 y L_2 son retículos, en $L_1 \times L_2$ definimos $(x_1, x_2) \leq (y_1, y_2)$ si $x_i \leq y_i$ para $i = 1, 2$.

Veamos que $L_1 \times L_2$ es un retículo. Dados (x_1, x_2), $(y_1, y_2) \in L_1 \times L_2$, y $(z_1, z_2) \in L_1 \times L_2$ tales que $(x_1, x_2) \leq (z_1, z_2)$ y $(y_1, y_2) \leq (z_1, z_2)$, se tiene $x_i \leq z_i$ y $y_i \leq z_i$, luego $x_i \vee y_i \leq z_i$, para $i = 1, 2$. Como consecuencia $(x_1 \vee y_1, x_2 \vee y_2) \leq (z_1, z_2)$. Luego $(x_1, x_2) \vee (y_1, y_2) = (x_1 \vee y_1, x_2 \vee y_2)$.

De la misma forma se puede probar $(x_1, x_2) \wedge (y_1, y_2) = (x_1 \wedge y_1, x_2 \wedge y_2)$.

Así pues $L_1 \times L_2$ es un retículo.

Para ver que es distributivo si L_1 y L_2 lo son procedemos como sigue:

$$\begin{aligned} & (x_1, x_2) \wedge [(y_1, y_2) \vee (z_1, z_2)] \\ = & (x_1, x_2) \wedge (y_1 \vee z_1, y_2 \vee z_2) \\ = & (x_1 \wedge (y_1 \vee z_1), x_2 \wedge (y_2 \vee z_2)) \\ = & ((x_1 \wedge y_1) \vee (x_1 \wedge z_1), (x_2 \wedge y_2) \vee (x_2 \wedge z_2)) \\ = & (x_1 \wedge y_1, x_2 \wedge y_2) \vee (x_1 \wedge z_1, x_2 \wedge z_2) \\ = & [(x_1, x_2) \wedge (y_1, y_2)] \vee [(x_1, x_2) \wedge (z_1, z_2)]. \end{aligned}$$

Del mismo modo se puede probar la igualdad:

$$(x_1, x_2) \vee [(y_1, y_2) \wedge (z_1, z_2)] = [(x_1, x_2) \vee (y_1, y_2)] \wedge [(x_1, x_2) \vee (z_1, z_2)].$$

Para cualesquiera (x_1, x_2), (y_1, y_2), $(z_1, z_2) \in L_1 \times L_2$. □

Capítulo V

Álgebras de Boole

17. Álgebras de Boole

Ejercicio. 17.1.
Sea $\mathcal{B}$ un álgebra de Boole, entonces para cada elemento $x \in \mathcal{B}$ el complemento $\overline{x}$ es único.

SOLUCIÓN. Supongamos que x tiene dos complementos, y que estos son a y $b \in \mathcal{B}$, entonces se verifica:

$$x \vee a = 1 = x \vee b \qquad x \wedge a = 0 = x \wedge b.$$

Procedemos como sigue:

$$a = a \wedge 1 = a \wedge (x \vee b) = (a \wedge x) \vee (a \wedge b) = 0 \vee (a \wedge b) = a \wedge b.$$

Del mismo modo podemos probar que $b = b \wedge a$, luego $a = b$. □

Ejercicio. 17.2.
Sea $f : \mathcal{B} \longrightarrow \mathcal{B}'$ un homomorfismo de álgebras de Boole, esto es, es una aplicación que verifica:

$$\begin{aligned} &f(x \vee y) = f(x) \vee f(y), \\ &f(x \wedge y) = f(x) \wedge f(y) \quad \text{y} \\ &f(\overline{x}) = \overline{f(x)} \end{aligned}$$

para cualesquiera $x, y \in \mathcal{B}$. Probar que si f es sobreyectivo, entonces $f(1) = 1$ y $f(0) = 0$.

SOLUCIÓN. Por ser f sobreyectivo existen $a \in \mathcal{B}$ y $b \in \mathcal{B}$ tales que $f(a) = 1$ y $f(b) = 0$. Entonces se tiene

$$f(1) = f(1 \vee a) = f(1) \vee f(a) = f(1) \vee 1 = 1.$$

Del mismo modo tenemos que $f(0) = 0$. □

Ejercicio. 17.3.
Sea $\mathbb{B}$ un álgebra de Boole. Si $a, b \in \mathcal{B}$ son átomos y $a \neq b$, entonces $ab = 0$.

SOLUCIÓN. Tenemos $a = ab + a\overline{b}$, y por ser a un átomo resulta $a = ab$ ó $a = a\overline{b}$.

Si $a = ab$, entonces procedemos como sigue:

$$b = ab + \overline{a}b = a + \overline{a}b \Rightarrow \begin{cases} b = a, \text{ ó} \\ b = \overline{a}b, \text{ que implica } a = ab = a\overline{a}b = 0 \end{cases}$$

en ambos casos se llega a una contradicción. Luego necesariamente $a = a\overline{b}$, y por tanto $ab = a\overline{b}b = 0$. □

Ejercicio. 17.4.
Sea $f : L \longrightarrow L'$ un homomorfismo de retículos sobreyectivo. Demuestra que si L es un álgebra de Boole entonces L' también lo es.

SOLUCIÓN. Recordemos que un homomorfismo de retículos $f : L \longrightarrow L'$ es una aplicación que verifica: $f(x \vee y) = f(x) \vee f(y)$ y $f(x \wedge y) = f(x) \wedge f(y)$ para cualesquiera $x, y \in L$. Si L y L' son álgebras de Boole, entonces $f : L \longrightarrow L'$ es un homomorfismo de álgebras de Boole si se verifica: $f(x \vee y) = f(x) \vee f(y)$, $f(x \wedge y) = f(x) \wedge f(y)$ y $f(\overline{x}) = \overline{f(x)}$ para cualesquiera $x, y \in L$. Así pues falta ver que se verifica $f(\overline{x}) = \overline{f(x)}$ para cada $x \in L$.

Tenemos $f(1) = 1$ y $f(0) = 0$, luego tenemos para cada $x \in L$ tenemos las relaciones siguientes:

$$\begin{aligned} 1 = f(1) = f(x \vee \overline{x}) = f(x) \vee f(\overline{x}); \\ 0 = f(0) = f(x \wedge \overline{x}) = f(x) \wedge f(\overline{x}). \end{aligned}$$

Como L' es un álgebra de Boole resulta que el complemento, $\overline{f(x)}$, de $f(x)$ es único, y $f(\overline{x})$ verifica ser un complemento de $f(x)$, luego $f(\overline{x}) = \overline{f(x)}$, y tenemos el resultado. □

Ejercicio. 17.5.
Sea $(\mathcal{B}, +, \cdot)$ un álgebra de Boole y sean $a, b \in \mathcal{B}$. Demuestra que las siguientes afirmaciones son equivalentes:

(1) $a\overline{b} = 0$,

(2) $a + b = b$,

(3) $\overline{a} + b = 1$,

(4) $a.b = a$.

SOLUCIÓN. (a) $\Rightarrow$ (b). $[a.\overline{b} = 0 \Rightarrow a + b = b]$

$$a + b = (a + b),1 = (a + b).(b + \overline{b}) = a.b + a.\overline{b} + b.b + b.\overline{b} = a.b + b = b.$$

(b) $\Rightarrow$ (c). $[a + b = b \Rightarrow \overline{a} + b = 1]$

$$\overline{a} + b = \overline{a} + (a + b) = (\overline{a} + a) + b = 1 + b = 1.$$

(c) $\Rightarrow$ (d). $[\overline{a} + b = 1 \Rightarrow a.b = a]$

$$a.b = 0 + a.b = a.\overline{a} + a.b = a.(\overline{a} + b) = a,1 = a.$$

(d) $\Rightarrow$ (a). $[a.b = a \Rightarrow a.\overline{b} = 0]$

$$a.\overline{b} = (a.b).\overline{b} = a.(b.\overline{b}) = a,0 = 0.$$

Observar la dualidad existente entre $(a) \Rightarrow (b)$ y $(c) \Rightarrow (d)$ y entre $(b) \Rightarrow (c)$ y $(d) \Rightarrow (a)$ □

Ejercicio. 17.6.
¿Cuántos átomos tiene un álgebra de Boole con 32 elementos?

SOLUCIÓN. Recordemos que un átomo de un álgebra de Boole $\mathcal{B}$ es un elemento $a \neq 0$ que verifica si $a = b_1 \vee b_2$, entonces $b_1 = a$ ó $b_2 = a$. En nuestro caso si tenemos 32 átomos, como cada elemento de $\mathcal{B}$ se escribe en al forma $b_{i_1} \vee \cdots \vee b_{i_s}$, en donde no importa el orden y en donde a lo más aparece una vez cada átomo b_{i_j}, resulta que el número es:

$$\binom{32}{0} + \binom{32}{1} + \cdots + \binom{32}{31} + \binom{32}{32} = 2^{32}.$$

□

Ejercicio. 17.7.
Demuestra que el producto cartesiano de álgebras de Boole es un álgebra de Boole.

SOLUCIÓN. Ya conocemos que el resultado es cierto para retículos distributivos. Para obtener el resultado que aquí nos ocupa, basta considerar dos álgebras de Boole $\mathcal{B}_1$ y $\mathcal{B}_2$ y ver que se verifica:

$$\overline{(x_1, x_2)} = (\overline{x_1}, \overline{x_2}),$$

para cada $(x_1, x_2) \in \mathcal{B}_1 \times \mathcal{B}_2$, lo cual es inmediato. □

Ejercicio. 17.8.
Si para un álgebra de Boole finita $\mathcal{B}$ conocemos el conjunto M de todos sus átomos, así como la expresión de un elemento x de $\mathcal{B}$ como supremo de átomos. ¿Cómo podríamos obtener la expresión de $\overline{x}$ como supremo de átomos?

SOLUCIÓN. Sea $x \in \mathcal{B}$ y sean $\{a_i \mid i = 1, \ldots, t\}$ la familia de átomos. Supongamos que $x = \sum_{i=1}^{s} a_i$, con $s \leq t$. Llamamos $y = \sum_{i=s+1}^{t}$. Es claro que se tiene:

$$x + y = \sum_{i=1}^{s} a_i + \sum_{i=s+1}^{t} a_i = \sum_{i=1}^{s} a_i = 1.$$
$$x \cdot y = (\sum_{i=1}^{s} a_i) \cdot (\sum_{i=s+1}^{t} ai) = \sum_{i=1}^{s} \sum_{j=s+1}^{t} a_i a_j = 0,$$

ya que si a_i y a_j son átomos y $a_i \neq a_j$, entonces $a_i \cdot a_j = 0$. □

Ejercicio. 17.9.
Sea I el conjunto de los números reales que pertenecen al intervalo cerrado $[0, 1]$. Para todo $a, b \in I$ definimos $a \vee b = max\{a, b\}$, $a \wedge b = min\{a, b\}$ y $\overline{a} = 1 - a$
¿Es I respecto de estas operaciones un álgebra de Boole?

SOLUCIÓN. Debe ocurrir $a \vee \overline{a} = 1$, pero tenemos $a \vee \overline{a} = max\{a, 1 - a\}$, que es igual a 1 solo cuando $a = 1$ ó $a = 0$. Luego no es un álgebra de Boole. □

Ejercicio. 17.10.
Se conocen los siguientes hechos sobre cuatro personas A, B, C y D y una película:

(1) Si A ve la película entonces B también la ve.

(2) C y D no ven la película juntos.

(3) B y C o bien ven la película juntos o no la ve ninguno de los dos.

(4) Si A no ve la película entonces B y C la ven.

¿Quién o quienes están viendo la película?

SOLUCIÓN. (1). $A \Rightarrow B$, esto es, $\overline{A} \vee B$.
(2). $C \Leftrightarrow \overline{D}$.
(3). $B \Leftrightarrow C$.
(4). $\overline{A} \Rightarrow (B \wedge C)$, esto es, $\overline{A} \Leftrightarrow B$, o equivalentemente $A \vee B$.
Como todas las condiciones se verifican, resulta:

$$(\overline{A} \vee B) \wedge (A \vee B).$$

Al desarrollar esta expresión resulta:

$$
\begin{array}{l}
(\overline{A} \vee B) \wedge (A \vee B) \\
[(\overline{A} \vee B) \wedge A] \vee [(\overline{A} \vee B) \wedge B] \\
(\overline{A} \wedge A) \vee (B \wedge A) \vee (\overline{A} \wedge B) \vee (B \wedge B) \\
(B \wedge A) \vee (\overline{A} \wedge B) \vee B \\
(B \wedge (A \vee \overline{A})) \vee B \\
B \vee B \\
B
\end{array}
$$

Por lo tanto B está viendo la película, entonces C también la ve y D no lo hace. De A no podemos afirmar nada. □

18. Formas canónicas de funciones booleanas

Ejercicio. 18.1.
Calcula la forma normal canónica disyuntiva, es decir, suma de minitérminos (=minterms), y simplifica las funciones booleanas dadas por las tablas

x	y	z	f	g
0	0	0	0	0
0	0	1	1	0
0	1	0	1	1
0	1	1	1	1
1	0	0	0	1
1	0	1	1	1
1	1	0	0	1
1	1	1	0	1

SOLUCIÓN. El caso de f. Los valores para los que f toma en valor 1 son:

$$\overline{x}\overline{y}z, \overline{x}y\overline{z}, \overline{x}yz, x\overline{y}z,$$

entonces la expresión de f expresada según los minitérminos es:

$$\overline{x}\overline{y}z + \overline{x}y\overline{z} + \overline{x}yz + x\overline{y}z.$$

El caso de g. Los valores para los que g toma en valor 1 son:

$$\overline{x}y\overline{z}, \overline{x}yz, x\overline{y}\overline{z}, x\overline{y}z, xy\overline{z}, xyz,$$

entonces la expresión de f expresada según los minitérminos es:

$$\overline{x}y\overline{z} + \overline{x}yz + x\overline{y}\overline{z} + x\overline{y}z + xy\overline{z} + xyz.$$

□

Ejercicio. 18.2.
Calcula la forma normal canónica disyuntiva de la aplicación $f(x, y, z) = (x \uparrow y) \vee z$.

SOLUCIÓN. Construimos la tabla de verdad de la expresión $(x \uparrow y) \vee z$.

$(x$	$\uparrow$	$y)$	$\vee$	z
1	0	1	1	1
1	0	1	0	0
1	1	0	1	1
1	1	0	1	0
0	1	1	1	1
0	1	1	1	0
0	1	0	1	1
0	1	0	1	0

entonces la forma canónica normal disyuntiva es:

$$xyz + x\overline{y}z + x\overline{y}\overline{z} + \overline{x}yz + \overline{x}y\overline{z} + \overline{x}\overline{y}z + \overline{x}\overline{y}\overline{z}$$

□

Ejercicio. 18.3.
Expresa, utilizando sólo la función $\downarrow$, la aplicación $f(x, y, z) = (x \vee z) \wedge y$.

SOLUCIÓN. Recordemos la definición de $\downarrow$:

x	$\downarrow$	y
1	0	1
1	0	0
0	0	1
0	1	0

Esto es: $x \downarrow y := \overline{x \vee y}$. Como consecuencia se tiene: $\overline{x} = x \downarrow x$ y además:

$$x \wedge y = \overline{\overline{x}} \wedge \overline{\overline{y}} = \overline{\overline{x} \vee \overline{y}} = \overline{x} \downarrow \overline{y} = (x \downarrow x) \downarrow (y \downarrow y).$$

$$x \vee y = \overline{x \downarrow y} = (x \downarrow y) \downarrow (x \downarrow y).$$

En nuestro caso tenemos:

$$\begin{aligned} & (x \vee z) \wedge y \\ = & [(x \downarrow z) \downarrow (x \downarrow z)] \wedge y \\ = & [[(x \downarrow z) \downarrow (x \downarrow z)] \downarrow [(x \downarrow z) \downarrow (x \downarrow z)]] \downarrow [y \downarrow y] \end{aligned}$$

y ocurre que $[[(x \downarrow z) \downarrow (x \downarrow z)] \downarrow [(x \downarrow z) \downarrow (x \downarrow z)]] = x \downarrow z$ (comprobarlo mediante la tabla de verdad), luego tenemos:

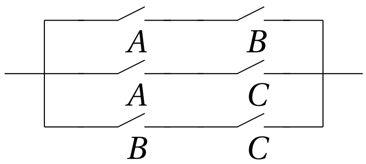
$$(x \vee z) \wedge y = (x \downarrow z) \downarrow (y \downarrow y).$$

□

19. El álgebra Boole de las proposiciones lógicas

Ejercicio. 19.1.
Un comité formado por tres personas toma decisiones mediante votación por mayoría. Cada miembro del comité puede "votar S-"pulsando un botón. Diseñar una red lógica mediante la cual se encienda una luz cuando y sólo cuando haya una mayoría de "votos S-".

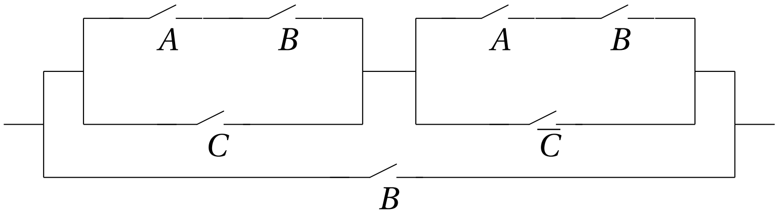
Solución. El circuito pedido es:



□

20. Circuitos lógicos

Ejercicio. 20.1.
Simplifica el circuito de conmutadores de la figura.



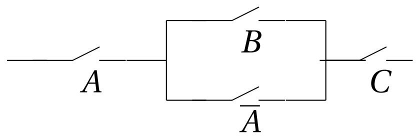
SOLUCIÓN. Únicamente tenemos que escribir la expresión que define el circuito y aplicar las reglas que se verifican en un álgebra de Boole:

$$\begin{aligned} & B \vee [((A \wedge B) \vee C) \wedge ((A \wedge B) \vee \overline{C})] \\ = & B \vee [(A \wedge B) \vee (C \wedge \overline{C})] \\ = & B \vee ((A \wedge B) \vee 0) \\ = & B \vee (A \wedge B) = B. \end{aligned}$$

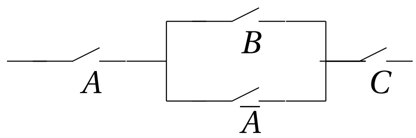
□

21. Circuitos de conmutadores

Ejercicio. 21.1.
Determina una expresión booleana cuya función booleana se corresponda con el circuito de conmutadores que aparece en la figura.

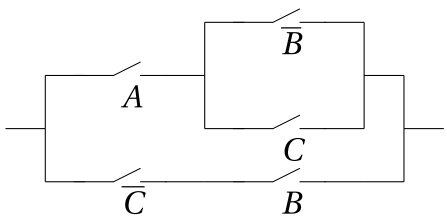


SOLUCIÓN. La expresión del circuito de conmutadores

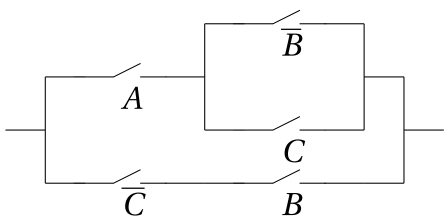


es: $A \wedge (B \vee \overline{A}) \wedge C$. □

Ejercicio. 21.2.
Determina una expresión booleana cuya función booleana se corresponda con el circuito de conmutadores que aparece en la figura.

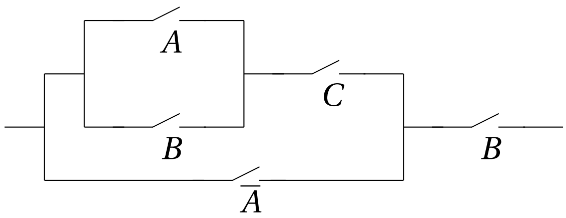


SOLUCIÓN. La expresión del circuito de conmutadores

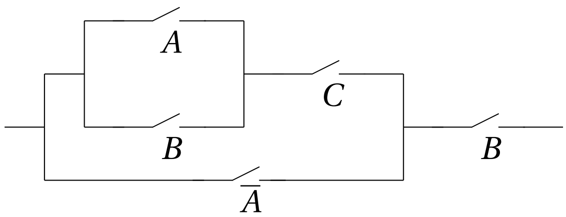


es: $(A \wedge (\overline{B} \vee C)) \vee (\overline{C} \wedge B)$. □

Ejercicio. 21.3.
Determina una expresión booleana cuya función booleana se corresponda con el circuito de conmutadores que aparece en la figura.



SOLUCIÓN. La expresión del circuito de conmutadores



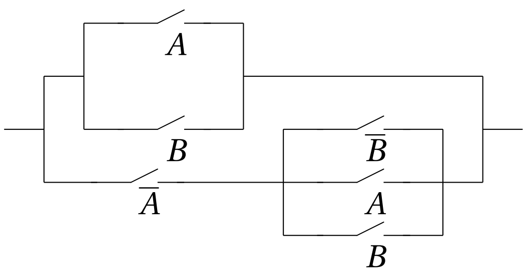
es: $[((A \vee B) \wedge C) \vee (\overline{A})] \wedge B$.

□

Ejercicio. 21.4.
Construye un circuito conmutador asociado a la función booleana representada por la siguiente expresión:

$$(A \vee B) \vee (\overline{A} \wedge (\overline{B} \vee A \vee B)).$$

SOLUCIÓN. El circuito de conmutadores de la expresión $(A \vee B) \vee (\overline{A} \wedge (\overline{B} \vee A \vee B))$ es:

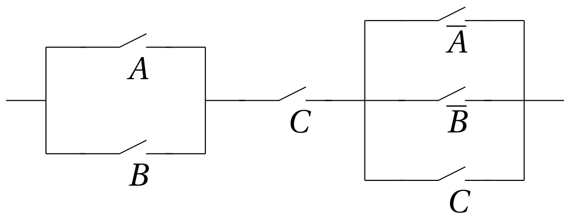


□

Ejercicio. 21.5.
Construye un circuito conmutador asociado a la función booleana representada por la siguiente expresión:

$$(A \vee B) \wedge C \wedge (\overline{A} \vee \overline{B} \vee \overline{C}).$$

SOLUCIÓN. El circuito de conmutadores de la expresión $(A \vee B) \wedge C \wedge (\overline{A} \vee \overline{B} \vee \overline{C})$ es:

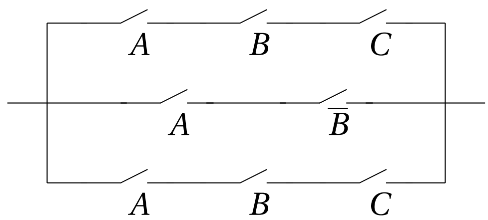


□

Ejercicio. 21.6.
Construye un circuito conmutador asociado a la función booleana representada por la siguiente expresión:

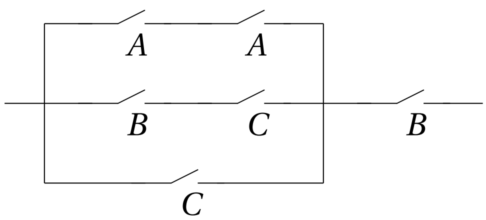
$$(A \wedge B \wedge C) \vee (A \wedge \overline{B}) \vee (A \wedge B \wedge C).$$

Solución. El circuito de conmutadores de la expresión $(A \wedge B \wedge C) \vee (A \wedge \overline{B}) \vee (A \wedge B \wedge C)$ es:



□

Ejercicio. 21.7.
Simplifica el circuito de conmutadores de la figura.



Solución. Únicamente tenemos que escribir la expresión que define el circuito y aplicar las reglas que se verifican en un álgebra de Boole:

$$
\begin{aligned}
&((A \wedge A) \vee (B \wedge C) \vee C) \wedge B \\
=\ &(A \vee (B \wedge C) \vee C) \wedge B \\
=\ &(A \vee C) \wedge B.
\end{aligned}
$$

□

22. Minimización de circuitos

Ejercicio. 22.1.
Minimizar la expresión booleana

$$x + xy + xyz + xy\overline{z} + xt$$

SOLUCIÓN. Es claro que se tiene $x + xy + xyz + xy\overline{z} + xt = x$. □

Ejercicio. 22.2.
Minimizar la siguiente expresión booleana:

$$xy\overline{z} + x\overline{y}\,\overline{z} + x\overline{y}z + \overline{x}yz$$

SOLUCIÓN. Utilizar el diagrama de Karnaugh para minimizar la expresión.

Basándonos en él tenemos:

$$\begin{array}{l} xy\overline{z} + x\overline{y}\,\overline{z} + x\overline{y}z + \overline{x}yz \\ = xy\overline{z} + x\overline{z} + \overline{x}yz \\ = x\overline{z}(y+1) + \overline{x}yz \\ = x\overline{z} + \overline{x}yz \end{array}$$

□

Ejercicio. 22.3.
Obtener una expresión minimal para la función booleana en cinco variables f definida por:

$$1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 00, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1$$

SOLUCIÓN. Las variables son: x, y, z, t y s, y la expresión booleana es:

$$xyzts + \cdots$$

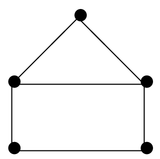
□

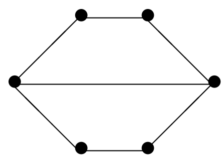
Capítulo VI

Introducción a la teoría de grafos

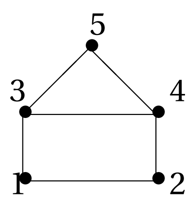
23. Introducción a la teoría de grafos

Ejercicio. 23.1.
Expresa en forma matricial (matrices de adyacencia) los grafos



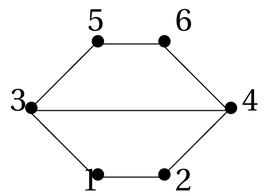


SOLUCIÓN. Numeramos los vértices para fijar las filas y columnas de la matriz.



$$\begin{pmatrix} 0 & 1 & 1 & 0 & 0 \\ 1 & 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 & 0 \end{pmatrix}$$

La matriz de adyacencia.



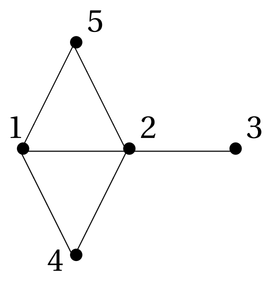
$$\begin{pmatrix} 0 & 1 & 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 & 0 \end{pmatrix}$$

La matriz de adyacencia. □

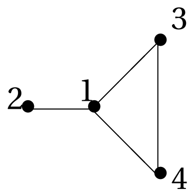
Ejercicio. 23.2.
Representa gráficamente los siguientes grafos cuyas matrices de adyacencia son

$$\begin{pmatrix} 0 & 1 & 0 & 1 & 1 \\ 1 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 \end{pmatrix} \qquad \begin{pmatrix} 0 & 1 & 1 & 1 \\ 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 \\ 1 & 0 & 1 & 0 \end{pmatrix}$$

SOLUCIÓN. La matriz $\begin{pmatrix} 0 & 1 & 0 & 1 & 1 \\ 1 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 \end{pmatrix}$ tiene como grafo asociado al grafo:



La matriz $\begin{pmatrix} 0 & 1 & 1 & 1 \\ 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 \\ 1 & 0 & 1 & 0 \end{pmatrix}$ tiene como grafo asociado al grafo:


3
2
1
4

□

24. Lados en grafos

Ejercicio. 24.1.
(No se ha visto en clase.) Calcula las geodésicas que unen el vértice 4 *con el vértice* 9 *en el grafo siguiente:*

$$\begin{tikzcd}
1 \arrow[r, dash, "2"] \arrow[d, dash, "2"] & 2 \arrow[r, dash, "2"] \arrow[d, dash, "1"] & 3 \arrow[r, dash, "3"] \arrow[d, dash, "2"] & 4 \arrow[d, dash, "1"] \\
5 \arrow[r, dash, "2"'] \arrow[d, dash, "2"] & 6 \arrow[r, dash, "3"] \arrow[ur, dash, "3"] \arrow[d, dash, "3"] & 7 \arrow[r, dash, "1"] \arrow[ur, dash, "2"] \arrow[d, dash, "1"] & 8 \arrow[d, dash, "2"] \\
9 \arrow[r, dash, "3"] & 10 \arrow[r, dash, "1"] & 11 \arrow[r, dash, "1"] & 12
\end{tikzcd}$$

SOLUCIÓN. □

Ejercicio. 24.2.
Sea G un grafo completo con cuatro vértices. Construye todos sus subgrafos salvo isomorfismos.

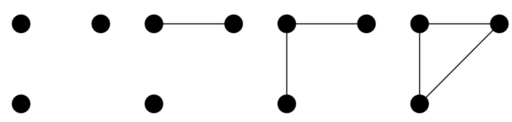
SOLUCIÓN. Todo grafo que tenga cuatro o menos de cuatro vértices y no tenga lazos es un subgrafo de G.

Con 0 vértices tenemos 1.

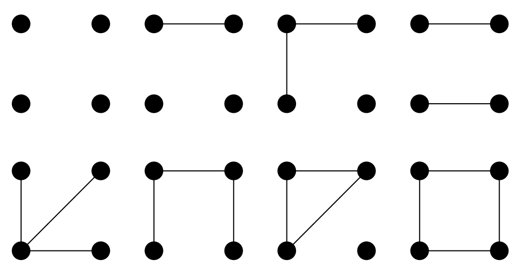
Con 1 vértice tenemos 1.

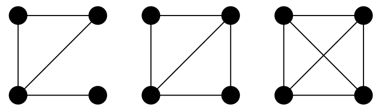
Con 2 vértices tenemos 2.

Con 3 vértices tenemos 4.



Con 4 vértices tenemos 11.





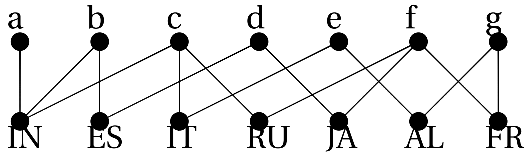
□

Ejercicio. 24.3.
Se conocen los siguientes datos sobre las personas a, b, c, d, e, f y g:

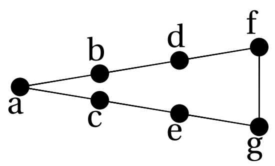
1. *La persona a habla inglés.*
2. *La persona b habla inglés y español.*
3. *La persona c habla inglés, italiano y ruso.*
4. *La persona d habla japonés y español.*
5. *La persona e habla alemán e italiano.*
6. *La persona f habla francés, japonés y ruso.*
7. *La persona g habla francés y alemán.*

¿Es cierto que cada par de personas se pueden comunicar entre ellas utilizando si, es necesario, a otra persona como intérprete?

SOLUCIÓN. Para simplificar utilizamos la siguientes abreviaturas para los que hablan cada uno de los idiomas: IN (Inglés), ES (español), IT (italiano), RU (ruso), JA (japonés), AL (alemán) y FR (francés). Tenemos entonces un grafo bipartido:



Cuando consideramos los caminos de longitud 2 que no son cerrados se obtiene el siguientes grafo:



Como consecuencia siempre se podrán comunicar dos personas aunque se a través de un intermediario. □

Ejercicio. 24.4.
Demuestra que en un grafo el número de vértices de grado impar es par.

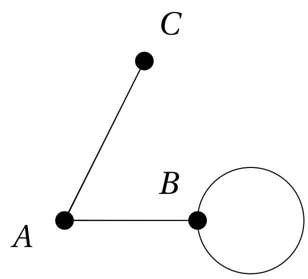
SOLUCIÓN. Como la suma de los grados de todos los vértices es un número par, el resultado es inmediato. □

Ejercicio. 24.5.
Obtén una fórmula para el número de lados de $K_{m,n}$.

SOLUCIÓN. $n \times m$. □

Ejercicio. 24.6.
Estudia si en todo grafo con más de un vértice existen dos vértices con el mismo grado.

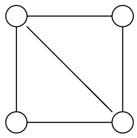
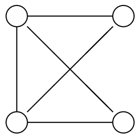
SOLUCIÓN. Esto no es cierto, por ejemplo en el grafo siguiente los tres vértice tienen grados 1, 2 y 3.



□

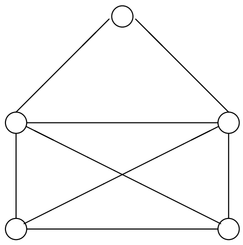
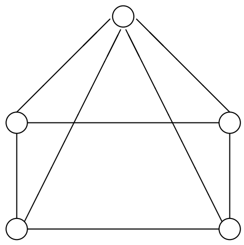
25. Invariantes de grafos

Ejercicio. 25.1.
¿Son isomorfos los grafos de la figura?

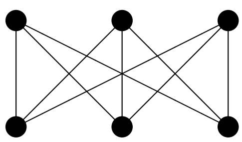
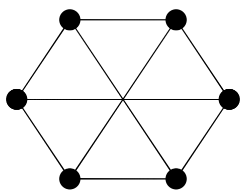
SOLUCIÓN. SI □

Ejercicio. 25.2.
¿Son isomorfos los grafos de la figura?

SOLUCIÓN. NO. El grafo de la derecha tiene un vértice de grado 4 y ninguno del de la izquierda tiene este grado. □

Ejercicio. 25.3.
¿Son isomorfos los grafos de la figura?

SOLUCIÓN. SI. □

Ejercicio. 25.4.
¿Existe algún grafo regular de grado cinco con veinticinco vértices?

SOLUCIÓN. Supongamos que existe un tal grafo, entonces la suma de los grafos es $5 \times 25 = 125$, como no es un número par, resulta que no puede existir el grafo señalado. □

Ejercicio. 25.5.
¿Existe un grafo completo con quinientos noventa y cinco lados?

SOLUCIÓN. Tenemos que un grafo completo es aquel en el que existe un lado entre cada dos vértices. Luego el número de lados, que no son lazos, es $\frac{v(v+1)}{2}$. Este número debe ser menor o igual que 595. Veamos cual es el mayor valor de v.

$$\begin{array}{l} \frac{v(v+1)}{2} \leq 595 \\ v(v+1) \leq 2 \times 595 = 1190 \end{array}$$

Para $v = 34$ se tiene $\frac{34\times 35}{2} = 595$, luego una solución sería el grafo completo K_{34}. Si $v = 33$, entonces K_{33} tiene $\frac{33\times 34}{2} = 561$ lados, como la diferencia 595-561 es igual a 34, resulta que con K_{33} añadiendo todos los lazos que podemos, en este caso 33, llegamos solo a 561+33=594 lados. Luego el único caso posible es el grafo K_{34}. $\square$

26. Caminos en grafos

27. Grafos conexos

Ejercicio. 27.1.
Calcular un árbol generador para los grafos de los ejercicios 25.1., 25.2. y 25.3..

SOLUCIÓN. HACER □

Ejercicio. 27.2.
Demuestra que en cualquier árbol con dos o más vértices existe, al menos, un vértice de grado uno.

SOLUCIÓN. Como es conexo no hay vértices de grado cero. Si todos los vértices tienen grado par, entonces tiene un ciclo y por tanto no puede ser un árbol. □

Ejercicio. 27.3.
Prueba que si un grafo G contiene sólo dos vértices de grado impar, entonces ambos han de encontrarse en la misma componente conexa.

SOLUCIÓN. Ya hemos visto que en este caso existe un camino de uno al otro, luego tenemos el resultado. □

28. Árboles

Ejercicio. 28.1.
Construye todos los árboles binarios completos con siete vértices.

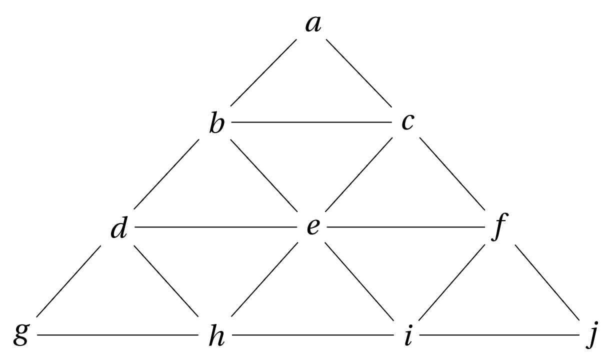
SOLUCIÓN. Está en el texto. □

Ejercicio. 28.2.
¿Cuántas ramas tiene un árbol binario completo con treinta y cinco vértices?

SOLUCIÓN. 18. □

29. Caminos de Euler

Ejercicio. 29.1.
Encuentra un circuito de Euler para el grafo



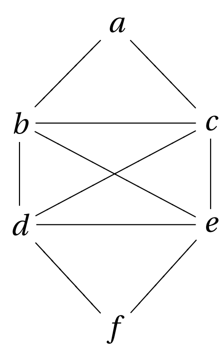
SOLUCIÓN. Un circuito de Euler es un camino simple cerrado en el que aparecen todos los lados, y se caracterizan por que todos los vértices tienen grado 2.

Un circuito de Euler es:

$$a, c, f, j, i, f, e, i, h, g, d, h, e, d, b, e, c, b, a$$

□

Ejercicio. 29.2.
Encuentra un circuito de Euler para el grafo



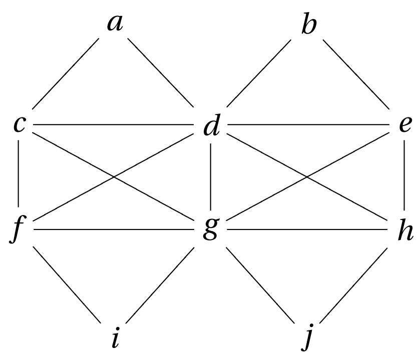
SOLUCIÓN. Un circuito de Euler es un camino simple cerrado en el que aparecen todos los lados, y se caracterizan por que todos los vértices tienen grado 2.

Un circuito de Euler es:

$$a, c, e, f, d, e, b, d, c, b, a$$

□

Ejercicio. 29.3.
Encuentra un camino de Euler para el grafo



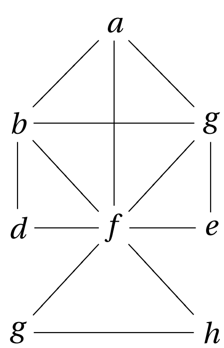
SOLUCIÓN. En este aso, como tenemos vértices de grado impar no podemos tener un circuito de Eules, sino un camino de Euler, esto es un camino simple que para una vez por todos los lados, pero que no es necesariamente cerrado.

Los vértices de grado impar son d y g, entonces un camino de Euler debe ir de d a f o viceversa. Un camino de Euler es:

$$d, b, e, d, h, e, g, h, j, g, i, f, d, c, f, g, c, a, d, g$$

□

Ejercicio. 29.4.
Encuentra un camino de Euler para el grafo



SOLUCIÓN. En este aso, como tenemos vértices de grado impar no podemos tener un circuito de Eules, sino un camino de Euler, esto es un camino simple que para una vez por todos los lados, pero que no es necesariamente cerrado.

Los vértices de grado impar son b y c, entonces un camino de Euler debe ir de b a c o viceversa. Un camino de Euler es:

$$c, a, b, d, f, g, h, f, e, c, f, b$$

□

Ejercicio. 29.5.
¿Para qué valores de n el grafo K_n es un circuito de Euler?

SOLUCIÓN. En K_n el grado de cada vértice es $n-1$, como un grado es de Euler si sus vértices tienen grado par, entonces K_n es de Euler si n es un entero positivo impar. □

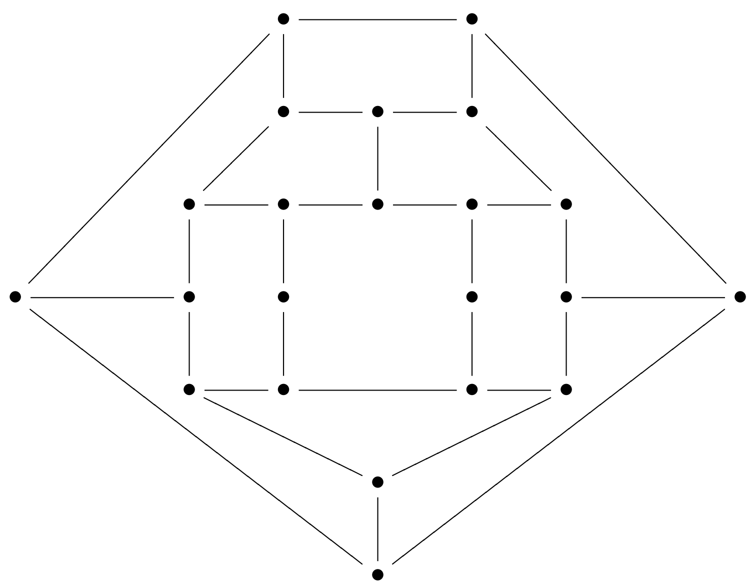
Ejercicio. 29.6.
¿Para qué valores de m y n el grafo $K_{m,n}$ es un circuito de Euler?

SOLUCIÓN. Como necesitamos que los vértices tengan grado par y como el grado de un vértice de $K_{m,n}$ es n ó m, resulta $K_{n,m}$ es un grafo de Euler si n y m son enteros positivos pares.

□

30. Caminos de Hamilton

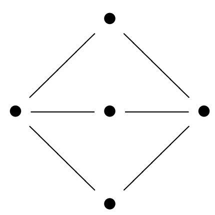
Ejercicio. 30.1.
¿Contiene el siguiente grafo un circuito Hamiltoniano?



SOLUCIÓN. Un circuito de Hamilton es un recorrido cerrado que pasa por todos los vértices.

NO contiene un circuito de Hamilton, por tanto no es un grafo de Hamilton. □

Ejercicio. 30.2.
¿Contiene el siguiente grafo un circuito Hamiltoniano?



SOLUCIÓN. Un circuito de Hamilton es un recorrido cerrado que pasa por todos los vértices.

NO contiene un circuito de Hamilton, por tanto no es un grafo de Hamilton.

Etiquetamos los vértices de izquierda a derecha y de arriba a abajo con A, B, C, D, y E. Como el circuito de Hamilton contiene a A, debe contener los lados $\{BA\}\{AD\}x_1x_2\cdots$. Si $x_1)\{DC\}$, entonces $x_2 = \{CB\}$ y no tenemos un circuito de Hamilton. Si $x_1 = \{DE\}$, entonces $x_2 = \{EB\}$, y no tenemos un circuito de Hamilton. $\square$

Ejercicio. 30.3.
Demuestra que si $n \geq 3$, entonces K_n contiene un circuito hamiltoniano.

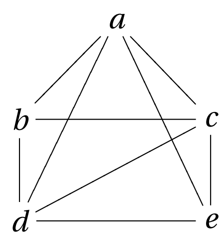
SOLUCIÓN. El número de lados de K_n es $n+(n-1)+\cdots+1+0 = \frac{n(n+1)}{2}$, y como este número es mayor o igual que $\frac{(n-1)(n-2)}{2}+2$ para $n \geq 3$, tenemos el resultado. $\square$

Ejercicio. 30.4.
¿Cuándo $K_{m,n}$ contiene un circuito de Hamilton?

SOLUCIÓN. Cuando $n = m$. $\square$

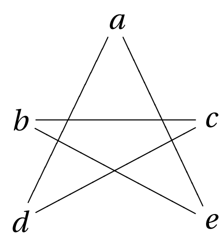
31. Grafos planos

Ejercicio. 31.1.
Determina si el siguiente grafo es plano.



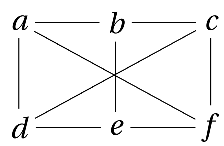
SOLUCIÓN. SI □

Ejercicio. 31.2.
Determina si el siguiente grafo es plano.



SOLUCIÓN. SI. Es un pentágono. □

Ejercicio. 31.3.
Determina si el siguiente grafo es plano.

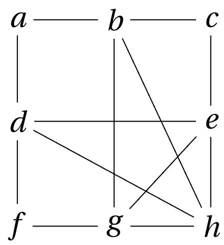


SOLUCIÓN. Cada cara tiene grado 4, ya que cada camino cerrado tiene al menos 4 lados, entonces las relaciones entre lados y vértices de un grafo plano establecen que se debe verificar

$$(t-2)e \leq t(v-2), \qquad t = 4.$$

Esto es, como $v = 6$ y $e = 9$ y no se verifica $2 \times 9 \leq 4 \times 4$, entonces no es un grafo plano. □

Ejercicio. 31.4.
Determina si el siguiente grafo es plano.



SOLUCIÓN. Al identificar, mediante contracciones, vértices adyacentes, obtenemos el grafo completo K_5. Los vértices que identificamos son:
(1). a y b
(2). f y g
(3). c y e □

Ejercicio. 31.5.
Demuestra que cualquier grafo con cuatro vértices o menos es siempre plano.

SOLUCIÓN. Los casos $n = 1, 2, 3$ son fáciles de analizar. Para el caso de $n = 4$, prescindiendo de los lazos tenemos un subgrafo de K_4 que e sun grafo plano, luego todo grafo con cuatro vértices es un grafo plano. □

Ejercicio. 31.6.
Demuestra que si un grafo tiene a lo sumo cinco vértices y uno de ellos es de grado dos entonces es plano.

SOLUCIÓN. Basta analizar el caso de cinco vértices. El grado máximo de cada vértices es 4, y si uno tiene grado 2, resulta que el valor máximo de la suma de los grados es 18, y por tanto tenemos como máximo 9 lados, entonces G es un subgrafo del grafo completo del que hemos eliminado un lado, y este grafo es un grado plano. □

Ejercicio. 31.7.
¿Depende el número de caras resultante de una representación plana de un grafo plano de la representación que escojamos?

SOLUCIÓN. No, ya que si el grafo es plano (conexo) se verifica la relación $v - e + c = 2$, luego c está determinado por v y e, que son invariantes del grafo. □

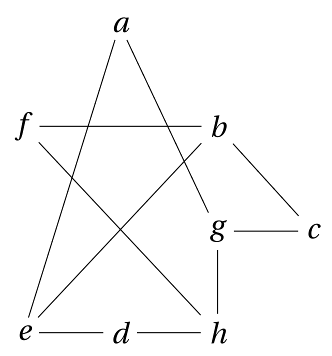
Ejercicio. 31.8.
¿Existe un grafo con seis vértices cuyos grados sean uno, dos, dos, tres, cuatro y cuatro respectivamente?

SOLUCIÓN. Si, ya que la suma 1+2+2+3+4+4 es un número par. □

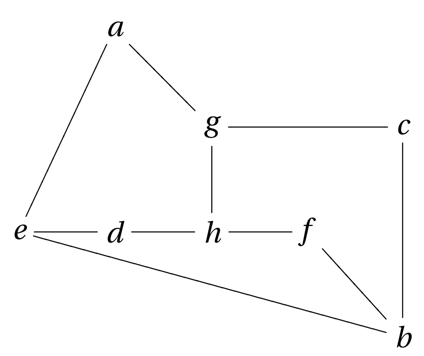
Ejercicio. 31.9.
Sea un grafo plano y conexo con nueve vértices de grados dos (tres de ellos), tres (tres de ellos), cuatro (dos de ellos) y cinco (uno de ellos). ¿Cuántos lados tiene? ¿Cuántas caras tiene?

SOLUCIÓN. Tenemos 9 vértices, $v = 9$. La sucesión de grados es: $2+2+2+3+3+3+4+4+5 = 30$, luego el número de lados es $e = 15$. Como el grafo es plano, se tiene la relación: $v-e+c = 2$, luego $c = 2 + e - v = 2 + 15 - 9 = 8$. □

Ejercicio. 31.10.
¿Es plano el grafo siguiente?

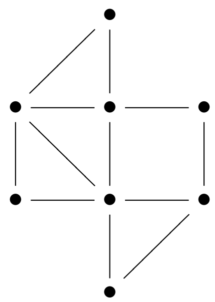


SOLUCIÓN. SI, una representación plano es:

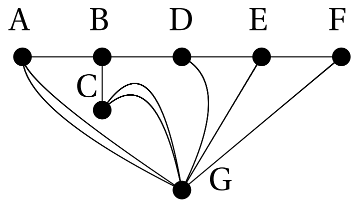


□

Ejercicio. 31.11.
Calcula el dual del grafo



SOLUCIÓN. El grafo dual tiene 7 vértices, Si numeramos las caras de derecha a izquierda y de arriba a abajo los vértices son *A*, *B*, *C*, *D*, *E*, *F* y la cara exterior es *G*. una representación del grafo es:



□

32. Coloración de grafos

Ejercicio. 32.1.
¿Es cierto que todo grafo se puede colorear con, a lo sumo, cuatro colores?

SOLUCIÓN. Es resultado es cierto solo para grafos planos, por ejemplo, para colorear K_5 necesitamos al menos 5 colores. □

Capítulo VII

Combinatoria

33. Principio de la suma

Ejercicio. 33.1.
Calcula cuantos números con tres cifras significativas:

(1) no son divisibles por 3,7 ni 11.

(2) son divisibles por 3 y 7.

(3) son divisibles por 3 y 11.

(4) son divisibles por 7 y 11.

(5) son divisibles por 3, 7 y 11.

SOLUCIÓN. Los números que tratamos son del 100 al 999.

De estos el primer múltiplo de 3 es al $102 = 3 \times 34$, y el último es $999 = 3 \times 333$, luego tenemos $333 - 33 = 300$ múltiplos de 3.

El primer múltiplo de 7 es $105 = 7 \times 15$, y el último es $994 = 7 \times 142$, luego tenemos $142 - 14 = 128$ múltiplos de 7.

El primer múltiplo de 11 es $110 = 11 \times 10$, y el último es $990 = 11 \times 90$, luego tenemos $90 - 9 = 81$ múltiplos de 11.

El primer múltiplo de $21 = 3 \times 7$ es $105 = 21 \times 5$, y el último es $987 = 21 \times 47$, luego tenemos $47 - 4 = 43$ múltiplos de 21.

El primer múltiplo de $33 = 3 \times 11$ es $132 = 33 \times 4$, y el último es $990 = 33 \times 30$, luego tenemos $30 - 3 = 27$ múltiplos de 33.

El primer múltiplo de $77 = 7 \times 11$ es $154 = 77 \times 2$, y el último es $924 = 77 \times 12$, luego tenemos $12 - 1 = 11$ múltiplos de 77.

El primer múltiplo de $231 = 3 \times 7 \times 11$ es $231 = 231 \times 1$, y el último es $924 = 231 \times 4$, luego tenemos $4 - 0 = 4$ múltiplos de 231.

(1) Para calcular los que no son divisibles por 3, 7 ni por 11, basta calcular el número total de números, que es $999 - 99 = 900$, y restar el de números que son divisibles por 3, 5 u 11. Este último número es:

$$300 + 128 + 81 - (43 + 27 + 11) + 4 = 432.$$

Entonces el número pedido es: $900 - 431 = 469$.

(2) Entonces serían divisibles por 21. El número pedido es: 43.

(3) Entonces serían divisibles por 33. El número pedido es: 27.

(4) Entonces serían divisibles por 77. El número pedido es: 11.

(5) Entonces serían divisibles por 231. El número pedido es: 4

□

Ejercicio. 33.2.
Si queremos hacer un dominó que vaya desde cero hasta n. ¿Cuántas fichas necesitaremos?

SOLUCIÓN. Las fichas que contienen un 0 son $n+1$. De las restantes las que contienen un 1 son n, y siguiendo de este modo las que contienen un número t son $n-t$. El número de ficha es la suma de estos números hasta el número n. Así pues el número total de fichas es:

$$(n+1) + n + (n-1) + \cdots + 2 + 1 = \frac{(n+2)(n+1)}{2}.$$

□

Ejercicio. 33.3.
Considerando los números que escritos en base 3 *tienen seis dígitos. ¿Cuántos de ellos tienen exactamente dos dígitos iguales a* 0*?*

SOLUCIÓN. La primero cifra ha de ser el dígito 1 ó 2, luego podemos tomar cualquiera de los dígitos 0, 1, ó 2 para las demás cifras. Como queremos que dos de las cifras sean el dígito 0, vamos a ver de cuantas formas podemos elegir dos posiciones de las cinco en que puede aparecer el dígito 0. Este número es $\binom{5}{2} = 10$. Para cada uno de estos casos hay que determinar ahora cuatro posiciones que puede ir ocupadas por cualquiera de los dígitos 1 ó 2. Por tanto cada uno de estas casos presenta 2^4 posibilidades. Como consecuencia el número pedido es: $10 \times 2^4 = 160$. □

Ejercicio. 33.4.
Demostrar que $\mathrm{Card}(A\Delta B) = \mathrm{Card}(a) + \mathrm{Card}(B) - dir\,\mathrm{Card}(A \cap B)$.

SOLUCIÓN. Tenemos que

$$\begin{array}{l} A\Delta B = (A \setminus B) = \cup(A \cap B) \cup (B \setminus A) \text{ y} \\ A = (A \setminus B) \cup (A \cap B) \end{array}$$

son particiones de $A\Delta B$, y A, respectivamente. □

Ejercicio. 33.5.
Sea $A\cup B\cup C = X$. *si* $\mathrm{card}(X) = n$, $\mathrm{card}(A) = n/2$, $\mathrm{Card}(A\cap B) = \mathrm{Card}(A\cap C) = \mathrm{card}(B\cap C) = n/5$ *y* $\mathrm{Card}(A \cap B \cap C) = n/10$. *¿Cuántos elementos tiene el conjunto* $B \cup C$*?*

SOLUCIÓN. Representamos por $|X|$ al cardinal del conjunto X. Tenemos la siguiente igualdad:

$$|X| = |A| + |B| + |C| - |A \cap B| - |A \cap C| - |B \cap C| + |A \cap B \cap C|,$$

entonces

$$n = \frac{n}{2} + |B| + |C| - \frac{n}{5} - \frac{n}{5} - \frac{n}{5} + \frac{n}{10},$$

Se tiene:

$$|B| + |C| = -\frac{n}{2} + \frac{3n}{5} - \frac{n}{10} = \frac{10n - 5n + 6n - n}{10} = n.$$

Por lo tanto resulta:

$$|B \cup C| = |B| + |C| - |B \cap C| = n - \frac{n}{5} = \frac{4n}{5}.$$

□

Ejercicio. 33.6.
¿Cuántos enteros en el conjunto $X = \{1, 2, 3, 4, \ldots, 1000\}$ *son múltiplos de 4 ó de 6?*

SOLUCIÓN. Llamamos C al conjunto de los múltiplos de 4 en X y S al conjunto de los múltiplos de 6.

Si un número es múltiplo de 4 y de 6 es también múltiplo de su mínimo común múltiplo, en este caso de 12, y viceversa. Si llamamos D al conjunto de los múltiplos de 12 en X, tenemos $D = C \cap S$.

El número pedido es $\mathrm{Card}(C \cup S$, y por tanto bastará averiguar los cardinales de C, S y D.

Tenemos:

$$|C| = \frac{1000}{4} = 250,$$
$$|S| = \lfloor \frac{1000}{6} \rfloor = 166,$$
$$|D| = \lfloor \frac{1000}{12} \rfloor = 83.$$

$$|C \cap S| = |C| + |S| - |C \cap S| = |C| + |S| - |D| = 250 + 166 - 83 = 333.$$

□

34. Principio del producto

Ejercicio. 34.1.
Sea $s(n, k)$ el número de subconjuntos del conjunto $\{1, 2, \cdots, n\}$ que tienen cardinal k y que no contienen dos números consecutivos. Demuestra que:

(1) $s(n, k) = s(n - 2, k - 1) + s(n - 1, k)$

(2) $s(n, k) = \binom{n-k+1}{k}$.

SOLUCIÓN. Fijamos un elemento, por ejemplo n. Los subconjuntos que no contienen a n son los subconjuntos de $\{1, 2, \dots, n - 1\}$ de cardinal k que verifican la condición. Los que contienen a n se pueden formar con los subconjuntos de cardinal $k - 1$ de $\{1, 2, \dots, n - 2\}$ que verifican la condición. Tenemos entonces el resultado:

$$s(n, k) = s(n - 2, k - 1) + s(n - 1, k).$$

Para obtener el resultado $s(n, k) = \binom{n-k+1}{k}$ hacemos inducción sobre n y k. Si $k = 1$, entonces se verifica $s(n, 1) = n$ y el resultado es cierto. Si $n = 2$ el resultado es cierto y para todo k. Supongamos que sea cierto para valores menores o iguales que n y para todo $k \leq n$. Veamos que ocurre para $n + 1$.

$$\begin{aligned} s(n, k) &= s(n - 1, k) + s(n - 2, k - 2) \\ &= \binom{n-1-k+1}{k} + \binom{n-2-(k-1)+1}{k-1} \\ &= \binom{n-k}{k} + \binom{n-k}{k-1} \\ &= \binom{n-k+1}{k}. \end{aligned}$$

□

Ejercicio. 34.2.
¿De cuantas formas se pueden obtener 11 aciertos en una quiniela de 14? ¿Y 11 ó más aciertos?

SOLUCIÓN. Dados los 14 aciertos el número de subconjuntos de 11 resultados es $\binom{14}{11}$. Fijados 11 resultados, la forma en que se pueden rellenar las restantes tres casillas para que no se tengan más aciertos es 2^3, luego el número pedido es $\binom{14}{11} \cdots 2^3$.

Si permitimos más aciertos podemos quitar la restricción para rellenar estas tres casillas, y por lo tanto tendremos 3^3 posibilidades, y el número pedido es $\binom{14}{11} \cdot 3^3$. □

Ejercicio. 34.3.
Realizamos una apuesta de quiniela con 2 triples y 4 dobles. Supongamos que hemos acertado los 14 resultados. ¿Cuántas apuestas tenemos con 13, 12, 11 y 10 aciertos?

SOLUCIÓN. Solo tenemos que estudiar qué ocurre con los 6 resultados a que hace mención el enunciado. Primero calculamos el número total de combinaciones: $3^2 \times 2^4 = 144$.

Para tener 13 aciertos debemos cambiar sólo uno de los resultados. Las combinaciones que se tendrán serán: $2 + 2 + 1 + 1 + 1 + 1 = 8$.

Para tener 12 aciertos debemos cambiar dos de los resultados. Tenemos que elegir dos de las casillas, y para esto tenemos las siguientes posibilidades:
$3 + 3$. Solo hay un caso, que tiene $2 \times 2 = 4$ posibilidades.
$3 + 2$. Tenemos $\binom{2}{1}\binom{4}{1} = 2 \times 4 = 8$ casos, cada tiene $2 \times 1 = 2$ posibilidades, el total es: $8 \times 2 = 16$.
$2 + 2$. Tenemos $\binom{4}{2} = 6$ casos y cada uino tiene una sola posibilidad, en total tenemos 6 posibilidades.
El número combinaciones de 12 aciertos es: $4 + 16 + 6 = 26$.

Para tener 11 aciertos debemos cambiar tres de los resultados. Tenemos que elegir tres de las casillas, y para esto tenemos las siguientes posibilidades:
$3 + 3 + 2$. Tenemos $\binom{4}{1} = 4$ casos, y cada uno tiene $2 \times 2 = 4$ posibilidades, en total tenemos: $4 \times 4 = 16$ aciertos.
$3+2+2$. Tenemos $\binom{2}{1}\binom{4}{2} = 2\times 6 = 12$ casos, y cada uno con 2 posibilidades, en total tenemos: $12 \times 2 = 24$ aciertos.
$2 + 2 + 2$. Tenemos $\binom{4}{3} = 4$ casos, cada uno con una sola posibilidad, en total tenemos 4 aciertos.
El número de combinaciones de 11 aciertos es: $16 + 24 + 4 = 44$.

Para tener 10 aciertos debemos cambiar cuatro de los resultados. Tenemos que elegir cuatro de las casillas, y para esto tenemos las siguientes posibilidades:
$3 + 3 + 2 + 2$. Tenemos $\binom{4}{2} = 6$ casos, cada uno con $2 \times 2 = 4$ posibilidades, en total tenemos $6 \times 4 = 24$ aciertos.
$3+2+2+2$. Tenemos $\binom{2}{1}\binom{4}{3} = 2\times 4 = 8$ casos, cada uno con 2 posibilidades, en total tenemos $8 \times 2 = 16$ aciertos.
$2 + 2 + 2 + 2$. Tenemos un solo caso y una sola posibilidad, luego un solo acierto.
El número de combinaciones de 10 aciertos es: $24 + 16 + 1 = 41$. □

35. Variaciones sin repetición

36. Permutaciones

Ejercicio. 36.1.
Ocho miembros de un equipo de baloncesto deben alojarse en un hotel. El hotel dispone de una habitación triple, dos dobles y una individual. ¿De cuántas formas pueden repartirse en las distintas habitaciones?

Supongamos además que de los ocho miembros hay dos que son hermanos y se alojan siempre juntos. ¿De cuántas formas pueden entonces repartirse?

SOLUCIÓN. Tenemos a los ocho jugadores, que evidentemente son distinguibles, y por otro lado las cuatro habitaciones que también son distinguibles. Podemos proceder de la siguiente forma: ordenamos los jugadores, por ejemplo $1, 2, 3, 4, 5, 6, 7, 8$ y las habitaciones *A, B, C* y *D*. Se trata pues de asignar a cada uno de los jugadores la letra de la habitación. Una posible distribución es: *AAABBCCD*. Observar que estamos ante un caso de permutación de ocho elementos de los cuales 3, 2 y 2 con iguales entre sí. El resultado es: $\frac{8!}{3!\,2!\,2} = 1\,680$.

En el caso de dos hermanos fijando uno de ellos solo tenemos que ver la distribución de los siete jugadores restantes. Supongamos que los hermanos son 1 y 2. Vamos a analizar entonces los diferentes casos.
Caso 1. 1 y 2 están en la habitación triple A. En este caso solo tenemos que distribuir a $3, 4, 5, 6, 7, 8$ pero ahora sólo hay una plaza en la habitación triple, y por tanto una posible distribución es: *ABBCCD*. Observar que se trata de permutar seis elementos de los cuales 2 y 2 son iguales entre sí. El resultado es: $\frac{6!}{2|\,2!} = 180$.
Caso 2. 1 y 2 están en una de las habitaciones dobles. Como los dos casos posible se tratan de la misma forma, analizaremos solo el caso en que ocupen la habitación *B*. En este caso sólo tenemos que distribuir a $3, 4, 5, 6, 7, 8$ y las habitaciones de que disponemos son: *A, C* y *D*. Una posible distribución es: *AAACCD*, se trata pues de permutaciones de seis elementos de los cuales 3 y 2 son iguales entre sí. El resultado es: $\frac{6!}{3!\,2!} = 60$.

El resultado final es la suma de los casos hallados: $180 + 60 + 60 = 300$. □

Ejercicio. 36.2.
¿Cuántos números en base 3 tienen exactamente 5 cifras?

(a) 3^4, *(b)* 3^5, *(c)* $2 \cdot 3^4$, *(d)* $5 \cdot 3$.

SOLUCIÓN. (c) □

37. Principio del palomar

Ejercicio. 37.1.
Se eligen 10 números distintos del conjunto $\{1, 2, \dots, 100\}$*. Comprueba que existen al menos 2 tales que* $|\sqrt{x} - \sqrt{y}| \leq 1$.

SOLUCIÓN. Hecha una elección $a_1, \dots, a_{10}$, asignamos a cada a_i el intervalo $(h, h+1]$ al que pertenece su raíz cuadrada. Tenemos 10 intervalos distintos y diez números. Si a dos números distintos les asignamos el mismo intervalo, la diferencia entre sus raíces cuadradas es menor que 1. Si a cada dos números distintos les asignamos intervalos distintos, entonces a uno de los números le asignamos el intervalo $(0, 1]$. Por tanto el número es el $a_i = 1$. Al número al que asignamos el intervalo $(1, 2]$, sea a_j, verifica entonces $|\sqrt{a_i} - \sqrt{a_j}| \leq 1$.

Observar que siempre hay dos elementos a_i, a_j tales que $|\sqrt{a_i} - \sqrt{a_j}| < 1$ salvo en el caso en el que la elección es: 1, 4, 9, 16, 25, 36, 49, 72, 81 y 100. □

38. Combinaciones

Ejercicio. 38.1.
Una apuesta de la Lotería Primitiva consiste en marcar seis números entre 1 y 49. El sorteo se realiza extrayendo 6 de los 49 números, y un séptimo número llamado complementario.

(1) ¿Cuántas apuestas distintas pueden realizarse?.

(2) ¿De cuántas maneras pueden acertarse los seis números de la combinación ganadora?.

(3) ¿De cuántas maneras pueden acertarse cinco números más el complementario de la combinación ganadora?.

(4) ¿De cuántas maneras pueden acertarse cinco números de la combinación ganadora (sin el complementario)?.

(5) ¿De cuántas maneras pueden acertarse cuatro números de la combinación ganadora?.

(6) ¿De cuántas maneras pueden acertarse tres números de la combinación ganadora?.

(7) ¿De cuántas maneras pueden acertarse dos números de la combinación ganadora?.

(8) ¿De cuántas maneras puede acertarse un número de la combinación ganadora?.

(9) ¿De cuántas maneras puede no acertarse ningún número de la combinación ganadora?.

SOLUCIÓN.

(1) Como hay que elegir 6 números, el número total de apuestas posibles es $\binom{49}{6} = 13\,983\,816$, ya que no importa el orden de los números.

(2) De una.

(3) De los seis números primero vemos cuantos grupos de cinco podemos hacer, en este caso $\binom{6}{5} = 6$. Como el sexto número ha de ser el número complementario, no tenemos ninguna posibilidad de elección y el resultado es 6.

(4) De los seis números primero vemos cuantos grupos de cinco podemos hacer, en este caso $\binom{6}{5} = 6$. A cada uno de estos grupos tenemos que agregar un sexto número que no ha de ser el sexto de la combinación ganadora ni el número complementario, luego este número podemos elegirlo de entre $49 - 5 - 1 - 1 = 42$ números, luego el resultado será el producto $6 \times 42 = 252$.

(5) Se trata de ver cuantos grupos de cuatro podemos hacer con los seis números de la combinación ganadora, en este caso $\binom{6}{4} = 15$. Los dos números restantes tenemos que elegirlos de entre los 49 a los que hemos quitado los cuatro elegidos, los dos que faltan para completar la combinación ganadora y el número complementario, esto es, de entre $49 - 4 - 2 - 1 = 42$, luego el resultado es el producto $15 \times \binom{42}{2} = 12\,950$.

(6) Se trata de ver cuantos grupos de tres podemos hacer con los seis números de la combinación ganadora, en este caso $\binom{6}{3} = 20$. Los tres números restantes tenemos que elegirlos de entre los 49 a los que hemos quitado los tres elegidos, los tres que faltan para completar la combinación ganadora y el número complementario, esto es, de entre $49 - 3 - 3 - 1 = 42$, luego el resultado es el producto $20 \times \binom{42}{3} = 229\,600$.

(7) Se trata de ver cuantos grupos de dos podemos hacer con los seis números de la combinación ganadora, en este caso $\binom{6}{2} = 15$. Los cuatro números restantes tenemos que elegirlos de entre los 49 a los que hemos quitado los dos elegidos, los cuatro que faltan para completar la combinación ganadora y el número complementario, esto es, de entre $49 - 2 - 4 - 1 = 42$, luego el resultado es el producto $15 \times \binom{42}{4} = 1\,678\,950$.

(8) Se trata de ver cuantos grupos de uno podemos hacer con los seis números de la combinación ganadora, en este caso $\binom{6}{1} = 6$. Los cinco números restantes tenemos que elegirlos de entre los 49 a los que hemos quitado el elegido, los cinco números que faltan para completar la combinación ganadora y el número complementario, esto es, de entre $49 - 1 - 5 - 1 = 42$, luego el resultado es el producto $6 \times \binom{42}{5} = 5\,104\,008$.

(9) En este caso, al número total de combinaciones tenemos que restar los números que al menos aciertan uno de los números:

$$\begin{aligned}&\binom{49}{6} - 1 - 6 - 6\binom{42}{1} - 15 \times \binom{42}{2} - 20 \times \binom{42}{3} - 15 \times \binom{42}{4} - 6 \times \binom{42}{5}\\ &= 13\,983\,816 - 1 - 6 - 252 - 12\,950 - 229\,600 - 1\,678\,950 - 5\,104\,008\\ &= 6958049\end{aligned}$$

□

Ejercicio. 38.2.
Sea p un número primo. Prueba que si $a, b \in \mathbb{Z}_p$ entonces $(a+b)^p = a^p + b^p$. Comprueba que si m no es primo, entonces $(a+b)^m$ y $a^m + b^m$ son generalmente distintos en $\mathbb{Z}_m$.

SOLUCIÓN. Tenemos $(a+b)^p = \sum_{i=0}^{p} \binom{p}{i} a^i b^{p-i}$, entonces basta ver que para cada entero i tal que $0 < i < p$ el número combinatorio $\binom{p}{i}$ es múltiplo de p, pero por definición $\binom{p}{i} = \frac{p(p-1)\cdots(p-i+1)}{i(i-1)\cdots 2\cdot 1}$, y como todos los factores en el denominador de esta fracción son menores que p, resulta que podemos escribir la fracción como producto de dos números enteros: $p\frac{(p-1)\cdots(p-i+1)}{i(i-1)\cdots 2\cdot 1}$, y tenemos el resultado.

Consideramos $m = 4$ y en $\mathbb{Z}_4$ las clases $a = 1$ y $b = 1$, entonces $a + b = 2$, luego $(a+b)^4 = 0$ y por otro lado $a^4 + b^4 = 1 + 1 = 2$. Como se puede observar son distintos. □

Ejercicio. 38.3.
Comprueba las siguientes identidades con números combinatorios:

(1) $\sum_{k=0}^{n} \binom{n}{k} = 2^n$

(2) $\sum_{k=0}^{n} (-1)^k \binom{n}{k} = 0$

(3) $\sum_{k=0}^{\left[\frac{n}{2}\right]} \binom{n}{2k} = \sum_{k=0}^{\left[\frac{n-1}{2}\right]} \binom{n}{2k+1} = 2^{n-1}$

(4) $\sum_{k=0}^{n} 2^k \binom{n}{k} = 3^n$

(5) $\sum_{k=0}^{n} \binom{n}{k}^2 = \binom{2n}{n}$

(6) $\binom{m+n}{k} = \sum_{i=0}^{k} \binom{m}{i}\binom{n}{k-i}$
(Indicación: $(1+x)^n(1+x)^m = (1+x)^{n+m}$*).*

SOLUCIÓN. HACER □

Ejercicio. 38.4.
¿Cuántos números positivos hay con las cifras en orden estrictamente decreciente?.

SOLUCIÓN. El número mayor que se puede obtener es 9876543210, por lo tanto es un número finito el que andamos buscando. Un número de estos ha de tener como máximo diez cifras, entonces vamos a contar los que hay de n cifras, para $n = 1, 2, \dots, 10$, y después sumamos los resultados. Para dar un número de este tipo con n cifras basta elegir n cifras de $\{1, 2, \dots, 9\}$ y después ordenarlas. Las formas distintas de elegir estas cifras es $\binom{10}{n}$.

El resultado es $\sum_{n=1}^{10} \binom{10}{n} = \binom{10}{1} + \binom{10}{2} + \cdots + \binom{10}{10}$. Una forma de calcular este número es sumar $\binom{10}{0}$, de este forma obtenemos 2^{10}, y el resultada es: $2^{10} - 1$. □

Ejercicio. 38.5.
Queremos formar un comité de 12 personas a escoger entre 10 hombres y 10 mujeres.

(1) *¿De cuántas formas podemos hacerlo?*

(2) *¿Y si queremos que haya igual número de hombres que de mujeres?.*

(3) ¿Y si queremos que haya un número par de hombres?

(4) ¿Y si queremos que haya más mujeres que hombres?.

SOLUCIÓN.

(1) Tenemos que elegir 12 de un total de 20, el número de formas distintas es $\binom{20}{12}$.

(2) Tenemos que elegir 6 hombres, esto se puede hacer de $\binom{10}{6}$ formas distintas y para elegir 6 mujeres tenemos $\binom{10}{6}$ formas distintas. El total es: $\binom{10}{6}\binom{10}{6}$.

(3) Para que hay un número de hombres este número debe ser 2, 4, 6, 8 ó 10. Vamos a analizar cada uno de estos casos. Si hay t hombres entonces hay $12 - t$ mujeres, y en este caso el número de posibilidades es: $\binom{10}{t}\binom{10}{12-t}$. El número total de posibilidades es:

$$\binom{10}{2}\binom{10}{10} + \binom{10}{4}\binom{10}{8} + \binom{10}{6}\binom{10}{6} + \binom{10}{8}\binom{10}{4} + \binom{10}{10}\binom{10}{2}.$$

(4) En este caso el número de mujeres será $7, 8, 9, 10$, para cada uno de los casos ya sabemos el número de posibilidades, por tanto el total es:

$$\binom{10}{7}\binom{10}{5} + \binom{10}{8}\binom{10}{4} + \binom{10}{9}\binom{10}{3} + \binom{10}{10}\binom{10}{2}.$$

□

39. Combinaciones con repetición

Ejercicio. 39.1.
Tenemos 3 cajas y 24 bolas, de las cuales 10 son rojas, 8 azules y 6 verdes. ¿De cuántas formas diferentes podemos repartir las bolas en las cajas?.

SOLUCIÓN. Se trata de hacer hasta 3 grupos con las bolas de cada uno de los colores, y posteriormente componer las distribuciones obtenidas.

Para hacer tres grupos con las 10 bolas rojas incluimos dos nuevas bolas, que serán las separadores para los tres grupos que se trata de formar, entonces hay que elegir ahora los dos separadores de un total de 12 posibilidades; el número es: $CR(10,3) = \binom{12}{2}$. En el caso de las 8 bolas azules el resultado es: $CR(8,3) = \binom{10}{2}$. En el caso de las 6 bolas verdes el resultado es: $CR(6,3) = \binom{8}{2}$.

El total de distribuciones posibles es:

$$CR(10,3)CR(8,3)CR(6,3) = \binom{12}{2} \cdot \binom{10}{2} \cdot \binom{8}{2} = 83\,160.$$

Observar que hemos supuesto que las cajas se pueden distinguir una de otra. □

Ejercicio. 39.2.
Se lanzan tres dados indistinguibles. ¿Cuántos posibles resultados pueden salir?. ¿Y si se lanzan n dados?.

SOLUCIÓN. Supongamos que los dados tienen seis caras numeradas de 1 a 6. Entonces los resultados posibles son los siguientes:

1	1	1	1	1	1	2	2	2	2	2	3	3	3	3	4	4	4	5	5	6
1	2	3	4	5	6	2	3	4	5	6	3	4	5	6	4	5	6	5	6	6

Son en total 21 posibles resultados. Para hacerlo basta considerar las dos tiradas como elementos indistinguibles, cada uno de los números de las caras del cubo como una caja, de forma que una tirada será lu mismo que distribuir dos elementos indistinguibles en 6 cajas distinguibles. Esto ya lo hemos estudiado, y el resultado es $CR(2,6) = \binom{2+6-1}{6-1} = \binom{7}{5} = \binom{7}{2} = 21$.

El caso de n dados se hace igual, en este caso tendríamos n objetos indistinguibles que hay que distribuir en 6 cajas; el resultado es: $CR(n,6) = \binom{n+6-1}{6-1} = \binom{n+5}{5} = \frac{n(n-1)(n-2)(n-3)(n-4)}{5!} = \frac{n(n-1)(n-2)(n-3)(n-4)}{120}$. □

Ejercicio. 39.3.
¿Cuántos números de cinco dígitos (en base 10*) empiezan por* 4*, terminan en* 5 *y sus cifras suman* 18*?*

SOLUCIÓN. El número debe comenzar por 4 y acabar en 5, entonces solo quedan tres posibles variables que cubrir; un tal número es de la forma $4XYZ5$. Como la suma $4+X+Y+Z+5$ ha de ser 18, resulta $X+Y+Z=9$, y por tanto los valores de X, Y y Z son los de las posibles soluciones naturales de la ecuación $X+Y+Z=9$. El número de soluciones naturales de esta ecuación es $\binom{9+3-1}{3-1}=\binom{11}{2}=66$. □

Ejercicio. 39.4.
Las formas distintas en las que 12 bolas iguales pueden repartirse entre tres cajas numeradas son:

(a) $\binom{12}{3}$, *(b)* $\binom{14}{2}$, *(c)* $\binom{12}{3}\cdot 3!$, *(d)* $\binom{15}{3}$.

SOLUCIÓN. (b) □

40. Permutaciones con repetición

Ejercicio. 40.1.
¿Cuántos números de 6 cifras, escritos en binario, no contienen la secuencia 101?

SOLUCIÓN. Cada número de 6 cifras en binario es de la forma 1 _ _ _ _ _, en donde cada posición puede llenarse con los dígitos 0 ó 1, por tanto el número de números es $2^5 = 32$.

La secuencia 101 se puede conseguir en los siguientes casos:

Caso 1. 101 _ _ _ Las tres posiciones restantes se pueden rellenar de $2^3 = 8$ formas diferentes.

Caso 2. 1 _ 101 _ Las dos posiciones restantes se pueden rellenar de $2^2 = 4$ formas diferentes.

Caso 3. 1 _ _ 101 Las dos posiciones restantes se pueden rellenar de $2^2 = 4$ formas diferentes.

Por tanto el número de números que no contienen la secuencia 101 es:

$$2^5 - (2^3 + 2^2 + 2^3) = 32 - (8 + 4 + 4) = 32 - 16 = 16.$$

□

Bibliografía

[1] N. L. Biggs, *Matemática discreta*, Vicens-Vives, 1994.

[2] F. García Merayo, G. Hernández Peñalver, A. Nevot Luna, *Problemas resueltos de matemática discreta*, Thonson, 2003.

[3] Ralph P. Grimaldi, *Matemática discreta y combinatoria: una introducción con aplicaciones*, Addison-Wesley Iberoamericana, 1998.

[4] Paul R. Halmos, *Teoría intuitiva de conjuntos*, Compañía Editorial Continental, 1982.

[5] R. Johnsonbaugh, *Matemáticas discretas*, Iberoamericana, 1988.

[6] J. D. Lipson, *Elements of Algebra and Algebraic Computing*, Benjamin/Cummings, 1981

[7] N. Peermingeat, *Algebra de Boole. Teoría, métodos de cálculo. Aplicaciones*, Alianza editorial, 1988.

[8] Robin J. Wilson. *Introduction to Graph Theory*, Longman Scientific and Technical, 1999.

[9] K. Rosen, *Matemática Discreta y sus Aplicaciones*, 5ª Edición, McGraw-Hill, 2004.

[10] K. A. Ross, C. R. B. Wright, *Discreta Mathematics*, Prentice-Hall, 1992.

Índice alfabético