UNIVERSIDAD NACIONAL DE CÓRDOBA

FACULTAD DE MATEMÁTICA, ASTRONOMÍA Y FÍSICA

SERIE " C "

TRABAJOS DE MATEMATICA

Nº 32/04

Álgebra I – Matemática Discreta I

N. Patricia Kisbye – Roberto Miatello

Editores: Jorge R. Lauret–Elvio A. Pilotta

CIUDAD UNIVERSITARIA – 5000 CÓRDOBA

REPÚBLICA ARGENTINA

Índice general

Parte 1

Notas de Álgebra I - Matemática Discreta I

Introducción

Estas notas tienen la intención de ofrecer al estudiante un curso introductorio de Álgebra. Las mismas han sido utilizadas repetidas veces como material de apoyo para el dictado de las materias Álgebra I y Matemática Discreta I de la Facultad de Matemática, Astronomía y Física de la UNC. Comprenden los siguientes temas: axiomas de los números reales, los números naturales y el principio de inducción, técnicas de conteo, los números enteros, divisibilidad, números primos, congruencias y grafos.

La guía de ejercicios que se encuentra en la Parte 2 ha sido elaborada en base a la recopilación y selección de ejercicios propuestos en diversas oportunidades.

Esperamos que estas notas sean útiles y accesibles al estudiante para entender las primeras herramientas del Álgebra, y al mismo tiempo agradecemos sugerencias y comentarios a fin de mejorarlas.

Los autores.

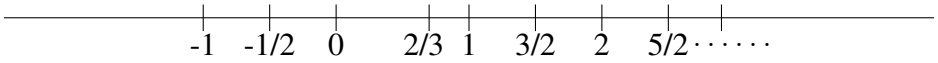
CAPÍTULO 1

Los números naturales

1. Introducción

En esta sección y la siguiente daremos una breve introducción a los números reales, desde un punto de vista intuitivo y luego formalmente a partir de los axiomas de números reales. Acordamos denotar con $\mathbb{N}$, $\mathbb{Z}$ y $\mathbb{Q}$ al conjunto de los números naturales, enteros y racionales respectivamente, y con $\mathbb{R}$ al conjunto de los números reales. En las secciones §3 y §4 daremos la definición y propiedades de conjunto inductivo e introduciremos el conjunto $\mathbb{N}$ de los números naturales.

Al igual que los números naturales y enteros, los números racionales se representan en la recta de la manera usual. Por ejemplo:



Si bien existen infinitos números racionales, los puntos correspondientes a los números racionales no llenan la recta. Como es bien sabido, un segmento de longitud $\sqrt{2}$ no se corresponde con ningún número racional, ya que los números racionales no bastan para medir la diagonal de un cuadrado cuyo lado es de longitud igual a 1. La introducción de los números irracionales remedia este problema, de tal modo que los números racionales y los irracionales conforman el sistema de los números reales, con lo cual se tiene una correspondencia biunívoca entre los números reales y los puntos de la recta.

Si nos referimos a la representación de los números reales en el sistema decimal, los números racionales se pueden caracterizar por ser aquellos que admiten una expresión decimal periódica, por ejemplo:

$$\begin{aligned} \frac{7}{2} &= \frac{35}{10} = 3{,}5 \\ \frac{4}{3} &= 1{,}333\ldots, \\ 0,234234234\ldots &= 234 \times (0{,}001001001\ldots) = 234 \times \frac{1}{999} = \frac{234}{999} \end{aligned}$$

Las expresiones decimales no periódicas, en cambio, se corresponden con los números irracionales. Por ejemplo, el número

$$\alpha = 2,101001000100001000001\ldots$$

no posee ningún período, luego es irracional. Es fácil construir una infinidad de números irracionales, por ejemplo, basta tomar $\alpha + q$ donde q es cualquier número racional. Así vemos que

$$2,201001000100001000001\ldots, \qquad 2,301001000100001000001\ldots,$$

$$2,401001000100001000001\ldots, \qquad 2,501001000100001000001\ldots,$$

son todos números irracionales. En realidad puede verse que hay *muchos más* números irracionales que racionales (en un sentido preciso) pero la demostración de esto es bastante más difícil.

En el conjunto de los números reales están definidas las operaciones de suma, multiplicación y división. Esto quiere decir que si a y b son dos números reales, entonces la suma $a + b$ y la multiplicación ab dan como resultado números reales, y si además b es distinto de 0 entonces la división de a por b, $\dfrac{a}{b}$, es un número real.

Hasta aquí hemos presentado a los números reales de una manera intuitiva, refiriéndonos a su representación en la recta y a su escritura en notación decimal. Sin embargo, para introducir la noción de *números reales* desde el punto de vista de la matemática, debemos ser más precisos en la definición. Existen distintas formas de definir el conjunto de los números reales de una manera formal, en estas notas elegimos la siguiente.

Para formalizar la definición de los números reales, se acostumbra introducirlos definiéndolos como un conjunto dotado de dos operaciones y una relación de orden que satisfacen ciertos axiomas. Los axiomas son enunciados o sentencias que no requieren demostración y se aceptan como tales. Toda otra propiedad de los reales que no esté enunciada en la lista de los axiomas deberá deducirse a partir de este conjunto inicial de propiedades básicas. Es posible demostrar la existencia de un tal conjunto con dos operaciones $+$ y $\cdot$ y un orden $<$, pero esta demostración no será incluida en estas notas. Para simplificar el enunciado de la lista inicial de axiomas será conveniente fijar algunas notaciones de la teoría de conjuntos y de la lógica elemental, que serán utilizadas sistemáticamente a lo largo del curso.

Notación: Dados dos conjuntos X e Y se denotará:

$$\begin{aligned}
x \in X &: x \text{ pertenece a } X,\\
X \cup Y &= \{z \mid z \in X \text{ ó } z \in Y\} \quad \text{unión de } X \text{ con } Y,\\
X \cap Y &= \{z \mid z \in X \text{ y } z \in Y\} \quad \text{intersección de } X \text{ con } Y,\\
\Rightarrow &: \text{ implica , entonces}\\
\Leftrightarrow &: \text{ si y sólo si,}\\
\forall\, x \in X &: \text{para todo } x \text{ perteneciente a } X,\\
\exists\, x \in X &: \text{existe } x \text{ perteneciente a } X,\\
X \subseteq Y &: X \text{ está incluido en } Y, \text{ es decir,} \forall x \in X,\ x \in Y\\
X \times Y &= \{(x,y) \mid x \in X,\ y \in Y\} : \text{producto cartesiano de } X \text{ por } Y.
\end{aligned}$$

2. Los números reales

Llamaremos *conjunto de números reales* y lo denotaremos con $\mathbb{R}$ a un conjunto en el cual hay definidas dos operaciones, suma $(+)$ y producto o multiplicación $(\cdot)$, y una relación de orden $(<)$:

$$\begin{aligned}
+ :\ \mathbb{R} \times \mathbb{R} &\mapsto \mathbb{R} & \qquad \cdot :\ \mathbb{R} \times \mathbb{R} &\mapsto \mathbb{R}\\
(a,b) &\mapsto a+b & \qquad (a,b) &\mapsto a \cdot b
\end{aligned}$$

Estas operaciones junto con la relación de orden cumplen ciertas propiedades o axiomas que listamos a continuación.

S1) *Ley asociativa de la suma:*

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

para todo a, b y c en $\mathbb{R}$.

S2) *Ley conmutativa de la suma:*

$$a + b = b + a,$$

para todo a y b en $\mathbb{R}$.

S3) *Existencia de cero:* Existe un número real 0 tal que para todo $a \in \mathbb{R}$,

$$a + 0 = a.$$

S4) *Existencia de opuesto:* Para cada $a \in \mathbb{R}$, existe $a' \in \mathbb{R}$, tal que

$$a + a' = 0.$$

P1) *Ley asociativa del producto:*

$$a \cdot (b \cdot c) = (a \cdot b) \cdot c,$$

para todo a, b y c en $\mathbb{R}$.

P2) *Ley conmutativa del producto:*

$$a \cdot b = b \cdot a,$$

para todo a y b en $\mathbb{R}$.

P3) *Existencia de identidad:* Existe un número real, 1, con $1 \neq 0$, tal que para todo $a \in \mathbb{R}$ se satisface

$$a \cdot 1 = a.$$

P4) *Existencia de inverso:* para cada $a \in \mathbb{R}$, $a \neq 0$, existe $a'' \in \mathbb{R}$ tal que

$$a \cdot a'' = 1.$$

D) *Ley distributiva:* Para todo $a,\ b,\ c \in \mathbb{R}$, se satisface:

$$a \cdot (b + c) = a \cdot b + a \cdot c.$$

O1) *Ley de tricotomía:* dados a, b en $\mathbb{R}$, vale una y sólo una de las siguientes afirmaciones:

$$a = b, \quad a < b \quad \text{o} \quad b < a.$$

O2) *Ley de transitividad:* Para todo a, b y c en $\mathbb{R}$ se verifica:

$$a < b \text{ y } b < c \Rightarrow a < c.$$

CS) *Consistencia de la relación de orden con la suma:* Para todo a, b, c en $\mathbb{R}$ se tiene:

$$a < b \Rightarrow a + c < b + c.$$

CP) *Consistencia de la relación de orden con el producto:* Para todo a, b, c en $\mathbb{R}$ se tiene:

$$a < b \text{ y } 0 < c \Rightarrow a \cdot c < b \cdot c.$$

Existe un último axioma, llamado el axioma del supremo, que no enunciaremos pues no será necesario en este curso. Observamos que suelen enunciarse los axiomas de orden (O1), (O2), (CS) y (CP) de un modo ligeramente diferente, pero el sistema de axiomas resultantes es equivalente al que presentamos en estas Notas.

Recordamos que toda otra propiedad de los números reales deberá deducirse o demostrarse a partir de estos axiomas, aún cuando pueda parecer por demás obvia. Una *prueba* o *demostración* es la deducción de una propiedad a partir de axiomas u otras propiedades ya establecidas. A seguir mostraremos cómo deducir algunas propiedades conocidas de los números reales.

LEMA 2.1. *El cero es único.*

PRUEBA. Este enunciado afirma que existe un único número real que cumple la propiedad S3. Para demostrar esta afirmación, seleccionamos un número real 0^* que sea neutro para la suma, es decir que satisface $a + 0^* = a$, $\forall a \in \mathbb{R}$. Por el axioma S3, existe un número real denotado por 0 que es neutro para la suma. Por lo tanto, por el axioma S3, $0^* + 0 = 0^*$, y por hipótesis $0 + 0^* = 0$. Luego

$$\begin{aligned} 0^* &= 0^* + 0, \text{ por S3} \\ 0^* + 0 &= 0 + 0^* \text{ por S2,} \\ 0 + 0^* &= 0, \text{por hipótesis,} \end{aligned}$$

y entonces $0^* = 0$ por transitividad. En consecuencia existe un único elemento neutro para la suma, y es el 0. □

LEMA 2.2. *El opuesto de un elemento $a \in \mathbb{R}$ es único.*

PRUEBA. Por el axioma S4 sabemos que dado un número real a, existe un número a' llamado opuesto de a para el cual se cumple que

$$a + a' = 0.$$

Para mostrar que a' es único con tal propiedad suponemos que existe $\tilde{a}$ tal que $a + \tilde{a} = 0$. Entonces

$$\begin{aligned} \tilde{a} &= \tilde{a} + 0 \quad \text{por S3} \\ a + 0 &= \tilde{a} + (a + a') \quad \text{por S4} \\ \tilde{a} + (a + a') &= (\tilde{a} + a) + a' \quad \text{por S1,} \\ (\tilde{a} + a) + a' &= 0 + a' \quad \text{por hipótesis, y} \\ 0 + a' &= a' \quad \text{S3 y S2.} \end{aligned}$$

Por transitividad se sigue que $\tilde{a} = a'$ y por lo tanto a tiene un único opuesto. □

El opuesto de a se denotará $-a$. Similarmente, se escribirá $b - a$ para denotar $b + (-a)$.

La siguiente propiedad afirma que si un sumando aparece en ambos miembros de una igualdad, entonces el mismo puede cancelarse.

LEMA 2.3. *Dados a, b y $c \in \mathbb{R}$, si $a + b = a + c$ entonces $b = c$.*

PRUEBA. Si $a + b = a + c$, sumamos a ambos miembros de la igualdad el opuesto de a y aplicamos los axiomas S1, S4 y S3 respectivamente:

$$\begin{aligned} (-a) + (a + b) &= (-a) + (a + c) \\ ((-a) + a) + b &= ((-a) + a) + c \\ 0 + b &= 0 + c \\ b &= c. \end{aligned}$$

□

A continuación, listamos un conjunto de propiedades conocidas de los números reales. Las demostraciones respectivas utilizan los axiomas y algunas propiedades que acabamos de probar. Invitamos al lector a reconocer estos axiomas y propiedades utilizados y a ensayar pruebas alternativas.

LEMA 2.4.

(i) $a \cdot 0 = 0$, $\forall a \in \mathbb{R}$.

(ii) *Dados a y $b \in \mathbb{R}$, si $a \cdot b = 0$ entonces $a = 0$ ó $b = 0$.*

(iii) *Regla de los signos: dados* a *y* $b \in \mathbb{R}$*, entonces* $(-a) \cdot b = a \cdot (-b) = -(a \cdot b)$ *y* $(-a) \cdot (-b) = a \cdot b$*.*

(iv) *Dados* a *y* $b \in \mathbb{R}$*, entonces* $a^2 = b^2 \Leftrightarrow a = b$ *ó* $a = -b$*. En particular,* $(-a)^2 = a^2$*.*

(v) $a^2 = 1 \Leftrightarrow a = 1$ *ó* $a = -1$*,*

(vi) *Si* $a \in \mathbb{R}$ *entonces* $(-1) \cdot a = -a$*.*

PRUEBA. (i) Sabemos que $0 + 0 = 0$. Luego $a \cdot 0 + a \cdot 0 = a \cdot (0 + 0) = a \cdot 0$. Sumando el opuesto de $a \cdot 0$ a ambos miembros de la igualdad $a \cdot 0 + a \cdot 0 = a \cdot 0$, concluimos que $a \cdot 0 = 0$.

(ii) Si $a = 0$, la afirmación está demostrada. Si $a \neq 0$, entonces $\exists\, a''$ tal que $a'' \cdot a = 1$. Luego

$$b = 1 \cdot b = (a'' \cdot a) \cdot b = a'' \cdot (a \cdot b) = a'' \cdot 0 = 0 \quad \text{lo que implica } b = 0.$$

(iii) Notemos que

$$(-a) \cdot b + a \cdot b = ((-a) + a) \cdot b = 0 \cdot b = 0,$$

luego $(-a) \cdot b$ es el opuesto de $a \cdot b$, es decir que $(-a) \cdot b = -(a \cdot b)$. De una manera análoga se muestra que $a \cdot (-b) = -(a \cdot b)$.

Usando esto vemos que

$$(-a) \cdot (-b) = -(a \cdot (-b)) = -(-(a \cdot b)) = a \cdot b.$$

(iv) Primero notamos que $(a - b) \cdot (a + b) = a^2 - b^2$, luego

$$\begin{aligned} a^2 - b^2 &= 0 \quad \Leftrightarrow \\ (a - b) \cdot (a + b) &= 0 \quad \Leftrightarrow \\ a - b = 0 \quad &\text{ó} \quad a + b = 0 \quad \Leftrightarrow \\ a = b \quad &\text{ó} \quad a = -b. \end{aligned}$$

(v) Aplicamos el item anterior tomando $b = 1$. Entonces $a^2 = 1^2$ si y sólo si $a = 1$ o $a = -1$.

(vi) De (iii) tenemos que $(-1) \cdot a = -(1 \cdot a) = -a$. □

El inverso de un número real a no nulo también es único, pues si $a \cdot a'' = 1$ y $a \cdot c = 1$ entonces

$$c = 1 \cdot c = (a'' \cdot a) \cdot c = a'' \cdot (a \cdot c) = a'' \cdot 1 = a''.$$

Llamaremos a a'' el *inverso* de a, y lo denotaremos por a^{-1} o por $\frac{1}{a}$.

El siguiente teorema incluye algunas de las propiedades conocidas de la relación de orden. La notación $x > y$ significa que $y < x$ y además $x \geq y$ significa que $x > y$ ó $x = y$. Notemos que la propiedad (ii) que afirma que $0 < 1$; si bien puede parecer evidente, como no figura en la lista inicial de axiomas requiere una demostración.

TEOREMA 2.5.

(i) $a < b \Leftrightarrow -b < -a$, *para todo* a, b *reales,*

(ii) $0 < 1$,

(iii) $a < b$ *y* $c < d \Rightarrow a + c < b + d$, $\forall a,\ b,\ c,\ d \in \mathbb{R}$,

(iv) *Si* $a \in \mathbb{R}$, *entonces* $a^2 \geq 0$; $a^2 = 0$ *si y sólo si* $a = 0$.

(v) *sean* $a,\ b \in \mathbb{R}$, $a^2 + b^2 = 0 \Leftrightarrow a = b = 0$,

(vi) *no existe ningún número real tal que* $x^2 + 1 = 0$,

(vii) *si* $a \in \mathbb{R}$, *entonces*

$$\begin{cases} a > 0 \Rightarrow a + \frac{1}{a} \geq 2 \\ a < 0 \Rightarrow a + \frac{1}{a} \leq -2 \end{cases}.$$

PRUEBA. (i) Si $a < b$ entonces

$$\begin{aligned} a + (-a) &< b + (-a) \\ 0 &< b + (-a) \\ -b + 0 &< (-b) + (b + (-a)) \quad \text{y} \qquad (-b) + (b + (-a)) = (-b + b) + (-a) = 0 + (-a) \\ -b &< -a \end{aligned}$$

(ii) Observamos que una vez probada (iv), (ii) sigue de inmediato pues $1 = 1^2$. Alternativamente, damos la siguiente demostración.

Sabemos que $0 \neq 1$ implica que $0 < 1$ ó $1 < 0$. Entonces,

$$1 < 0 \Rightarrow 1 + (-1) < 0 + (-1) \quad \Rightarrow \quad 0 < -1,$$

luego podemos multiplicar los miembros de la desigualdad $1 < 0$ por (-1):

$$(-1) \cdot 1 < (-1) \cdot 0 = 0 \quad \Rightarrow \quad -1 < 0$$

lo cual es absurdo. Por lo tanto $0 < 1$.

(iii) Si $a < b$ entonces $a + c < b + c$, y si $c < d$ entonces $b + c < b + d$. Luego, por la ley de transitividad se sigue que $a + c < b + d$.

(iv) Si $a \neq 0$, entonces $a > 0$ o $a < 0$.

Si $a > 0$ entonces $a \cdot a > a \cdot 0$, es decir, $a^2 > 0$.

Si $a < 0$ entonces $-a > 0$. Luego $(-a) \cdot (-a) > 0$ o bien $(-a)^2 > 0$. Por la regla de los signos (Lema 2.4, (iii)) tenemos que $(-a)^2 = a^2$, luego $a^2 > 0$ para cualquier $a \neq 0$.
(v) Sean a y b tales que $a^2 + b^2 = 0$. Si $a \neq 0$ entonces por el ítem anterior $a^2 > 0$ y por lo tanto

$$a^2 + b^2 > 0 + b^2 \geq 0,$$

y análogamente, si $b \neq 0$ resulta

$$a^2 + b^2 > a^2 + 0 \geq 0.$$

Por lo tanto debe cumplirse $a = 0$ y $b = 0$. La recíproca es clara.
(vi) Para todo $x \in \mathbb{R}$, se cumple $x^2 \geq 0$, luego

$$x^2 + 1 \geq 0 + 1 = 1 > 0.$$

(vii) Sabemos por (iv) que $(a-1)^2 \geq 0$. Luego $a^2 - 2a + 1 \geq 0$ o lo que es lo mismo

$$a^2 + 1 \geq 2a. \tag{1}$$

Si $a > 0$ entonces $\frac{1}{a} > 0$ y multiplicando ambos miembros de la desigualdad (1) por $\frac{1}{a}$ concluimos que

$$a + \frac{1}{a} > 2.$$

Si $a < 0$ entonces $-a > 0$. Por lo tanto

$$-a - \frac{1}{a} \geq 2, \qquad \text{es decir} \qquad a + \frac{1}{a} \leq -2.$$

□

3. Principio de Inducción

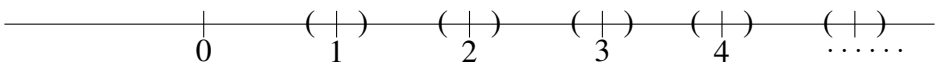
En el conjunto de los números reales tenemos dos elementos distinguidos: 0 y 1. Si operamos con el 0 por la suma obtenemos el mismo número, sin embargo no ocurre lo mismo si sumamos 1. Si sumamos 1 a un número real a obtenemos $a + 1$, que es un número distinto de a y se llama su *siguiente* o *sucesor*. Por ejemplo: $1 + 1$ es distinto de 1 (porque el $1 \neq 0$) y lo denotamos con 2; $2 + 1 = 3$, $2 \neq 3$, $3 \neq 1$ y así siguiendo. De esta manera es como *intuitivamente* se pueden obtener todos los *números naturales*. Pero nos interesa dar una definición más formal de número natural, para ello introduciremos la definición de conjunto inductivo:

DEFINICIÓN 3.1. Un subconjunto H de $\mathbb{R}$ se dice *inductivo* si $1 \in H$ y si $k \in H$ implica que $k + 1 \in H$.

Dicho de otro modo, H es inductivo si 1 es un elemento de H y si para cada elemento x de H, el sucesor $x+1$ también pertenece a H.

EJEMPLO 3.2.

1. $\mathbb{R}$ es inductivo,
2. $\mathbb{R}_{>0}$ es inductivo, $\mathbb{R}_{\geq 1}$ es inductivo,
3. $X = [1,2] = \{x \mid 1 \leq x \leq 2\}$ no es inductivo, pues si bien $1 \in X$, tenemos que $2 \in X$ y $2+1 > 2$, por lo que $2+1 \notin X$,
4. la unión infinita de los siguientes intervalos abiertos es un conjunto inductivo:



LEMA 3.3. *La intersección arbitraria de conjuntos inductivos es un conjunto inductivo.*

PRUEBA. Consideremos una familia de subconjuntos inductivos de $\mathbb{R}$. A cada uno de estos conjuntos le asignamos un índice i, con $i \in I$, y lo denotamos con X_i. Sea X la intersección de todos estos conjuntos. Escribimos entonces

$$X = \bigcap_{i \in I} X_i = \{x \mid x \in X_i, \forall i \in I\}$$

Como $1 \in X_i$, para todo $i \in I$, entonces $1 \in X$.
Veamos que el sucesor de cada elemento de X también pertenece a X. En efecto, si $k \in X$ significa que $k \in X_i$ para todo $i \in I$. Como cada X_i es inductivo, esto implica que $k+1 \in X_i$ para cada $i \in I$ y por lo tanto $k+1$ pertenece a cada X_i y por lo tanto a X. Se sigue que el conjunto X es inductivo. □

Dado que el número 1 pertenece a todos los conjuntos inductivos, la intersección de todos los conjuntos inductivos no es vacía.

DEFINICIÓN 3.4 (El conjunto $\mathbb{N}$). Definimos el conjunto $\mathbb{N}$ de *números naturales* como la intersección de todos los subconjuntos inductivos de $\mathbb{R}$.

Por el lema anterior, $\mathbb{N}$ es un conjunto inductivo. De hecho es el *menor* subconjunto inductivo de $\mathbb{R}$ en el sentido que $\mathbb{N}$ es un subconjunto inductivo y está contenido en todos los subconjuntos inductivos de $\mathbb{R}$.

Visualmente, si denotamos $2 = 1 + 1$, $3 = (1 + 1) + 1$, $4 = ((1 + 1) + 1) + 1$, ... e intersecamos todos los conjuntos inductivos

nos quedan 1, $1 + 1$, $(1 + 1) + 1$, $((1 + 1) + 1) + 1$, ...

Hemos definido al conjunto de los números naturales como intersección de conjuntos inductivos. Otra forma es caracterizar al conjunto de los números naturales por medio del llamado *principio de inducción*:

TEOREMA 3.5. *Sea H un subconjunto de $\mathbb{N}$ tal que:*

(i) $1 \in H$,

(ii) *si $h \in H$ entonces $h + 1 \in H$.*

Entonces $H = \mathbb{N}$.

En efecto, (i) y (ii) implican que H es inductivo, luego $H \supseteq \mathbb{N}$. Pero como por hipótesis $H \subset \mathbb{N}$, entonces debe ser $H = \mathbb{N}$.

El principio de inducción es útil para probar la veracidad de propiedades relativas a los números naturales. Por ejemplo, consideremos las siguientes propiedades $P(n)$, $Q(n)$ y $R(n)$:

(a) $P(n)$ es la propiedad: $2n - 1 < n^2 + 1$,

(b) $Q(n)$ es la afirmación: *si n es par entonces n es divisible por 4*,

(c) $R(n)$ es la afirmación: $2^n < n - 1$.

Intuitivamente notamos que $P(n)$ es verdadera para cualquier n natural, $Q(n)$ lo es para algunos valores de n y es falsa para otros y $R(n)$ es falsa para todo valor de n (ver Ejemplo 3.7). Sin embargo, para verificar realmente que la propiedad $P(n)$ es verdadera para todo n natural no podemos hacerlo probando para cada n en particular. Resulta entonces muy útil la siguiente versión equivalente del principio de inducción.

TEOREMA 3.6. *Sea $P(n)$ una propiedad de $n \in \mathbb{N}$ tal que:*

1. *$P(1)$ es verdadera*
2. *Para todo $k \in \mathbb{N}$, $P(k)$ verdadera implica $P(k + 1)$ verdadera.*

Entonces $P(n)$ es verdadera para todo $n \in \mathbb{N}$.

PRUEBA. Basta tomar

$$H = \{n \in \mathbb{N} \mid P(n) \text{ es verdadera } \}.$$

Entonces H es un subconjunto de $\mathbb{N}$ y las condiciones (1) y (2) nos dicen que es un conjunto inductivo. Por el Teorema 3.5 se sigue que $H = \mathbb{N}$, es decir que $P(n)$ es verdadera para todo n natural. □

El principio de inducción admite la siguiente interpretación visual. Supongamos que tenemos una cantidad indefinida de piezas de dominó paradas en fila, una atrás de la otra. El principio de inducción afirma que si sabemos que la primera pieza se cae, y que cada vez que cae una pieza, cae la siguiente, entonces deberán caer eventualmente todas las piezas.

Enunciamos a continuación algunas propiedades de los números naturales, y la demostración de su veracidad usando el principio de inducción.

EJEMPLO 3.7. Probar que $2^n > n$, para todo n natural.

SOLUCIÓN. Sea $P(n)$ la siguiente propiedad del número natural n, $P(n) : 2^n > n$. Entonces $P(1)$ es verdadera pues $2^1 > 1$. Veamos ahora que si k es un número natural tal que $P(k)$ es verdadera, entonces $P(k+1)$ es verdadera. Esta condición supuesta, es decir, $P(k)$ verdadera, la llamaremos *hipótesis inductiva*.

Efectivamente, supongamos que $2^k > k$. Entonces $2^{k+1} = 2 \cdot 2^k = 2^k + 2^k$ y $2^k + 2^k > k + k$ por hipótesis inductiva. Dado que $k + k \geq k + 1$ para todo $k \in \mathbb{N}$, por transitividad se sigue que

$$2^{k+1} > k + 1.$$

Por lo tanto $P(n)$ es verdadera para todo n natural. □

EJEMPLO 3.8. Demostrar que $n^2 + 3 \geq n$ para todo n natural.

SOLUCIÓN. Sea $P(n)$ la propiedad: $n^2 + 3 \geq n$.

$P(1)$ es la afirmación $1^2 + 3 \geq 1$, esto es $4 \geq 1$, que es una afirmación verdadera.

Asumamos ahora que $P(k)$ es verdadera para cierto k, es decir que $k^2 + 3 \geq k$. Veamos que esto implica que $P(k+1)$ es verdadero. En efecto:

$$(k+1)^2 + 3 = k^2 + 2k + 1 + 3 = (k^2 + 3) + 2k + 1 \geq (k^2 + 3) + 1 \geq k + 1,$$

luego se concluye que $P(n)$ es cierta para todo n natural. □

En algunos casos, una determinada propiedad $P(n)$ se cumple solamente para todo n mayor o igual que un cierto número natural N. Por ello resulta útil contar con una versión más general del principio de inducción.

TEOREMA 3.9. *Sea $P(n)$ una propiedad del número natural n, y sea $N \in \mathbb{N}$. Si $P(N)$ es verdadera, y para todo $k \geq N$ vale que $P(k)$ implica $P(k+1)$, entonces $P(n)$ es verdadera para todo $n \geq N$.*

PRUEBA. Sea $H = \{n \in \mathbb{N} \mid P(n+N-1)\text{es verdadera}\}$.

Si probamos que H es un conjunto inductivo, habremos demostrado que $P(n+N-1)$ es verdadera para todo n natural, o equivalentemente que $P(m)$ es verdadera para todo $m \geq N$.

En efecto, $1 \in H$ puesto que $P(1+N-1) = P(N)$, y $P(N)$ es verdadera por hipótesis. Si ahora suponemos $k \in H$, entonces $k+N-1 \geq N$, y por lo tanto $P(k+N)$ es verdadera. Luego $k+1 \in H$ y se sigue que H es un conjunto inductivo.

□

EJEMPLO 3.10. Para todo $n \geq 3$ se cumple que $2^n > 2n+1$.

PRUEBA. Consideramos la propiedad $P(n) : 2^n > 2n+1$ y probemos que $P(n)$ es verdadera para todo $n \geq 3$. (Notemos que $P(1)$ y $P(2)$ son falsas).

Vemos que $P(3)$ es verdadera puesto que $2^3 = 8$ y $8 > 2 \cdot 3 + 1$. Si suponemos que $P(k)$ es verdadera para algún $k \geq 3$, entonces

$$2^{k+1} = 2^k + 2^k > (2k+1) + (2k+1) = 2(k+1) + 2k > 2(k+1) + 1,$$

por lo que $P(n)$ es verdadera para todo $n \geq 3$. □

La siguiente proposición enuncia las propiedades más básicas de las operaciones entre números naturales.

PROPOSICIÓN 3.11.

(i) *Si $n \in \mathbb{N}$, $n \neq 1$, entonces $n-1 \in \mathbb{N}$. Equivalentemente, existe $m \in \mathbb{N}$ tal que $m+1 = n$.*

(ii) *Si $a, b \in \mathbb{N}$ entonces $a+b \in \mathbb{N}$ y $a \cdot b \in \mathbb{N}$.*

(iii) *Si $a, b \in \mathbb{N}$ entonces $a < b \Rightarrow b-a \in \mathbb{N}$.*

(iv) *Si $n \in \mathbb{N}_0 := \mathbb{N} \cup \{0\}$ y si $a \in \mathbb{R}$ es tal que $n < a < n+1$, entonces $a \notin \mathbb{N}$.*

PRUEBA. (i) Este enunciado afirma que todo número natural n, excepto el 1, es el sucesor o siguiente de otro número natural. Para demostrarlo, consideremos el conjunto

$$H = \{1\} \cup \{x \in \mathbb{N} \mid x \text{ es siguiente de algún } y \in \mathbb{N}\}.$$

Veamos que H es inductivo. En primer lugar, $1 \in H$. Si $k \in H$ entonces $k \in \mathbb{N}$, luego $k+1 \in \mathbb{N}$ y $k+1$ es el siguiente de k. Luego $k+1 \in H$. Como $H \subset \mathbb{N}$ se concluye que que $H = \mathbb{N}$, lo que implica (i).

(ii) Queremos demostrar que la suma y el producto de números naturales es también un número natural. Para probar esta afirmación, veremos que para cada b fijo en $\mathbb{N}$ se cumple que $a+b \in \mathbb{N}$ para todo natural a. Sea $P(a)$ la afirmación $a + b \in \mathbb{N}$.

$P(1)$ establece que $1 + b \in \mathbb{N}$. Esto es verdadero, pues $b \in \mathbb{N}$ y $\mathbb{N}$ es inductivo. Además, si $P(k)$ es verdadera, se tiene que $k+b \in \mathbb{N}$, luego $(k+b)+1 \in \mathbb{N}$. Pero $(k+b)+1 = (k+1)+b$ y por lo tanto $P(k+1)$ es verdadera. Entonces $P(a)$ es verdadera para todo $a \in \mathbb{N}$.

Como esta prueba es válida para cualquier b natural concluimos que $a + b \in \mathbb{N}$ para todo a, $b \in \mathbb{N}$.

Análogamente, para probar que $a \cdot b$ es natural fijamos primero $b \in \mathbb{N}$ y consideramos la proposición $P(a) : a \cdot b \in \mathbb{N}$. Se tiene que $P(1)$ es verdadera, pues $1 \cdot b = b$ y $b \in \mathbb{N}$. Si $P(k)$ es verdadera, esto es, si $k \cdot b \in \mathbb{N}$, entonces $(k+1) \cdot b = k \cdot b + b$. Dado que $k \cdot b$ y b son naturales, entonces $k \cdot b + b \in \mathbb{N}$ por la propiedad de la suma de naturales, de donde se sigue que $P(k+1)$ es verdadera. Por lo tanto $a \cdot b \in \mathbb{N}$ para todo $a \in \mathbb{N}$. Como esta prueba es independiente de la elección de b entonces $a \cdot b \in \mathbb{N}$ para todo a, $b \in \mathbb{N}$.

(iii) Este enunciado afirma que la resta entre dos números naturales es un número natural siempre que el minuendo sea mayor que el sustraendo. En este caso fijamos $b \in \mathbb{N}$ y consideremos la propiedad $P(n)$ que afirma $n < b \Rightarrow b - n \in \mathbb{N}$.

$P(1)$ es verdadera, por (i).

Supongamos que $P(k)$ es verdadera, es decir, si $k < b$ entonces $b - k \in \mathbb{N}$, y probemos $P(k+1)$.

Si $k + 1 < b$, entonces

$$k < b - 1 < b,$$

luego $b - k \in \mathbb{N}$ pues suponemos $P(k)$ verdadera. Como $b - k \neq 1$ entonces $(b - k) - 1 \in \mathbb{N}$ por (i). Pero $(b - k) - 1 = b - (k + 1)$, de donde resulta que $P(k + 1)$ es verdadera.

Luego $P(n)$ es verdadera para todo $n \in \mathbb{N}$. Como la prueba es independiente de b entonces $n < b$ implica $b - n \in \mathbb{N}$ para todo b, $n \in \mathbb{N}$.

(iv) Aquíafirmamos que entre un número natural y su siguiente no existen números naturales. En efecto, si $0 < a < 1$, entonces $a \notin \mathbb{N}$ pues $\mathbb{R}_{\geq 1}$ es inductivo y $a \notin \mathbb{R}_{\geq 1}$.

Si $n < a < n + 1$, $a \in \mathbb{R}$, $n \in \mathbb{N}$, entonces $a \in \mathbb{N}$ implicaría $0 < n + 1 - a < 1$ y $n + 1 - a \in \mathbb{N}$, lo cual acabamos de ver que es un absurdo, por lo tanto, $a \notin \mathbb{N}$. □

4. Definiciones recursivas

Con frecuencia se define una sucesión de números reales

$$u_1,\ u_2,\ \ldots,\ u_n, \ldots,$$

describiendo al elemento u_n en términos de los elementos anteriores; por ejemplo: $u_1 = 1$ y $u_n = 2u_{n-1}$ si $n > 1$. Esto se llama una definición del tipo *recursiva*.

Si la sucesión tiene este tipo de definición recursiva, para conocer el término u_n de la sucesión debemos conocer u_{n-1}; para conocer el término u_{n-1} debemos conocer u_{n-2}, y así sucesivamente. De este modo para calcular el n-ésimo término debemos calcular primero los $n - 1$ anteriores. En lo posible es conveniente entonces obtener una forma general del término u_n que permita calcularlo explícitamente sin calcular todos los términos anteriores de la sucesión.

EJEMPLO 4.1. Consideremos la sucesión u_n dada por

$$u_1 = 1, \qquad \text{y} \qquad u_n = 2u_{n-1} \text{ si } n > 1.$$

Si calculamos los primeros términos tenemos:

$$\begin{aligned} u_1 &= 1 \\ u_2 &= 2u_1 = 2 \\ u_3 &= 2u_2 = 4 \\ u_4 &= 2u_3 = 8 \\ &\vdots \end{aligned}$$

Ya que cada término se obtiene por duplicación del anterior, podemos intuir que el término general de la sucesión es $u_n = 2^{n-1}$. Para probar que nuestra afirmación es cierta para todo n natural, utilizamos el principio de inducción:

Sea $P(n)$ la afirmación $u_n = 2^{n-1}$.

$P(1)$ es verdadera, pues $u_1 = 1 = 2^0$. Si suponemos $P(k)$ verdadera, resulta

$$u_{k+1} = 2u_k = 2\,2^{k-1} = 2^k = 2^{(k+1)-1},$$

es decir que $P(k+1)$ es verdadera. Luego $P(n)$ es verdadera para todo n natural.

Dados n números reales x_1, x_2, ..., x_n simbolizaremos a la suma y al producto de estos n términos como

$$\begin{aligned} \sum_{i=1}^{n} x_i &= x_1 + x_2 + \cdots + x_n \\ \prod_{i=1}^{n} x_i &= x_1 \cdot x_2 \cdots x_n. \end{aligned}$$

Esta suma y producto serán llamados respectivamente *sumatoria* y *productoria* de x_1, x_2, ..., x_n. De una manera más formal definimos:

DEFINICIÓN 4.2. Dados números reales $\{x_i \mid i \in \mathbb{N}\}$, se define la sumatoria $\sum_{i=1}^{n} x_i$ y la productoria $\prod_{i=1}^{n} x_i$ por:

$$\sum_{i=1}^{1} x_i = x_1, \qquad \sum_{i=1}^{k+1} x_i = \Big(\sum_{i=1}^{k} x_i\Big) + x_{k+1} \tag{2}$$

$$\prod_{i=1}^{1} x_i = x_1, \qquad \prod_{i=1}^{k+1} x_i = \Big(\prod_{i=1}^{k} x_i\Big) \cdot x_{k+1} \tag{3}$$

Las fórmulas dadas en (2) y (3) son ejemplos de definiciones recursivas ya que se define el primer elemento de la sucesión y cada elemento se definen en función de los anteriores.

EJEMPLO 4.3. Sea $x_1 = 1$, $x_2 = 2$, $x_3 = 3$, ..., es decir $x_i = i$ para cada i natural. Entonces

$$\sum_{i=1}^{n} x_i = \sum_{i=1}^{n} i = 1 + 2 + 3 + \cdots + n \tag{4}$$

$$\prod_{i=1}^{n} x_i = 1 \cdot 2 \cdot 3 \ldots n. \tag{5}$$

En particular, la fórmula dada en (5) se llama *factorial de* n y se denota $n!$

$$n! := \prod_{i=1}^{n} x_i = 1 \cdot 2 \cdot 3 \cdots n \quad \text{el factorial de } n$$

En los siguientes ejemplos aplicamos el principio de inducción para probar propiedades que involucran sumatorias y productorias.

EJEMPLO 4.4. Para todo $n \geq 4$ se cumple que $n! \geq 2^n$.

PRUEBA. Sea $P(n)$ la propiedad: $n! \geq 2^n$. Queremos ver que $P(n)$ es verdadera para todo $n \geq 4$. Por el Teorema 3.9 basta ver que $P(4)$ es verdadera y que $P(k)$ implica $P(k+1)$, para todo $k \geq 4$.

$P(4)$ es verdadera puesto que

$$4! = 4 \cdot 3 \cdot 2 \cdot 1 = 24 \geq 16 = 2^4.$$

Si $P(k)$ es verdadera entonces

$$(k+1)! = (k+1)k! \geq (k+1) \cdot 2^k \geq 2 \cdot 2^k = 2^{k+1},$$

luego $P(n)$ es verdadera para todo $n \geq 4$. □

EJEMPLO 4.5. Si $x_i = x \in \mathbb{R}$, para todo i, entonces

$$\sum_{i=1}^{n} x_i = n \cdot x \qquad \forall n \in \mathbb{N}.$$

PRUEBA. Probemos esto usando el principio de inducción. Sea $P(n)$ la propiedad:

$$P(n) : \sum_{i=1}^{n} x_i = n \cdot x.$$

Entonces, $P(1)$ es verdadera, puesto que

$$\sum_{i=1}^{1} x_i = x_1 = 1 \cdot x.$$

Probaremos ahora que $P(k) \Rightarrow P(k+1)$, para $k \geq 1$. En efecto, si suponemos que $P(k)$ es verdadera, entonces por (2)

$$\sum_{i=1}^{k+1} x_i = \left(\sum_{i=1}^{k} x \right) + x = k \cdot x + x = (k+1) \cdot x,$$

por lo tanto $P(k+1)$ es verdadera. □

EJEMPLO 4.6. Si $x_i = x \in \mathbb{R}$, para todo i, entonces para cada n natural denotamos o simbolizamos con x^n a la productoria

$$x^n := \prod_{i=1}^{n} x_i.$$

Observemos que entonces,

$$x^{n+1} = x^n \cdot x, \qquad \forall n \in \mathbb{N}.$$

EJEMPLO 4.7.

(a) Probar que $x^{n+m} = x^n \cdot x^m$, para todo n y m natural.

(b) Probar que $(x^n)^m = x^{nm}$ para todo n y m natural.

Sugerencia: Usar el principio de inducción, dejando $m \in \mathbb{N}$ fijo.

PRUEBA. Demostraremos el inciso (a) y dejamos a cargo del lector el caso (b).

Sea m un número natural fijo, y sea $P(n)$ la propiedad del número natural n

$$P(n): \ x^{n+m} = x^n \cdot x^m.$$

$P(1)$ es verdadera, por la observación vista en el Ejemplo 4.6.

Queremos probar entonces que si $P(k)$ es verdadera para algún k natural, es decir, $x^{k+m} = x^k \cdot x^m$, entonces $P(k+1)$ es verdadera. En efecto, aplicando la hipótesis inductiva y haciendo uso de los axiomas de los números reales tenemos que

$$x^{(k+1)+m} = x^{(k+m)+1} = x^{k+m} \cdot x = (x^k \cdot x^m) \cdot x = (x^k \cdot x) \cdot x^m = x^{k+1} \cdot x^m,$$

y por tanto $P(n)$ es verdadera para todo $n \in \mathbb{N}$.

Puesto que m es un número natural arbitrario, entonces $P(n)$ es válida para todo n natural.

□

EJEMPLO 4.8. Probar que para todo $n \in N$ se cumple que

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

PRUEBA. En efecto, $P(1)$ es verdadera, pues

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

Si suponemos $P(k)$ verdadera, es decir $\displaystyle\sum_{i=1}^{k} i = \frac{k(k+1)}{2}$, entonces

$$\sum_{i=1}^{k+1} i = \frac{k(k+1)}{2} + (k+1) = \frac{(k+1) \cdot (k+2)}{2}$$

es decir que $P(k+1)$ es verdadera; luego $P(n)$ vale para todo n natural. □

NOTA 4.1. Cuentan que siendo niño, el célebre matemático Gauss estaba un tanto inquieto en su clase. Para que tuviera algo con qué entretenerse su maestro le pidió que sumara todos los números del 1 al 100. Gauss tardó pocos minutos en dar la respuesta: 5050. El niño observó que si sumaba los números agrupando el primero con el último, el segundo con el penúltimo y así sucesivamente el cálculo se simplificaba bastante:

$$(6)\quad (1+100)+(2+99)+(3+98)+\cdots+(50+51)=$$
$$\underbrace{101+101+101+\cdots+101}_{50}=50\cdot 101=5050.$$

EJEMPLO 4.9. Sea $x_1=2$, $x_n=x_{n-1}+2\,n$ si $n\geq 2$. Probar que $x_n=n\cdot(n+1)$, $\forall n\in\mathbb{N}$.

PRUEBA. Sea $P(n)$ la propiedad $x_n=n\cdot(n+1)$. $P(1)$ es la propiedad $x_1=1\cdot(1+1)=2$, luego $P(1)$ es verdadera.
Si asumimos que $P(k)$ es verdadera, entonces $x_{k+1}=x_k+2(k+1)$ por definición, y por hipótesis inductiva tenemos que

$$x_k+2(k+1)=k(k+1)+2(k+1)=(k+1)(k+2),$$

por lo tanto

$$x_{k+1}=(k+1)((k+1)+1).$$

Esto prueba que $P(k+1)$ es verdadera y se sigue que $P(n)$ vale para todo n natural. □

PRUEBA. Sea $P(n)$ la propiedad $u_n=(n!)^2$.

$P(1)$ es verdadera pues $u_1=1$ y $(1!)^2=1$. Si asumimos que $P(k)$ es cierta, entonces por definición

$$u_{k+1}=(k+1)^2u_k$$

y por hipótesis inductiva

$$(k+1)^2u_k=(k+1)^2k!^2=(k+1)!^2.$$

Por lo tanto la propiedad vale $\forall n\in\mathbb{N}$. □

EJERCICIO 4.1. Si $a\in\mathbb{R}$, $a\neq 0,1$, entonces

$$\sum_{i=0}^{n}a^i=\frac{a^{n+1}-1}{a-1}\qquad\text{para cada } n \text{ natural.}$$

Como consecuencia del resultado de este ejercicio tenemos las igualdades:

$$\sum_{i=0}^{n} 2^i = 1 + 2 + 2^2 + \cdots + 2^n = 2^{n+1} - 1,$$

$$\sum_{i=0}^{5} 3^i = 1 + 3 + 3^2 + 3^3 + 3^4 = \frac{3^5 - 1}{2}.$$

EJEMPLO 4.10. Para todo $n \in \mathbb{N}$ se cumple que

$$\sum_{i=1}^{n} \frac{1}{i(i+1)} = \frac{n}{n+1}. \tag{7}$$

PRUEBA. Sea $P(n)$ la propiedad del número n dada por (7). Entonces $P(1)$ es verdadera pues

$$\frac{1}{1 \cdot (1+1)} = \frac{1}{2} = \frac{1}{1+1}.$$

Si $P(k)$ es verdadera para algún $k \in \mathbb{N}$ entonces para $k+1$ se tiene que

$$\sum_{i=1}^{k+1} \frac{1}{i(i+1)} = \frac{k}{k+1} + \frac{1}{(k+1) \cdot (k+2)}, \qquad \text{y}$$

$$\frac{k}{k+1} + \frac{1}{(k+1) \cdot (k+2)} = \frac{k \cdot (k+2) + 1}{(k+1) \cdot (k+2)} = \frac{(k+1)^2}{(k+1)(k+2)} = \frac{k+1}{k+2},$$

luego $P(k+1)$ vale y la afirmación es válida para todo n natural. □

Invitamos al lector a resolver los siguientes ejercicios:

EJERCICIO 4.2.

(a) $3^{2n+2} + 2^{6n+1}$ es múltiplo de 11, $\forall n \in \mathbb{N}$.

Nota: Decimos que $m \in \mathbb{N}$ es múltiplo de 11 si existe un $k \in \mathbb{N}$ tal que $m = k \cdot 11$.

(b) $\sum_{i=1}^{n} 2i - 1 = 1 + 3 + \cdots + (2n-1) = n^2$, $\forall n \in \mathbb{N}$.

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

(d) $\sum_{k=1}^{n} k^3 = 1^3 + 2^3 + \cdots + n^3 = \left(\frac{n(n+1)}{2}\right)^2$, $\forall n \in \mathbb{N}$.

4.1. Principio de Buena Ordenación.

DEFINICIÓN 4.11. Sea A un subconjunto de $\mathbb{R}$. Decimos que A posee *primer elemento* si existe un elemento $a \in A$ tal que $a \leq x$, para todo $x \in A$.

Un subconjunto L de $\mathbb{R}$ se dice *bien ordenado* si todo subconjunto no vacío de L posee primer elemento.

EJEMPLO 4.12. $\mathbb{R}_{>0}$, $\mathbb{R}_{>\sqrt{2}}$ no tienen primer elemento. Por lo tanto $\mathbb{R}$ no es bien ordenado.

$-\mathbb{N} = \{-n \mid n \in \mathbb{N}\}$ no es un conjunto bien ordenado pues no posee primer elemento.

$\mathbb{R}_{\geq 0}$ tiene primer elemento pero el subconjunto $\mathbb{R}_{>0}$ no, por lo tanto $\mathbb{R}_{\geq 0}$ no es bien ordenado.

El *principio de buena ordenación* asegura que el conjunto de números naturales es un conjunto bien ordenado.

PRINCIPIO DE BUENA ORDENACIÓN . $\mathbb{N}$ es un conjunto bien ordenado. Es decir, para todo subconjunto $H \neq \emptyset$ de $\mathbb{N}$, H tiene primer elemento.

PRUEBA. (Razonando por el absurdo) Probaremos que todo subconjunto H de $\mathbb{N}$ que no tiene primer elemento es el conjunto vacío.

Supongamos que H es un subconjunto de $\mathbb{N}$ que no tiene primer elemento. Sea H' el complemento de H en $\mathbb{N}$, es decir

$$H' = \{n \in \mathbb{N} \mid n \notin H\}.$$

Para simplificar la notación denotaremos con $[1, n]$ al intervalo natural de los primeros n números naturales, esto es $[1, n] = \{x \in \mathbb{N} : 1 \leq x \leq n\} = \{1, 2, \ldots, n\}$. Consideremos el conjunto

$$K = \{n \in \mathbb{N} \mid [1, n] \subset H'\}.$$

Si probamos que K es inductivo, entonces tendremos que $K = \mathbb{N}$, y por lo tanto que $H = \emptyset$.

En efecto, notemos que $1 \in H'$ pues de lo contrario tendríamos que $1 \in \mathbb{N}$ y 1 sería el primer elemento de H. Por lo tanto $1 \in K$ pues $\{1\} \subset H'$.

Además, si $k \in K$, es decir, si $[1, k] \subset H'$, entonces $k + 1$ debe pertenecer a H', pues de lo contrario $k + 1$ estaría en H y sería su primer elemento. Luego $[1, k + 1] \subset H'$, lo que indica que $k + 1 \in K$. Con esto probamos que K es un conjunto inductivo, y por lo tanto $K = \mathbb{N}$. Pero si $K = \mathbb{N}$ entonces $H = \emptyset$, como queríamos demostrar. □

4.2. Principio de Inducción Fuerte. El siguiente teorema es una variante del principio de inducción llamado *principio de inducción fuerte*:

TEOREMA 4.13. *Sea $H \subseteq \mathbb{N}$. Si $1 \in H$ y si $[1,k] \subset H$ implica $k+1 \in H$, entonces $H = \mathbb{N}$.*

PRUEBA. Sea H como en la hipótesis; entonces $H = \mathbb{N}$ o $H \subset N$. Si $H = \mathbb{N}$, no hay nada que probar. Supongamos que $H \neq \mathbb{N}$, y sea H' el complemento de H en $\mathbb{N}$. Entonces H' tiene primer elemento, llamémoslo y. Luego $y > 1$ y 1, 2, ..., $y-1$ pertenecen a H. Por hipótesis, si $[1, y-1] \subset H$ entonces $y \in H$. Pero $y \in H'$ e $y \in H$ es un absurdo que provino de suponer que $H \neq \mathbb{N}$. □

El siguiente teorema es equivalente al principio de inducción fuerte:

TEOREMA 4.14. *Sea $P(n)$ una propiedad que satisface*

(i) *$P(1)$ es verdadera.*

(ii) *Si $P(1)$, $P(2)$, ..., $P(k)$ son todas verdaderas, entonces $P(k+1)$ es verdadera.*

Entonces $P(n)$ es verdadera para todo $n \in \mathbb{N}$.

PRUEBA. Sea

$$H = \{n \in \mathbb{N} \mid P(n) \text{ es verdadera}\}.$$

De (i) se ve que $1 \in H$. Si $1, 2, \ldots k \in H$ entonces $P(m)$ es verdadera para todo $m \in [1,k]$, luego por (ii) $P(k+1)$ es verdadera, es decir se concluye que $P(m)$ vale para todo $m \in [1, k+1]$. Por lo tanto $k+1 \in H$. Sigue del principio de inducción que $H = \mathbb{N}$, esto es, $P(n)$ es verdadera para todo $n \in \mathbb{N}$. □

Veamos el siguiente ejemplo de aplicación del principio de inducción fuerte.

EJEMPLO 4.15. Sea $u_1 = 3$, $u_2 = 5$, $u_n = 3 \cdot u_{n-1} - 2 \cdot u_{n-2}$ si $n \geq 3$. Probar que $u_n = 2^n + 1$, $\forall n \in \mathbb{N}$.

PRUEBA. Si quisiéramos aplicar el Principio de Inducción, veríamos que no es posible deducir $P(k+1)$ a partir de $P(k)$. Esto se debe a que u_{k+1} no sólo está dado en términos de u_k sino de u_{k-1} también.

Sin embargo, sí es posible probar la afirmación utilizando el Principio de Inducción Fuerte. En efecto, sabemos que la propiedad $P(n)$ que afirma $u_n = 2^n + 1$ se cumple para $n = 1$. Supongamos que es válida para $n = 1$, $n = 2$, hasta $n = k$. Es decir:

$$u_1 = 2 + 1, \quad u_2 = 2^2 + 1 = 5, \quad \ldots \quad u_k = 2^k + 1.$$

Entonces

$$u_{k+1} = 3 \cdot u_k - 2 \cdot u_{k-1} = 3(2^k + 1) - 2(2^{k-1} + 1) =$$
$$= (3-1) \cdot 2^k + (3-2) = 2^{k+1} + 1,$$

por lo que $P(k+1)$ es verdadera. Luego $P(n)$ es verdadera para todo n natural. □

CAPÍTULO 2

Conteo

1. Técnicas de conteo

El objetivo del presente capítulo es presentar una introducción a la combinatoria elemental, junto con una variedad de problemas de aplicación. Esencialmente, *contar* significa establecer una correspondencia biunívoca entre los elementos del conjunto y los números naturales, o un subconjunto de $\mathbb{N}$. (y un subconjunto finito $[1, n]$ de $\mathbb{N}$. Según veremos, para cada conjunto finito X, el número n está unívocamente determinado por X) Las técnicas de conteo consisten en contar la cantidad de elementos de un conjunto. Comenzamos entonces dando la definición de correspondencia biunívoca o biyección, para continuar luego con propiedades del conteo y ejemplos de combinatoria.

DEFINICIÓN 1.1. Sean X e Y conjuntos arbitrarios, no vacíos Sea $f : X \mapsto Y$ una función.

1. f es una función *inyectiva* o *uno a uno* si

$$x \neq y \Rightarrow f(x) \neq f(y),$$

   o equivalentemente, $f(x) = f(y) \Rightarrow x = y$,
2. f es *suryectiva* si

$$\forall y \in Y,\ \exists x \in X \text{ tal que } f(x) = y,$$

   es decir Im $f = Y$,
3. f es *biyectiva* si es inyectiva y suryectiva.

DEFINICIÓN 1.2. Sean X, Y, Z conjuntos y sean $f : X \mapsto Y$ y $g : Y \mapsto Z$ funciones. Se define la *composición* de g con f a la función $g \circ f : X \mapsto Z$ tal que $(g \circ f)(x) = g(f(x))$, $\forall x \in X$.

EJERCICIO 1.1.

(i) Demuestre que si f, g son inyectivas (resp. suryectivas), entonces $g \circ f$ es inyectiva (resp. suryectiva).

(ii) Demuestre que si $g \circ f$ es inyectiva (resp. suryectiva), entonces f (resp. g) es inyectiva (resp. suryectiva).

EJEMPLO 1.3.

(a) Sea $f : \mathbb{R} \mapsto \mathbb{R}$, $f(x) = 2x + 1$. Entonces f es biyectiva.

En efecto, sean $x_1, x_2 \in \mathbb{R}$ tales que $f(x_1) = f(x_2)$. Entonces

$$2x_1 + 1 = 2x_2 + 1 \Rightarrow 2x_1 = 2x_2 \Rightarrow x_1 = x_2,$$

luego f es inyectiva. Para ver que f es suryectiva tomemos $y \in \mathbb{R}$ y veamos que $y = f(x)$ para algún $x \in \mathbb{R}$. Si tomamos $x = \dfrac{y-1}{2}$, entonces

$$f(x) = 2\left(\frac{y-1}{2}\right) + 1 = y.$$

Hemos probado que f es inyectiva y suryectiva, por lo tanto f es biyectiva.

(b) Sea $f : \mathbb{R} \mapsto \mathbb{R}$, $f(x) = x^2$. Entonces f no es inyectiva ni suryectiva.

En efecto, f no es suryectiva pues la imagen de f es $\mathbb{R}_{\geq 0}$, y f no es inyectiva pues $f(x) = f(-x)$ para todo $x \in \mathbb{R}$.

(c) Sea $f : \mathbb{R} \mapsto [-1, 1]$, $f(x) = \operatorname{sen}(x)$. Entonces Im $f = [-1, 1]$ por lo que f es suryectiva. Pero $\operatorname{sen}(x) = \operatorname{sen}(x + 2\pi)$, para todo $x \in \mathbb{R}$; luego f no es inyectiva.

EJEMPLO 1.4. Sea $X = \{1,\ 2,\ 3\}$. Determinemos *todas* las funciones $f : X \mapsto X$. Una tal función f queda determinada por los valores $f(1)$, $f(2)$ y $f(3)$. Usaremos la siguiente convención: a la terna (a, b, c), donde a, b y c pertenecen a $\{1,\ 2,\ 3\}$, la identificaremos con la función f tal que $f(1) = a$, $f(2) = b$ y $f(3) = c$. Por ejemplo, la terna (1, 3, 3) se corresponde con la función f tal que $f(1) = 1$, $f(2) = 3$ y $f(3) = 3$. Dicho de otro modo, representaremos a cada f, $f : X \mapsto Y$ por la terna $(f(1), f(2), f(3))$.

Con esta convención, la lista completa de funciones es la siguiente:

$(1,\ 1,\ 1)$	$(2,\ 1,\ 1)$	$(3,\ 1,\ 1)$
$(1,\ 1,\ 2)$	$(2,\ 1,\ 2)$	$(\mathbf{3},\ \mathbf{1},\ \mathbf{2})$
$(1,\ 1,\ 3)$	$(\mathbf{2},\ \mathbf{1},\ \mathbf{3})$	$(3,\ 1,\ 3)$
$(1,\ 2,\ 1)$	$(2,\ 2,\ 1)$	$(\mathbf{3},\ \mathbf{2},\ \mathbf{1})$
$(1,\ 2,\ 2)$	$(2,\ 2,\ 2)$	$(3,\ 2,\ 2)$

$(\mathbf{1},\ \mathbf{2},\ \mathbf{3})$	$(2,\ 2,\ 3)$	$(3,\ 2,\ 3)$
$(1,\ 3,\ 1)$	$(\mathbf{2},\ \mathbf{3},\ \mathbf{1})$	$(3,\ 3,\ 1)$
$(\mathbf{1},\ \mathbf{3},\ \mathbf{2})$	$(2,\ 3,\ 2)$	$(3,\ 3,\ 2)$
$(1,\ 3,\ 3)$	$(2,\ 3,\ 3)$	$(3,\ 3,\ 3)$

Luego hay $27 = 3^3$ funciones y entre ellas hay $6 = 3 \cdot 2$ funciones *biyectivas*, que son las que hemos remarcado.

Veamos por qué hay exactamente 27 funciones. En primer lugar, hay 3 valores posibles para $f(1)$. Por cada uno de éstos, existen tres posibles valores de $f(2)$; en total hay $3 \cdot 3 = 9$ posibles valores para el par $(f(1), f(2))$. Por cada uno de estos pares, podemos elegir tres valores posibles de $f(3)$, luego hay $9 \cdot 3 = 27$ posibilidades para la terna $(f(1), f(2), f(3))$.

Veamos por qué hay 6 funciones biyectivas. Notemos que para $f(1)$ hay 3 posibles valores. Una vez fijado $f(1)$, $f(2)$ sólo tiene 2 valores posibles. Luego hay $3 \cdot 2$ valores posibles para el par $f(1)$ y $f(2)$. Una vez fijado el par $f(1)$, $f(2)$, queda para $f(3)$ un único valor posible, luego hay $3 \cdot 2 \cdot 1 = 6$ funciones biyectivas.

Como ejemplo de una modelización concreta de la situación anterior, notemos que hay 6 maneras distintas de sentarse 3 alumnos en 3 sillas, uno en cada silla.

El siguiente lema caracteriza a las funciones biyectivas de un conjunto X en un conjunto Y como aquellas funciones que poseen una *función inversa* de Y en X. Denotemos con $Id_X : X \mapsto X$ a la función *identidad* en X definida por

$$Id_X(a) = a, \qquad \text{para todo } a \in X.$$

LEMA 1.5. *Si $f : X \mapsto Y$, entonces f es biyectiva si y sólo si existe $g : Y \mapsto X$, llamada* inversa de f *tal que $g \circ f = Id_X$ y $f \circ g = Id_Y$. La inversa es única.*

PRUEBA. Veamos que si f tiene una inversa g entonces f es biyectiva. Probemos en primer lugar que f es inyectiva. En efecto, si $f(x_1) = f(x_2)$ entonces $g\left(f(x_1)\right) = g\left(f(x_2)\right)$. Dado que $g(f(x)) = (g \circ f)(x) = Id_X(x) = x$, se sigue que

$$f(x_1) = f(x_2) \qquad \text{implica que} \qquad x_1 = x_2.$$

Luego f es inyectiva.

Para probar que f es suryectiva, notemos que si $y \in Y$ entonces $g(y) \in X$ y $f\left(g(y)\right) = y$. Luego $y \in \text{Im}\ (f)$. Dado que y es un elemento arbitrario de Y, se sigue que $\text{Im}\ (f) = Y$ y por lo tanto f es suryectiva.

Recíprocamente, si f es biyectiva entonces para cada $y \in Y$ existe un *único* $x \in X$ tal que $f(x) = y$. Definimos entonces a la función $g : Y \mapsto X$ por

$$g(y) = x \qquad \text{si y sólo si} \qquad f(x) = y.$$

Entonces $f(g(y)) = y$ por lo cual $f \circ g = Id_Y$. Además, por la definición de g tenemos que $g(f(x)) = x$, luego $g \circ f = Id_X$. □

Si g es la inversa de f denotaremos a g por f^{-1}.

EJEMPLO 1.6. Sea $f : \mathbb{R} \mapsto \mathbb{R}$, $f(x) = x^3$, y tomemos $g : \mathbb{R} \mapsto \mathbb{R}$ dada por $g(x) = x^{1/3}$. Entonces

$$(g \circ f)(x) = g\left(x^3\right) = \sqrt[3]{x^3} = x \qquad \text{y}$$

$$(f \circ g)(y) = f\left(\sqrt[3]{y}\right) = \left(\sqrt[3]{y}\right)^3 = y.$$

Por lo tanto g es la inversa de f y entonces f es biyectiva.

Si $h : \mathbb{R} \mapsto \mathbb{R}$ está dada por $h(x) = x^2$ entonces h no tiene inversa puesto que no es inyectiva: si $y > 0$, $h(\sqrt{y}) = h(-\sqrt{y})$. Tampoco h es suryectiva pues $Im(h) = \mathbb{R}_{\geq 0}$. En general, $f(x) = x^n$ es biyectiva como función de $\mathbb{R}$ en $\mathbb{R}$ si y sólo si n es impar.

EJEMPLO 1.7. Si $f(x) = 2x+1$ entonces f es biyectiva y su inversa está dada por $f^{-1}(y) = \dfrac{y-1}{2}$.

Notación: Si m y $n \in \mathbb{N}$, $m \leq n$, denotaremos con $[m, n]$ al intervalo natural $\{m, m+1, \ldots, n\} = \{k \in \mathbb{N} \mid m \leq k \leq n\}$.

El siguiente teorema expresa una propiedad fundamental de los números naturales.

TEOREMA 1.8. *Si n y $m \in \mathbb{N}$ y $n > m$, entonces no existe una función $f : [1, n] \mapsto [1, m]$ inyectiva.*

PRUEBA. Sea

$$H = \{n \in \mathbb{N} \mid \text{ existe } m,\ m < n \text{ y } f : [1, n] \mapsto [1, m] \text{ inyectiva}\}.$$

El objetivo será probar que necesariamente $H = \emptyset$.

Supongamos que $H \neq \emptyset$, entonces por el principio de buena ordenación existe $h \in H$, h el primer elemento de H. Por la definición del conjunto H, existe una función inyectiva $f : [1, h] \mapsto [1, m]$ donde m es un natural menor que h. Si $m = 1$ entonces f no es inyectiva.

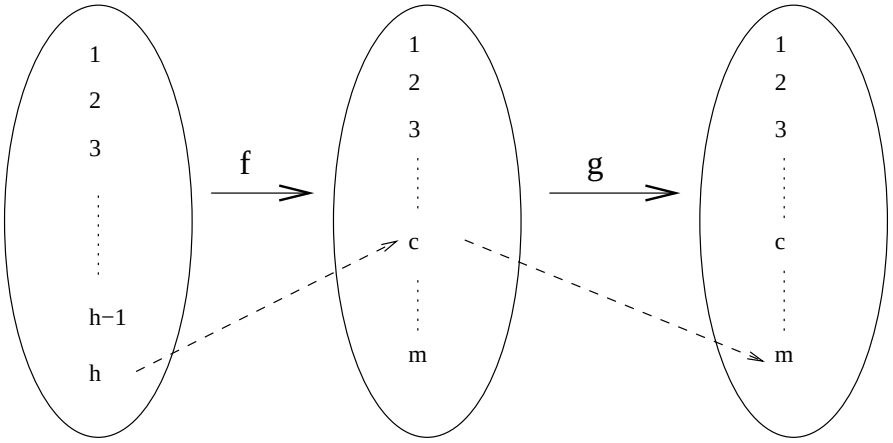


FIGURA 1

Si $1 < m < h$ hay dos posibilidades: $f(h) = m$ o $f(h) = c$, para algún $c < m$. Si $f(h) = m$, entonces podemos *restringir* f al intervalo $[1, h-1]$, y tendremos que

$$f : \{1, 2, \ldots, h-1\} \mapsto \{1, 2, \ldots, m-1\}$$

es una función inyectiva. Por lo tanto $h-1 \in H$. Pero esto es absurdo puesto que h es el primer elemento de H.

Si $f(h) = c$ y $c < m$ entonces componemos a f con la función $g : [1, m] \mapsto [1, m]$ biyectiva, dada por

$$g(c) = m, \quad g(m) = c \quad y \quad g(x) = x$$

para todo x distinto de c y de m. (Ver Figura 1) Luego la función $f^* = g \circ f : [1, h] \mapsto [1, m]$ satisface

$$f^*(h) = g(f(h)) = m,$$

y además es inyectiva por ser composición de funciones inyectivas. Si restringimos f^* al intervalo $[1, h-1]$, f^* continúa siendo inyectiva y tenemos que $f^* : [1, h-1] \mapsto [1, m-1]$. Por la definición de H se tiene que $(h-1) \in H$, un absurdo pues h es el primer elemento de H. Por consiguiente $H = \emptyset$ como habíamos afirmado. □

COROLARIO 1.9. *Si $n \neq m$, entonces no existe una función biyectiva $f : [1, n] \mapsto [1, m]$*

PRUEBA. Si $n > m$, por el Teorema 1.8 no existe tal f inyectiva. Si $n < m$ y tal f existiera, entonces $f^{-1} : [1, m] \mapsto [1, n]$ sería inyectiva, pero por el teorema esto no es posible. □

El Teorema 1.8 suele llamarse *principio de los casilleros*, el cual afirma que

Si n objetos son distribuídos en m casillas y $n > m$, entonces por lo menos una casilla contiene al menos 2 objetos.

COROLARIO 1.10. *Sea $f : [1, n] \to [1, n]$. Entonces f es inyectiva si y sólo si f es suryectiva.*

PRUEBA. Daremos la idea de la prueba dejando los detalles al lector.

Si $f : [1, n] \to [1, n]$ es inyectiva y no suryectiva, entonces existe una función biyectiva $h : \text{Im}(f) \mapsto [1, m]$ para algún m, $m < n$. Luego, se tiene que $h \circ f : [1, n] \mapsto [1, m]$ es una función inyectiva, lo que contradice el principio de los casilleros.

Por otra parte, si $f : [1, n] \to [1, n]$, es suryectiva y no inyectiva, entonces existe un subconjunto propio $H \subset [1, n]$ de tal modo que la función $h := f_{|H} : H \mapsto [1, n]$ es biyectiva (verificar). Ahora bien, siendo H un subconjunto propio de $[1, n]$, existe una función biyectiva $g : [1, m] \mapsto H$, para algún natural $m < n$. Por consiguiente $h \circ g : [1, m] \mapsto [1, n]$ es biyectiva, lo cual contradice el corolario anterior. □

EJERCICIO 1.2.

1. Dadas 13 personas, hay al menos 2 que cumplen años el mismo mes.
2. Dado un conjunto de 10^6 personas, hay al menos dos de ellas con el mismo número de cabellos en la cabeza.

EJEMPLO 1.11. Sea A un conjunto de m personas, $m \geq 2$. Probar que existen al menos dos personas en A con el mismo número de amigos en A.
Convenimos en que si a es amigo de b entonces b es amigo de a y también que cada uno es amigo de sí mismo.

SOLUCIÓN. Consideremos la función

$$f(x) = \text{ número de amigos de } x \text{ en } A.$$

Luego f toma valores en el conjunto $\{1, 2, \ldots, m\}$. Ahora si alguien tiene m amigos entonces es amigo de todos, luego en ese caso ninguno puede tener sólo **un** amigo. Luego 1 y m no pueden estar ambos simultáneamente en la imagen de f. Por lo tanto la imagen de f tiene menos de m elementos. Aplicando el principio de los casilleros concluimos que existen x_1 y x_2 tales que $f(x_1) = f(x_2)$, es decir que existen dos personas con el mismo número de amigos en A. □

Estamos en condiciones ahora de definir la noción de *cardinal* o *cardinalidad* de un conjunto.

DEFINICIÓN 1.12. Sea $[1, n] = \{1,\ 2,\ 3, \ldots, n\}$. Se dice que un conjunto X *tiene n elementos* si existe una biyección $f : [1, n] \mapsto X$. En tal caso n se llama la *cardinalidad* de X,

que se denota $|X|$. Un conjunto X es finito si $X = \emptyset$ ó existe $n \in \mathbb{N}$ tal que $|X| = n$. Se define $|\emptyset| = 0$.

El cardinal de un conjunto finito es usualmente llamado el número de elementos de un conjunto. Notemos que una función biyectiva $f : [1, n] \mapsto X$ hace corresponder a cada elemento de X un número natural, comenzando con el 1 y siguiendo en forma ordenada hasta n. Esto es esencialmente lo que hacemos cuando contamos. Si queremos saber cuántas personas hay en un aula, las numeramos del uno en adelante, sin contar ninguna dos veces: *uno, dos, tres, ...* Si por ejemplo contamos hasta quince, decimos que hay quince personas.

En el siguiente teorema probaremos que si dos conjuntos A y B son disjuntos y finitos, es decir de cardinal finito, entonces la unión de ambos también es un conjunto finito cuyo cardinal es igual a la suma de los cardinales de A y B.

TEOREMA 1.13 (Principio de Adición). *Sean A y B conjuntos finitos disjuntos. Entonces* $|A \cup B| = |A| + |B|$.

PRUEBA. Por hipótesis existen $f : [1, n] \mapsto A$ y $g : [1, m] \mapsto B$ biyectivas. Entonces $|A| + |B| = n + m$. Queremos ver que existe una función biyectiva $h : [1, n + m] \mapsto A \cup B$. Notemos que la función $k : [n + 1, n + m] \mapsto [1, m]$ definida por

$$k(x) = x - n,$$

es biyectiva. Luego

$$h(x) = \begin{cases} f(x) & x \in [1, n] \\ g(k(x)) & x \in [n + 1, n + m] \end{cases}$$

es una función que lleva $[1, n] \cup [n + 1, n + m] = [1, n + m] \mapsto A \cup B$ biyectivamente pues A, B son disjuntos, con lo que queda probada nuestra afirmación. □

Este resultado se generaliza al caso de la unión de una cantidad finita de conjuntos disjuntos, todos con cardinalidad finita:

COROLARIO 1.14. *Si $A_1, \ldots, A_m$ son conjuntos finitos disjuntos dos a dos, entonces*

$$|A_1 \cup \cdots \cup A_m| = \sum_{i=1}^{m} |A_i|.$$

PRUEBA. La prueba puede hacerse aplicando inducción en m y usando el principio de adición. □

Notar que el Teorema 1.13 no es válido si la intersección entre ambos conjuntos es no vacía. En este caso, la propiedad que se cumple es la siguiente, que dejamos como ejercicio para el lector:

EJERCICIO 1.3. (a) Probar que si A y B son conjuntos finitos, entonces

$$|A \cup B| + |A \cap B| = |A| + |B|.$$

(b) Probar que dados conjuntos finitos A_1, A_2, A_3, se tiene

$$|A_1 \cup A_2 \cup A_3| = |A_1| + |A_2| + |A_3| - |A_1 \cap A_2| - |A_1 \cap A_3| - |A_2 \cap A_3| + |A_1 \cap A_2 \cap A_3|.$$

(c) Enuncie y pruebe una generalización a n conjuntos.

Dados A y B dos conjuntos no vacíos cualesquiera, el producto cartesiano $A \times B$ está definido como el conjunto de todos los pares ordenados (a, b) donde $a \in A$ y $b \in B$:

$$A \times B = \{(a, b) \mid a \in A,\ b \in B\}.$$

TEOREMA 1.15. *Sean A, B conjuntos finitos. Entonces $|A \times B| = |A| \cdot |B|$.*

PRUEBA. Sean n y m los cardinales de A y B respectivamente. Entonces existen funciones f y g biyectivas: $f : [1, n] \mapsto A$, $g : [1, m] \mapsto B$. Luego podemos escribir $A = \{a_1, \ldots, a_n\}$, $B = \{b_1, \ldots, b_m\}$ donde $a_i = f(i)$ para $1 \leq i \leq n$ y $b_j = g(j)$ para $1 \leq j \leq m$.

Tenemos que

$$A \times B = (A \times \{b_1\}) \cup (A \times \{b_2\}) \cup \cdots \cup (A \times \{b_m\})$$

y la unión es disjunta. Como $|A \times \{b_j\}| = |\{(a_1, b_j), (a_2, b_j), \ldots, (a_n, b_j)\}| = |A| = n$ entonces $|A \times B| = \underbrace{n + n + \cdots + n}_{m} = n \cdot m$. □

Si $A_1, A_2, \ldots, A_m$ son m conjuntos no vacíos, se define el producto cartesiano $\prod_{i=1}^{m} A_i$ como

$$\prod_{i=1}^{m} A_i = \{(a_1, a_2, \ldots, a_m) \mid a_i \in A_i,\ 1 \leq i \leq m\}.$$

El siguiente corolario se refiere a la cardinalidad del producto cartesiano de m conjuntos finitos:

COROLARIO 1.16. *Sean $A_1, \ldots, A_m$ conjuntos finitos no vacíos. Entonces*

$$|A_1 \times A_2 \times \cdots \times A_m| = \prod_{i=1}^{m} |A_i|.$$

PRUEBA. Se prueba usando el Teorema 1.15 y aplicando el principio de inducción. □

Observación: cuando usamos "puntos suspensivos.[en] una definición en verdad queremos indicar que la definición debiera darse recursivamente. Este es el caso, por ejemplo, para la union o producto cartesiano de conjuntos X_i.

PROPOSICIÓN 1.17. *Sean A y B conjuntos finitos de cardinales n y m respectivamente.*

(a) *Si $\mathcal{F}(A, B)$ es el conjunto de todas las funciones de A en B, entonces*

$$|\mathcal{F}(A, B)| = m^n.$$

(b) *Si $\mathcal{P}(A)$ es la familia de todos los subconjuntos de A, entonces*

$$|\mathcal{P}(A)| = 2^n.$$

PRUEBA. (a) Notemos que podemos identificar a cada elemento de $\mathcal{F}(A, B)$ con una n-upla en $\prod_{i=1}^{n} B = B \times B \times \cdots \times B$. En efecto, si $A = \{a_1, a_2, \ldots, a_n\}$ y $f : A \mapsto B$, entonces hacemos corresponder a f la n-upla $(f(a_1), f(a_2), \ldots, f(a_n))$.

Recíprocamente, si $\mathbf{b} = (b_1, b_2, \ldots, b_n) \in \underbrace{B \times B \times \cdots \times B}_{n}$, entonces $\mathbf{b}$ se corresponde con la función g dada por $g(a_i) = b_i$, $1 \leq i \leq n$.
Por lo tanto queda definida una biyección

$$\mathcal{F}(A, B) \mapsto \underbrace{B \times B \times \cdots \times B}_{n},$$

de donde concluimos que $|\mathcal{F}(A, B)| = |B|^n = m^n$.

(b) Cada subconjunto de A, y por lo tanto cada elemento de $\mathcal{P}(A)$, puede identificarse con una función $f : A \mapsto \{0, 1\}$. En efecto, si $B \subseteq A$, hacemos corresponder a B la función χ_B, que vale 1 si $x \in B$ y 0 si $x \notin B$:

$$\chi_B(x) = \begin{cases} 1 & x \in B \\ 0 & x \notin B \end{cases}$$

Recíprocamente, cada función $f : A \mapsto \{0,\ 1\}$ se corresponde con el subconjunto

$$B_f = \{b \in A \mid f(b) = 1\}.$$

Luego, la familia de subconjuntos de A está en correspondencia biunívoca con las funciones de A en $\{0,\ 1\}$, y por el inciso (a) se sigue que

$$|\mathcal{P}(A)| = |\mathcal{F}(A, \{0, 1\})| = 2^{|A|} = 2^n.$$

□

EJEMPLO 1.18. ¿Cuántas banderas se pueden hacer con 3 bandas verticales con los colores rojo, blanco, azul y verde, si se permiten 2 o más franjas del mismo color?

SOLUCIÓN. La pregunta equivale a determinar el número de aplicaciones de un conjunto de 3 elementos (franjas) en un conjunto de 4 elementos (colores):

$$\left|\mathcal{F}(\{1,2,3\},\{\text{rojo, blanco, azul, verde}\})\right| = 4^3 = 64,$$

se pueden hacer 64 banderas distintas. □

EJEMPLO 1.19. ¿Cuántas posiciones hacen falta para hacer (al menos) un millón de llaves diferentes? Las llaves se construyen haciendo incisiones de profundidad variable en distintas posiciones, y supondremos que hay 8 profundidades posibles.

SOLUCIÓN. Sea m el número de posiciones. Queremos que el cardinal del conjunto

$$F(\{1,\dots,m\},\{1,2,\dots,8\}),$$

es decir 8^m sea mayor que 10^6. Ahora bien,

$$2^8 = 256 \quad \Rightarrow \quad 2^8 \cdot 4 > 10^3, \quad \Rightarrow \quad 2^{10} > 10^3 \quad \Rightarrow \quad 2^{20} > 10^6 \quad \Rightarrow \quad 2^{21} = 8^7 > 10^6.$$

Como $8^7 > 10^6$, entonces con 7 posiciones se logran más de 10 millones de llaves. Dejamos como ejercicio comprobar que $8^6 < 1000000$ (es decir que no es suficiente hacer 6 incisiones). □

EJEMPLO 1.20. ¿Cuántos números de 5 dígitos capicúas hay?

SOLUCIÓN. Cada número será de la forma $xyzuv$, con $x = v$ e $y = u$, es decir que de la forma $xyzyx$. Tenemos que y, z toman valores en $\{0,1,\dots,9\}$ y x en $\{1,\dots,9\}$. Luego la cantidad de números capicúas de 5 dígitos es $9 \cdot 10^2 = 900$. □

Sea $\mathcal{F}_i(A,B)$ el conjunto de todas las funciones inyectivas de A en B y $\mathcal{F}_b(A,B)$ el conjunto de todas las funciones biyectivas de A en B, donde $|A| = n$ y $|B| = m$. Ya hemos visto que si $n > m$ entonces $|\mathcal{F}_i(A,B)| = 0$. Supongamos ahora que $n \leq m$. Entonces vale lo siguiente:

TEOREMA 1.21. *Sean* $A = \{a_1,\dots,a_n\}$, $B = \{b_1,\dots,b_m\}$, *con* $n \leq m$. *Entonces*

$$|\mathcal{F}_i(A,B)| = m(m-1)\dots(m-n+1) = \frac{m!}{(m-n)!},$$

donde $m! = m(m-1)\cdots 2 \cdot 1$.

PRUEBA. Si $f : A \mapsto B$ es una función inyectiva, entonces $f(a_1)$ tiene como posibles valores a b_1, b_2, ..., b_m, o sea m posibilidades. Ahora, fijado $f(a_1)$, hay $(m-1)$ posibles valores para $f(a_2)$ ya que debe ser distinto a $f(a_1)$. Luego hay $m \cdot (m-1)$ valores posibles para el par $(f(a_1), f(a_2))$.

Fijos $f(a_1)$ y $f(a_2)$ hay $(m-2)$ posibles valores para $f(a_3)$:

$$f(a_3) \in B - \{f(a_1), f(a_2)\}.$$

Así sucesivamente, fijados $f(a_1)$, $f(a_2)$, $\dots f(a_{n-1})$ hay $m-(n-1)$ posibles valores para $f(a_n)$:

$$f(a_n) \in B - \{f(a_1), f(a_2), \dots, f(a_{n-1})\}.$$

Luego

$$|\mathcal{F}_i(A,B)| = m(m-1)(m-2)\dots(m-(n-1)) = \frac{m!}{(m-n)!},$$

y este es el número de funciones inyectivas distintas. Observar que para una demostración formal habría que reemplazar el ´´Así sucesivamente"por un razonamiento inductivo (Ejercicio). □

EJERCICIO 1.4. Demuestre el Teorema 1.21 aplicando el principio de inducción.

EJERCICIO 1.5. ¿Cuántas banderas distintas se pueden hacer de 3 bandas verticales con los colores rojo, blanco, azul y verde, si no puede haber dos bandas del mismo color?

SOLUCIÓN. En este caso debemos determinar el número de aplicaciones inyectivas de un conjunto de 3 elementos (bandas) en un conjunto de 4 elementos (colores):

$$\left|\mathcal{F}_i(\{1,2,3\}, \{\text{rojo, blanco, azul, verde}\})\right| = \frac{4!}{(4-3)!} = \frac{4!}{1!} = 4!,$$

luego pueden hacerse $4!$ banderas diferentes. □

COROLARIO 1.22. *Si $n = m$ se tiene que el número de funciones biyectivas de A en B es*

$$|\mathcal{F}_b(A,B)| = m(m-1)\dots 3 \cdot 2 \cdot 1 = m!$$

Recordemos del Ejemplo 1.4 que $|\mathcal{F}_b(\{1,2,3\}, \{1,2,3\})| = 3 \cdot 2 = 6$.

EJEMPLO 1.23. Si en un ómnibus hay 10 asientos vacíos, ¿de cuántas maneras pueden sentarse 7 personas?

RESPUESTA. Debemos calcular el número de funciones inyectivas que hay de un conjunto de 7 elementos (personas) en uno de 10 elementos (asientos). Esto es:

$$|\mathcal{F}_i(\{p_1,\ldots,p_7\},\{a_1,\ldots,a_{10}\})| = \frac{10!}{(10-7)!} = 10\cdot 9\ldots 5\cdot 4 = 604800.$$

□

Si A es un conjunto de cardinal m, una *selección ordenada* de n elementos de A es una función inyectiva $f : [1,n] \mapsto A$.

DEFINICIÓN 1.24. Un *arreglo* de n objetos tomados de un conjunto de m objetos es una selección *ordenada* de n objetos entre los m dados. Si $n = m$ el arreglo se llama también *permutación* de $\{1,\ldots,m\}$. Equivalentemente, una permutación es una función biyectiva de $\{1,\ldots,m\}$ en $\{1,\ldots,m\}$.

EJEMPLO 1.25. Sea $A = \{a,\ b,\ c,\ d\}$. Entonces (a,b,c), (b,a,c) y (b,c,a) son 3 arreglos distintos de 3 elementos tomados de un conjunto de 4 elementos.

EJEMPLO 1.26. Las permutaciones del conjunto $B = \{x,\ y,\ z\}$ son (x,y,z), (x,z,y), (y,x,z), (y,z,x), (z,x,y), (z,y,x).

Dar un arreglo de n objetos tomados de un conjunto de m objetos es equivalente a elegir una función inyectiva de un conjunto de cardinal n en otro de cardinal m. Por lo tanto, la cantidad de arreglos de este tipo es igual al número de funciones inyectivas de $\{1,\ldots,n\} \mapsto \{1,\ldots,m\}$, es decir, $\dfrac{m!}{(m-n)!}$.

Se denota por $A(n,m)$ al conjunto de los arreglos de n elementos tomados de un conjunto de m elementos y por $\mathcal{P}_m$ al conjunto de permutaciones de m elementos. Si dejamos a un lado el orden y seleccionamos objetos de entre m dados se tiene una *combinación* de m elementos de un conjunto de n. Se denota al conjunto de estas combinaciones por $C(n,m)$.

EJEMPLO 1.27. Una lista de todos los subconjuntos de 3 elementos del conjunto $\{1,2,3,4,5\}$ es la siguiente:

$\{1,2,3\}, \{1,2,4\}, \{1,2,5\}, \{1,3,4\}, \{1,3,5\}, \{1,4,5\}, \{2,3,4\}, \{2,3,5\}, \{2,4,5\}, \{3,4,5\}$.

En cuanto a las cardinalidades, tenemos, si $1 \le n \le m$,

$$\begin{aligned} |A(n,m)| &= m(m-1)\ldots(m-n+1) = \frac{m!}{(m-n)!}, \\ |\mathcal{P}_m| &= |A(m,m)| = m! \\ |C(n,m)| &= \frac{|A(n,m)|}{|\mathcal{P}_n|} = \frac{m!}{n!(m-n)!} \end{aligned}$$

Se define el *número combinatorio* $\binom{m}{n}$ como

$$\binom{m}{n} := \frac{m!}{n!(m-n)!}.$$

Por convención se toma $0! = 1$, de donde se tiene $\binom{m}{0} := 1$ para todo $m \in \mathbb{N}_0$. Según acabamos de ver, $\binom{m}{n}$ representa el número total de subconjuntos de n elementos de un conjunto de m elementos. En el caso particular $m = 5, n = 3$ tenemos $\binom{m}{n} = \frac{5!}{3!2!} = \frac{5 \cdot 4}{2} = 10$, coincidentemente con lo hallado en el Ejemplo 1.27.

Se tienen las siguientes propiedades de los números combinatorios:

TEOREMA 1.28. *Sea m natural y $n \leq m$. Entonces se tiene*

(i) $\binom{m}{1} = m.$

(ii) $\binom{m}{n} = \binom{m}{m-n}$, *si* $n \geq 0$.

(iii) $\binom{m}{n-1} + \binom{m}{n} = \binom{m+1}{n}$, *si* $n \geq 1$.

(iv) *El total de subconjuntos de un conjunto de m elementos es 2^m. El total de subconjuntos de n elementos de un conjunto de m elementos es $\binom{m}{n}$, luego*

$$\sum_{n=0}^{m} \binom{m}{n} = 2^m.$$

PRUEBA. (i)

$$\binom{m}{1} = \frac{m!}{1!(m-1)!} = m.$$

(ii) Se sigue de la definición de $\binom{m}{n}$.

(iii) Se tiene

$$\binom{m}{n-1} + \binom{m}{n} = \frac{m!}{(n-1)!(m-n+1)!} + \frac{m!}{n!(m-n)!} = \tag{8}$$

$$m!\left(\frac{n+(m-n+1)}{n!(m-n+1)!}\right) = \frac{(m+1)!}{n!(m+1-n)!} = \binom{m+1}{n}$$

(iv) Ya hemos visto en la Proposición 1.17 que $|\mathcal{P}(\{1,\ldots,m\})| = 2^m$. A continuación veremos una prueba diferente de este hecho, por inducción.
Si $m = 1$, entonces $\mathcal{P}(\{1\}) = \{\emptyset, \{1\}\}$; luego $|\mathcal{P}(\{1\})| = 2 = 2^1$. Si la proposición es verdadera para un cierto k, veamos que también se cumple para $k+1$.

Dividimos los subconjuntos de $\{1,\ 2,\ \ldots,\ k,\ k+1\}$ en dos tipos: los que no contienen a $k+1$ y los que sí lo contienen. Si Y es un subconjunto que no tiene a $k+1$ como elemento, entonces es un subconjunto de $\{1,\ 2,\ \ldots,\ k\}$; si Y contiene a $k+1$ entonces es unión de un subconjunto de $\{1,\ 2,\ \ldots,\ k\}$ y $\{k+1\}$. Por hipótesis inductiva, hay 2^k subconjuntos de $\{1,\ 2,\ \ldots,\ k\}$, por lo tanto:

$$|\mathcal{P}(\{1,\ldots,k+1\})| \ = \ 2^k + 2^k = 2^{k+1}.$$

Por lo tanto $|\mathcal{P}(\{1,\ldots,m\})| = 2^m$ para todo m natural.

En particular, si $|A| = m$, entonces $\mathcal{P}(A)$ se expresa como la unión del todos los subconjuntos de A de n elementos, con n variando entre 0 y m, o sea:

$$\mathcal{P}(\{a_1,\ldots,a_m\}) = \bigcup_{n=0}^{m} \{\text{ subconjuntos de } n \text{ elementos}\},$$

y como dicha unión es disjunta tenemos que

$$|\mathcal{P}(A)| = \sum_{n=0}^{m} |\{\text{ subconjuntos de } n \text{ elementos}\}| = \sum_{n=0}^{m} \binom{m}{n},$$

luego $2^m = \sum_{n=0}^{m} \binom{m}{n}$. □

EJEMPLO 1.29. 1. $\binom{8}{3} = \dfrac{8\cdot 7\cdot 6\cdot 5\cdot 4\cdot 3\cdot 2\cdot 1}{(5\cdot 4\cdot 3\cdot 2\cdot 1)(1\cdot 2\cdot 3)} = \dfrac{8\cdot 7\cdot 6}{1\cdot 2\cdot 3} = 56.$

2. $\binom{5}{3} + \binom{5}{4} = \binom{6}{4} = \binom{6}{2} = \dfrac{6\cdot 5}{2\cdot 1} = 15$

3. $\binom{6}{0} + \binom{6}{1} = 1 + 6 = 7 = \binom{7}{1}.$

Los siguientes ejercicios han sido seleccionados del libro *Notas de Álgebra* de Enzo Gentile.

EJERCICIO 1.6. Hallar n tal que $3\binom{n}{4} = 5\binom{n-1}{5}$.

SOLUCIÓN. Planteamos la ecuación

$$3\frac{n!}{4!(n-4)!} = 5\frac{(n-1)!}{5!(n-6)!}.$$

Esta ecuación tiene sentido sólo para $n \geq 6$. Bajo esta hipótesis, podemos dividir ambos miembros por $(n-1)!$ y multiplicar por $(n-4)!$:

$$\begin{aligned} 3\frac{n!}{(n-1)!} &= \frac{(n-4)!}{(n-6)!} \\ 3\frac{n!}{(n-1)!} &= (n-4)(n-5) \\ \text{de donde resulta} \qquad 3n &= n^2 - 9n + 20 \\ n^2 - 12n + 20 &= 0. \end{aligned}$$

Las raíces de la ecuación son $n = 2$ y $n = 10$. La solución al problema es entonces $n = 10$, ya que para $n = 2$ el número combinatorio $\binom{n}{4}$ no tiene sentido. □

EJERCICIO 1.7. ¿Cuántos equipos de fútbol se pueden formar con 18 jugadores?

SOLUCIÓN. Considerando que para formar un equipo de fútbol se necesitan 11 jugadores, la cantidad de equipos posibles es igual al número combinatorio $\binom{18}{11}$. □

EJERCICIO 1.8. ¿Cuántos equipos de fútbol se pueden formar con 1 arquero, 4 defensores, 4 mediocampistas y 2 atacantes si hay 3 arqueros, 6 defensores, 5 mediocampistas y 4 atacantes.

SOLUCIÓN. Hay $\binom{3}{1}$ maneras de elegir un arquero, por cada una de estas elecciones hay $\binom{6}{4}$ maneras de elegir un defensor, y así sucesivamente. Luego en este caso la cantidad de equipos posibles que se pueden formar es:

$$\binom{3}{1}\binom{6}{4}\binom{5}{4}\binom{4}{2} = 3 \cdot 15 \cdot 5 \cdot 6 = 45 \cdot 30 = 1350.$$

□

EJERCICIO 1.9. ¿Cuántas rectas hay en el plano determinadas por 10 puntos no alineados de a 3?

PRUEBA. Respuesta: Si no hay tres puntos alineados, entonces dos puntos cualesquiera determinan una única recta. Luego el número de rectas distintas es $\binom{10}{2} = \frac{10 \cdot 9}{2} = 45$. □

EJERCICIO 1.10. ¿Cuántos paralelogramos determinados por 8 rectas paralelas y 6 paralelas (no paralelas a las anteriores) hay?

SOLUCIÓN. Por cada par de rectas que se toman de las 8 paralelas hay $\binom{6}{2}$ maneras de elegir dos rectas paralelas entre las otras 6. Luego la cantidad de paralelogramos determinados es:

$$\binom{8}{2}\binom{6}{2} = 28 \cdot 15 = \frac{28 \cdot 30}{2} = 14 \cdot 30 = 420.$$

□

EJERCICIO 1.11. ¿Cuántas palabras distintas se pueden formar con las letras de la palabra *neuquen* alterando el orden de las letras?

SOLUCIÓN. Calculemos primero cuántas palabras se pueden formar con la palabra *mano*. Esto es exactamente el número de permutaciones de un conjunto de 4 letras, o sea $4!$.

Si ahora pensamos en la palabra *mono* tenemos una letra (la letra o) repetida. Luego el número de palabras distintas es el número de permutaciones de un conjunto de 4 elementos dividido por el número de permutaciones de un conjunto de 2 elementos (pues al permutar las dos letras "o" iguales se obtiene la misma palabra) o sea: $\frac{4!}{2!}$.

En cuanto a la palabra *neuquen*, la cantidad de palabras distintas es $\frac{7!}{2!2!2!} = 630$, puesto que n, e y u se repiten cada una 2 veces. □

EJERCICIO 1.12. ¿Cuántos números distintos se pueden formar con los dígitos de 1112233345?

SOLUCIÓN. Por un razonamiento análogo al del ejercicio anterior hay

$$\frac{10!}{3!2!3!} \text{ números distintos.}$$

□

EJERCICIO 1.13. ¿Cuántos números distintos de 7 cifras se pueden formar con los dígitos de 1122200?

SOLUCIÓN. Debemos contar sólo los que empiezan con 1 ó 2. Números de 7 cifras que empiecen con 1 hay $\frac{6!}{3!2!} = 60$, y números de 7 cifras que empiecen con 2 hay $\frac{6!}{2!2!2!} = 90$. En total son $60 + 90 = 150$ números. □

EJERCICIO 1.14. (i) ¿Cuántos comités distintos posibles de 3 personas se pueden formar, si hay 5 hombres y 4 mujeres?

(ii) ¿Cuántos de estos comités tienen al menos una mujer?

SOLUCIÓN. (i) La cantidad total de personas es $4 + 5 = 9$. Luego se pueden formar $\binom{9}{3}$ comités distintos.

(ii) A la cantidad total de comités posibles debemos restarle la cantidad de comités que se pueden formar con hombres solamente, es decir $\binom{5}{3}$. Luego la respuesta es

$$\binom{9}{3} - \binom{5}{3} = \frac{9 \cdot 8 \cdot 7}{1 \cdot 2 \cdot 3} - \frac{5 \cdot 4 \cdot 3}{1 \cdot 2 \cdot 3} = 84 - 10 = 74.$$

□

EJERCICIO 1.15. ¿En cuántas disposiciones distintas se pueden sentar 8 personas alrededor de una mesa circular?

SOLUCIÓN. Acordamos que una disposición es diferente de otra si las posiciones relativas de las personas cambian; es decir, si alguna de las personas tiene un compañero diferente a su derecha (o lo que es lo mismo, alguna persona tiene un compañero diferente a la izquierda). Así, si todos cambian de silla rotando uno o más lugares, la disposición sigue siendo misma.

Luego al número total de distribuciones de 8 personas en 8 sillas debemos dividirlo por el número de rotaciones en una ronda de 8 personas, es decir por 8; luego la respuesta es $\frac{8!}{8} = 7!$.

Otra manera de resolverlo, es asumir que una de las personas queda fija en un lugar, y las demás ocupan alguno de los 7 lugares restantes. Puesto que hay 7 sillas, hay $7!$ formas diferentes de sentar a las 8 personas. □

EJERCICIO 1.16. Idem al ejercicio anterior, pero suponiendo que hay 4 hombres y 4 mujeres y deben intercalarse.

EJERCICIO 1.17. ¿Cuántas banderas distintas se pueden hacer con 3 bandas verticales rojas y 2 blancas?

RESPUESTA. $\frac{5!}{3!2!} = 10$. □

EJERCICIO 1.18. ¿Cuántas líneas quedan determinadas por m puntos en el plano si k puntos de ellos (y sólo estos) están sobre una recta?

SOLUCIÓN. La cantidad total de rectas determinadas por m puntos es $\binom{m}{2}$. Como hay k puntos alineados, estos pares de puntos determinan la misma recta. Luego debemos restar $\binom{k}{2} - 1$. El número total de líneas es entonces

$$\binom{m}{2} - \binom{k}{2} + 1.$$

□

EJERCICIO 1.19. De 20 naturales consecutivos, ¿cuántos pares (m, n) pueden formarse tal que la suma sea par (resp. impar) ? (m y n pueden ser iguales o distintos).

EJERCICIO 1.20. Supongamos que Sergio tiene 12 amigos: 7 mujeres y 5 varones y Ernesto tiene 12 amigos, 5 mujeres y 7 varones. Además suponemos que no tienen amigos en común. ¿De cuántas formas se pueden invitar 6 mujeres y 6 varones de modo que haya 6 amigos de cada uno?

EJERCICIO 1.21. ¿En cuántas formas se pueden disponer en una línea de un tablero de ajedrez las piezas "grandes"(o sea, todas menos los peones)?

SOLUCIÓN. Usemos la notación T: torre, C: caballo, A: alfil, D: dama, R: rey; luego hay que encontrar todas las disposiciones distintas de estas piezas, esto se puede pensar como el número de palabras distintas que se pueden formar alterando el orden de las letras de TCADRACT, y este número es

$$\frac{8!}{2!2!2!} = 7!.$$

□

EJEMPLO 1.30. En el juego del *póker* se tienen una cantidad $n = 4k$ cartas. Si por ejemplo $n = 32$ entonces $k = 8$, y se juega con los ases A, la K, la Q, la J, 10, 9, 8 y 7. Se reparten 5 cartas a cada jugador.

(a) ¿Cuántas manos posibles hay? Es decir, ¿cuántas combinaciones distintas de 5 cartas hay si no se tiene en cuenta el orden en que aparecen?
(b) Un *póker* se forma juntando 4 cartas del mismo valor; por ejemplo un póker de Ases se obtiene juntando 4 ases y una carta diferente. ¿Cuántas maneras hay de formar póker de ases? ¿Cuántas formas hay de formar póker?

(c) Un *full de ases y reyes* se obtiene con 3 ases y 2 reyes, un *full de reyes y ases* se forma con 3 reyes y dos ases. ¿Cuántas maneras hay de formar full de ases y reyes? ¿Cuántas maneras hay de formar algún full?

(d) Se tiene *color* si en una mano se tienen las 5 cartas del mismo palo. ¿Cuántas maneras hay de obtener color?

(e) ¿Cuántas maneras hay de obtener la escalera 8, 9, 10, J, Q? ¿Cuántas maneras hay de obtener una escalera?

SOLUCIÓN. (a) Debemos calcular el número de maneras de tomar 5 cartas de un grupo de n cartas, este número es $\binom{n}{5}$.

(b) Si tenemos 5 cartas y 4 de ellas son ases, quedan $n-4$ posibilidades para la quinta carta restante. Luego hay $n-4$ maneras de formar un póker de ases. Si a $n-4$ lo multiplicamos por la cantidad de valores distintos de las cartas de un mismo palo, es decir por k, obtenemos la cantidad total de póker distintos que podemos formar; es decir $(n-4)\cdot k = \dfrac{(n-4).n}{4}$.

(c) Hay $\binom{4}{3}$ maneras distintas de elegir 3 ases de un conjunto de 4 ases. Por cada una de estas hay $\binom{4}{2}$ maneras distintas de elegir 2 reyes. Luego hay

$$\binom{4}{3}\binom{4}{2}$$

maneras de formar un full de ases y reyes. Para calcular la cantidad total de fulls hay que multiplicar por todos los arreglos posibles de k elementos tomados de a 2. Esto es todas las formas de elegir dos cartas distintas (c_1, c_2) para formar un full de c_1 y c_2. El resultado es

$$k(k-1)\binom{4}{3}\binom{4}{2}.$$

(d) Dada una escalera, por ejemplo 8, 9, 10, J y Q, podemos elegir 4 palos distintos para el 8, 4 para el 9, 4 para el 10, y así sucesivamente. Luego hay 4^5 escaleras de 8, 9, 10, J y Q. Dejamos como ejercicio calcular cuántas escaleras posibles se pueden formar.

□

EJERCICIO 1.22. Se define la *probabilidad* de un evento por medio de la fórmula $p = \frac{F}{P}$, donde F denota el total de casos favorables y P el total de casos posibles.

Para $n = 28$ y $n = 32$, calcular las probabilidades de obtener póker, full y color.

2. Fórmula del binomio

A continuación obtendremos una fórmula para calcular la potencia entera de un binomio. Sabemos que:

$$\begin{aligned}(a+b)^2 &= a^2+2ab+b^2\\ (a+b)^3 &= (a+b)^2(a+b) = a^3+3a^2b+3ab^2+b^3.\end{aligned}$$

Para una potencia n, tenemos que

$$(a+b)^n = (a+b)\cdot(a+b)\ldots(a+b) = \prod_{i=1}^{n}(a+b).$$

Probaremos que esta potencia del binomio puede escribirse como una sumatoria

$$\sum_{k=0}^{n} c_k a^k b^{n-k},$$

donde el coeficiente c_k es igual al número de maneras distintas en que se pueden elegir k factores iguales a a (y por lo tanto $n-k$ factores iguales a b). Es decir que $c_k = \binom{n}{k}$ y por lo tanto se tiene:

TEOREMA 2.1. *Si a y b son números reales y $n \in \mathbb{N}$, entonces*

$$(a+b)^n = \sum_{k=0}^{n}\binom{n}{k}a^k b^{n-k}. \tag{9}$$

PRUEBA. Daremos una prueba alternativa, por inducción. El teorema es cierto para $n=1$. Si vale para un cierto natural n, entonces

$$\begin{aligned}(a+b)^{n+1} &= (a+b)^n(a+b) = (a+b)^n a + (a+b)^n b\\ &= \sum_{k=0}^{n}\binom{n}{k}a^{k+1}b^{n-k} + \sum_{k=0}^{n}\binom{n}{k}a^k b^{n+1-k}\\ &= \binom{n}{n}a^{n+1} + \sum_{k=0}^{n-1}\binom{n}{k}a^{k+1}b^{(n+1)-(k+1)} + \binom{n}{0}b^{n+1} + \sum_{k=1}^{n}\binom{n}{k}a^k b^{(n+1)-k}\\ &= \binom{n+1}{n+1}a^{n+1} + \binom{n+1}{0}b^{n+1} + \sum_{k=1}^{n}\left(\binom{n}{k-1}+\binom{n}{k}\right)a^k b^{(n+1)-k}.\end{aligned}$$

Usando las propiedades de números combinatorios vistas en el Teorema 1.28, concluimos que

$$(a+b)^{n+1} = \sum_{k=0}^{n+1}\binom{n+1}{k}a^k b^{n+1-k},$$

como queríamos probar. Por lo tanto el teorema es cierto para todo n natural. □

Del teorema del binomio se obtiene una nueva demostración del siguiente resultado conocido.

COROLARIO 2.2. $|\mathcal{P}(\{x_1, \ldots, x_n\}| = 2^n$.

PRUEBA. Puesto que en un conjunto de cardinal n hay $\binom{n}{k}$ subconjuntos de k elementos, usando el principio de adición y la fórmula (9), tenemos que

$$|\mathcal{P}(\{x_1, \ldots, x_n\}| = \sum_{k=0}^{n} \binom{n}{k} = (1+1)^n = 2^n.$$

□

COROLARIO 2.3.

$$\sum_{k=0}^{n} (-1)^k \binom{n}{k} = 0.$$

PRUEBA. Se deduce de la fórmula del binomio (9), tomando $a = -1$ y $b = 1$. □

COROLARIO 2.4.

$$(1+x)^n = \sum_{k=0}^{n} \binom{n}{k} x^k.$$

EJERCICIO 2.1. Considerando al número combinatorio $\binom{m}{n}$ como el número de subconjuntos de n elementos de un conjunto de m elementos, explique la identidad

$$\binom{m}{n-1} + \binom{m}{n} = \binom{m+1}{n}.$$

EJERCICIO 2.2. Usando que $(1+x)^m(1+x)^n = (1+x)^{m+n}$, concluya que

$$\binom{m+n}{r} = \binom{m}{0}\binom{n}{r} + \binom{m}{1}\binom{n}{r-1} + \cdots + \binom{m}{r}\binom{n}{0}, \qquad r \leq m, n \geq 1.$$

EJERCICIO 2.3. En el juego del truco calcular:

(i) número total de manos de 3 cartas posibles,

(ii) número total de modos de tener 33,

(iii) número total de modos de tener A de espadas,

(iv) número total de modos de tener A de espadas y un 3.

CAPÍTULO 3

Divisibilidad

1. Los números enteros

En este capítulo desarrollaremos los temas referidos al conjunto de los números enteros, que denotaremos con $\mathbb{Z}$. Estos temas incluyen el concepto de divisibilidad, el algoritmo de la división, el desarrollo s-ádico de un número entero, la noción de máximo común divisor y mínimo común múltiplo, números primos y factorización, y el Teorema Fundamental de la Aritmética.

Comenzamos entonces con la definición del conjunto $\mathbb{Z}$ como el conjunto formado por todos los números naturales, sus opuestos y el cero.

DEFINICIÓN 1.1. Se define el conjunto de números enteros $\mathbb{Z}$ como

$$\mathbb{Z} = \mathbb{N} \cup \{0\} \cup -\mathbb{N}.$$

donde $-\mathbb{N} = \{-n \mid n \in \mathbb{N}\}$. Vemos que $\mathbb{N} = \{x \in \mathbb{Z} \mid x > 0\}$.

La siguiente proposición asegura que el conjunto de números enteros es cerrado para la suma, el producto y la diferencia, y que los únicos números enteros que tienen inverso multiplicativo son los números 1 y -1.

PROPOSICIÓN 1.2.

(i) *Si* $a, b \in \mathbb{Z}$ *entonces* $a + b \in \mathbb{Z}$, $ab \in \mathbb{Z}$ *y* $a - b \in \mathbb{Z}$,

(ii) *Si* $a, b \in \mathbb{Z}$ *entonces* $ab = 1$ *si y sólo si* $\begin{cases} a = b = 1 \\ \text{ó} \\ a = b = -1 \end{cases}$

PRUEBA. (i) Sean $a, b \in \mathbb{Z}$. Si a y b son números naturales ya hemos visto en la Proposición 3.11 que $a + b \in \mathbb{N}$.

Si a y $b \in -\mathbb{N}$ entonces $-a,\ -b \in \mathbb{N}$. Luego $(-a) + (-b) = -(a + b) \in \mathbb{N}$, es decir que $a + b \in -\mathbb{N}$. Por lo tanto $a + b \in \mathbb{Z}$.

Si $a \in \mathbb{N}$ y $b \in -\mathbb{N}$ entonces $a + b = a - (-b)$. Luego si $a > -b$ entonces $a - (-b) \in \mathbb{N}$ y si $a < -b$ entonces $a + b = -(-a - b) \in -\mathbb{N}$. Si $a = -b$ entonces $a + b = 0$. En cualquiera de los casos, $a + b \in \mathbb{Z}$.

Si $a, b \in \mathbb{N}$ entonces $ab \in \mathbb{N}$. Si $-a$ y $-b \in \mathbb{N}$ entonces $ab = (-a)(-b) \in \mathbb{N}$. Si $-a \in \mathbb{N}$ y $b \in \mathbb{N}$ entonces $ab = -(-a)b = -((-a)b)$, luego $ab \in -\mathbb{N}$. Si $a = 0$ o $b = 0$ entonces $ab = 0$. En cualquiera de los casos, $ab \in \mathbb{Z}$.

Por último, si $a, b \in \mathbb{Z}$, entonces $-b \in \mathbb{Z}$. Luego, como $a - b = a + (-b)$ se deduce de la primera parte que $a - b \in \mathbb{Z}$.

(ii) Si $ab = 1$ y a, b pertenecen a $\mathbb{N}$ entonces $a = 1$ y $b = 1$, de lo contrario ocurriría $ab > 1$.

Si $a < 0$ y $b < 0$, y $ab = 1$ entonces $(-a)(-b) = ab = 1$. Luego $-a = 1$ y $-b = 1$, es decir, $a = b = -1$.

Ya hemos visto en el item (i) que si a y b tienen distinto signo entonces $ab \in -\mathbb{N}$, por lo que no se puede dar $ab = 1$. Por otro lado, tampoco puede ser $a = 0$ o $b = 0$. □

Si a y b son dos números reales, y $b \neq 0$, podemos escribir $a = b(ab^{-1})$, siendo ab^{-1} un número real. Es decir, si $a, b \in \mathbb{R}$, y $b \neq 0$, entonces existe $c \in \mathbb{R}$ tal que $a = bc$.

Si ahora nos restringimos al conjunto de los números enteros, entonces ya no podemos asegurar que para cualquier par $a, b \in \mathbb{Z}$, se cumple que ab^{-1} sea un número entero. En los casos en que sea cierto, diremos que b divide a a o que b es un divisor de a. Precisamos esto en la siguiente definición.

DEFINICIÓN 1.3. Sean $a, b \in \mathbb{Z}$, $b \neq 0$. Decimos que b divide a a y denotamos $b \mid a$ si existe $c \in \mathbb{Z}$ tal que $a = bc$.

El siguiente lema enuncia algunas propiedades básicas de divisibilidad.

LEMA 1.4.

(i) *Para cada* $x \in \mathbb{Z}$, $1 \mid x$. *Para cada* $x \neq 0$, $x \mid x$.

(ii) *Si* $a \mid b$ *y* $b \mid c$ *entonces* $a \mid c$.

(iii) *Si* $a \mid (b + c)$ *y* $a \mid b$ *entonces* $a \mid c$.

(iv) *Si* $a \mid b$ *y* $a \mid c$ *entonces* $a \mid (b + c)$ *y* $a \mid (b - c)$.

PRUEBA. (i) Es claro, dado que $x = 1x$, y $x = x1$ para todo $x \in \mathbb{Z}$.

(ii) Sean r, s enteros tal que $c = rb$ y $b = sa$. Entonces

$$c = rb = r(sa) = (rs)a \quad \text{y por lo tanto } a \mid c.$$

(iii) Sean s, $t \in \mathbb{Z}$ tal que $b + c = as$ y $b = at$. Entonces

$$c = as - b = a(s - t). \qquad \text{Luego } a \mid c$$

(iv) Sean s, $t \in \mathbb{Z}$ tal que $b = as$ y $c = at$. Entonces $b + c = a(s + t)$, luego $a \mid (b + c)$.

De manera análoga se puede probar que $a \mid (b - c)$. □

2. Algoritmo de la división

Como lo hemos comentado anteriormente, dados dos números enteros a y b, no siempre ocurre que $a \mid b$. Por ejemplo, 5 no divide a 33, y 3 no divide a 13. Esto es, si queremos repartir equitativamente 33 objetos entre 5 personas entonces podremos darle 6 objetos a cada uno y sobrarán 3. Eso significa que podemos escribir:

$$33 = 5 \cdot 6 + \mathbf{3}, \quad 0 \leq 3 < 5.$$

Aquí el número **3** se llama el *resto de la división* de 33 por 5.

Este ejemplo expresa un hecho general. Dados dos números a y b, $b > 0$, existe un único número entero no negativo r con la propiedad que $0 \leq r < b$ y que $b \mid (a - r)$.

TEOREMA 2.1. *Sean a, $b \in \mathbb{Z}$, $b > 0$, entonces existen enteros q y r tales que*

$$a = bq + r, \text{ con} \qquad 0 \leq r < b.$$

Además, q y r son únicos con esta propiedad, es decir, si

$$a = bq + r, \quad a = bq' + r', \quad \text{con } 0 \leq r, r' < b$$

entonces $q = q'$ y $r = r'$.

Dados a, b, q y r como en el teorema, los números q y r son llamados respectivamente, *cociente* y *resto* de la división de a por b. Notemos que cuando b divide a a, se tiene $r = 0$.

PRUEBA. Sea $a > 0$. Sea

$$H = \{h \in \mathbb{N} \mid hb > a\}.$$

H no es vacío pues $(a + 1)b > a$, es decir, $(a + 1) \in H$. Por el principio de buena ordenación H tiene un primer elemento, $h_0 \in H$. En particular $h_0 - 1 \notin H$. Esto significa que

$$b(h_0 - 1) \leq a < bh_0. \tag{10}$$

Sea $q = h_0 - 1$. Restando a cada miembro de la desigualdad (10) el término bq tenemos que $0 \leq a - bq < b$. Llamamos $r = a - bq$.

Si $a < 0$, entonces $-a > 0$. Luego existen q y r tales que

$$-a = bq + r, \qquad 0 \leq r < b.$$

Si $r = 0$ entonces $a = b(-q) + 0$. Si $r > 0$ tenemos que

$$a = b(-q) - r = b(-q - 1) + (b - r), \qquad 0 < b - r < b.$$

Es decir, si $a < 0$, entonces el resto de la división de a por b es $b - r$, siendo r el resto de la división de $-a$ por b.

Si $a = 0$ entonces $a = b0 + 0$.

Hemos probado entonces que dados a y b enteros, con $b > 0$, existen enteros q y r tales que $a = bq + r$ y $0 \leq r < b$. Veamos que q y r son únicos con esa propiedad. Supongamos que b, b', q, q', r y r' satisfacen:

$$\begin{aligned} a &= bq + r \qquad 0 \leq r < b \\ a &= bq' + r' \qquad 0 \leq r', r < b \text{ con } r' \leq r. \end{aligned}$$

Entonces $0 = b(q - q') + (r - r')$. Sabemos que $0 \leq (r - r') < b$ y que $r - r' = b(q' - q)$; luego $q' - q$ debe ser un natural o $q' - q = 0$. En el primer caso se tiene que $r - r' \geq b$, lo cual es absurdo. Luego debe ser $q' = q$ y en consecuencia $r = r'$. □

EJEMPLO 2.2. Calcular el cociente y el resto de la división de 4231 por 7.

SOLUCIÓN.

$$4231 = 7 \cdot 604 + 3,$$

luego $q = 604$ y $r = 3$ □

EJEMPLO 2.3. Calcular el cociente y el resto de la división de 19 por 6 y de -19 por 6.

SOLUCIÓN.

$$\begin{aligned} 19 &= 3 \cdot 6 + 1, \qquad \textbf{q=3}, \ \textbf{r=1}, \\ -19 &= (-3) \cdot 6 - 1 = (-3) \cdot 6 - 6 + 6 - 1 \\ &= (-4) \cdot 6 + 5, \qquad \textbf{q=-4}, \ \textbf{r=5}. \end{aligned}$$

□

3. Desarrollos en base b, $(b \geq 2)$

El algoritmo de la división es útil para encontrar desarrollos en distintas bases de un número a natural. Usualmente se utiliza el desarrollo en base 10, representándose cada número natural por medio de un conjunto de 10 símbolos:

$$\{0,\ 1,\ 2,\ 3,\ 4,\ 5,\ 6,\ 7,\ 8,\ 9\}.$$

En este sistema, el siguiente de 1 es 2, el siguiente de 2 es 3, y así sucesivamente hasta el 9. Para denotar al siguiente del 9 reemplazamos el 9 por el 0 y escribimos un 1 a la izquierda, luego el siguiente del 9 es el '10' . Al 10 le siguen 11, 12, 13, etc y el siguiente de 19 se obtiene cambiando el 9 por el 0 y sumando 1 al anterior: se obtiene así el número 20. Notemos que si un natural n tiene la escritura

$$a_k a_{k-1} \ldots a_1 a_0,$$

significa que

$$n = a_0 + a_1 \cdot 10 + a_2 \cdot 10^2 + \cdots + a_k 10^k.$$

Si utilizamos un conjunto de b símbolos, y representamos de manera análoga a los números naturales, se dice que se usa un sistema de base b. Por ejemplo, en un sistema de base 4, se utilizan 4 símbolos: 0, 1, 2 y 3. El siguiente de 1 es 2, el siguiente de 2 es 3 y el siguiente de 3 es 10. Luego el número *siete* en base 4 se representa 13, o también $(13)_4$. Es decir,

$$7_{10} = 13_4 \qquad \text{o también} \qquad 7 = 13_4.$$

Si no se coloca el subíndice se sobreentiende que se está escribiendo en base 10. Para encontrar el desarrollo en base b de un número natural usamos el algoritmo de la división dividiendo sucesivamente por potencias de b. Por ejemplo, supongamos que queremos encontrar el desarrollo en base 2 de 13:

$$\begin{aligned} 13 &= 1 \cdot 2^3 + 5, & q_3 &= 1 \\ 5 &= 1 \cdot 2^2 + 1, & q_2 &= 1 \\ 1 &= 0 \cdot 2^1 + 1, & q_1 &= 0 \\ 1 &= 1 \cdot 2^0 + 0, & q_0 &= 1. \end{aligned}$$

Afirmamos que la expresión en sistema binario de 13 es 1101. En efecto,

$$13 = 1 \cdot 2^3 + 5 = 1 \cdot 2^3 + 1 \cdot 2^2 + 1 = 1 \cdot 2^3 + 1 \cdot 2^2 + 0 \cdot 2^2 + 1 = 1 \cdot 2^3 + 1 \cdot 2^2 + 0 \cdot 2^2 + 1 \cdot 2^0.$$

Este mismo procedimiento se efectúa para la expresión de un número $a \in \mathbb{N}$ cualquiera en una base b, $b \geq 2$.

EJERCICIO 3.1. Hallar la expresión del número 53 en base 2 y en base 3.

EJERCICIO 3.2. ¿Cómo averiguar un número de teléfono de 5 cifras con preguntas que sólo se responden por sí o no, haciendo el menor número de preguntas posible?

EJERCICIO 3.3.

1. Escribir el número 1996 en las bases 2, 5 y 11.

2. Expresar el número $(4165)_7$ en base 10.

4. Máximo común divisor

DEFINICIÓN 4.1. Dados a, $b \in \mathbb{Z}$, con $b \neq 0$, decimos que d es *el máximo común divisor* (MCD) de a y b si $d \in \mathbb{N}$ y además

(i) $d \mid a$, $d \mid b$,
(ii) Si $c \mid a$ y $c \mid b$, entonces $c \mid d$.

EJEMPLO 4.2. Calculemos el *máximo común divisor* entre 48 y 72.

SOLUCIÓN. Observemos que

$$\begin{aligned} 48 &= 24 \cdot 2 & 72 &= 36 \cdot 2 \\ 48 &= 16 \cdot 3 & 72 &= 24 \cdot 3 \\ 48 &= 12 \cdot 4 & 72 &= 18 \cdot 4 \\ 48 &= \ 8 \cdot 6 & 72 &= 12 \cdot 6 \\ 48 &= \ 6 \cdot 8 & 72 &= 9 \cdot 8 \\ 48 &= 4 \cdot 12 & 72 &= 6 \cdot 12 \\ 48 &= 2 \cdot 24 & 72 &= 3 \cdot 24, \end{aligned}$$

luego 1, 2, 3, 4, 6, 8, 12, 24 son divisores comunes de 48 y 72, y todo divisor común divide a 24. Luego 24 es un máximo común divisor de 48 y 72. □

NOTA 4.1. Si existe el MCD de a y de b entonces es único, pues si d_1 y d_2 son MCD de a y b, entonces $d_1 \mid d_2$ y $d_2 \mid d_1$. Luego:

$$d_2 = d_1 c = (d_2 c')c = d_2(c'c),$$

por lo tanto $c' = c = 1$ ó $c' = c = -1$; c no puede ser -1 pues d_1 y d_2 son positivos, luego $d_1 = d_2$.

Como prueba alternativa, vemos que $d_1 \mid d_2$ implica $d_1 \leq d_2$ y $d_2 \mid d_1$ implica $d_2 \leq d_1$, luego, ambas en conjunto implican que $d_1 = d_2$.

TEOREMA 4.3. *Dados a, $b \in \mathbb{Z}$, no simultáneamente nulos, existe un único número $d \in \mathbb{N}$ que satisface las condiciones (i) y (ii) de la Definición 4.1. Se llama* el máximo común divisor *de a y b y se denota $d = (a, b)$ o $d = MCD(a, b)$.*

PRUEBA. Podemos suponer que $b \neq 0$. Para probar este teorema usamos un algoritmo debido a Euclides (300 AC) que también permite hallar (a, b). La idea es que, si $b > 0$, entonces existen q_1 y r_1 tales que

$$a = bq_1 + r_1 \qquad 0 \leq r_1 < b.$$

Si $r_1 \neq 0$ dividimos a b por r_1:

$$b = r_1 q_2 + r_2 \qquad 0 \leq r_2 < r_1.$$

Nuevamente, si $r_2 \neq 0$ dividimos r_1 por r_2:

$$r_1 = r_2 q_3 + r_3 \qquad 0 \leq r_3 < r_2$$

Como $r_1 > r_2 > r_3 \ldots$, eventualmente tendremos $r_n = 0$ para algún n, esto es, llegaremos a la situación

$$\begin{aligned} r_{n-3} &= r_{n-2} q_{n-1} + r_{n-1}, \qquad 0 \leq r_{n-1} < r_{n-2} \\ r_{n-2} &= r_{n-1} q_n. \end{aligned}$$

Luego $r_{n-1} \mid r_{n-2}$. Esto implica que $r_{n-1} \mid r_{n-3}$. Como $r_{n-1} \mid r_{n-2}$ y $r_{n-1} \mid r_{n-3}$ entonces $r_{n-1} \mid r_{n-4}$. Así siguiendo concluiremos que r_{n-1} divide a r_1 y r_{n-1} divide a b, y por lo tanto $r_{n-1} \mid a$.

Luego r_{n-1} es divisor de a y de b. Veamos entonces que si c es un divisor de a y de b entonces $c \mid r_{n-1}$.

Invirtiendo el razonamiento observamos que si $c \mid a$ y $c \mid b$ entonces $c \mid r_1$. Si $c \mid b$ y $c \mid r_1$ entonces $c \mid r_2$. Si $c \mid r_1$ y $c \mid r_2$ entonces $c \mid r_3$. Siguiendo así sucesivamente, concluiremos que $c \mid r_{n-1}$. Luego si $c \mid a$ y $c \mid b$ entonces $c \mid r_{n-1}$. Luego $r_{n-1} = (a, b)$.

Esto prueba la existencia del máximo común divisor. La unicidad ya ha sido probada. (ver la Nota 4.1).

Si $b < 0$ el cálculo de (a, b) se hace igual entre a y $-b$, puesto que $(a, -b) = (a, b)$. □

EJEMPLO 4.4. Calcular el máximo común divisor entre a y b siendo $a = 2406$ y $b = 654$.

SOLUCIÓN.

$$\begin{aligned} 2406 &= 654 \cdot 3 + 444 \\ 654 &= 444 \cdot 1 + 210 \\ 444 &= 210 \cdot 2 + 24 \\ 210 &= 24 \cdot 8 + 18 \\ 24 &= 18 \cdot 1 + \boxed{6} \\ 18 &= 6 \cdot 3 + 0 \end{aligned}$$

luego $(2406, 654) = 6$. □

NOTA 4.2. (a) Si $a = 0$ y $b \neq 0$, entonces $d = (0, b) = b$.
(b) Si $c \mid a$ y $c \mid b$, entonces $c \leq (a, b)$.

DEFINICIÓN 4.5. Dos números enteros a y b, no simultáneamente iguales a 0, se dicen *coprimos* si $(a, b) = 1$.

Por ejemplo, $(15, 26) = 1$ luego 15 y 26 son coprimos. $(14, 35) = 7$, luego 14 y 35 no son coprimos. Notemos que 1 es coprimo con todos los enteros.

TEOREMA 4.6. *Dados a, $b \in \mathbb{Z}$, $b \neq 0$, existen s, $t \in \mathbb{Z}$ tales que $sa + tb = (a, b)$. Se dice que (a, b) es combinación lineal entera de a y b.*

PRUEBA. Suponemos $b > 0$ y aplicamos el algoritmo de Euclides. Vemos del Teorema 2.1 que

$$r_{n-1} = (a, b) = r_{n-3} - r_{n-2}q_{n-1} = 1r_{n-3} + (-q_{n-1})r_{n-2}.$$

Luego (a, b) se puede escribir como combinación lineal entera de r_{n-3} y r_{n-2}. Reemplazando r_{n-2} por $r_{n-4} - r_{n-3}q_{n-2}$ llegamos a

$$(a, b) = 1r_{n-3} - (r_{n-4} - r_{n-3}q_{n-2})q_{n-1} = (1 + q_{n-2}q_{n-1})r_{n-3} - q_{n-1}r_{n-4},$$

es decir que (a, b) es una combinación lineal entre r_{n-3} y r_{n-4}. Reemplazando a r_{n-3} por

$$r_{n-5} - r_{n-4}q_{n-3}$$

podemos escribir a (a, b) en términos de r_{n-4} y r_{n-5}. Así siguiendo llegaremos a escribir a (a, b) como una combinación lineal entera de a y b. □

EJEMPLO 4.7. Hemos visto en el Ejemplo 4.4 que $(2406, 654) = 6$. Veamos que 6 se puede escribir como una combinación lineal entre 2406 y 654.

SOLUCIÓN.

$$\begin{aligned}
6 &= 24 - 18 \cdot 1 \\
&= 24 - \overbrace{(210 - 24 \cdot 8)}^{=18} \cdot 1 \\
&= 24 \cdot 9 - 210. \\
6 &= \overbrace{(444 - 210 \cdot 2)}^{=24} \cdot 9 - 210 = 444 \cdot 9 - 210 \cdot 19 \\
&= 444 \cdot 9 - \overbrace{(654 - 444 \cdot 1)}^{=210} \cdot 19 \\
6 &= 444 \cdot 28 - 654 \cdot 19 \\
&= \overbrace{(2406 - 3 \cdot 654)}^{=444} \cdot 28 - 654 \cdot 19 \\
6 &= 2406 \cdot 28 + 654 \cdot (-103)
\end{aligned}$$

luego $s = 28$ y $t = -103$. Observemos que 444, 210, 24 y 18 son los sucesivos restos que se obtuvieron en el Ejemplo 4.4. □

De este teorema se deduce fácilmente el siguiente corolario:

COROLARIO 4.8. *Si* $(a, b) = 1$ *entonces existen* $s, t \in \mathbb{Z}$ *tales que* $sa + tb = 1$.

EJEMPLO 4.9. Vemos que $(9, 32) = 1$. y $(-7) \cdot 9 + 2 \cdot 32 = -63 + 64 = 1$.

NOTA 4.3. El recíproco del Corolario 4.8 también es cierto. Es decir, si existen enteros s y t tales que $sa + tb = 1$ entonces a y b son coprimos.

EJERCICIO 4.1. Probar que si $a, b \in \mathbb{Z}, a \neq 0, b \neq 0$ entonces $\left(\frac{a}{(a,b)}, \frac{b}{(a,b)}\right) = 1$.

5. Números primos

DEFINICIÓN 5.1. Si $p \in \mathbb{Z}$ entonces p se dice un *número primo* si $p \neq \pm 1$ y si p admite como únicos divisores a ± 1 y $\pm p$.

EJEMPLO 5.2. 2 es primo.

SOLUCIÓN. Pues supongamos que $2 = cd$, $c, d \in \mathbb{N}$. Si $c \neq 1$, $d \neq 1$ entonces $c \geq 2$ y $d \geq 2$. Luego $2 = cd \geq 2{,}2 = 4 > 2$. Esto es absurdo. Luego $c = 1$ ó $d = 1$.

Si $2 = cd$, $c, d \in -\mathbb{N}$, entonces $2 = (-c)(-d)$, $-c, -d \in \mathbb{N}$. Luego $-c = 1$ ó $-d = 1$, equivalentemente $c = -1$ y $d = -2$ ó $d = -1$ y $c = -2$. □

EJEMPLO 5.3. 0 no es primo pues todo entero m, $m \neq 0$ divide a 0. Esto es, $0 = m \cdot 0$, $\forall m \in \mathbb{Z}$.

EJERCICIO 5.1. Pruebe que 3 y 5 son números primos.

LEMA 5.4. *Sea $p \in \mathbb{Z}$. Si p es primo, cada vez que p divide a un producto ab de enteros, p divide necesariamente a uno de ellos. En símbolos*

$$p \mid ab \Rightarrow p \mid a \qquad \text{ó} \qquad p \mid b.$$

PRUEBA. Podemos suponer $p > 0$. Supongamos que $p \mid ab$, a y b enteros. Si $p \mid a$ queda demostrado, supongamos entonces que p no dividea a a. Entonces p y a son coprimos y podemos escribir

$$1 = ra + sp$$

para ciertos enteros r y s. Multiplicando ambos miembros por b obtenemos

$$b = rab + spb.$$

Como $p \mid ab$ y $p \mid p$ tenemos que p divide al segundo miembro de la igualdad, y por lo tanto al primero, es decir que $p \mid b$. □

El lema anterior se puede generalizar para un producto de n factores:

LEMA 5.5. *Si p es primo y p divide a un producto de enteros $a_1 a_2 \cdots a_n$, entonces $p \mid a_j$, para algún j, $1 \leq j \leq n$.*

Si p y q son primos positivos y $p \mid q$ entonces $p = q$.

PRUEBA. Probaremos este lema haciendo inducción sobre el número de factores n. Si $n = 1$ es claro: $p \mid a_1$. Supongamos que el teorema se cumple para $n = k$, es decir: si p divide a un producto de k factores entonces p divide a alguno de ellos. Entonces, si p divide a $(a_1 a_2 \cdots a_k)a_{k+1}$, por el Lema 5.4 sabemos que $p \mid (a_1 a_2 \ldots a_k)$ ó $p \mid a_{k+1}$. En el primer caso y por hipótesis inductiva sabemos que p divide a algún a_j, $1 \leq j \leq k$. Si p no divide a este producto de k factores, entonces $p \mid a_{k+1}$. En cualquiera de los casos vemos que p divide a algún a_j, $1 \leq j \leq k+1$.

La segunda afirmación es consecuencia directa de la definición de número primo. □

El Teorema Fundamental de la Aritmética enuncia que todo número entero, distinto de 0, 1 y -1, se factoriza como producto de un número finito de primos. Además, bajo ciertas hipótesis que precisamos en el teorema, esa factorización es única.

TEOREMA FUNDAMENTAL DE LA ARITMÉTICA . Sea $m \in \mathbb{Z}$, $m \neq 0$, $m \neq 1$ y $m \neq -1$. Entonces m se factoriza como producto de primos positivos p_1, p_2, $\ldots$, p_r de una de las siguientes formas:

$$m = \prod_{j=1}^{r} p_j \qquad \text{ó} \qquad m = -\prod_{j=1}^{r} p_j$$

y esta factorización es única salvo por el orden de los factores.

PRUEBA. Primero veremos la existencia de una tal factorización y luego probaremos la unicidad. En primer lugar, si m es un número primo, entonces m admite una tal factorización. En segundo lugar, probemos que todo número entero positivo no primo se factoriza como producto de dos o más números primos.

Sea entonces $m \in \mathbb{N}$. Sea

$$H = \{m \in \mathbb{N},\, m > 1 \mid m \text{ no es primo y no admite factorización en primos } \}.$$

Si $H \neq \emptyset$, entonces H tiene primer elemento, llamémoslo h. Luego si $h \in H$ entonces h no es primo, por lo tanto $h = ab$, para ciertos naturales a, b con $a \neq 1$, $b \neq 1$. Luego $a < h$ y $b < h$, lo que implica que $a \notin H$ y $b \notin H$. Esto significa que a y b son o bien primos o producto de dos o más primos. Luego h se factoriza en primos y por lo tanto $h \notin H$. Esto es un absurdo, y por lo tanto $H = \emptyset$.

Si m es un entero negativo entonces $-m \in \mathbb{N}$, luego $-m$ se factoriza en primos, es decir, $-m = \prod_{j=1}^{r} p_j$, donde $p_1, \ldots, p_r$ son todos primos. Luego

$$m = (-1) \prod_{j=1}^{r} p_j.$$

Veamos la unicidad de la factorización en primos. Suponemos primero que $m > 1$ admite dos factorizaciones como producto de primos:

$$m = \prod_{j=1}^{r} p_j \qquad \text{y} \qquad m = \prod_{j=1}^{s} p'_j.$$

Probaremos que estas dos factorizaciones sólo pueden diferir en el orden de los factores. Hacemos inducción en r siendo r es el número de primos en la primera factorización.

Es decir, consideramos la siguiente propiedad $P(r)$ del número natural r:

Todo natural m que es producto de r primos tiene una factorización única en primos, salvo a lo sumo en el orden.

Si $r = 1$ entonces $m = p_1$, es decir que m es primo. Luego $m = p_1 = \prod_{j=1}^{s} p'_j$ es primo, lo que implica que $s = 1$ y $p'_1 = p_1$, y por lo tanto $P(1)$ es verdadera.

Si $P(k)$ es cierto para algún natural k, probemos que $P(k+1)$ también lo es. Sea entonces m tal que

$$m = \prod_{j=1}^{k+1} p_j = \prod_{j=1}^{s} p'_j.$$

El primo p_{k+1} divide a m y $m = \prod_{j=1}^{s} p'_j$, luego p_{k+1} divide a algún p'_i. Por el Lema 5.5, debe existir un l tal que $p_{k+1} = p'_l$. Así

$$\frac{m}{p_{k+1}} = \prod_{j=1}^{k} p_j = \prod_{j=1 \ i \neq l}^{s} p'_j.$$

Tenemos entonces que $\frac{m}{p_{k+1}}$ es producto de k primos, y siendo cierto $P(k)$ tal factorización es única salvo en el orden. Luego $s - 1 = k$ y los primos p'_j, $(j \neq l)$ difieren de los primos p_j, $1 \leq j \leq k$, a lo sumo en el orden. Luego $s = k + 1$ y los primos p'_i difieren de los p_i, $1 \leq i \leq k+1$, a lo más en el orden.

Hemos probado que si $m \in \mathbb{N}$, $m > 1$ entonces m se factoriza de manera única salvo en el orden. Si m es un entero negativo $m < -1$, entonces $-m \in \mathbb{N}$ y por lo que acabamos de ver $-m = \prod_1^r p_j$, donde la factorización es única salvo a lo sumo en el orden. Luego $m = -\prod_{j=1}^{r} p_j$ y la factorización es única salvo en el orden de los factores. □

COROLARIO 1. Existe una infinidad de números primos.

PRUEBA. Razonemos por el absurdo. Supongamos que existen solamente un número finito de primos, a saber: $p_1, \ldots, p_m$. Consideremos el número natural $N = 1 + p_1 \cdots p_m$. Como $N > 1$, N admite un divisor primo p, el cual necesariamente es uno de los p_j's. Luego $p = p_j$ para $1 \leq j \leq m$, de donde resulta que p_j divide a $N - p_1 \cdots p_m = 1$, un absurdo. □

EJEMPLO 5.6. Los siguientes enunciados son corolarios del Teorema Fundamental de la Aritmética:

(i) No existen m, n enteros no nulos tales que $m^2 = 15n^2$.
(ii) $\sqrt{2}$ es irracional.
(iii) La ecuación $x^4 = 2^7$ no tiene solución entera.

SOLUCIÓN. Veamos (i), ((ii) y (iii) son similares). Supongamos que existen m y n enteros tales que $m^2 = 15n^2$. Podemos suponer que m y n son positivos. Además, se cumple que $m > 1$ pues $15 > 1$, y $n > 1$ pues 15 no es un cuadrado.

Se tiene entonces que m y n se factorizan de manera única como producto de números primos:

$$m = \prod_{j=1}^{r} p_j, \qquad n = \prod_{i=1}^{s} p'_i$$

luego

$$m^2 = \prod_{j=1}^{r} p_j^2 \qquad \text{y} \qquad 15n^2 = 3 \cdot 5 \prod_{i=1}^{s} p'^2_i.$$

Resulta entonces que:

$$\prod_{j=1}^{r} p_j^2 = 3{,}5 \prod_{i=1}^{s} p'^2_i.$$

Por unicidad de la factorización esto es imposible, pues el primo 3 aparece en la factorización de m^2 un número par de veces (teniendo en cuenta el miembro de la izquierda) y un número impar de veces (de acuerdo al de la derecha). □

EJERCICIO 5.2. Verifique si 1531 es primo.

SOLUCIÓN. Si 1531 no es primo, entonces existe un primo menor que 1531 que lo divide. Sea p el menor primo que divide a 1531. Entonces $1531 = pb$, con $p \leq b$. Luego

$$1531 = pb \qquad \text{y} \qquad p^2 \leq pb = 1531.$$

Esto implica que $p^2 \leq 1531 < 40^2$, y si 1531 no es primo, debe admitir un divisor primo menor que 40, es decir uno de los siguientes:

$$3,\ 5,\ 7,\ 11,\ 13,\ 17,\ 19,\ 23,\ 29,\ 31,\ 37.$$

Haciendo los cálculos necesarios puede verificarse que ninguno de estos primos es divisor de 1531, por lo tanto 1531 es primo. □

Problema abierto: ¿Hay infinitas parejas de primos de la forma n, $n+2$? Ejemplo: 3 y 5, 5 y 7, 29 y 31...

EJERCICIO 5.3. ¿Existen infinitas ternas de primos de la forma n, $n+2$, $n+4$?

RESPUESTA. No. Si n es primo, tomemos el resto de su división por 3.
Si el resto es 0 entonces $3 \mid n$, luego $n = 3$ o $n = -3$. Por lo tanto $n+2 = 5$ y $n+4 = 7$ o bien $n+2 = -1$ y $n+4 = 1$. Luego si 3 divide a n sólo tenemos la terna de primos $(3, 5, 7)$.

Si el resto es 1 entonces n es de la forma $n = 3k+1$. Luego $n+2 = 3k+3 = 3(k+1)$ y $n+4 = 3k+5$. Luego $n+2$ no es primo a menos que $k = 0$ ó $k = -2$. No puede ser $k = 0$ pues $n \neq 1$. Tampoco puede ser $k = -2$ pues tendríamos $n+4 = -1$. En este caso no obtenemos ninguna terna de primos.
Por último, si el resto es 2, n es de la forma $n = 3k+2$. Luego $n+2 = 3k+4$ y $n+4 = 3k+6 = 3(k+2)$. Luego $n+4$ es primo sólo si $k = -1$ o $k = -3$. No puede ser $k = -1$ pues $n \neq -1$. Entonces $k = -3$ y la terna de primos obtenida es $(-7, -5, -3)$.

Por lo tanto las únicas ternas de primos de la forma n, $n+2$ y $n+4$ son $(3, 5, 7)$ y $(-7, -5, -3)$. □

Conociendo la descomposición de dos números a y b en sus factores primos, podemos calcular fácilmente el máximo común divisor (a, b) entre ellos. Precisamente (a, b) se obtiene como el producto de todos los primos que dividen a a **y** a b elevados a la mayor potencia que divide a a y a b simultáneamente.

EJEMPLO 5.7. El máximo común divisor entre $54 = 2 \cdot 3^3$ y $45 = 5 \cdot 3^2$ es $(54, 45) = 2^0 \cdot 3^2 \cdot 5^0 = 9$.

El ejemplo anterior es un caso particular del siguiente resultado general.

PROPOSICIÓN 5.8. *Sean $a, b \in \mathbb{Z}$, $a \neq 0$, $b \neq 0$, tal que $a = \epsilon \prod_{j=1}^{r} p_j^{k_j}$, $b = \epsilon' \prod_{j=1}^{r} p_j^{h_j}$; ϵ, $\epsilon' = \pm 1$, y todos los p_j son primos positivos distintos entre sí, para $1 \leq j \leq r$. (Notar que se*

puede suponer que r es el mismo para a y b completando con $k_j = 0$ ó $h_j = 0$ si un primo no aparece en la factorización de a ó b, respectivamente.) Entonces

$$(a, b) = \prod_{j=1}^{r} p_j^{\text{mín}(k_j, h_j)}.$$

PRUEBA. Sea c un divisor de a: $c = \prod_{j=1}^{r} p_j^{l_j}$. Cada primo p_j aparece en la factorización de c una cantidad menor o igual a la cantidad de veces que aparece en la factorización de a, dicho formalmente

$$c \mid a \Leftrightarrow l_j \leq k_j, \qquad 1 \leq j \leq r.$$

Luego c divide a a y c divide a b si y sólo si $l_j \leq k_j$ y $l_j \leq h_j$, para cada j, esto es si y sólo si $l_j \leq \text{mín}(k_j, h_j)$.

Por lo tanto

$$c \mid a \quad \text{y} \quad c \mid b \quad \Leftrightarrow \quad c \mid \prod_{j=1}^{r} p_j^{\text{mín}(k_j, h_j)},$$

y esto implica que $(a, b) = \prod_{j=1}^{r} p_j^{\text{mín}(k_j, h_j)}$. □

EJEMPLO 5.9. Sea $a = 72$, $b = 192$. Entonces $72 = 2^3 \cdot 3^2$ y $192 = 2^6 \cdot 3$. Por lo tanto $(72, 192) = 2^3 \cdot 3 = 24$.

DEFINICIÓN 5.10. Dados $a, b \in \mathbb{N}$, $m \in \mathbb{Z}$ se llama el *mínimo común múltiplo* de a y b si $m \geq 1$ y además

(i) $a \mid m$ y $b \mid m$,

(ii) si $a \mid n$ y $b \mid n$ entonces $m \mid n$.

Esto es, $m \geq 1$ es el mínimo común múltiplo de a y b si m es un múltiplo positivo de a y de b que divide a cualquier otro múltiplo de a y de b. Se deja como ejercicio para el lector la verificación de que el mínimo común múltiplo está bien definido, es decir, que si existe entonces es único.

Denotaremos m.c.m(a, b) o $[a, b]$ al mínimo común múltiplo de a y b.

TEOREMA 5.11. *Si $a, b \in \mathbb{Z} - \{0\}$, el mínimo común múltiplo está dado por*

(i) $[a, b] = \dfrac{|ab|}{(a, b)}$,

(ii) *si* $a = \prod_{j=1}^{r} p_j^{k_j}$, $b = \prod_{j=1}^{r} p_j^{h_j}$, $k_j,\ h_j \geq 0$, *entonces*

$$[a, b] = \prod_{j=1}^{r} p_j^{\text{máx}(k_j, h_j)}.$$

PRUEBA. (i) Podemos suponer $a > 0$ y $b > 0$ ya que $[a, b] = [|a|, |b|]$.

Como $(a, b) \mid a$ y $(a, b) \mid b$, entonces $\dfrac{b}{(a,b)}$, $\dfrac{a}{(a,b)}$ son enteros. Luego

$$\frac{ab}{(a,b)} = a\frac{b}{(a,b)} = \frac{a}{(a,b)}b,$$

es decir que a y b dividen a $\dfrac{ab}{(a,b)}$.

Si $a \mid n$ y $b \mid n$, entonces existen enteros x e y tales que $n = xa = yb$. Luego

$$x\frac{a}{(a,b)} = y\frac{b}{(a,b)}$$

y dado que $\dfrac{a}{(a,b)}$ y $\dfrac{b}{(a,b)}$ son coprimos (ver Ejercicio 5.4) resulta que $\dfrac{b}{(a,b)}$ divide a x. Luego, si $x = z\dfrac{b}{(a,b)}$ concluimos que

$$n = z\frac{ab}{(a,b)}.$$

(ii) Usando (i), tenemos que

$$\frac{|ab|}{(a,b)} = \frac{\prod_{j=1}^{r} p_j^{k_j+h_j}}{\prod_1^r p_j^{\text{mín}(k_j,h_j)}} = \prod_{j=1}^{r} p_j^{\text{máx}(k_j,h_j)}.$$

□

EJEMPLO 5.12. Calculemos el mínimo común múltiplo entre -192 y 72.

$$[-192, 72] = [192, 72] = [2^6 \cdot 3, 2^3 \cdot 3^2] = 2^6 \cdot 3^2 = 64 \cdot 9 = 576,$$

o también

$$[-192, 72] = \frac{|-192| \cdot |72|}{(-192, 72)} = \frac{192 \cdot 72}{24} = 192 \cdot 3 = 576.$$

EJERCICIO 5.4.

1. Probar que si $xy = u^2$, $u \in \mathbb{Z}$ y $(x, y) = 1$, entonces x e y son cuadrados perfectos.
2. Hallar todos los posibles valores de $(m, m + 6)$, $(m \in \mathbb{N})$.
3. Probar que $3^{2n+2} + 2^{6n+1}$ es divisible por 11, para todo $n \in \mathbb{N}$.

CAPÍTULO 4

Congruencias

En este capítulo estudiaremos la congruencia entre números enteros. La congruencia es una relación de equivalencia asociada con un natural n, en la que cada clase de equivalencia consta de todos los números enteros cuya división por n arroja un mismo resto. Por ejemplo, si $n = 3$, tendremos tres clases de equivalencia:

enteros cuyo resto en la división por 3 es 1: $\ldots, -5, -2, 1, 4, \ldots$,

enteros cuyo resto en la división por 3 es 2: $\ldots, -4, -1, 2, 5, \ldots$,

y enteros cuyo resto en la división por 3 es 0: $\ldots, -3, 0, 1, 4, \ldots$.

1. La relación de congruencia

DEFINICIÓN 1.1. Fijo $n \in \mathbb{N}$, $a, b \in \mathbb{Z}$, se dice que a es *congruente a* b *módulo* n, si $a - b$ es divisible por n. Esto es, si existe $k \in \mathbb{Z}$ tal que $a - b = kn$. En este caso se escribe

$$a \equiv b \mod (n) \quad \text{ó} \quad a \equiv b\,(n).$$

EJEMPLO 1.2. Para $n = 1$ tenemos que $a \equiv b$ para todo $a, b \in \mathbb{Z}$. Para $n = 2$, $a \equiv b\,(2)$ si y sólo si a y b son ambos pares o ambos impares.

EJEMPLO 1.3. Se tiene $3 \equiv 1(2)$, $-2 \equiv 16(9)$.

NOTA 1.1. Por el algoritmo de división, todo $a \in \mathbb{Z}$ es congruente módulo n a un entero r tal que $0 \leq r < n$. Esto es, existen q y r enteros, $0 \leq r < n$ tales que $a = qn + r$, luego $a \equiv r\,(n)$.

Claramente, se tiene que $a \equiv 0(n)$ si y sólo si $n|a$.

PROPOSICIÓN 1.4. *Si* $a \equiv a_1\,(n)$ *y* $b \equiv b_1\,(n)$ *entonces:*

(i) $a + b \equiv a_1 + b_1\,(n)$,

(ii) $ab \equiv a_1 b_1\,(n)$.

PRUEBA.

(i) $(a+b)-(a_1+b_1)=(a-a_1)+(b-b_1)$, como $(a-a_1)$ y $(b-b_1)$ son divisibles por n su suma también lo es. Luego

$$(a+b)\equiv(a_1+b_1)\ (n).$$

(ii) Sumamos y restamos a $ab-a_1b_1$ el término a_1b. Entonces

$$ab-a_1b_1=ab-a_1b+a_1b-a_1b_1=(a-a_1)b+a_1(b-b_1),$$

esta suma es divisible por n y por lo tanto

$$ab\equiv a_1b_1\ (n).$$

□

COROLARIO 1.5. *Si* $a\equiv b\ (n)$, *y* $j\in\mathbb{N}$, *entonces* $a^j\equiv b^j\ (n)$.

PRUEBA. Aplicamos el principio de inducción. Para $j=1$ el resultado es trivial. Si $a^j\equiv b^j\ (n)$, usamos que $a^{j+1}=a^ja$ y $b^{j+1}=b^jb$, y por el inciso (ii) de la proposición anterior se deduce que

$$a^{j+1}\equiv b^{j+1}\ (n).$$

□

La Proposición 1.4 y el Corolario 1.5 son útiles para deducir algunas reglas de divisibilidad. Recordemos que todo número natural se escribe de la forma $x=a_Na_{N-1}\dots a_0$, donde a_0, a_1, $\dots$, a_N son los dígitos de x. Es decir,

$$x=\sum_{i=0}^{N}a_i10^i.$$

Regla de divisibilidad por 3 y por 9: Sea $x=a_Na_{N-1}\dots a_0$. Entonces

$$x=\sum_{i=0}^{N}a_i10^i=\sum_{i=0}^{N}a_i(9+1)^i.$$

Puesto que $(9+1)\equiv 1\ (3)$ y $(9+1)\equiv 1\ (9)$, por el Corolario 1.5 tenemos que $(9+1)^i\equiv 1\ (3)$ y $(9+1)^i\equiv 1\ (9)$, para todo $i\in\mathbb{N}$. Luego

$$\sum_{i=0}^{N}a_i(9+1)^i\ \equiv\ \sum_{i=0}^{N}a_i\ (3)\qquad\text{y}$$

$$\sum_{i=0}^{N}a_i(9+1)^i\ \equiv\ \sum_{i=0}^{N}a_i\ (9).$$

Es decir que x es divisible por 3 (respectivamente por 9) si y sólo si la suma de sus dígitos, $\sum_{i=0}^{N} a_i$, es divisible por 3 (respectivamente por 9).

Regla de divisibilidad por 11: Por un razonamiento análogo al anterior, tenemos que

$$x = \sum_{i=0}^{N} a_i 10^i = \sum_{i=0}^{N} a_i (11-1)^i.$$

Puesto que $(11-1) \equiv -1\ (11)$, se sigue que

$$\sum_{i=0}^{N} a_i (11-1)^i \equiv \sum_{i=0}^{N} a_i (-1)^i\ (11),$$

luego x es divisible por 11 si y sólo si la suma alternada de sus dígitos

$$a_0 - a_1 + a_2 - \cdots + (-1)^N a_N$$

es divisible por 11.

EJEMPLO 1.6. 121 es divisible por 11 pues la suma alternada de sus coeficientes es $1-2+1=0$, que es divisible por 11.

12321 no es divisible por 11 pues $1-2+3-2+1=1$ no es divisible por 11.

1234321 sí es divisible por 11 pues la suma alternada de sus coeficientes es igual a 0. ¿Qué puede decir de los números 123454321, 12345654321, 1234567654321, 123456787654321 y 12345678987654321?

EJEMPLO 1.7. Dar una regla de divisibilidad por 4 y por 8, usando congruencias.

SOLUCIÓN. Como $10^2 = 100$ es divisible por 4, entonces 10^i es divisible por 4 para todo i natural mayor o igual a 2. Luego, si $x = a_N a_{N-1} \ldots a_0$, entonces

$$x = \sum_{i=0}^{N} a_i 10^i \equiv a_0 + a_1 10\ (4).$$

También tenemos que 10^i es divisible por 8 para todo $i \in \mathbb{N}$, $i \geq 3$. Luego

$$x \equiv a_0 + a_1 10 + a_2 10^2 \equiv a_0 + 2a_1 + 4a_2\ (8).$$

Podemos decir entonces que un número entero es divisible por 4 si el número formado por sus dos últimas cifras lo es, y un número es divisible por 8 si la suma de las unidades más el doble de las decenas más el cuádruple de las centenas lo es, o si el número formado por las 3 últimas cifras lo es. □

2. Ecuaciones en congruencias

Los siguientes ejemplos se resuelven aplicando las propiedades de congruencia de números enteros.

EJEMPLO 2.1. Resolver la congruencia $7^{12} \equiv x\ (11)$.

SOLUCIÓN. Debemos hallar un valor de x, entero, que resuelva dicha ecuación. Tenemos que

$$7^2 \equiv 5\ (11) \qquad \Rightarrow 7^2 \cdot 7 \equiv 5 \cdot 7\ (11) \qquad \Rightarrow \qquad 7^3 \equiv 2\ (11).$$

Dado que $7^{12} = (7^3)^4$ y $2^4 \equiv 5\ (11)$, se sigue que

$$7^{12} \equiv 5\ (11).$$

Luego 7^{12} es congruente a 5 módulo 11 y también es congruente a todos los enteros de la forma $11 \cdot k + 5$, con $k \in \mathbb{Z}$. □

EJEMPLO 2.2. Hallar la cifra de las unidades de 17^{15}.

SOLUCIÓN. La cifra de las unidades se obtiene tomando el resto de la división por 10. Es decir, debemos hallar un valor de x entero, con $0 \leq x < 10$ tal que $17^{15} \equiv x\ (10)$. Ahora

$$17^{15} = (10+7)^{15} \equiv 7^{15}\ (10),$$

$$7^{15} = (10-3)^{15} \equiv (-3)^{15}\ (10),$$

$$(-3)^{15} = (-1)3^{15} = (-1)3^{2\cdot 7+1} \equiv (-1)9^7 \cdot 3\ (10),$$

$$9^7 = (10-1)^7 \equiv (-1)^7 \equiv -1\ (10), \quad \text{y entonces}$$

$$17^{15} \equiv (-1)9^7 \cdot 3 \equiv 3\ (10).$$

Otra forma es:

$$7^2 = 49 \equiv 9\ (10) \Rightarrow 7^3 \equiv 3\ (10) \Rightarrow 7^4 \equiv 1\ (10)$$

luego

$$7^{15} = 7^{12+3} = (7^4)^3 \cdot 7^3 \equiv 1 \cdot 3\ (10).$$

La cifra de las unidades de 17^{15} es 3. □

EJERCICIO 2.1. Hallar los restos de la división de 3^8, 2^{21} y 8^{25} por 5, 13 y 127, respectivamente.

EJEMPLO 2.3. Resolver las congruencias

(i) $x^2 \equiv 1\ (4)$,

(ii) $x^2 \equiv x\ (12)$,

(iii) $x^2 \equiv 2\ (3)$,

(iv) $x^2 \equiv 0\ (12)$,

(v) $x^2 \equiv 1\ (16)$.

SOLUCIÓN. (i) Notemos que si x es solución, entonces $x + 4k$ también es solución, para todo $k \in \mathbb{Z}$, ya que

$$x + 4k \equiv x\ (4) \quad \Rightarrow \quad (x + 4k)^2 \equiv x^2 \equiv 1\ (4).$$

Luego es suficiente encontrar las soluciones x tales que $0 \leq x < 4$.

Tenemos que $1^2 \equiv 3^2\ (4)$ y $2^2 \equiv 0^2\ (4)$; además $0 \not\equiv 1\ (4)$. Por lo tanto $x^2 \equiv 1\ (4)$ si y sólo si $x \equiv 1\ (4)$ ó $x \equiv 3\ (4)$.

(ii) Nuevamente es fácil ver que si x es solución, entonces $x+12k$ es solución, para todo $k \in \mathbb{Z}$. Si $12 \mid x(x-1)$ entonces 3 y 2^2 dividen a $x(x-1)$. Si $2 \mid x$ entonces 2 no divide a $x-1$, y viceversa. Luego debe ser que $x \equiv 0\ (4)$ o $x \equiv 1\ (4)$. Las posibilidades entonces son:

$x \equiv 0\ (4)$ y $x \equiv 0\ (3)$,
$x \equiv 0\ (4)$ y $x \equiv 1\ (3)$,
$x \equiv 1\ (4)$ y $x \equiv 0\ (3)$,
$x \equiv 1\ (4)$ y $x \equiv 1\ (3)$.

Esto nos dice que las soluciones son:

$x \equiv 0\ (12)$,
$x \equiv 4\ (12)$,
$x \equiv 9\ (12)$,
$x \equiv 1\ (12)$.

(iii) Si x es solución, entonces $x + 3k$ es solución para cada k entero, pues $(x + 3k)^2 \equiv x^2\ (3)$. Por lo tanto si existe una solución debe haber también una entre 0 y 3. Pero 0, 1 y 2 no son soluciones, luego $x^2 \equiv 2\ (3)$ no tiene solución.

(iv) Se deja como ejercicio.

(v) En este caso vemos que si x es solución, entonces $x + 8k$ es solución, pues

$$(x + 8k)^2 = x^2 + 16(xk + 4k^2) \equiv x^2\ (16).$$

Por otro lado, $x^2 \equiv 1\ (16)$ implica que $16 \mid x^2 - 1 = (x-1)(x+1)$. Si $x-1$ es divisible por 4 entonces $x+1$ no lo es, y viceversa. Luego debe ser

$$x \equiv 1\ (8) \quad \text{o} \quad x \equiv -1\ (8).$$

Luego las soluciones son $x \equiv 1\ (8)$ y $x \equiv 7\ (8)$. □

Es claro que las soluciones de la ecuación $x \equiv a\ (n)$ son los números de la forma $x = a+nk$, con $k \in \mathbb{Z}$ arbitrario. Ahora bien, no todas las ecuaciones lineales en congruencias, es decir del tipo

$$ax \equiv b\ (n), \text{ con } a \in \mathbb{N}. \tag{11}$$

tienen solución.

Por ejemplo, no existe ningún x tal que $2x \equiv 1\ (4)$, puesto que $2x-1$ es impar para cualquier valor entero de x y en consecuencia no es divisible por 4. Sí en cambio existe solución de la ecuación $2x \equiv 5\ (3)$, en particular $x = 4$ es solución, (y también 1, 7, 10, 13, ...) La siguiente proposición asegura en qué casos la ecuación (11) tiene solución.

PROPOSICIÓN 2.4. *Sean a, $b \in \mathbb{Z}$ y $n \in \mathbb{N}$. La ecuación*

$$ax \equiv b\ (n)$$

tiene solución si y sólo si $(a,n) \mid b$. La solución es única módulo $\dfrac{n}{(a,n)}$. Esto es, si x_0 es una solución, toda otra solución es de la forma $x = x_0 + \dfrac{n}{(a,n)}k$ con $k \in \mathbb{Z}$.

PRUEBA. Supongamos primero que a y n son coprimos, esto es $(a,n) = 1$. Entonces existen s, t enteros tales que $1 = sa + tn$. Luego $b = b\,(sa + tn) = (bs)a + (bt)n$, y por lo tanto

$$(bs)\, a \equiv b\ (n).$$

Se sigue que $x = bs$ es una solución.

Por otro lado, si x_0 es solución, entonces $x_0 + kn$ también lo es, pues $a(x_0 + kn) \equiv ax_0\ (n)$. Recíprocamente, si x_0 y x_1 son soluciones entonces

$$ax_0 \equiv b \quad (n)$$

$$ax_1 \equiv b \quad (n).$$

Luego $a(x_0 - x_1) \equiv 0\ (n)$, es decir que n divide a $a(x_0 - x_1)$. Puesto que $(a,n) = 1$, se sigue que n divide a $(x_0 - x_1)$; es decir que $x_1 = x_0 + kn$, para algún entero k.

Veamos ahora el caso general. Sea $(a,n) = sa + tn$; luego se tiene

$$1 = s\frac{a}{(a,n)} + t\frac{n}{(a,n)} \quad \text{y} \quad b = bs\frac{a}{(a,n)} + bt\frac{n}{(a,n)}.$$

En el caso en que (a,n) divide a b, se tiene que $x = s\dfrac{b}{(a,n)}$ es una solución de $ax \equiv b\ (n)$.

Por otro lado, si x es solución de la ecuación (11), entonces $ax - b = kn$, para algún $k \in \mathbb{Z}$. Como (a,n) divide a a y divide a n, se sigue que (a,n) divide a b. Por lo tanto, la solución existe si y sólo si (a,n) divide a b.

Supongamos entonces que (a,n) divide a b y determinemos, en este caso, todas las soluciones de la ecuación. Tenemos que x_0 es solución de (11) si y sólo si x_0 es solución de

$$\frac{a}{(a,n)}x \equiv \frac{b}{(a,n)}\ \left(\frac{n}{(a,n)}\right). \tag{12}$$

Puesto que $\dfrac{a}{(a,n)}$ y $\dfrac{n}{(a,n)}$ son coprimos, se tiene por la primera parte de la demostración que dicha solución es única módulo $\dfrac{n}{(a,n)}$, esto es, toda solución es de la forma $x_0 + k\frac{n}{(a,n)}$, con $k \in \mathbb{Z}$. □

EJEMPLO 2.5. Resolver la congruencia $2x \equiv 3\ (6)$.

SOLUCIÓN. No existe solución pues $(2,6) = 2$ no divide a 3. □

EJEMPLO 2.6. Resolver la congruencia $5x \equiv 6\ (7)$.

SOLUCIÓN. Tenemos que $(5,7) = 1$, luego la solución existe y es única módulo 7. Tenemos que $(5,7) = 1 = 3 \cdot 5 + (-2) \cdot 7$, de donde se sigue que

$$(6 \cdot 3) \cdot 5 + 6(-2) \cdot 7 = 6,$$

y por lo tanto $18 \cdot 5 \equiv 6\ (7)$. Entonces todas las soluciones de $5x \equiv 6\ (7)$ son de la forma $x = 18 + k \cdot 7$, $k \in \mathbb{Z}$. Por ejemplo, -3, 4, 11, 18, 25, son soluciones y $x = 4$ es la única solución entre 0 y 7. □

EJERCICIO 2.2. Resolver la congruencia $23x \equiv 41\ (52)$.

EJEMPLO 2.7. Resolver la congruencia $42x \equiv 50\ (76)$.

SOLUCIÓN. En este caso a y n no son coprimos puesto que $(42,76) = 2$. Dado que 2 divide a 50, entonces la ecuación tiene solución, y es única salvo múliplos de 38. Para hallar una solución, basta resolver la congruencia

$$21x \equiv 25\ (38).$$

Queremos encontrar s y t tales que $21s + 38t = 1$. Aplicamos el algoritmo de división:

$$\begin{aligned} 38 &= 21 \cdot 1 + 17 \\ 21 &= 17 \cdot 1 + 4 \\ 17 &= 4 \cdot 4 + 1 \\ 4 &= 4 \cdot 1 + 0, \end{aligned}$$

luego $1 = 17 - 4 \cdot 4 = 17 - 4(21 - 17) = 17 \cdot 5 - 4 \cdot 21 = (38 - 21) \cdot 5 - 4 \cdot 21 = 38 \cdot 5 - 9 \cdot 21$, por lo que podemos escribir

$$25 = 38 \cdot 5 \cdot 25 + (-9) \cdot 21 \cdot 25, \qquad \text{y por lo tanto} \qquad 25 \equiv (-9 \cdot 25) \cdot 21 \ (38).$$

Como $-9 \cdot 25 = -225 = -6 \cdot 38 + 3$, entonces $x = 3$ es la única solución entre 0 y 38. □

EJERCICIO 2.3. Hallar el menor $x \in \mathbb{N}$ tal que $4^{1000} \equiv x \ (9)$.

SOLUCIÓN. Tenemos que

$$4^2 \equiv 7 \ (9) \qquad \Rightarrow \qquad 4^3 \equiv 28 \equiv 1 \ (9),$$

puesto que $1000 = 3 \cdot 333 + 1$, entonces

$$4^{3 \cdot 333 + 1} = (4^3)^{333} \cdot 4 \equiv 1^{333} \cdot 4 \equiv 4 \ (9),$$

luego 4 es la menor solución natural. □

EJEMPLO 2.8. Se disponen de 3 jarras de m, n y $m + n$ litros cada una, con $m < n$. Sólo esta última está llena. Si $(m, n) = 1$ y $m + n$ es par, probar que es posible trasvasar $\frac{m+n}{2}$ litros a la de n litros.

SOLUCIÓN. Denotamos con A, B y C las jarras de m, n y $m + n$ litros respectivamente. Una forma de resolver este problema es usar la jarra A para trasvasar el contenido de la jarra C a la jarra B. Si B se llena, se vuelcan los n litros nuevamente en C y se termina de vaciar A en B. Queremos ver que con este procedimiento es posible trasvasar exactamente la mitad de C en B.

Según este procedimiento, el contenido de la jarra B será siempre una cantidad $xm - dn$, es decir, una cantidad congruente a xm módulo n, para algún natural x. Por lo tanto queremos ver que la ecuación

$$xm \equiv \frac{m+n}{2} \ (n)$$

tiene solución. Dado que m y n son coprimos, la ecuación

$$mx \equiv h\ (n)$$

tiene siempre una solución, cualquiera sea $h \in \mathbb{Z}$. En particular, es posible resolver

$$mx \equiv \frac{m+n}{2}\ (n).$$

Si k es el menor natural tal que $mk \equiv \frac{m+n}{2}\ (n)$, entonces para obtener $\frac{m+n}{2}$ litros en la jarra de n litros hacen falta k jarras de m litros. □

Veámoslo en un ejemplo. Si $m = 3$, $n = 5$, la jarra más grande tiene 8 litros de agua. Puesto que $k = 3$ es solución de la ecuación

$$3x \equiv 4\ (5),$$

esto nos dice que con 3 jarras de 3 litros podemos obtener 4 litros en la jarra de 5 litros. El procedimiento es el siguiente:

- echamos 3 litros en la de 5 litros. Quedan entonces 5 l. en la más grande,
- volvemos a echar 3 litros. Como $n = 5$, con 2 l. se llena, arrojamos los 5 litros nuevamente a la jarra más grande, y echamos el litro restante $(3 = 2 + 1)$ en la de 5 lt.
- en el tercer paso, $(k = 3)$, echamos 3 litros nuevamente y obtenemos entonces $4 = \frac{3+5}{2}$ litros en la jarra de 5 litros.

EJERCICIO 2.4. Resolver el problema anterior para $m = 15$ y $n = 23$.

EJERCICIO 2.5. Cinco marineros recogen una cantidad x de cocos en una isla; el primero se despierta a la noche y retira su parte, sobra un coco y se lo da al mono. Después se despierta el segundo y retira su parte. Le sobra un coco y se lo da al mono. Luego se despierta el tercero y retira su parte, le sobra un coco y se lo da al mono. Lo mismo ocurre con el cuarto y el quinto marinero. ¿Cuál es el mínimo número inicial de cocos?

3. Sistemas de ecuaciones en congruencias

Supongamos que se quiere resolver simultáneamente las congruencias

$$\begin{aligned} x &\equiv 1\ (3) \\ x &\equiv 2\ (5), \end{aligned}$$

es decir que se quiere encontrar un x que satisfaga ambas congruencias. Las soluciones de cada una de estas dos ecuaciones son respectivamente, entre otras,

$$1,\ 4,\ \mathbf{7},\ 10,\ 13,\ 16,\ 19,\ \mathbf{22},\ 25,\ 28,\ 31,\ 34,\ \mathbf{37},\ 40,\ldots$$

$$2,\ \mathbf{7},\ 12,\ 17,\ \mathbf{22},\ 27,\ 32,\ \mathbf{37},\ 42,\ 47,\ldots$$

respectivamente. Por otro lado, 7, 22, 37, ... son soluciones de ambas congruencias, y estas soluciones difieren en un múltiplo de 15. Es posible probar que:

(a) la solución es única módulo $15 = 3 \cdot 5$,

(b) la solución general es de la forma $7 + 15k$, $k \in \mathbb{Z}$.

El item (a) es fácil de ver, puesto que si x_1 y x_2 son soluciones entonces $x_1 - x_2$ es un múltiplo de 3 y también de 5. Como 3 y 5 son coprimos entonces $x_1 - x_2$ debe ser un múltiplo de 15.

Para ver (b) observemos que $x = 7$ es una solución. Como además $15 \equiv 0\ (3)$ y $15 \equiv 0\ (5)$, concluimos que $7 + 15k$ satisface ambas congruencias. La siguiente proposición da una generalización de dicho ejemplo.

PROPOSICIÓN 3.1. a) *El sistema de congruencias*

$$\begin{aligned} x &\equiv b_1\ (n_1) \\ x &\equiv b_2\ (n_2), \end{aligned} \tag{13}$$

admite solución si sólo si (n_1, n_2) *divide a* $b_1 - b_2$. *La solución es única módulo* $[n_1, n_2]$, *esto es*

$$\{x_0 + k[n_1, n_2],\ k \in \mathbb{Z}\}$$

es el conjunto de todas las soluciones de (13).

Si $(n_1, n_2) = 1$ *la solución es única módulo* $n_1 n_2$.

b) *El sistema* $x \equiv b_i\ (n_i)$, $i = 1, \ldots, r$, $(n_i, n_j) = 1$, $i \neq j$ *admite solución única módulo* $n = \prod_{i=1}^{r} n_i$.

PRUEBA.

(a) Supongamos que x es una solución del sistema (13). Luego

$$\left.\begin{aligned} x &= b_1 + kn_1 \\ x &= b_2 + hn_2 \end{aligned}\right\} \Rightarrow n_1 \mid (x - b_1) \quad \text{y} \quad n_2 \mid (x - b_2).$$

Como (n_1, n_2) divide a n_1 y a n_2 se sigue que $(n_1, n_2) \mid b_1 - b_2$.

Recíprocamente, si $(n_1, n_2) \mid (b_1 - b_2)$, entonces por la Proposición 2.4 existe solución de

$$n_1 x \equiv b_1 - b_2 \ (n_2)$$

y por tanto existen k y h enteros tales que

$$hn_1 = b_1 - b_2 + kn_2.$$

Sea $x_0 = b_2 - kn_2 = b_1 - hn_1$. Luego

$$\begin{cases} x_0 \equiv b_1 \quad (n_1) \\ x_0 \equiv b_2 \quad (n_2) \end{cases},$$

es decir que x_0 es solución.

Si x_1 y x_2 son soluciones entonces $x_1 - x_2 \equiv 0 \ (n_1)$ y $x_1 - x_2 \equiv 0 \ (n_2)$, luego $[n_1, n_2]$ divide a $x_1 - x_2$. Recíprocamente, no es difícil ver que si x es solución, entonces $x + k[n_1, n_2]$ también es una solución. Luego todas las soluciones son de la forma $x_0 + k[n_1, n_2]$, $k \in \mathbb{Z}$.

(b) Un sistema de n ecuaciones puede resolverse fácilmente aplicando el llamado *Teorema chino del resto*.

TEOREMA CHINO DEL RESTO . Sean n_1, n_2, ..., n_h números naturales. Si $(n_i, n_j) = 1$, para todo par $i \neq j$, entonces el sistema de congruencias

$$\begin{aligned} x &\equiv b_1 \ (n_1) \\ x &\equiv b_2 \ (n_2) \\ &\vdots \\ x &\equiv b_h \ (n_h) \end{aligned}$$

tiene solución única módulo $\prod_{j=1}^{h} n_j$.

Consideramos primero los siguientes números:

$$n'_1 = \frac{n_1 n_2 \cdots n_h}{n_1}, \quad n'_2 = \frac{n_1 n_2 \cdots n_h}{n_2}, \quad \ldots \quad n'_h = \frac{n_1 n_2 \cdots n_h}{n_h},$$

es decir

$$n'_i = \frac{\prod_{j=1}^{h} n_j}{n_i}, \quad \text{para} \quad 1 \leq i \leq h.$$

Puesto que $(n'_i, n_i) = 1$ podemos resolver cada una de las siguientes ecuaciones:

$$yn'_1 \equiv b_1 \ (n_1), \qquad yn'_2 \equiv b_2 \ (n_2), \qquad \ldots, \qquad yn'_h \equiv b_h \ (n_h).$$

Para cada i, $1 \leq i \leq h$, sea y_i una solución de la ecuación $yn'_i \equiv b_i \ (n_i)$. Sea

$$z = \sum_{i=1}^{h} y_i n'_i.$$

Para cada i resulta

$$z \equiv b_i \ (n_i) \quad \text{pues si} \quad j \neq i \text{ entonces } n'_j \equiv 0 \ (n_i).$$

Por lo tanto z es una solución.

Por otro lado, dadas dos soluciones z_1, z_2 resulta que $z_1 - z_2 \equiv 0 \ (n_i)$, luego $z_1 - z_2 \equiv 0$ módulo $[n_1, n_2, \ldots, n_h] = \prod_{j=1}^{h} n_j$. □

EJEMPLO 3.2. Una banda de 13 piratas se reparten N monedas de oro, le sobran 8. Dos mueren, las vuelven a repartir y sobran 3. Luego 3 se ahogan y sobran 5. ¿Cuál es la mí nima cantidad posible N de monedas?

SOLUCIÓN. En un principio vemos que al repartir las N monedas de oro entre 13 piratas sobran 8 monedas. Escrito en términos más matemáticos esto significa que

$$N \equiv 8 \ (13).$$

Luego vemos que al morir 2 piratas (quedan 11) vuelven a repartir el total N de monedas y sobran 3, esto quiere decir que también

$$N \equiv 3 \ (11).$$

Por último quedan $11 - 3 = 8$ piratas, y al volver a repartir las monedas les sobran 5, esto significa que

$$N \equiv 5 \ (8).$$

Por lo tanto hay que resolver el sistema

$$\begin{cases} N \equiv 8 & (13) \\ N \equiv 3 & (11) \\ N \equiv 5 & (8). \end{cases} \tag{14}$$

Puesto que 13, 11 y 8 son coprimos el sistema tiene solución. Una solución se obtiene calculando las soluciones de las siguientes ecuaciones en congruencias:

$$13 \cdot 11 \cdot r \equiv 5\ (8) \tag{15}$$

$$13 \cdot 8 \cdot s \equiv 3\ (11) \tag{16}$$

$$11 \cdot 8 \cdot t \equiv 8\ (13). \tag{17}$$

Si r, s y t son soluciones de las respectivas ecuaciones, entonces una solución al sistema (14) es

$$z = 13 \cdot 11 \cdot r + 13 \cdot 8 \cdot s + 11 \cdot 8 \cdot t.$$

Las ecuaciones (15), (16) y (17) son respectivamente equivalentes a

$$\begin{aligned} 5 \cdot 3 \cdot r &\equiv 5\ (8) \\ 2(-3) \cdot s &\equiv 3\ (11) \\ (-2) \cdot 8 \cdot t &\equiv 8\ (13). \end{aligned}$$

Haciendo las cuentas correspondientes podemos elegir $r = -5$, $s = 5$ y $t = 6$, de modo que una solución del sistema (14) es

$$z = 13 \cdot 11 \cdot (-5) + 13 \cdot 8 \cdot 5 + 11 \cdot 8 \cdot 6 = 333.$$

Cualquier otra solución se obtiene sumando un múltiplo de $8 \cdot 11 \cdot 13 = 1144$, por lo que el menor número de monedas es 333. □

TEOREMA 3.3 (Pequeño Teorema de Fermat). *Si $a \in \mathbb{Z}$ y $p \in \mathbb{N}$ es primo, entonces $a^p \equiv a\ (p)$.*

PRUEBA. Tomemos $p = 2$. Entonces $a^2 - a = a(a-1)$ y esto siempre es un número par. Luego $a^2 \equiv a\ (2)$.

Supongamos entonces que p es un primo impar. Probamos primero el teorema para $a \in \mathbb{N}$, haciendo inducción en a. Si $a = 1$, $a^p = 1^p = 1 \equiv 1\ (p)$. Luego vale para $a = 1$.

Supongamos que el teorema es válido para un cierto a, veamos que también se cumple para $a + 1$. Tenemos que

$$(a+1)^p = \sum_{i=0}^{p} \binom{p}{i} a^i.$$

Dado que $\binom{p}{i} \equiv 0\ (p)$, para $0 < i < p$, se sigue que

$$(a+1)^p \equiv a^p + 1 \equiv a + 1\ (p).$$

Luego $a^p \equiv a\ (p)$ para todo $a \in \mathbb{N}$.

Si $a < 0$, entonces $(-a)^p \equiv (-a)\ (p)$. Pero $(-a)^p = (-1)^p a^p = -a^p$, de donde se sigue que $-a^p \equiv -a\ (p)$. Por lo tanto

$$a^p \equiv a\ (p), \qquad \forall a \in \mathbb{Z}.$$

□

COROLARIO 3.4. *Sea $a \in \mathbb{Z}$, p primo. Entonces $a^{(p^n)} \equiv a\ (p)$, $\forall n \in \mathbb{N}$. Si $(a,p) = 1$ entonces $a^{(p^n-1)} \equiv 1\ (p)$, $\forall n \in \mathbb{N}$.*

PRUEBA. La propiedad $a^{(p^n)} \equiv a\ (p)$ se cumple para $n = 1$. Si es válida para un natural k, es decir, $a^{(p^k)} \equiv a\ (p)$, entonces

$$a^{(p^{k+1})} = (a^{p^k})^p \qquad \text{implica que } a^{(p^{k+1})} \equiv a^p\ (p).$$

Se sigue que $a^{(p^{k+1})} \equiv a\ (p)$, y por lo tanto la propiedad vale para todo n natural.

Si $(a,p) = 1$ entonces $a^p \equiv a\ (p)$ implica que p divide a $(a^p - a)$, es decir que p divide a $a(a^{p-1} - 1)$. Dado que p no divide a a, se sigue que $a^{p-1} \equiv 1\ (p)$.

Veamos que $a^{(p^n-1)} \equiv 1\ (p)$. Para $n = 1$ ya está probado. Además, si $k \in \mathbb{N}$ entonces

$$a^{p^{k+1}-1} = a^{p^{k+1}-p^k+p^k-1} = a^{p^k(p-1)} a^{p^k-1} = (a^{p-1})^{p^k} a^{p^k-1}.$$

Por lo tanto, si $a^{p^k-1} \equiv 1\ (p)$, entonces

$$a^{p^{k+1}-1} \equiv 1\ (p).$$

Se sigue que, si $(a,p) = 1$, entonces $a^{p^n-1} \equiv 1\ (p)$.

Veamos una prueba más simple. Hemos visto que $a^{(p^n)} - a = a\left(a^{(p^n-1)} - 1\right) \equiv 0\ (p)$. Ahora bien, como $(a,p) = 1$, se concluye que $a^{(p^n-1)} - 1 \equiv 0\ (p)$. □

EJEMPLO 3.5. Hallar el resto de dividir 3^{1000} por 7.

SOLUCIÓN. Tenemos que $(3,7) = 1$; luego $3^6 \equiv 1\ (7)$. Ahora $1000 = 166 \cdot 6 + 4$. Entonces

$$3^{1000} = 3^{6 \cdot 166 + 4} = (3^6)^{166} \cdot 3^4.$$

Como $3^4 = 81 = 77 + 4 \equiv 4\ (7)$ entonces $\quad 3^{1000} \equiv 4\ (7)$. □

TEOREMA 3.6 (Wilson). *Si p es primo entonces $(p-1)! \equiv -1\ (p)$.*

PRUEBA.

$$(p-1)! = 1 \cdot 2 \cdot 3 \cdot 4 \ldots (p-1),$$

Si $0 < a < p$ entonces a y p son coprimos. Luego $ax \equiv 1\ (p)$ tiene solución única b en el intervalo $[1, p-1]$. Es decir, para cualquier natural a comprendido entre 0 y p, existe un único natural b en el mismo intervalo tal que $ab \equiv 1\ (p)$.

Por unicidad del inverso, se sigue que si $a \neq a_1$, entonces también los inversos de a y a_1 son distintos.

Veamos ahora para qué valores de a se cumple que el inverso es el mismo a, es decir,

$$a.a \equiv 1\ (p).$$

En este caso tenemos que $(a-1)(a+1) = kp$, para algún $k \in \mathbb{Z}$. Luego

$$a - 1 \equiv 0\ (p) \qquad \text{o} \qquad a + 1 \equiv 0\ (p).$$

Como p es coprimo con todos los naturales menores que él, concluimos que debe ser $a + 1 = 0$ o $a + 1 = p$, es decir, $a = 1$ o $a = p - 1$.

Así, en el cálculo de $(p-1)!$ módulo p, los elementos comprendidos entre 1 y $p-1$ se cancelan de a dos, cada uno con su inverso, excepto 1 y $(p-1)$. Luego

$$1 \cdot 2 \cdot 3 \cdot 4 \ldots (p-1) \equiv 1 \cdot (p-1) \equiv p - 1 \equiv -1\ (p).$$

□

EJEMPLO 3.7. Veamos que $6! \equiv 1\ (7)$.

PRUEBA. Observemos que $2 \cdot 4 = 8 \quad$ y $\quad 8 \equiv 1\ (7), \quad 3 \cdot 5 = 15 \quad$ y $\quad 15 \equiv 1\ (7)$, luego

$$7! = 6 \cdot 5 \cdot 4 \cdot 3 \cdot 2 \cdot 1 = (5 \cdot 3)(4 \cdot 2) \cdot 6$$

y en consecuencia

$$7! \equiv 6\ \equiv -1\ (7).$$

□

CAPÍTULO 5

Grafos

1. Introducción

Sea $\mathcal{V}$ un conjunto no vacío. Definimos $\mathcal{P}_2(\mathcal{V})$ como el conjunto formado por todos los subconjuntos de dos elementos de $\mathcal{V}$; esto es

$$\mathcal{P}_2(\mathcal{V}) = \{\{v, w\} \mid v,\ w \in \mathcal{V},\ v \neq w\}.$$

DEFINICIÓN 1.1. Un grafo es un conjunto finito de *vértices* $\mathcal{V}$, y de *aristas* $\mathcal{A}$, en el cual $\mathcal{A}$ es un subconjunto de $\mathcal{P}_2(\mathcal{V})$.

EJEMPLO 1.2.

Consideremos $\mathcal{V} = \{a,\ b,\ c,\ d,\ z\}$ y $\mathcal{A} = \{\{a, b\},\ \{a, d\},\ \{b, z\},\ \{c, d\},\ \{d, z\}\}$, entonces el par $(\mathcal{V}, \mathcal{A})$ es un grafo.

Dos vértices v y w de un grafo se dicen *adyacentes* si $\{v, w\}$ es una arista del grafo. En el Ejemplo 1.2 los vértices a y d son adyacentes pues $\{a, d\} \in \mathcal{A}$, en cambio $\{a, c\}$ no es una arista del grafo y por lo tanto a y c no son adyacentes.

Los grafos suelen representarse gráficamente de la siguiente manera. A cada elemento de $\mathcal{V}$ le corresponde un punto del plano, y a cada arista de $\mathcal{A}$ le corresponde un arco o segmento que une los dos vértices de dicha arista. El grafo del Ejemplo 1.2 se puede representar como en la Figura 1.

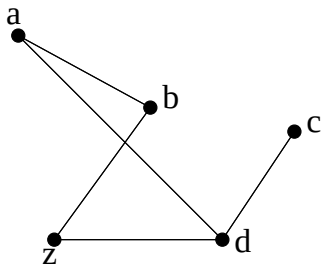


FIGURA 1. Representación gráfica de un grafo

Un *subgrafo* de un grafo $G = (\mathcal{V}, \mathcal{A})$ es un grafo $H = (\mathcal{V}', \mathcal{A}')$, tal que $\mathcal{V}' \subseteq \mathcal{V}$ y $\mathcal{A}' \subseteq \mathcal{A}$. En la Figura 2, H es un subgrafo de G.

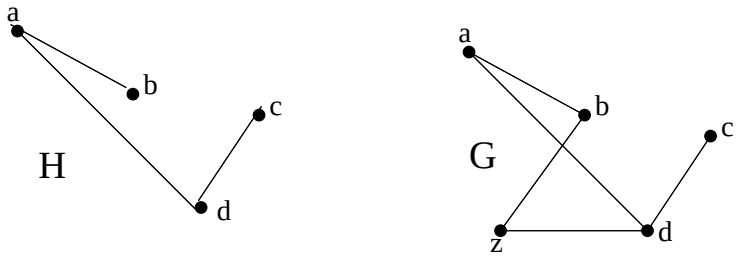


FIGURA 2. H es subrafo de G

Otra forma de representar un grafo es por medio de una *lista de adyacencia*. Esta lista consiste de una tabla en la cual se listan para cada vértice, todos los vértices adyacentes a él. El Cuadro 1 muestra una lista de adyacencia para el grafo del Ejemplo 1.2.

Vértices				
a	b	c	d	z
b	a	d	a	b
d	z		c	d
			z	

CUADRO 1. Lista de adyacencia de un grafo

En un grafo $G = (\mathcal{V}, \mathcal{A})$, al número de vértices adyacentes a un vértice v se lo denomina *valencia* o *grado* de v y se lo denota con el símbolo $\delta(v)$. Esto es,

$$\delta(v) = |\{w \in \mathcal{V} \mid \{v, w\} \in \mathcal{A}\}|.$$

En el Ejemplo 1.2, tenemos que $\delta(a) = 3$, $\delta(b) = 2$ y $\delta(c) = 1$.

Un vértice se dice *par* o *impar* según que $\delta(v)$ sea par o impar, respectivamente. Un grafo G se dice *regular* de grado r si todos los vértices tienen la misma valencia r, esto es, si para todos los vértices v se cumple que $\delta(v) = r$.

Un grafo G se dice *completo* si cada par de vértices forma una arista. En este caso, el conjunto de aristas coincide con el conjunto de *todos* los subconjuntos de $\mathcal{V}$ con exactamente dos elementos. Notemos que en este caso, si el grafo tiene n vértices entonces el número de aristas es $\binom{n}{2}$.

TEOREMA 1.3. *En un grafo G, la suma de las valencias de los vértices es igual al doble del número de aristas, esto es*

$$\sum_{v \in \mathcal{V}} \delta(v) = 2|\mathcal{A}|. \tag{18}$$

Para ver esto, notemos que el número de aristas a las cuales pertenece un vértice v es igual a la valencia de v. Por lo tanto, si sumamos todas las valencias de todos los vértices, habremos contado cada arista $\{v, w\}$ dos veces, en un caso al contar las aristas a las que v pertenece, y en otro caso en las que w pertenece.

COROLARIO 1.4. *En un grafo, el número de vértices impares es par.*

PRUEBA. Notemos que en la fórmula (18) la suma puede escribirse como:

$$\sum_{\delta(v) \text{ es par}} \delta(v) + \sum_{\delta(v) \text{ es impar}} \delta(v).$$

La sumatoria en el primer sumando es una suma de números pares, y por lo tanto da como resultado un número par. La segunda sumatoria es una suma de números impares, cuyo resultado es par puesto que el miembro derecho de la fórmula (18) es par. Eso es posible únicamente si el número de términos de dicha sumatoria es par, es decir, si el número de vértices impares es par. □

Este corolario también es conocido como el *lema del apretón de manos*. Se debe a que en una reunión de personas donde varias de ellas se saludan entre sí, el número de personas que han dado la mano a un número impar de personas es par. El siguiente corolario es inmediato del Teorema 1.3:

COROLARIO 1.5. *Si G es un grafo de valencia r, se tiene que $r\,|\mathcal{V}| = 2|\mathcal{A}|$.*

EJERCICIO 1.1. ¿Pueden las siguientes listas ser valencias de un grafo?

i) 2, 2, 2, 3.
ii) 1, 2, 2, 3, 4.
iii) 3, 3, 3, 3.

SOLUCIÓN. : La lista dada en i) no puede corresponder a las valencias de un grafo, ya que el número de vértices con valencia impar es 1, que no es par.

En cambio, ii) y iii) sí corresponden a valencias de grafos, por ejemplo, los dados en la siguiente figura: □

EJERCICIO 1.2. Pruebe que si en una casa cada habitación tiene un número par de puertas y entre dos habitaciones hay a lo sumo una puerta, entonces hay un número par de puertas de entrada.

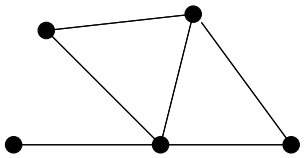
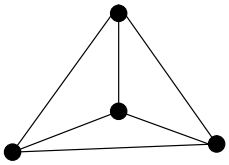
i)  ii) 

FIGURA 3. Grafos asociados a ii) y iii)

SOLUCIÓN. Este problema puede ser modelado con un grafo, en el cual cada vértice representa una habitación excepto uno que representa el exterior de la casa. Así, si hay n habitaciones, tenemos

$$\mathcal{V} = \{h_1,\, h_2,\, \ldots,\, h_n,\, e\},$$

donde cada h_i representa una habitación y e representa el exterior.

Las aristas del grafo representan a las puertas de la casa. Como en cada habitación hay un número par de puertas entonces cada vértice h_i tiene valencia par. Pero

$$\delta(h_1) + \delta(h_2) + \cdots + \delta(h_n) + \delta(e) = 2\,|\mathcal{A}|,$$

y por lo tanto $\delta(e)$ debe ser par. Esto es, hay un número par de puertas de entrada. □

Sea $\mathcal{A}$ el conjunto de aristas de un grafo $G = (\mathcal{V}, \mathcal{A})$. Denotamos con $\mathcal{A}'$ al complemento de $\mathcal{A}$ con respecto a $\mathcal{P}_2(\mathcal{V})$.

DEFINICIÓN 1.6. Dado un grafo $G = (\mathcal{V}, \mathcal{A})$, el *grafo complementario* de G es el grafo $\tilde{G} = (\mathcal{V}, \mathcal{A}')$.

DEFINICIÓN 1.7. Dos grafos $G_1 = (\mathcal{V}_1, \mathcal{A}_1)$ y $G_2 = (\mathcal{V}_2, \mathcal{A}_2)$ se dicen *isomorfos* si existe una biyección $\alpha : \mathcal{V}_1 \mapsto \mathcal{V}_2$ que induce una biyección entre $\mathcal{A}_1$ y $\mathcal{A}_2$; es decir,

$$\{v,\, w\} \in \mathcal{A}_1 \qquad \Leftrightarrow \qquad \{\alpha(v),\, \alpha(w)\} \in \mathcal{A}_2.$$

EJEMPLO 1.8. Los grafos de la Figura 4 son isomorfos, via el isomorfismo α dado por: $\alpha(a) = t$, $\alpha(b) = u$, $\alpha(c) = w$, $\alpha(d) = v$.

PROPOSICIÓN 1.9. *Si $G_1 = (\mathcal{V}_1, \mathcal{A}_1)$ y $G_2 = (\mathcal{V}_2, \mathcal{A}_2)$ son grafos isomorfos, entonces*

i) $|\mathcal{V}_1| = |\mathcal{V}_2|$, $|\mathcal{A}_1| = |\mathcal{A}_2|$;

ii) *para cada entero $k \geq 0$, si $n_i(k) = |\{v \in \mathcal{V}_i \mid \delta(v) = k\}|$, para $i = 1, 2$, entonces $n_1(k) = n_2(k)$.*

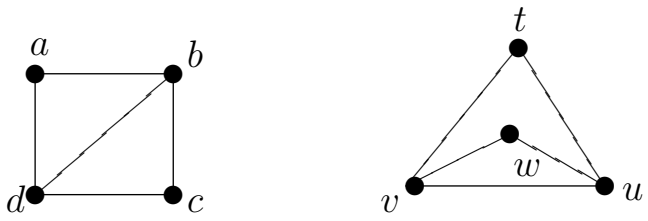


FIGURA 4. Grafos isomorfos

PRUEBA. La demostración de i) es inmediata por la existencia de una biyección entre los conjuntos de vértices y de aristas.

Por otro lado, $n_i(k)$ denota el número de vértices en G_i con valencia k. Cada uno de estos vértices está en correspondencia, via la biyección, con otro vértice de igual valencia. Luego se sigue ii). □

La Proposición 1.9 suele ser útil para probar que dos grafos *no* son isomorfos.

EJEMPLO 1.10. Si bien los grafos de la Figura 5 tienen el mismo número de vértices y el mismo número de aristas, no puede existir un isomorfismo entre ambos. Esto puede probarse argumentando que en el primer grafo existen tres vértices con valencia 3 mientras que en el segundo existen sólo dos.

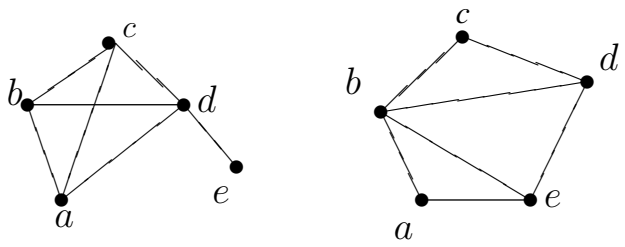


FIGURA 5. Grafos no isomorfos

DEFINICIÓN 1.11. Dado $G = (\mathcal{V}, \mathcal{A})$ un grafo, una *caminata* en G de longitud k ($k \geq 1$) es una sucesión de vértices $v_1, v_2, \ldots, v_{k+1}$ tal que $\{v_i, v_{i+1}\} \in \mathcal{A}$, para todo i tal que $1 \leq i \leq k$.

Un *camino* es una caminata en la que todos los vértices son distintos. Una caminata de longitud k, con $k > 2$, cuyos vértices son todos distintos excepto que $v_1 = v_{k+1}$ se llama *ciclo*, o k-ciclo, o ciclo de longitud k.

Notemos que una caminata puede recorrer una misma arista varias veces. Por ejemplo, en el grafo de la Figura 6, $a\,b\,c\;d\,b\,a$ es una caminata, $a\,b\,c\,d\,e$ es un camino y $b\,c\,d\,b$ es un ciclo de longitud 3.

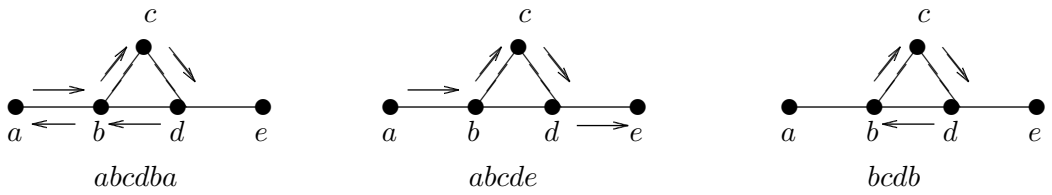


FIGURA 6. Caminatas, caminos y ciclos

Un grafo $G = (\mathcal{V}, \mathcal{A})$ se dice conexo si para todo $v, w \in \mathcal{V}$, existe una caminata o un camino que une v con w. Si existe tal camino escribimos $v \sim w$. Dejamos como ejercicio para el lector probar que $\sim$ define una relación de equivalencia en $\mathcal{V}$.

Notemos que si existe una caminata que une v con w, entonces existe un camino con la misma propiedad. Para ver esto, probaremos que si v_1, v_2, ..., v_k es una caminata tal que $v = v_1$ y $w = v_k$, entonces existe un camino contenido en dicha caminata, que une v con w.

En efecto, si hacemos inducción en k, vemos que para $k = 1$ el resultado es obvio. Si vale para $h < k$, consideremos una caminata $v_1, \ldots, v_k$. Si es un camino ya está probado. Si no lo es, es porque existen dos vértices iguales en la caminata, digamos $v_l = v_j$, para algún $l < j$. Eliminamos de la caminata los vértices v_i, con $l \leq i < j$, y obtenemos una caminata más corta,

$$v_1, \ldots, v_{l-1}, v_j, v_{j+1}, \ldots, v_k,$$

la cual por la hipótesis inductiva puede reemplazarse por un camino.

La relación de equivalencia $\sim$ en $\mathcal{V}$ parte a $\mathcal{V}$ en clases de equivalencia, llamadas *componentes conexas* de G. Así, G es conexo si posee una única componente conexa. Cada componente conexa es un *subgrafo* conexo maximal de G.

Una arista de G es un *puente* si al excluirla aumenta el número de componentes conexas.

DEFINICIÓN 1.12. Un *ciclo Hamiltoniano* en un grafo G es un ciclo que contiene a todos los vértices del grafo.

Una *caminata euleriana* en un grafo G es un caminata que usa todas las aristas de G exactamente una vez. Una caminata euleriana que comienza y termina en un mismo vértice se llama también *circuito euleriano*.

EJEMPLO 1.13. ¿Existe una forma de recorrer todos los casilleros de un tablero de ajedrez, con el movimiento de un caballo de ajedrez? Una forma de modelar este problema es considerar un grafo donde cada vértice represente un casillero del tablero, y dos vértices están unidos por

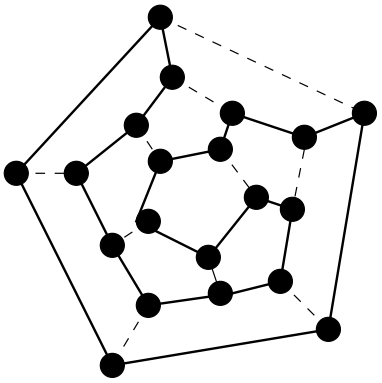


FIGURA 7. Ciclo hamiltoniano

una arista si es posible pasar de uno al otro por un movimiento del caballo. La pregunta es entonces: ¿existe un ciclo hamiltoniano en dicho grafo? Leonard Euler resolvió este problema en 1759, y la Figura 8 muestra un posible recorrido del caballo de ajedrez por todos los casilleros del tablero sin pasar dos veces por el mismo.

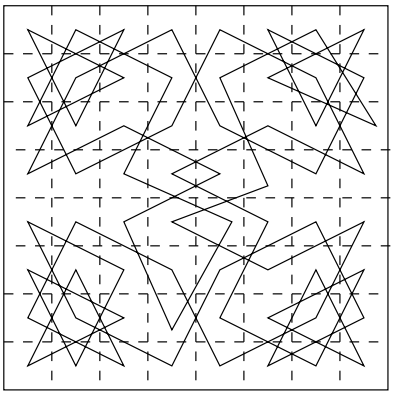


FIGURA 8. Ciclo hamiltoniano del caballo de ajedrez

Cabe preguntarse si en todo grafo existe un ciclo hamiltoniano o un camino euleriano, o bajo qué condiciones podemos asegurar que éstos existen.

TEOREMA 1.14. *Un grafo conexo con más de un vértice posee una caminata euleriana de v a w, con $v \neq w$, si y sólo si v y w son los únicos vértices de grado impar. Un grafo conexo con más de un vértice tiene un circuito euleriano si y sólo si todos los vértices tienen grado par.*

PRUEBA. Veamos primero que las condiciones son necesarias. En efecto, si $v_1 v_2 \dots v_n v_1$ es un circuito euleriano y x aparece h veces en la sucesión de vértices del circuito, entonces $\delta(x) = 2\,h$ (si $v_1 \neq x$) o $\delta(x) = 2\,(h-1)$ (si $v_1 = x$).

Si $vv_2 \dots w$ es una caminata euleriana en G, entonces agregamos al grafo un vértice z y las aristas $\{z, v\}$ y $\{w, z\}$. De este modo, obtenemos un grafo G' que posee un circuito euleriano que resulta de agregarle a la caminata euleriana de G las dos nueva aristas. Por lo que acabamos de probar, todos los vértices tienen grado par en G'. Esto implica que v y w tienen grado impar en G y los demás vértices mantienen el grado par.

Veamos ahora que las condiciones son suficientes. Si existen dos vértices v y w con valencia impar, agregamos como antes un vértice z y las aristas $\{z, v\}$ y $\{w, z\}$. Basta probar entonces que si todos los vértices tienen grado par, entonces existe un circuito euleriano.

Sea x un vértice cualquiera del grafo. Construimos en G una caminata comenzando por x, y recorriendo siempre aristas diferentes. Como el grafo tiene un número finito de aristas, eventualmente la caminata terminará en un vértice y del cual no salen aristas sin recorrer. Afirmamos que $x = y$. En efecto, notemos que para cada vértice v distinto de x y de y, se han recorrido un número par de aristas que lo contienen, pues por cada arista por la que se llega a v existe otra por la cual se lo abandona.

Si y fuera distinto de x, entonces el grado de y sería impar, puesto que la última vez que se visitó el vértice no fue posible abandonarlo. Esto contradice la hipótesis de que todas las valencias son pares, por lo tanto $y = x$ y la caminata es un circuito en G.

Si este circuito recorre todas las aristas del grafo, entonces hemos hallado un circuito euleriano en G. Si no, llamamos G' al grafo que resulta eliminando de G todas las aristas del circuito. Notemos que en G' todos los vértices tienen grado par, aunque no necesariamente es un grafo conexo.

Afirmamos que existe un vértice x_1 en el circuito que tiene grado mayor que 0 en G'. En efecto, sabemos que en G' existe un vértice v con grado distinto de 0.

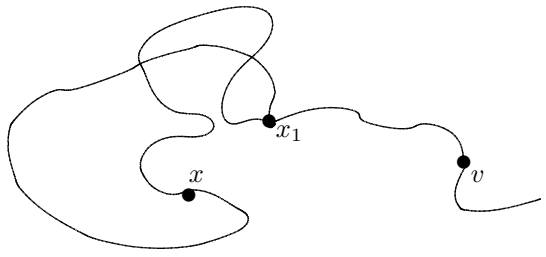


FIGURA 9. Existencia de circuitos eulerianos

Si v pertenece al circuito tomamos $x_1 = v$. Si no, dado que G es conexo, existe un camino en G con al menos una arista fuera del circuito, que une a v con un vértice del circuito. Siguiendo

este camino llegamos a un primer vértice del camino que pertenece al circuito y que posee grado distinto de 0 en G'. Llamamos x_1 a dicho vértice.

Ahora, según el procedimiento anterior, construimos un circuito en G' que comience y termine en x_1 y lo unimos, por el vértice x_1, al anterior circuito. Así siguiendo, puesto que G tiene un número finito de vértices, es posible hallar un circuito en G si todos los vértices de G tienen grado par.

□

DEFINICIÓN 1.15. Un *árbol* es un grafo conexo sin ciclos. Un *bosque* o *foresta* es un grafo sin ciclos. Los siguientes son ejemplos de árboles:

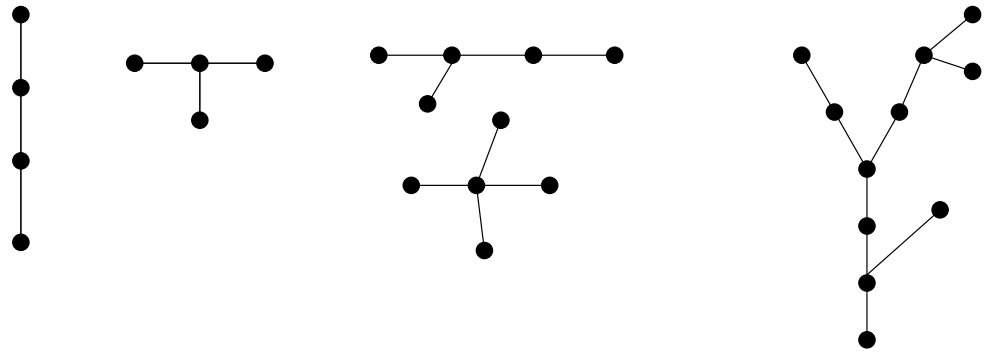


FIGURA 10. Árboles

TEOREMA 1.16. *Sea $G = (\mathcal{V}, \mathcal{A})$ un árbol. Si $|\mathcal{V}| \geq 2$, entonces:*

i) *para todo par v, w de vértices hay un único camino que va de v a w,*
ii) *el grafo que se obtiene de quitar cualquier arista posee exactamente dos componentes conexas,*
iii) $|\mathcal{A}| = |\mathcal{V}| - 1$.

PRUEBA. i) Puesto que G es conexo, si v y w son vértices del grafo existe un camino

$$vv_1v_2 \dots v_nw$$

de v a w. Si existe otro camino, digamos

$$vw_2 \dots w_rw,$$

entonces sea i el primer índice tal que $v_{i+1} \neq w_{i+1}$. Puesto que ambos caminos se encuentran en w, elegimos j el primer índice tal que

$$j > i \qquad \text{y} \qquad v_j = w_k \quad \text{para algún } k.$$

Entonces la caminata $v_i v_{i+1} \dots v_j w_{k-1} \dots v_i$ es un ciclo en G, lo cual contradice la hipótesis.

ii) Consideremos el subgrafo G' que se obtiene quitando a $\mathcal{A}$ una arista $\{u, v\}$, es decir $G' = (\mathcal{V}, \mathcal{A} - \{\{u, v\}\})$. Veamos que G' tiene exactamente dos componentes conexas. Sean $\mathcal{V}_1$ y $\mathcal{V}_2$ los siguientes conjuntos:

$$\mathcal{V}_1 = \{x \in \mathcal{V} \mid \text{ existe un camino en } G \text{ de } x \text{ a } v \text{ que pasa por } u\},$$

$$\mathcal{V}_2 = \{x \in \mathcal{V} \mid \text{ existe un camino en } G \text{ de } x \text{ a } v \text{ que no pasa por } u\}.$$

Luego $\mathcal{V} = \mathcal{V}_1 \cup \mathcal{V}_2$, $u \in \mathcal{V}_1$, $v \in \mathcal{V}_2$ y por i) se tiene que $\mathcal{V}_1$ y $\mathcal{V}_2$ son disjuntos.

Todo $x \in \mathcal{V}_1$ puede unirse con u y todo vértice de $\mathcal{V}_2$ puede unirse con v. Significa que hay a lo sumo dos componentes conexas. Dado que la arista $\{u, v\}$ ha sido excluida, entonces no hay ningún camino de u a v, y por lo tanto pertenecen a dos componentes conexas distintas.

iii) Para probar esta afirmación haremos inducción en el número de vértices de G. Claramente si $|\mathcal{V}| = 1$, entonces no existen aristas, y por lo tanto la afirmación es verdadera.

Supongamos que la afirmación es cierta si $|\mathcal{V}| \leq k$. Entonces, si el grafo G tiene $k + 1$ vértices quitamos alguna arista $\{u, v\}$. El grafo resultante posee dos componentes conexas: $H_1 = (\mathcal{V}_1, \mathcal{A}_1)$ y $H_2 = (\mathcal{V}_2, \mathcal{A}_2)$. Notemos que H_1 y H_2 son árboles, puesto que son grafos conexos y sin ciclos. Además $|\mathcal{V}_1| \leq k$ y $|\mathcal{V}_2| \leq k$. Dado que $\mathcal{V}$ es unión disjunta de $\mathcal{V}_1$ y $\mathcal{V}_2$, y aplicando hipótesis inductiva tenemos que:

$$|\mathcal{V}| = |\mathcal{V}_1| + |\mathcal{V}_2| = (|\mathcal{A}_1| + 1) + (|\mathcal{A}_2| + 1).$$

Pero $\mathcal{A} = \mathcal{A}_1 \cup \mathcal{A}_2 \cup \{\{u, v\}\}$, (unión disjunta), y por lo tanto $|\mathcal{A}_1| + |\mathcal{A}_2| + 1 = |\mathcal{A}|$; luego

$$|\mathcal{V}| = |\mathcal{A}| + 1 \qquad \text{o bien} \qquad |\mathcal{A}| = |\mathcal{V}| - 1.$$

□

En los ejemplos de la Figura 11, podemos comprobar que el número de vértices de cada árbol excede en uno al número de aristas:

COROLARIO 1.17. *En un árbol T con 2 o más vértices, existen al menos dos vértices de valencia 1.*

PRUEBA. Sea n el número de vértices de T, y $\mathcal{A}$ el conjunto de aristas de T. Entonces, por el Teorema 1.16, iii) tenemos que

$$2|\mathcal{A}| = 2n - 2, \tag{19}$$

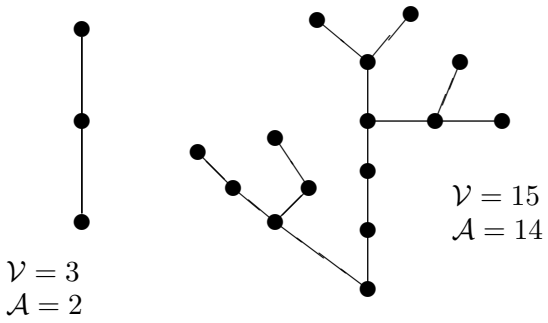


FIGURA 11. $|\mathcal{V}| = |\mathcal{A}| - 1$

y además sabemos que si $v_1, v_2, \ldots, v_n$ son los vértices de T entonces

$$2|\mathcal{A}| = \sum_{i=1}^{n} \delta(v_i), \qquad \text{con } \delta(v_i) \geq 1,\ 1 \leq i \leq n.$$

Pero si existieran $n-1$ vértices con valencia mayor que 1, entonces tendríamos

$$2|\mathcal{A}| \geq 2(n-1) + 1 = 2n - 1,$$

lo cual contradice (19). Luego existen al menos dos vértices con valencia igual a 1. □

DEFINICIÓN 1.18. Sea $G = (\mathcal{V}, \mathcal{A})$ un grafo. Una *coloración con k colores* en G es una función $c : \mathcal{V} \mapsto \mathbb{N}_k$, tal que si $\{x, y\} \in \mathcal{A}$ entonces $c(x) \neq c(y)$.

El *número cromático* de G, denotado con $\chi(G)$, es el menor entero k tal que G admite una coloración con k colores.

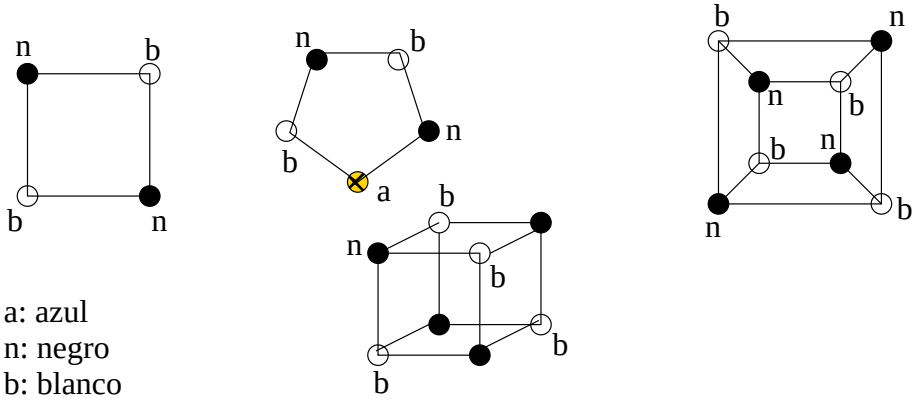


FIGURA 12. Coloración de grafos

APLICACIÓN 1.1. Un grupo de 6 conferencistas darán cada uno una charla de una hora de duración, y existen oyentes que desean asistir a dos o más de estas charlas. Se desea entonces confeccionar un horario de modo que todos puedan asistir a las charlas que les interesa.

Este problema se puede modelar con un grafo, en el que cada vértice represente una charla, y la arista $\{v, w\}$ indique que existen oyentes que deseam asistir a las charlas v y w. Si se realiza una coloración del grafo, entonces dos vértices con un mismo color se corresponden con dos charlas que pueden ser dictadas simultáneamente.

Llamemos v_1, v_2, v_3, v_4, v_5 y v_6 a los vértices del grafo, y supongamos que las aristas son: $\{v_1, v_2\}$, $\{v_1, v_4\}$, $\{v_3, v_5\}$, $\{v_2, v_6\}$, $\{v_4, v_5\}$, $\{v_5, v_6\}$, $\{v_1, v_6\}$.

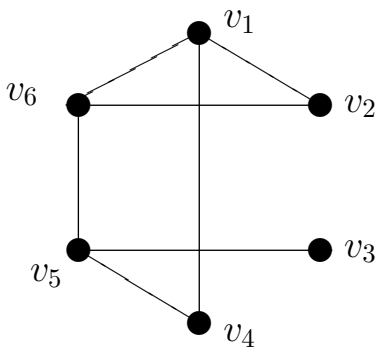


FIGURA 13. Representación en grafo

Una posible solución es asignar a cada vértice un color distinto, es decir, hacer que cada clase sea dictada en un horario diferente. Sin embargo es posible utilizar menos horas. Veamos el siguiente método de coloración:

Comenzamos con el vértice v_1, y le asignamos el color 1:

$$c : v_1 \mapsto 1.$$

Seguimos con el vértice v_2. Como es adyacente a v_1 le corresponde un color distinto, así:

$$c : v_2 \mapsto 2.$$

Ahora v_3 no es adyacente ni a v_1 ni a v_2; luego podemos asignarle el color 1 nuevamente. El vértice v_4 es adyacente a v_1 pero no a v_2, y entonces le asignamos el color 2. Como v_5 no es adyacente a v_1, podría usar el mismo color que v_1. Pero ya ha sido usado para v_3 que sí es adyacente con v_5. Luego necesitamos un tercer color para v_5. Por último, a v_6 se le debe asignar un cuarto color, y queda entonces:

$$c : \begin{cases} v_1, v_3 & \mapsto 1 \\ v_2, v_4, & \mapsto 2 \\ v_5 & \mapsto 3 \\ v_6 & \mapsto 4 \end{cases}$$

Esto significa que es posible confeccionar un horario con cuatro turnos, como el que sigue:

Turno	Charla
Primer	v_1, v_3
Segundo	v_2, v_4
Tercer	v_5
Cuarto	v_6

Notemos que para hacer dicha coloración usamos un orden determinado en la elección de los vértices: v_1, v_2, v_3, v_4, v_5 y v_6. Si seguimos el siguiente orden: v_4, v_3, v_2, v_6, v_1 y v_5 entonces necesitaremos menos colores para la coloración. En efecto, obtendremos una coloración c' con 3 colores dada por:

$$c' : \begin{cases} v_1 & \mapsto 1 \\ v_3, v_4, v_6 & \mapsto 2 \\ v_2, v_5 & \mapsto 3, \end{cases}$$

como observamos en el grafo de la Figura 14.

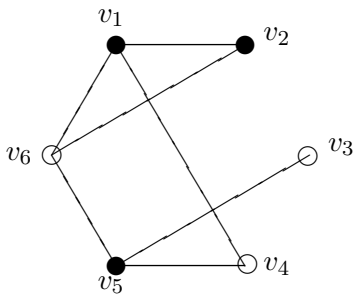


FIGURA 14. Coloración c'

A su vez el horario sería el siguiente:

Turno	Charla
Primer	v_1
Segundo	v_3, v_4, v_6
Tercer	v_2, v_5

¿Es posible hacer una coloración con menos de tres colores? La respuesta es no, puesto que existe un 3-ciclo, $v_1v_2v_6$, y por ende se necesitan al menos tres colores. Puesto que hemos encontrado una coloración con tres colores podemos concluir que el número cromático del grafo es $\chi(G) = 3$.

El método utilizado en el ejemplo anterior es a menudo óptimo, y se denomina *algoritmo greedy*.

2. Algoritmo greedy

Este algoritmo consiste en asignar un color a cada vértice, de modo que cada vértice recibe el primer color que no esté asignado a sus adyacentes. En primer lugar se ordenan los vértices del grafo de alguna manera:

$$v_1,\ v_2,\ \ldots, v_n,$$

y se dispone del conjunto de colores $\{1,\ 2,\ \ldots\}$. Se asigna a v_1 el color 1:

$$v_1 \mapsto 1.$$

Luego, para cada i, $2 \leq i \leq n$ consideramos el conjunto:

$$\mathcal{S} = \{\text{colores utilizados en los vértices } v_j,\ 1 \leq j < i,\ \text{que son adyacentes a } v_i\}.$$

Asignamos a v_i el primer color que no pertenece a $\mathcal{S}$.

La coloración obtenida con el algoritmo greedy depende del orden que se le de a los vértices, y normalmente el número de colores que usará el algoritmo será mayor que el mínimo posible, o sea, $\chi(G)$. Sin embargo, puede probarse que hay un orden en los vértices tal que el algoritmo greedy da el número cromático $\chi(G)$.

TEOREMA 2.1. *Si G es un grafo con valencia máxima k, entonces $\chi(G) \leq k + 1$,*

PRUEBA. Sea v_1, v_2, $\ldots$, v_n un orden en los vértices. Cada vértice v tiene a lo sumo k vértices adyacentes. Por lo tanto, dados $k + 1$ colores, al menos uno de ellos no está asignado a ningún vecino de v. Luego puede ser asignado a v. □

Un grafo *bipartito* es un grafo tal que el conjunto de vértices $\mathcal{V}$ es unión de dos conjuntos disjuntos: $\mathcal{V} = \mathcal{V}_1 \cup \mathcal{V}_2$, $\mathcal{V}_1 \cap \mathcal{V}_2 = \emptyset$ y tal que toda arista de G une un vértice de $\mathcal{V}_1$ con un vértice de $\mathcal{V}_2$. En particular, un grafo sin aristas es un grafo bipartito ($\mathcal{V}_2 = \emptyset$).

TEOREMA 2.2. *Sea G un grafo con al menos una arista. Entonces las siguientes afirmaciones son equivalentes:*

- *G es bipartito.*
- *$\chi(G) = 2$.*
- *G no posee ciclos de longitud impar.*

PRUEBA. Supondremos en toda la demostración que G tiene al menos una arista.

Veamos que G es bipartito si y sólo si $\chi(G) = 2$. En efecto, si G es bipartito y tiene al menos una arista, entonces $\chi(G) > 1$. Por otro lado, la función $c : \mathcal{V} \mapsto \{1, 2\}$ dada por

$$c(v) = \begin{cases} 1 & \text{si } v \in \mathcal{V}_1, \\ 2 & \text{si } v \in \mathcal{V}_2. \end{cases}$$

es una coloración de G que utiliza dos colores. Por lo tanto $\chi(G) = 2$.

Recíprocamente, dada una coloración c con dos colores, llamemos $\mathcal{V}_i = c^{-1}(i)$, $i = 1, 2$. Claramente $\mathcal{V} = \mathcal{V}_1 \cup \mathcal{V}_2$, y dicha unión es disjunta. Además, si $\{v, w\} \in \mathcal{A}$, entonces $c(v) \neq c(w)$, lo que indica que v y w no pertenecen al mismo subconjunto V_i.

Veamos ahora que $\chi(G) = 2$ si y sólo si G no posee ciclos de longitud impar. Si G posee un ciclo de orden impar, entonces $\chi(G) \geq 3$. Esto implica que si $\chi(G) = 2$ entonces G no posee ciclos de longitud impar.

Veamos que si G no posee ciclos de longitud impar entonces es bipartito, y por ende, $\chi(G) = 2$. Podemos suponer que G es un grafo conexo, con más de un vértice.

Tomemos $v \in \mathcal{V}$ un vértice cualquiera, y consideremos los siguientes conjuntos:

$$\mathcal{V}_1 = \{w \in \mathcal{V} \mid \text{ el camino más corto de } v \text{ a } w \text{ tiene longitud par}\},$$

$$\mathcal{V}_2 = \{w \in \mathcal{V} \mid \text{ el camino más corto de } v \text{ a } w \text{ tiene longitud impar}\}.$$

Afirmamos que no existen aristas que unan dos vértices de $\mathcal{V}_1$ ni dos vértices de $\mathcal{V}_2$. En efecto, supongamos que existe una arista $\{x, y\}$ con ambos vértices en $\mathcal{V}_1$. Entonces existen dos caminos de longitud par que unen x con v e y con v respectivamente, y de longitud mínima. Sea z el primer vértice del camino de x a v que también pertenece al camino de y a v. Se tienen entonces dos caminos

$$xv_0 \dots z \dots v \qquad \text{y} \qquad yw_0 \dots z \dots v.$$

Los dos caminos de z a v tienen la misma longitud (que podría ser 0) ya que deben ser de longitud mínima. Por lo tanto, los caminos de x a z y de y a z tienen ambos longitud par o ambos longitud impar. (ver Figura 15) Pero entonces el ciclo que resulta de los caminos de x a

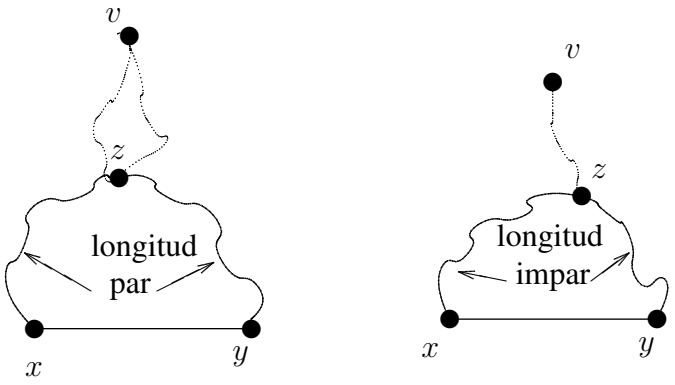


FIGURA 15. Ciclos de longitud impar

z, de z a y y de y a x tiene longitud impar, lo cual es un absurdo.

Por un argumento similar puede probarse que si y v, w pertenecen a V_2, existiría en G un ciclo de longitud impar.

Esto contradice la hipótesis, y por lo tanto G es un grafo bipartito. □

COROLARIO 2.3. *Un grafo bipartito con un número impar de vértices, no puede contener un ciclo hamiltoniano.*

Parte 2

GUÍA DE EJERCICIOS

ÁLGEBRA I / MATEMÁTICA DISCRETA I

PRÁCTICO 1

1. ¿Cuáles de las siguientes proposiciones son verdaderas?
   a) Todo rectángulo es un paralelogramo.
   b) Si un número entero es múltiplo de 6, entonces es múltiplo de 3.
   c) Si un número entero no es múltiplo de 6, entonces no es múltiplo de 3.
2. Decidir si las siguientes afirmaciones son verdaderas o falsas.

   a) $x^2 = x, \forall x \in \mathbb{R}$.
   b) $x^2 = x$, para algún $x \in \mathbb{R}$.
   c) $x^2 = x$, para exactamente un $x \in \mathbb{R}$.

3. En los siguientes enunciados, a y b representan nmeros reales. ¿Cuáles de estas afirmaciones son verdaderas? Justificar la respuesta.
   a) $a + a = a \Rightarrow\ a = 0$ (sugerencia: $a = a + 0$).
   b) $a \cdot b = 0 \Rightarrow\ a = 0$ o $b = 0$.
   c) $a^2 = b^2 \Rightarrow\ a = b$.
   d) $a^2 = b^2 \Rightarrow\ a = b\ \ a = -b$.
   e) No existe ningún número real x tal que $x^2 + 1 = 0$.
4. Analizar la validez de las siguientes afirmaciones:

   a) $a < b$ si y sólo si $a^2 < b^2$.
   b) $\forall a, b \in \mathbb{R}, \qquad \dfrac{1}{a+b} = \dfrac{1}{a} + \dfrac{1}{b}$.
   c) $\forall a \in \mathbb{R}, (a-1)(a+1) = a^2 - 1$.

5. Decidir si las siguientes proposiciones son verdaderas o falsas y dar la negación de cada una de ellas.

   a) $\exists x \in \mathbb{R} \mid x(x+4) = x^2 - 4$.
   b) $\forall x > 0, \exists y \in \mathbb{R} \mid 0 < y < x$.
   c) $\forall x \in \mathbb{R}, \forall y \in \mathbb{R},\ x + y = 0$.

6. Analizar la validez de las siguientes afirmaciones:

   a) $0 < a$ y $0 < b \Rightarrow\ 0 < a \cdot b$.
   b) $a < b$ y $c < 0 \Rightarrow\ b \cdot c < a \cdot c$.

ÁLGEBRA I / MATEMÁTICA DISCRETA I

PRÁCTICO 2

1. Decir cules de los siguientes conjuntos son inductivos. Justificar.
   a) $\mathbb{N} \cup \{\frac{1}{2}\}$.
   b) $\mathbb{N} \cup \{0\}$.
   c) Un subconjunto infinito de $\mathbb{N}$ que contenga al 1.
   d) Un subconjunto finito de $\mathbb{N}$.
   e) $\{x \in \mathbb{R} \mid x + 4$ es múltiplo de 5 $\}$.
   f) $\{x \in \mathbb{R} \mid x = \sqrt{n}, n \in \mathbb{N}\}$.

2. Calcular

   a) $\sum_{r=0}^{4} r$, *b)* $\prod_{i=1}^{5} i$ *c)* $\sum_{k=-3}^{-1} \frac{1}{k(k+4)}$ *d)* $\prod_{n=2}^{7} \frac{n}{n-1}$

3. Dado un natural m, probar que $\forall n \in \mathbb{N}$; x, $y \in \mathbb{R}$, se cumple:

   a) $x^n \cdot x^m = x^{n+m}$ *b)* $(x \cdot y)^n = x^n \cdot y^n$ *c)* $(x^n)^m = x^{n \cdot m}$

4. Analizar la validez de las siguientes afirmaciones:

   a) $(2^{2^n})^{2^k} = 2^{2^{n+k}}$; n, $k \in \mathbb{N}$
   b) $(2^n)^2 = 4^n$; $n \in \mathbb{N}$
   c) $2^{7+11} = 2^7 + 2^{11}$.

5. Calcular:

   a) $2^5 - 2^4$,
   b) $2^{n+1} - 2^n$,
   c) $(2^2)^n + (2^n)^2$
   d) $(2^{2^n} + 1)(2^{2^n} - 1)$

6. Demostrar por inducción que las siguientes igualdades se verifican para todo n natural:
   a) $\sum_{k=1}^{n}(a_k + b_k) = \sum_{k=1}^{n} a_k + \sum_{k=1}^{n} b_k$
   b) $\sum_{j=1}^{n} j = \frac{n(n+1)}{2}$

c) $\displaystyle\sum_{i=1}^{n} i^2 = \frac{n(n+1)(2n+1)}{6}$

d) $\displaystyle\sum_{k=0}^{n}(2k+1) = (n+1)^2$

e) $\displaystyle\sum_{i=1}^{n} i^3 = \left(\frac{n(n+1)}{2}\right)^2$

f) $\displaystyle\sum_{k=0}^{n} a^k = \frac{a^{n+1}-1}{a-1}$, donde $a \in \mathbb{R}$, $a \neq 0,\ 1$.

g) $\displaystyle\prod_{i=1}^{n} \frac{i+1}{i} = n+1$.

7. Probar que la suma de los ángulos interiores de un polígono regular de n lados es $(n-2)\cdot 180$ grados.

8. Probar las siguientes afirmaciones usando induccin en n:
   a) Si $a \in \mathbb{R}$ y $a \geq -1$, entonces $(1+a)^n \geq 1 + n\cdot a$, $\forall n \in \mathbb{N}$.
   b) $n^4 \leq 4^n$; $\quad \forall n \in \mathbb{N}, n \geq 5$.
   c) $\forall n \in \mathbb{N}$, $3^n \geq 1 + 2^n$.
   d) Si $a_1, \ldots, a_k \in \mathbb{R}$, entonces $\displaystyle\sum_{k=0}^{n} a_k^2 \leq \left(\sum_{k=0}^{n} |a_k|\right)^2$.

9. Hallar $n_0 \in \mathbb{N}$ tal que $\forall n \geq n_0$ se cumpla que $n^2 \geq 11\cdot n + 3$.

10. Sea $u_1 = 3$, $u_2 = 5$ y $u_n = 3u_{n-1} - 2u_{n-2}$ con $n \in \mathbb{N}$, $n \geq 3$. Probar que $u_n = 2^n + 1$.
11. Las siguientes proposiciones no son válidas para todo $n \in \mathbb{N}$. Indicar en qué paso del principio de inducción falla la demostración:

    a) $n = n^2$, *b*) $n = n+1$, *c*) $3^n = 3^{n+2}$, *d*) $3^{3n} = 3^{n+2}$.

12. Encuentre el error en los siguientes argumentos de inducción.
    a) Demostraremos que $5n+3$ es mltiplo de 5 para todo $n \in \mathbb{N}$.
    Supongamos que $5k+3$ es mltiplo de 5, siendo $k \in \mathbb{N}$. Entonces existe $p \in \mathbb{N}$ tal que $5k+3 = 5p$. Probemos que $5(k+1)+3$ es mltiplo de 5: Como

    $$5(k+1)+3 = (5k+5)+3 = (5k+3)+5 = 5p+5 = 5(p+1),$$

    entonces obtenemos que $5(k+1)+3$ es mltiplo de 5. Por lo tanto, por el principio de inducción, demostramos que $5n+3$ es mltiplo de 5 para todo $n \in \mathbb{N}$.

b) Sea $a \in \mathbb{R}$, con $a \neq 0$. Vamos a demostrar que para todo entero no negativo n, $a^n = 1$.

Como $a^0 = 1$ por definición, la proposición es verdadera para $n = 0$. Supongamos que para un entero k, $a^m = 1$ para $0 \leq m \leq k$. Entonces

$$a^{k+1} = \frac{a^k a^k}{a^{k-1}} = \frac{1 \cdot 1}{1} = 1.$$

Por lo tanto, el principio de inducción fuerte implica que $a^n = 1$ para todo entero no negativo n.

ÁLGEBRA I / MATEMÁTICA DISCRETA I
PRÁCTICO 3

1. Contar las aplicaciones de $X_3 = \{1, 2, 3\}$ en $X_4 = \{1, 2, 3, 4\}$. Mostrar que hay m^3 aplicaciones de X_3 en $X_m = \{1, 2, \ldots, m\}$, con $m \geq 1$.

2. La cantidad de dgitos o cifras de un nmero se cuenta a partir del primer dgito distinto de cero. Por ejemplo, 0035010 es un nmero de 5 dgitos.
   a) ¿Cuántos números de 5 dígitos hay?
   b) ¿Cuántos números pares de 5 dígitos hay?
   c) ¿Cuántos números de 5 dígitos existen con sólo un 3?
   d) ¿Cuántos números capicúas de 5 dígitos existen?
   e) ¿Cuántos números capicúas de a lo sumo 5 dígitos hay?

3. ¿Cuántos números de 6 cifras pueden formarse con los dígitos de 112200?

4. ¿Cuántos números impares de cuatro cifras hay?

5. ¿Cuántos números múltiplos de 5 y menores que 4999 hay?

6. En los boletos viejos de ómnibus, apareca un *nmero* de 5 cifras (en este caso podían empezar con 0), y uno tenía un *boleto capicúa* si el número lo era.
   a) ¿Cuántos boletos capicúas había?
   b) ¿Cuántos boletos había en los cuales no hubiera ningún dígito repetido?

7. Las antiguas patentes de auto tenían una letra indicativa de la provincia y luego 6 dígitos. (En algunas provincias, Bs. As. y Capital, tenían 7 dígitos, pero ignoremos eso por el momento). Las nuevas patentes tienen 3 letras y luego 3 dígitos. ¿Con cul de los dos criterios pueden formarse ms patentes?

8. Si uno tiene 8 CD distintos de Rock, 7 CD distintos de música clásica y 5 CD distintos de cuartetos.
   a) ¿Cuántas formas distintas hay de seleccionar un CD?

b) ¿Cuántas formas hay de seleccionar tres CD, uno de cada tipo?

c) Un sonidista en una fiesta de casamientos planea poner 3 CD, uno a continuación de otro. ¿Cuántas formas distintas tiene de hacerlo si le han dicho que no mezcle más de dos estilos?

9. Mostrar que si uno arroja un dado n veces, hay $\frac{6^n}{2}$ formas distintas de obtener una suma par.

10. ¿Cuántos enteros entre 1 y 10000 tienen exactamente un 7 y exactamente un 5 entre sus cifras?

11. ¿Cuántos subconjuntos de $\{0, 1, 2, \ldots, 8, 9\}$ contienen al menos un impar?

12. El truco se juega con un mazo de 40 cartas, y se reparten 3 cartas a cada jugador. Obtener el 1 de espadas (el *macho*) es muy bueno. También lo es, por otros motivos, obtener un 7 y un 6 del mismo palo (*tener 33*). ¿Qué es más probable: obtener el macho, o tener 33?

13. ¿Cuántos comités pueden formarse de un conjunto de 6 mujeres y 4 hombres, si el comité debe estar compuesto por 3 mujeres y 2 hombres?

14. ¿De cuántas formas puede formarse un comité de 5 personas tomadas de un grupo de 11 personas entre las cuales hay 4 profesores y 7 estudiantes, si:
    a) No hay restricciones en la selección?
    b) El comité debe tener exactamente 2 profesores?
    c) El comité debe tener al menos 3 profesores?
    d) El profesor X y el estudiante Y no pueden estar juntos en el comité?

15. En una clase hay n chicas y n chicos. Dar el número de maneras de ubicarlos en una fila de modo que todas las chicas estén juntas.

16. ¿De cuántas maneras distintas pueden sentarse 8 personas en una mesa circular?

17. a) ¿De cuántas maneras distintas pueden sentarse 6 hombres y 6 mujeres en una mesa circular si nunca deben quedar dos mujeres juntas?

    b) Idem, pero con 10 hombres y 7 mujeres.

18. a) ¿De cuántas formas distintas pueden ordenarse las letras de la palabra MATEMATICA?

    b) Idem con las palabras ALGEBRA, GEOMETRIA.

19. ¿De cuántas formas distintas pueden ordenarse las letras de la palabra MATEMATICA si se pide que las consonantes y las vocales se alternen?

20. ¿Cuántas diagonales tiene un polígono regular de n lados?

21. Dados m, n y k naturales tales que $m \leq k \leq n$, probar que se verifica
$$\binom{n}{k}\binom{k}{m} = \binom{n}{m}\binom{n-m}{k-m}.$$

22. Probar que para todo i, j, $k \in \mathbb{N}_0$ vale
$$\binom{i+j+k}{i}\binom{j+k}{j} = \frac{(i+j+k)!}{i!j!k!}$$

23. Demostrar que para todo $n \in \mathbb{N}$ vale:

    a) $\binom{n}{0} + \binom{n}{1} + \cdots + \binom{n}{n} = 2^n$.

    b) $\binom{n}{0} - \binom{n}{1} + \cdots + (-1)^n\binom{n}{n} = 0$

24. Probar que para todo natural n vale que
$$\binom{2n}{2} = 2\binom{n}{2} + n^2.$$

ÁLGEBRA I / MATEMÁTICA DISCRETA I
PRÁCTICO 4

1. Sean a, b, $c \in \mathbb{Z}$. Demostrar las siguientes afirmaciones:
   a) $\forall a$, $a \mid 0$. (En particular, $0 \mid 0$).
   b) $\forall a \neq 0$, $0 \nmid a$.
   c) Si $ab = 1$, entonces $a = b = 1$ ó $a = b = -1$.
   d) Si $a \neq 0$, $b \neq 0$, $a \mid b$ y $b \mid a$, entonces $a = b$ ó $a = -b$.
   e) Si $a \mid 1$, entonces $a = 1$ ó $a = -1$.
   f) Si $a \neq 0$, $a \mid b$ y $a \mid c$, entonces $a \mid (b + c)$ y $a \mid (b - c)$.
   g) Si $a \neq 0$, $a \mid b$ y $a \mid (b + c)$, entonces $a \mid c$.
   h) Si $a \neq 0$ y $a \mid b$, entonces $a \mid b \cdot c$.

2. Probar las siguientes propiedades:
   a) 0 es par.
   b) 1 es impar.
   c) Si b es par y $b \mid c$, entonces c es par. (Por lo tanto, si b es par, también lo es $-b$).
   d) Si b y c son pares, entonces $b+c$ también lo es. (Por lo tanto, la suma de una cantidad cualquiera de números pares es par).
   e) Si un número par divide a 2, entonces ese número es 2 o -2.
   f) La suma de un número par y uno impar es impar.

3. Probar que n es par si y sólo si n^2 es par.

4. Probar que $n(n + 1)$ es par.

5. Sean a, b, $c \in \mathbb{Z}$. ¿Cules de las siguientes afirmaciones son verdaderas? Justificar las respuestas.
   a) $a \mid b \cdot c \Rightarrow a \mid b$ ó $a \mid c$.
   b) $a \mid (b + c) \Rightarrow a \mid b$ ó $a \mid c$.
   c) $a \mid c$ y $b \mid c \Rightarrow a \cdot b \mid c$.
   d) $a \mid c$ y $b \mid c \Rightarrow (a + b) \mid c$.
   e) $a, b, c > 0$ y $a = b \cdot c$, entonces $a \geq b$ y $a \geq c$.

6. -"Pensá un número de dos cifras (que no sean iguales)".

   -" Ya está" (57).

   -" Invertí el orden de las cifras".

   -"Ya está" (75).

   - " El nuevo número, ¿es mayor o menor que el primero?"

   - "Mayor".

   - "Entonces, restá el número que pensaste del nuevo número".

   - "Ya está" $(75 - 57 = 18)$.

   - "Ahora, sumá las cifras del número que pensaste al principio".

   - "Ya está". (5+7=12).

   - "Decime los dos números que obtuviste".

   - "18 el primero y 12 el segundo".

   - (Calcula: $\frac{18}{9} = 2$, $\frac{12+2}{2} = 7$ y $\frac{12-2}{2} = 5$). "Pensaste en el 57".

   Ejercicio: Explicar cómo es el truco y por qué siempre funciona.

7. Probar que cualquiera sea $n \in \mathbb{N}$:
   a) $3^{2n+2} + 2^{6n+1}$ es múltiplo de 11.
   b) $3^{4n+2} + 2 \cdot 4^{3n+1}$ es múltiplo de 17.
   c) $2^{2n-1} \cdot 3^{n+2} + 1$ es divisible por 11.
   d) $3^{2n+2} - 8n - 9$ es divisible por 64.

8. Decir si es verdadero o falso justificando:
   a) $3^n + 1$ es múltiplo de n, $\forall n \in \mathbb{N}$.
   b) $2 \cdot 5^n + 1$ es múltiplo de 4, $\forall n \in \mathbb{N}$.
   c) $10^{2n} - 1$ es múltiplo de 11, $\forall n \in \mathbb{N}$.
   d) $3n^2 + 1$ es múltiplo de 2, $\forall n \in \mathbb{N}$.
   e) $n^3 - n$ es múltiplo de 2, $\forall n \in \mathbb{N}$.
   f) $(n + 1) \cdot (5n + 2)$ es múltiplo de 2, $\forall n \in \mathbb{N}$.
   g) $n \cdot (n + 4) \cdot (n + 2)$ es múltiplo de 3, $\forall n \in \mathbb{N}$.

9. Hallar el cociente y el resto de la división de:

   i) 135 por 23, ii) -135 por 23. iii) 135 por -23

   iv) -135 por -23, v) -98 por 73 vi) -98 por -73.

10. Si $a = b \cdot q + r$, con $b \leq r < 2b$, hallar el cociente y el resto de la división de a por b.

11. Repetir el ejercicio anterior, suponiendo ahora que $-b \leq r < 0$.

12. Expresar 1810, 1816 y 1972 en bases $s = 3,\ 5,\ 7,\ 11$.

13. Expresar en base 10 los siguientes enteros:

    a) $(1503)_6$ b)$(1111)_2$ c) $(1111)_{12}$

    d) $(123)_4$ e) $(12121)_3$ f) $(1111)_5$

14. Calcular:

    a) $(2234)_5 + (2310)_5$ b) $(10101101)_2 + (10011)_2$.

ÁLGEBRA I / MATEMÁTICA DISCRETA I
PRÁCTICO 5

1. Dar todos los números primos positivos menores que 100.

2. Para cada uno de los siguientes pares de nmeros:
   (i) 14 y 35, (ii) 11 y 15, (iii) 12 y 52, (iv) 12 y -52 v) 12 y 532,
   a) calcular el máximo común divisor y expresarlo como combinación lineal de los números dados,
   b) calcular el mínimo común múltiplo.

3. Encontrar $(7469, 2464)$, $(2689, 4001)$, $(2447, -3997)$, $(-1109, -4999)$.

4. Calcular el máximo común divisor entre 606 y 108 y expresarlo como combinación lineal de esos números.

5. Dado un entero a, $a \neq 0$, hallar $(0, a)$.

6. Probar que 3 es primo.

7. Probar que no existen enteros x e y que satisfagan $x + y = 100$ y $(x, y) = 3$.

8. Probar que si $(a, b) = 1$ y $n+2$ es un número primo, entonces $(a+b, a^2+b^2-nab) = 1$ ó $n + 2$.

9. Probar que $(a + b, [a, b]) = (a, b)$. En particular, si dos números son coprimos, también lo son su suma y su producto.

10. Probar que si $n \in \mathbb{Z}$, entonces $2n + 1$ y $\frac{1}{2}n(n + 1)$ son coprimos.

11. Probar: i) $(a, b) = 1$, $a \mid c$ y $b \mid c$, entonces $a \cdot b \mid c$.
    ii) $(a, b) = 1$ y $a \mid bc$ entonces $a \mid c$.

12. a)Probar que el producto de tres enteros consecutivos es divisible por 6.
    b) Probar que el producto de cuatro enteros consecutivos es divisible por 24.

13. Demostrar que $\forall n \in \mathbb{Z}$, $n > 2$, existe p primo tal que $n < p < n!$. (Ayuda: pensar qué primos dividen a $n! - 1$.)

14. Completar y demostrar:
    a) Si $a \in \mathbb{Z}$, entonces $[a, a] = \ldots$.
    b) Si $a, b \in \mathbb{Z}$, $[a, b] = b$ si y sólo si $\ldots$.
    c) $(a, b) = [a, b]$ si y sólo si $\ldots$.

15. ¿Existen enteros m y n tales que:
    a) $m^4 = 27$? b) $m^2 = 12n^2$? c) $m^3 = 47n^3$?

16. Encontrar todos los enteros positivos a y b tales que $(a, b) = 10$, y $[a, b] = 100$.

17. Si $a \cdot b$ es un cuadrado y a y b son coprimos, probar que a y b son cuadrados.

18. Mostrar que 725 y 441 son coprimos y encontrar enteros m, n tales que $1 = m \cdot 725 + n \cdot 441$.

19. Probar que $\sqrt{6}$ es irracional.

20. Probar que $2^{3n+4} + 7^{3n+1}$ es divisible por 9, para todo $n \in \mathbb{N}$, n impar.

21. Probar que todo entero impar que no es múltiplo de 3 es de la forma $6m \pm 1$ para algún $m \in \mathbb{Z}$.

22. Probar que si d es un divisor común de a y b, entonces
    (i) $\frac{(a,b)}{d} = (\frac{a}{d}, \frac{b}{d})$. (ii) $\frac{[a,b]}{d} = [\frac{a}{d}, \frac{b}{d}]$.

23. Probar que para todo $n \in \mathbb{Z}$, $n^2 + 2$ no es divisible por 4.

24. Dado un entero $a > 0$ fijo, caracterizar aquellos números que al dividirlos por a tienen cociente igual al resto.

25. Sea p primo positivo. Probar que $(p, (p-1)!) = 1$.

26. Hallar el menor múltiplo de 168 que sea un cuadrado.

27. Probar que si $(a, 4) = 2$ y $(b, 4) = 2$ entonces $(a + b, 4) = 4$.

28. Probar que el producto de dos enteros consecutivos no nulos no es un cuadrado. (Ayuda: usar el Teorema Fundamental de la Aritmética).

ÁLGEBRA I / MATEMÁTICA DISCRETA I
PRÁCTICO 6

1. a) Calcular el resto de la división de 1599 por 39 sin tener que hacer la división. (Ayuda: $1599 = 1600 - 1 = 40^2 - 1$).
   b) Lo mismo con el resto de 914 al dividirlo por 31.

2. Probar que todo número de la forma $4^n - 1$ es siempre divisible por 3.

3. Probar que el resto de dividir n^2 por 4 es igual a 0 si n es par y 1 si n es impar.

4. Probar que si las longitudes de los lados de un triángulo rectángulo son números enteros, entonces los catetos no pueden ser ambos impares.

5. Probar las reglas de divisibilidad por 2, 3, 4, 5, 6, 7, 8, 9 y 11 que no hayan sido probadas en el teórico.

6. Decir por cuáles de los números del 2 al 11 son divisibles los siguientes números:

   a) 12342 *b*) 5176 *c*) 314573 *d*) 899

7. Hallar los restos posibles en la división de n^2 por 3.

8. Sean a, b, c números enteros, ninguno divisible por 3. Probar que $a^2+b^2+c^2$ es divisible por 3.

9. Hallar la cifra de las unidades y la de las decenas del número 7^{15}.

10. Hallar el resto en la división de x por 5 y por 7 para:

    a) $x = 1^8+2^8+3^8+4^8+5^8+6^8+7^8+8^8$, *b*) $x = 3 \cdot 11 \cdot 17 \cdot 71 \cdot 101$.

11. Sean a, b, $m \in \mathbb{Z}$, $d > 0$ tales que $d \mid a$, $d \mid b$ y $d \mid m$. Probar que la ecuación $a \cdot x \equiv b\,(m)$ tiene solución si y sólo si la ecuación

$$\frac{a}{d} \cdot x \equiv \frac{b}{d}\,(\frac{m}{d})$$

tiene solución.

12. Resolver las siguientes ecuaciones:

a) $2x \equiv -21\ (8)$ *b*) $2x \equiv -12\ (7)$ *c*) $3x \equiv 5\ (4)$.

13. Resolver la ecuación $221.x \equiv 85\ (340)$. Hallar todas las soluciones x tales que $0 \leq x < 340$.

14. Hallar todos los x que satisfacen:

a) $x^2 \equiv 1\ (4)$
b) $x^2 \equiv x\ (12)$
c) $x^2 \equiv 2\ (3)$
d) $x^2 \equiv 0\ (12)$
e) $x^4 \equiv 1\ (16)$
f) $3x \equiv 1\ (5)$
g) $2x \equiv 5\ (6)$
h) $3x^3 \equiv 20\ (8)$.

15. Dado $t \in \mathbb{Z}$, decimos que t es *inversible módulo* m si existe $h \in \mathbb{Z}$ tal que $th \equiv 1\,(m)$.
    a) ¿Es 5 inversible módulo 17?
    b) ¿Existe algún m tal que m sea inversible módulo m?
    c) Probar que t es inversible módulo m, si y sólo si $(t, m) = 1$.
    d) Determinar los inversibles módulo m, para $m = 11, 12, 16$.

16. Encontrar los enteros cuyos cuadrados divididos por 19 dan resto 9.

17. Probar que todo número impar satisface: $a^4 \equiv 1(16)$, $a^8 \equiv 1(32)$; $a^{16} \equiv 1(64)$. ¿Se puede asegurar que $a^{2^n} \equiv 1(2^{n+2})$?

18. Encuentre el resto en la división de a por b en los siguientes casos:

a) $a = 11^{13} \cdot 13^8$; $\quad b = 12$,
b) $a = 4^{1000}$; $\quad b = 7$
c) $a = 123^{456}$; $\quad b = 31$
d) $a = 7^{83}$; $\quad b = 10$.

19. Obtenga el resto en la división de

    a) 2^{21} por 13 *b)* 3^8 por 5 *c)* 8^{25} por 127.

20. Probar que si $(a, 1001) = 1$ entonces 1001 divide a $a^{720} - 1$.

21. Hallar el menor entero positivo que satisface simultáneamente las siguientes congruencias:

    $x \equiv 1\ (3); \qquad x \equiv 1\ (5); \qquad x \equiv 1\ (7).$

22. Hallar todos los enteros que satisfacen:

    $x \equiv 2\ (3); \qquad x \equiv 3\ (5); \qquad x \equiv 5\ (2).$

23. Hallar 4 enteros consecutivos divisibles por 5, 7, 9 y 11 respectivamente.

24. a) Probar que no existen enteros no nulos tales que $x^2 + y^2 = 3z^2$.

    b) Probar que no existen números racionales no nulos a, b, r tales que $3(a^2 + b^2) = 7r^2$.

25. Cinco hombres recogieron en una isla un cierto número de cocos y resolvieron repartirlos al día siguiente. Durante la noche uno de ellos decidió separar su parte y para ello dividió el total en cinco partes y dió un coco que sobraba a un mono y se fue a dormir. Enseguida otro de los hombres hizo lo mismo, dividiendo lo que había quedado por cinco, dando un coco que sobraba a un mono y retirando su parte, se fue a dormir. Uno tras otro los tres restantes hicieron lo mismo, dándole a un mono el coco que sobraba. A la mañana siguiente repartieron los cocos restantes, dándole a un mono el coco sobrante.

    ¿Cuál es el número mínimo de cocos que se recogieron?

26. La producción diaria de huevos en una granja es inferior a 75. Cierto día el recolector informó que la cantidad de huevos recogida es tal que contando de a 3 sobran 2, contando de a 5 sobran 4 y contando de a 7 sobran 5. El capataz, dijo que eso era imposible. ¿Quién tenía razón?. Justificar.

ÁLGEBRA I / MATEMÁTICA DISCRETA I

PRÁCTICO 7 - **GRAFOS**

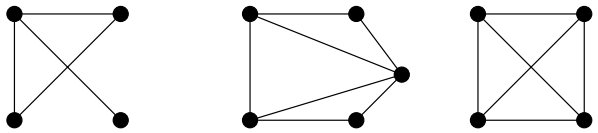
1. Probar que si G es un grafo con más de un vértice, entonces existen dos vértices con la misma valencia.

2. ¿Cuántas aristas tiene un grafo que tiene cuatro vértices de valencia 3, dos vértices de valencia 5, dos de valencia 6 y uno de valencia 8?

3. a) Sea G un grafo tal que todos sus vértices tienen valencia 21. Probar que el número de aristas es un múltiplo de 21.

   b) ¿Qué hay de particular acerca del número 21? ¿Valdría el ejercicio si se pusiera 15, 17 o 101 en vez de 21? Y si se pusiera 22, ¿qué se podría decir?

4. Sea $G = (\mathcal{V}, \mathcal{A})$ un grafo. Hallar el complemento de los siguientes grafos:



5. Si G es un grafo con n vértices y a aristas, calcular la cantidad de aristas de $\tilde{G}$ en términos de n y a. Si $\delta(v)$ es la valencia o grado de un vértice de un grafo G de n vértices, calcule la valencia $\tilde{\delta}(v)$ de v en $\tilde{G}$ en términos de n y $\delta(v)$.

6. Encontrar todos los grafos de 5 vértices y 2 aristas, no isomorfos entre sí.

7. Encontrar todos los grafos con cuatro vértices o menos, no isomorfos entre sí. *Ayuda:* Hay uno de 1 vértice, dos con 2, cuatro con 3 y once con 4 vértices.

8. Sean $G = (\mathcal{V}, \mathcal{A})$ y $G' = (\mathcal{V}, \mathcal{A})$ dos grafos isomorfos y sea α un isomorfismo entre ellos. Probar las siguientes afirmaciones:

   i) $|\mathcal{V}| = |\mathcal{V}'|$ y $|\mathcal{A}| = |\mathcal{A}'|$,

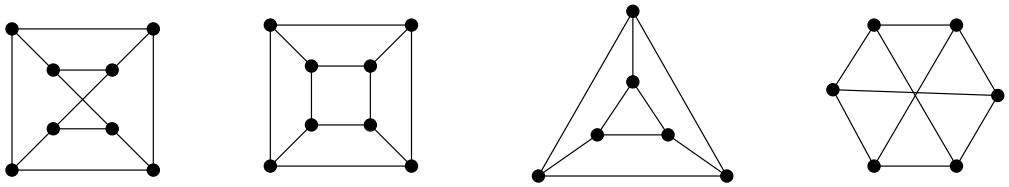
   ii) $\delta(v) = \delta(\alpha(v))$, para todo $v \in \mathcal{V}$.

9. Sean $G = (\mathcal{V}, \mathcal{A})$ y $G' = (\mathcal{V}', \mathcal{A}')$ dos grafos y sea $\alpha : \mathcal{V} \mapsto \mathcal{V}'$ una función biyectiva tal que $\delta(v) = \delta(\alpha(v))$, para todo $v \in \mathcal{V}$.

   i) ¿Se puede afirmar que α es un isomorfismo?

   ii) ¿Puede afirmarse si $|\mathcal{V}| = 3$ o $|\mathcal{V}| = 4$?

10. Probar que los siguientes pares de grafos no son isomorfos.



11. Denotamos con C_n al grafo *cíclico* de n vértices $\mathcal{V} = \{v_1, v_2, \ldots, v_n\}$ con aristas $\mathcal{A} = \{\{v_i, v_{i+1}\} \mid 1 \leq i < n\} \cup \{\{v_1, v_n\}\}$. Probar que C_5 es isomorfo a $\tilde{C}_5$. Luego probar que si $n \neq 5$, entonces C_n no es isomorfo a $\tilde{C}_n$.

12. Puesto que, de acuerdo con el ejercicio (7), hay 11 grafos no isomorfos con cuatro vértices, se deduce que debe haber un grafo con 4 vértices isomorfo a su complemento. Determinar este grafo.

13. Sea $G = (\mathcal{V}, \mathcal{A})$ un grafo, y sea $n = |\mathcal{V}|$.

    a) Probar que si $G_1 = (\mathcal{V}_1, \mathcal{A}_1)$ es una componente conexa de G tal que $|\mathcal{V}_1| = k$, con $1 < k < n$, entonces $|\mathcal{A}| \leq \binom{k}{2} + \binom{n-k}{2}$.

    b) Probar que si $1 < k < n$, entonces $\binom{k}{2} + \binom{n-k}{2} \leq \binom{n-1}{2}$.

    c) Probar que si $|\mathcal{A}| > \binom{n-1}{2}$, entonces G es un grafo conexo.

14. Probar que ningún grafo completo (salvo K_2) tiene una caminata euleriana abierta (es decir, que no es un circuito euleriano). ¿Cuáles grafos completos tienen un circuito euleriano?

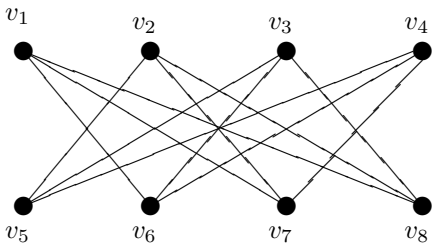
15. a) Probar que si G es un grafo en el que cada vértice tiene grado mayor que 1, entonces G tiene un ciclo.

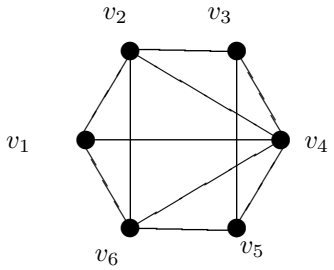
    b) El ítem a) afirma que si T es un árbol, entonces existe al menos un vértice de grado 1. Probar que si $T = (\mathcal{V}, \mathcal{A})$ es un árbol y $|\mathcal{V}| \geq 2$, entonces existen al menos dos vértices de grado 1 (hojas).

16. Sea $G = (\mathcal{V}, \mathcal{A})$ un grafo con $|\mathcal{V}| = n$. Probar que las siguientes afirmaciones son equivalentes:
    a) G es un árbol.
    b) G es conexo, y cualquiera sea $a \in \mathcal{A}$, $G' = (\mathcal{V}, \mathcal{A} - \{a\})$ no es conexo.
    c) G es acíclico y si se le agrega una arista deja de serlo.
    d) G es acíclico y tiene $n - 1$ aristas.
    e) G es conexo y tiene $n - 1$ aristas.

17. Probar que si $G = (T, A)$ es un bosque con c componentes conexas, entonces $|\mathcal{A}| = |\mathcal{V}| - c$.

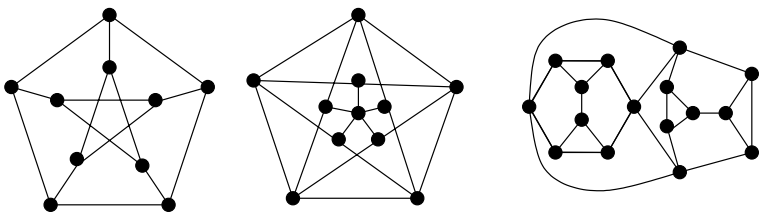
18. a) Aplicar el algoritmo greedy al grafo G_1 usando los siguientes órdenes en los vértices:
    i) $v_1, v_5, v_2, v_6, v_3, v_7, v_4, v_8$. ii) $v_1, v_2, v_3, v_4, v_5, v_6, v_7, v_8$.
    b) Para el grafo G_2 encontrar un orden de los vértices tal que el algoritmo greedy dé una coloración con 4 colores.

G_1 



G_2

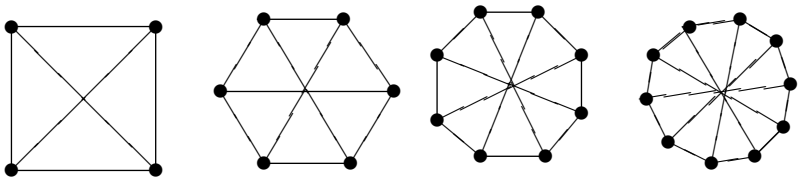
19. Encontrar los números cromáticos de los siguientes grafos:
    a) K_n, (grafo completo de n vértices).
    b) C_n, (ciclo de n vértices).
    c) Los siguientes tres grafos:



20. Pruebe que para todo grafo se puede encontrar un orden de los vértices tal que el algoritmo greedy requiera una cantidad de colores igual al número cromático del grafo.

21. Pruebe que para todo grafo $G = (\mathcal{V}, \mathcal{A})$ se cumple que $|\mathcal{A}| \geq \binom{\chi(G)}{2}$.

22. Para $r \geq 2$, el grafo M_r se obtiene del grafo C_{2r} agregando las aristas que unen vértices "opuestos", es decir las aristas $\{v_i, v_{r+i}\}$, para $1 \leq i \leq r$. Pruebe que:
    a) si r es impar, entonces M_r es bipartito,
    b) si r es par y $r > 2$, entonces $\chi(M_r) = 3$, y que
    c) $\chi(M_2) = 4$.



M_2 M_3 M_4 M_5

23. Pruebe que si G es un grafo bipartito con una cantidad impar de vértices, entonces G no tiene ciclos hamiltonianos.
24. ¿Tiene el siguiente grafo un ciclo hamiltoniano?