Apuntes de Matemática Discreta

Francisco José González Gutiérrez

19 de Diciembre de 2014

Contenido

Unidad Temática I

Lógica Matemática

Lección 1

Lógica de Proposiciones

Y ahora llegamos a la gran pregunta del porqué. El robo no ha sido el objeto del asesinato, puesto que nada desapareció. ¿Fue por motivos políticos, o fue una mujer? Esta es la pregunta con que me enfrento. Desde el principio me he inclinado hacia esta última suposición. Los asesinatos políticos se complacen demasiado en hacer su trabajo y huir. Este asesinato, por el contrario, había sido realizado muy deliberadamente, y quien lo perpetró ha dejado huellas por toda la habitación, mostrando que estuvo allí todo el tiempo.

Arthur Conan Doyle. Un Estudio en Escarlata. 1887

La estrecha relación existente entre la matemática moderna y la lógica formal es una de sus características fundamentales. La lógica aristotélica era insuficiente para la creación matemática ya que la mayor parte de los argumentos utilizados en ésta contienen enunciados del tipo "si, entonces", absolutamente extraños en aquella.

En esta primera lección de lógica estudiaremos uno de los dos niveles en los que se desenvuelve la moderna lógica formal: la lógica de enunciados o de proposiciones.

1.1 Proposiciones y Tablas de Verdad

Cuando planteamos cualquier idea o teoría, científica o no, hacemos afirmaciones en forma de frases y que tienen un sentido pleno. Tales afirmaciones, verbales o escritas, las denominaremos enunciados o proposiciones.

1.1.1 Proposición

Llamaremos proposición a cualquier afirmación que sea verdadera o falsa, pero no ambas cosas a la vez.

■

Ejemplo 1.1

Las siguientes afirmaciones son proposiciones.

(a) *Gabriel García Márquez escribió* Cien años de soledad.

(b) 6 *es un número primo.*

(c) $3 + 2 = 6$

(d) 1 *es un número entero, pero* 2 *no lo es.*

(e) *El resto de dividir* -5 *entre* 2 *es* 1.

■

Nota 1.1 Las proposiciones se notan con letras minúsculas, $p,\ q,\ r,\ s,\ t, \ldots\ldots$

La notación p :*Tres más cuatro es igual a siete* se utiliza para definir que p es la proposición "Tres más cuatro es igual a siete".

Este tipo de proposiciones se llaman *simples*, ya que no pueden descomponerse en otras.

■

Ejemplo 1.2

Las siguientes afirmaciones no son proposiciones.

(a) $x + y > 5$

(b) *¿Te vas?*

(c) *Compra cinco manzanas y cuatro peras.*

(d) $x = 2$

Solución

(a) $x + y > 5$. Aunque es una afirmación no es una proposición ya que será verdadera o falsa dependiendo de los valores que tomen x e y.

(b) ¿Te vas? No es una afirmación y, por tanto, no es una proposición.

(c) Compra cinco manzanas y cuatro peras. No es una proposición ya que, al igual que la anterior, no es una afirmación.

(d) $x = 2$. No es una proposición ya que será verdadera o falsa según el valor que tome x.

■

Desde el punto de vista lógico carece de importancia cual sea el contenido material de los enunciados o proposiciones, solamente nos interesa su *valor de verdad*.

1.1.2 Valor de verdad

Llamaremos valor verdadero o de verdad de una proposición a su veracidad o falsedad. El valor de verdad de una proposición verdadera es verdad y el de una proposición falsa es falso.

■

Ejemplo 1.3

Dígase cuáles de las siguientes afirmaciones son proposiciones y determinar el valor de verdad de aquellas que lo sean.

(a) p: Existe Premio Nobel de informática.

(b) q: La tierra es el único planeta del Universo que tiene vida.

(c) r: Teclee Escape para salir de la aplicación.

(d) s: Cinco más siete es grande.

Solución

(a) p es una proposición falsa, es decir su *valor de verdad* es Falso.

(b) No sabemos si q es una proposición ya que desconocemos si esta afirmación es verdadera o falsa.

(c) r no es una proposición ya que no es una afirmación, es un mandato.

(d) s no es una proposición ya que su enunciado, al carecer de contexto, es ambiguo. En efecto, cinco niñas más siete niños es un número grande de hijos en una familia, sin embargo cinco monedas de cinco céntimos más siete monedas de un céntimo no constituyen una cantidad de dinero grande.

■

1.1.3 Variables de enunciado

Es una proposición arbitraria, p, con un valor de verdad no especificado, es decir, puede ser verdad o falsa.

En el cálculo lógico, prescindiremos de los contenidos de las proposiciones y los sustituiremos por *variables de enunciado*. Toda variable de enunciado, p, puede ser sustituida por cualquier enunciado siendo sus posibles valores, verdadero o falso. El conjunto de los posibles valores de una proposición p, los representaremos en las llamadas *tablas de verdad*, ideadas por L.Wittgenstein[1].

■

[1] *Ludwig Wittgenstein* (Viena 1889-Cambridge 1951), nacionalizado británico en 1938. Estudió Ingeniería Mecánica en Berlin, posteriormente investigó Aeronáutica en Manchester. La necesidad de entender mejor las matemáticas lo llevó a estudiar sus fundamentos. Dejó Manchester en 1911 para estudiar lógica matemática con Russell en Cambridge. Escribió su primer gran trabajo en lógica, *Tractatus logico-philosophicus*, durante la primera guerra mundial, primero en el frente ruso y luego en el norte de Italia. Envió el manuscrito a Russell desde un campo de prisioneros en Italia. Liberado en 1919, regaló la fortuna que había heredado de su familia y trabajó en Austria como profesor en una escuela primaria. Volvió a Cambridge en 1929 y fue profesor en esta universidad hasta 1947, año en que renunció. Su segundo gran trabajo, *Investigaciones filosóficas* fue publicado en 1953, es decir, dos años después de su muerte. Otras obras póstumas de Wittgenstein son: *Observaciones filosóficas sobre los principios de la matemática*(1956), *Cuadernos azul y marrón*(1958) y *Lecciones y conversaciones sobre estética, sicología y fe religiosa*(1966).

1.1.4 Proposiciones simples

Llamaremos de esta forma a aquellas proposiciones que no puedan descomponerse en otras más sencillas.

1.1.5 Proposición compuesta

Si las proposiciones simples $p_1, p_2, \ldots, p_n$ se combinan para formar la proposición P, diremos que P es una proposición compuesta de $p_1, p_2, \ldots, p_n$.

Ejemplo 1.4

"La Matemática Discreta es mi asignatura preferida y Mozart fue un gran compositor" *es una proposición compuesta por las proposiciones* "La Matemática Discreta es mi asignatura preferida" *y* "Mozart fue un gran compositor".

"El es inteligente o estudia todos los días" *es una proposición compuesta por dos proposiciones:* "El es inteligente" *y* "El estudia todos los días".

"Si estudio todos los días, aprobaré esta asignatura" *es una proposición compuesta por las proposiciones* "estudio todos los días" *y* "aprobaré esta asignatura".

■

Nota 1.2 La propiedad fundamental de una proposición compuesta es que su *valor de verdad* está completamente determinado por los *valores de verdad* de las proposiciones que la componen junto con la forma en que están conectadas.

■

1.1.6 Tablas de verdad

La tabla de verdad de una proposición compuesta P, enumera todas las posibles combinaciones de los valores de verdad de las proposiciones $p_1, p_2, \ldots, p_n$ que la componen.

Ejemplo 1.5

Por ejemplo, si P es una proposición compuesta por las proposiciones simples p_1, p_2 y p_3, entonces la tabla de verdad de P deberá recoger los siguientes valores de verdad.

p_1	p_2	p_3
V	V	V
V	V	F
V	F	V
V	F	F
F	V	V
F	V	F
F	F	V
F	F	F

■

1.2 Conexión entre Proposiciones

Estudiamos en este apartado las distintas formas de conectar proposiciones entre sí. Prestaremos especial atención a las tablas de verdad de las proposiciones compuestas que pueden formarse utilizando las distintas conexiones.

1.2.1 Conjunción

Dadas dos proposiciones cualesquiera p y q, llamaremos conjunción de ambas a la proposición compuesta "p y q" y la notaremos $p \wedge q$. Esta proposición será verdadera únicamente en el caso de que ambas proposiciones lo sean.

Obsérvese que de la definición dada se sigue directamente que si al menos una de las dos, p ó q, es falsa, entonces $p \wedge q$ no puede ser verdad y, consecuentemente, será falsa. Por lo tanto su *tabla de verdad* vendrá dada por

p	q	$p \wedge q$
V	V	V
V	F	F
F	V	F
F	F	F

Obsérvese también que el razonamiento puede hacerse a la inversa, es decir si $p \wedge q$ es verdad, entonces p y q son, ambas, verdad y que si $p \wedge q$ es falsa, entonces una de las dos, al menos, ha de ser falsa.

■

1.2.2 Disyunción

Dadas dos proposiciones cualesquiera p y q, llamaremos disyunción de ambas a la proposición compuesta "p ó q" y la notaremos $p \vee q$. Esta proposición será falsa únicamente si ambas proposiciones, p y q, lo son.

De acuerdo con la definición dada se sigue que si una de las dos, p ó q, es verdad entonces $p \vee q$ no puede ser falsa y, consecuentemente, será verdadera. Su *tabla de verdad* será, por tanto,

p	q	$p \vee q$
V	V	V
V	F	V
F	V	V
F	F	F

Al igual que en la conjunción, podemos razonar en sentido inverso. En efecto, si $p \vee q$ es verdad, entonces una de las dos, al menos, ha de ser verdad y si $p \vee q$ es falsa, entonces ambas han de ser falsas.

■

La palabra "o" se usa en el lenguaje ordinario de dos formas distintas. A veces se utiliza en el sentido de "p ó q, ó ambos", es decir, al menos una de las dos alternativas ocurre y, a veces es usada en el sentido de "p ó q, pero no ambos" es decir, ocurre exactamente una de de las dos alternativas.

Por ejemplo, la proposición "El irá a Madrid o a Bilbao" usa "o" con el último sentido. A este tipo de disyunción la llamaremos *disyunción exclusiva.*

1.2.3 Disyunción exclusiva

Dadas dos proposiciones cualesquiera p y q, llamaremos disyunción exclusiva de ambas a la proposición compuesta "p ó q pero no ambos" y la notaremos $p \veebar q$. Esta proposición será verdadera si una u otra, pero no ambas, son verdaderas.

Según esta definición una disyunción exclusiva de dos proposiciones p y q será verdadera cuando tengan distintos valores de verdad y falsa cuando sus valores de verdad sean iguales. Su *tabla de verdad* es, por tanto,

p	q	$p \veebar q$
V	V	F
V	F	V
F	V	V
F	F	F

Haciendo el razonamiento contrario si $p \veebar q$ es verdad, únicamente podemos asegurar que una de las dos es verdad y si $p \veebar q$ es falsa, sólo podemos deducir que ambas tienen el mismo valor de verdad.

■

Nota 1.3 Salvo que especifiquemos lo contrario, "o" será usado en el primero de los sentidos. Esta discusión pone de manifiesto la precisión que ganamos con el lenguaje simbólico: $p \vee q$ está definida por su tabla de verdad y *siempre* significa p y/ó q.

■

1.2.4 Negación

Dada una proposición cualquiera, p, llamaremos "negación de p" a la proposición "no p" y la notaremos $\neg p$. Será verdadera cuando p sea falsa y falsa cuando p sea verdadera.

La *tabla de verdad* de esta nueva proposición, $\neg p$, es:

p	$\neg p$
V	F
F	V

De esta forma, el valor verdadero de la negación de cualquier proposición es siempre opuesto al valor verdadero de la afirmación original.

■

Ejemplo 1.6

Estudiar la veracidad o falsedad de las siguientes proposiciones:

p_1*: El Pentium es un microprocesador.*

p_2*: Es falso que el Pentium sea un microprocesador.*

p_3*: El Pentium no es un microprocesador.*

p_4*:* $2 + 2 = 5$

p_5*: Es falso que* $2 + 2 = 5$

Solución

- ✓ p_2 y p_3 son, cada una, la negación de p_1.
- ✓ p_5 es la negación de p_4.

Pues bien, de acuerdo con la tabla de verdad para la negación, tendremos:

- ✓ p_1 es verdad, luego p_2 y p_3 son falsas.
- ✓ p_4 es falsa, luego p_5 es verdad.

■

Ejemplo 1.7

Construir la tabla de verdad de la proposición $\neg(p \wedge \neg q)$.

Solución

p	q	$\neg q$	$p \wedge \neg q$	$\neg\,(p \wedge \neg q)$
V	V	F	F	V
V	F	V	V	F
F	V	F	F	V
F	F	V	F	V

■

1.2.5 Tautologías y contradicciones

Sea P *una proposición compuesta de las proposiciones simples* $p_1, p_2, \ldots, p_n$

P *es una Tautología si es verdadera para todos los valores de verdad que se asignen a* $p_1, p_2, \ldots, p_n$.

P *es una Contradicción si es falsa para todos los valores de verdad que se asignen a* $p_1, p_2, \ldots, p_n$.

En adelante, notaremos por "C" a una contradicción y por "T" a una tautología.

Una proposición P que no es tautología ni contradicción se llama, usualmente, *Contingencia.*

■

Ejemplo 1.8

Probar que la proposición compuesta $p \vee \neg p$ es una tautología y la $p \wedge \neg p$ es una contradicción.

Solución

Lo resolveremos escribiendo una tabla de verdad. En efecto,

p	$\neg p$	$p \vee \neg p$	$p \wedge \neg p$
V	F	V	F
F	V	V	F

Obsérvese que $p \vee \neg p$ es verdad, independientemente de quienes sean las variables de enunciado, p y $\neg p$ y lo mismo ocurre con la falsedad de $p \wedge \neg p$.

■

1.2.6 Proposición condicional

Dadas dos proposiciones p y q, a la proposición compuesta

"si p, entonces q"

se le llama "proposición condicional" y se nota por

$$p \longrightarrow q$$

A la proposición "p" se le llama hipótesis, antecedente, premisa o condición suficiente y a la "q" tesis, consecuente, conclusión o condición necesaria del condicional. Una proposición condicional es falsa únicamente cuando siendo verdad la hipótesis, la conclusión es falsa (no se debe deducir una conclusión falsa de una hipótesis verdadera).

De acuerdo con esta definición se sigue que si la hipótesis, p, es verdadera y la conclusión, q, es falsa, entonces el condicional $p \longrightarrow q$ es falso. En todos los demás casos, la proposición no es falsa y, por lo tanto, ha de ser verdadera. Consecuentemente, su *tabla de verdad* será:

p	q	$p \longrightarrow q$
V	V	V
V	F	F
F	V	V
F	F	V

Obsérvese que si $p \longrightarrow q$ es verdadero, entonces puede deducirse que la conclusión, q, es verdadera, independientemente del valor de verdad que tenga la hipótesis, p, o la hipótesis, p, es falsa, independientemente del valor de verdad que tenga la conclusión, q.

También puede observarse que si el condicional $p \longrightarrow q$ es falso, entonces lo único que puede deducirse es que la hipótesis, p, es verdadera y la conclusión, q, falsa.

■

Nota 1.4 El esquema siguiente presenta otras *formulaciones equivalentes* del condicional,

$p \longrightarrow q$	q si p
	p sólo si q
	p es una condición suficiente para q.
	q es una condición necesaria para p.
	q se sigue de p.
	q a condición de p.
	q cuando p.

Analizaremos con detalle cada uno de los cuatro casos que se presentan en la tabla de verdad.

1.– Antecedente y consecuente verdaderos.

En este caso parece evidente que el condicional "*si p, entonces q*" se evalúe como verdadero. Por ejemplo,

"*Si como mucho, entonces engordo*"

es una sentencia que se evalúa como verdadera en el caso de que tanto el antecedente como el consecuente sean verdaderos.

Ahora bien, obsérvese que ha de evaluarse también como verdadero un condicional en el que no exista una relación de causa entre el antecedente y el consecuente. Por ejemplo, el condicional

"*Si García Lorca fue un poeta, entonces Gauss fue un matemático*"

ha de evaluarse como verdadero y no existe relación causal entre el antecedente y el consecuente. Es por esta razón que no hay que confundir el condicional con la *implicación lógica.*

"*García Lorca fue un poeta implica que Gauss fue un matemático*"

Es una implicación falsa desde el punto de vista lógico. Más adelante estudiaremos la implicación lógica.

2.– Antecedente verdadero y consecuente falso.

En este caso parece natural decir que el condicional se evalúa como falso. Por ejemplo, supongamos que un político aspirante a Presidente del Gobierno promete:

"*Si gano las elecciones, entonces bajaré los impuestos*"

Este condicional será falso sólo si ganando las elecciones, el político no baja los impuestos. A nadie se le ocurriría reprochar al político que no ha bajado los impuestos si no ha ganado las elecciones. Obsérvese que el hecho de que p sea verdadero y, sin embargo, q sea falso viene, en realidad, a refutar la sentencia $p \longrightarrow q$, es decir la hace falsa.

3.– Antecedente falso y consecuente verdadero.

Nuestro sentido común nos indica que el condicional $p \longrightarrow q$ no es, en este caso, ni verdadero ni falso. Parece ilógico preguntarse por la veracidad o falsedad de un condicional cuando la condición expresada por el antecedente no se cumple. Sin embargo, esta respuesta del sentido común no nos sirve, estamos en lógica binaria y todo ha de evaluarse bien como verdadero, bien como falso, es decir, si una sentencia no es verdadera, entonces es falsa y viceversa.

Veamos que en el caso que nos ocupa, podemos asegurar que el condicional no es falso. En efecto, como dijimos anteriormente, $p \longrightarrow q$ es lo mismo que afirmar que

"p es una condición suficiente para q"

es decir, p no es la única condición posible, por lo cual puede darse el caso de que q sea verdadero siendo p falso. O sea, la falsedad del antecedente no hace falso al condicional y si no lo hace falso, entonces lo hace verdadero. Por ejemplo,

"*Si estudio mucho, entonces me canso*"

¿Qué ocurriría si no estudio y, sin embargo, me cansara? Pues que la sentencia no sería inválida, ya que no se dice que no pueda haber otros motivos que me puedan producir cansancio.

4.– Antecedente y consecuente falsos.

La situación es parecida a la anterior. La condición p no se verifica, es decir, es falsa, por lo que el consecuente q puede ser tanto verdadero como falso y el condicional, al no ser falso, será verdadero.

Obsérvese, anecdóticamente, que es muy frecuente el uso de este condicional en el lenguaje coloquial, cuando se quiere señalar que, ante un dislate, cualquier otro está justificado.

"*Si tú eres programador, entonces yo soy el dueño de Microsoft*"

■

Ejemplo 1.9

Dadas las proposiciones:

p: El número a es par.

q: Los resultados salen en pantalla.

r: Los resultados se imprimen.

Enunciar las formulaciones equivalentes de las siguientes proposiciones.

(a) $q \longrightarrow p$.

(b) $\neg q \longrightarrow r$.

(c) $r \longrightarrow (p \vee q)$.

Solución

(a) $q \longrightarrow p$.

Formulaciones equivalentes de $q \longrightarrow p$

Si q, entonces p	Si los resultados salen en pantalla, entonces a es par.
p si q	a es par si los resultados salen en pantalla.
q sólo si p	Los resultados salen en pantalla sólo si el número a es par.
q es suficiente para p	Es suficiente que los resultados salgan en pantalla para que a sea par.
p es necesaria para q	Para que los resultados salgan en pantalla es necesario que a sea par.

(b) $\neg q \longrightarrow r$.

Formulaciones equivalentes de $\neg q \longrightarrow r$	
Si $\neg q$, entonces r	Si los resultados no salen en pantalla, entonces se imprimen.
r si $\neg q$	Los resultados se imprimen si no salen en pantalla.
$\neg q$ sólo si r	Los resultados no salen en pantalla sólo si se imprimen.
$\neg q$ es suficiente para r	Es suficiente que los resultados no salgan en pantalla para que se impriman.
r es necesaria para $\neg q$	Es necesario que los resultados se impriman para que no salgan en pantalla.

(c) $r \longrightarrow (p \vee q)$.

Formulaciones equivalentes de $r \longrightarrow (p \vee q)$	
Si r, entonces $p \vee q$	Si los resultados se imprimen, entonces a es par o los resultados salen en pantalla.
$(p \vee q)$ si r	a es par o los resultados salen en pantalla si los resultados se imprimen.
r sólo si $(p \vee q)$	Los resultados se imprimen sólo si salen en pantalla o a es par.
r es suficiente para $(p \vee q)$	Es suficiente que los resultados se impriman para que a sea par o los resultados salgan en la pantalla.
$(p \vee q)$ es necesaria para r	Para que los resultados se impriman es necesario que a sea par o que salgan en pantalla.

■

Ejemplo 1.10

Sean las proposiciones

p : *Está lloviendo.*

q : *Iré a la playa.*

r : *Tengo tiempo.*

(a) Escribir, usando conectivos lógicos, una proposición que simbolice cada una de las afirmaciones siguientes:

(a.1) Si no está lloviendo y tengo tiempo, entonces iré a la playa.

(a.2) Iré a la playa sólo si tengo tiempo.

(a.3) No está lloviendo.

(a.4) Está lloviendo, y no iré a la ciudad.

(b) Enunciar las afirmaciones que se corresponden con cada una de las proposiciones siguientes:

(b.1) $q \longrightarrow (r \wedge \neg p)$

(b.2) $r \wedge q$

(b.3) $r \longrightarrow q$

(b.4) $\neg r \wedge \neg q$

Solución

(a) Escribimos en forma simbólica las afirmaciones propuestas.

(a.1) $(\neg p \wedge r) \longrightarrow q$

(a.2) $q \longrightarrow r$

(a.3) $\neg p$

(a.4) $p \wedge \neg q$

(b) Escribimos en forma de afirmaciones las proposiciones.

(b.1) Iré a la playa sólo si tengo tiempo y no está lloviendo.

(b.2) Tengo tiempo e iré a la playa.

(b.3) Iré a la playa si tengo tiempo.

(b.4) Ni tengo tiempo, ni iré a la ciudad.

■

1.2.7 Proposición recíproca

Dada la proposición condicional $p \longrightarrow q$, su recíproca es la proposición, también condicional, $q \longrightarrow p$.

Por ejemplo, la recíproca de "*Si la salida no va a la pantalla, entonces los resultados se dirigen a la impresora*" será "*Si los resultados se dirigen a la impresora, entonces la salida no va a la pantalla*".

■

1.2.8 Proposición contrarrecíproca

Dada la proposición condicional $p \longrightarrow q$, su contrarrecíproca es la proposición condicional, $\neg q \longrightarrow \neg p$.

Por ejemplo, la contrarrecíproca de la proposición *"Si María estudia mucho, entonces es buena estudiante"* es *"Si María no es buena estudiante, entonces no estudia mucho"*.

■

Ejemplo 1.11

Escribir la recíproca y la contrarrecíproca de cada una de las afirmaciones siguientes:

(a) Si llueve, no voy.

(b) Me quedaré, sólo si tú te vas.

(c) Si tienes 1 *euro, entonces puedes comprar un helado.*

Solución

(a) Si llueve, no voy.

Si llamamos p: llueve y q: no voy, la afirmación propuesta es el condicional $p \longrightarrow q$. Pues bien,

	$p \longrightarrow q$	Si llueve, entonces no voy.
Recíproca	$q \longrightarrow p$	Si no voy, entonces llueve. No voy sólo si llueve.
Contrarrecíproca	$\neg q \longrightarrow \neg p$	Si voy, entonces no llueve. No llueve si voy Voy sólo si no llueve.

(b) Me quedaré sólo si te vas.

Llamaremos p: me quedaré y q: te vas. Entonces,

	$p \longrightarrow q$	Me quedaré sólo si te vas.
Recíproca	$q \longrightarrow p$	Si te vas, entonces me quedaré. Me quedaré si te vas.
Contrarrecíproca	$\neg q \longrightarrow \neg p$	Si no te vas, entonces no me quedaré. No me quedaré si no te vas.

(c) Si tienes 1 euro, entonces puedes comprar un helado.

Tomando p: tienes 1 euro y q: puedes comprar un helado.

	$p \longrightarrow q$	Puedes comprar un helado si tienes un euro.
Recíproca	$q \longrightarrow p$	Si puedes comprar un helado, entonces tienes 1 euro. Tienes 1 euro si puedes comprar un helado. Puedes comprar un helado sólo si tienes un euro.
Contrarrecíproca	$\neg q \longrightarrow \neg p$	Si no puedes comprar un helado, entonces no tienes 1 euro. No tienes 1 euro si no puedes comprar un helado.

■

1.2.9 Proposición bicondicional

Dadas dos proposiciones p y q, a la proposición compuesta

"p si y sólo si q"

se le llama "proposición bicondicional" y se nota por

$$p \longleftrightarrow q$$

La interpretación del enunciado es:

p sólo si q y p si q

o lo que es igual

si p, entonces q y si q, entonces p

es decir,

$$(p \longrightarrow q) \wedge (q \longrightarrow p)$$

Por tanto, su *tabla de verdad* es:

p	q	$p \longrightarrow q$	$q \longrightarrow p$	$p \longleftrightarrow q$
V	V	V	V	V
V	F	F	V	F
F	V	V	F	F
F	F	V	V	V

Luego la proposición bicondicional $p \longleftrightarrow q$ es verdadera únicamente en caso de que ambas proposiciones, p y q, tengan los mismos valores de verdad.

Obsérvese también que el razonamiento puede hacerse a la inversa, es decir si $p \longleftrightarrow q$ es verdadera, entonces p y q han de tener, ambas, el mismo valor de verdad. En cambio, si $p \longleftrightarrow q$ es falsa, lo que puede deducirse es que p y q tienen distintos valores de verdad.

■

Nota 1.5 Obsérvese que la proposición condicional $p \longrightarrow q$, se enunciaba

Si p, entonces q

siendo una formulación equivalente,

Una condición necesaria para p es q

y la proposición condicional $q \longrightarrow p$, se enunciaba

Si q, entonces p

siendo una formulación equivalente,

Una condición suficiente para p es q

Por tanto, una formulación equivalente de la proposición bicondicional en estos términos, sería:

Una condición necesaria y suficiente para p es q

■

Ejemplo 1.12

Sean a, b y c las longitudes de los lados de un triángulo T siendo c la longitud mayor. El enunciado

$$T \text{ es rectángulo si, y sólo si } a^2 + b^2 = c^2$$

puede expresarse simbólicamente como

$$p \longleftrightarrow q$$

donde p es la proposición "T es rectángulo" y q la proposición "$a^2 + b^2 = c^2$".

Observemos lo siguiente: La proposición anterior afirma dos cosas

1. *Si T es rectángulo, entonces $a^2 + b^2 = c^2$*
   o también,
   Una condición necesaria para que T sea rectángulo es que $a^2 + b^2 = c^2$
2. *Si $a^2 + b^2 = c^2$, entonces T es rectángulo*
   o también,
   Una condición suficiente para que T sea rectángulo es que $a^2 + b^2 = c^2$

Consecuentemente, una forma alternativa de formular la proposición dada es

$$\text{Una condición necesaria y suficiente para que } T \text{ sea rectángulo es que } a^2 + b^2 = c^2.$$

es decir,

"Para que un triángulo sea rectángulo es necesario y suficiente que sus lados verifiquen el teorema de Pitágoras".

■

Nota 1.6 Los valores de verdad de una proposición compuesta pueden determinarse, a menudo, mediante la construcción de una *tabla de verdad abreviada.* Por ejemplo, si queremos probar que una proposición es una contingencia, es suficiente con que consideremos dos líneas de su tabla de verdad, una que haga que la proposición sea verdad y otra que la haga falsa. Para determinar si una proposición es una tautología, bastaría considerar, únicamente, aquellas líneas para las cuales la proposición pueda ser falsa. Veamos algún ejemplo para aclarar esta situación.

Ejemplo 1.13

Consideremos el problema de determinar si la proposición $(p \wedge q) \longrightarrow p$ es una tautología.

Solución

Construimos su tabla de verdad,

p	q	$p \wedge q$	$(p \wedge q) \longrightarrow p$
V	V	V	V
V	F	F	V
F	V	F	V
F	F	F	V

y, en efecto, $(p \wedge q) \longrightarrow p$ es una tautología.

Observemos ahora lo siguiente: Una proposición condicional sólo puede ser falsa en caso de que siendo la hipótesis verdadera, la conclusión sea falsa, por tanto si queremos ver si $(p \wedge q) \longrightarrow p$ es una tautología, bastaría comprobar los casos en que $p \wedge q$ sea verdad, o aquellos en los que p sea falsa ya que en todos los demás la proposición es verdadera. Lo haremos de las dos formas:

– Supongamos que la hipótesis, $p \wedge q$, es verdad y veamos que, en tal caso, la conclusión, p, no puede ser falsa. En efecto,

p	q	$p \wedge q$	$(p \wedge q) \longrightarrow p$
		V	

Entonces, por definición del valor de verdad del conectivo $\wedge$, p y q deben ser, ambas, verdad.

p	q	$p \wedge q$	$(p \wedge q) \longrightarrow p$
V	V	V	

Consecuentemente, el condicional $(p \wedge q) \longrightarrow p$ es verdad.

p	q	$p \wedge q$	$(p \wedge q) \longrightarrow p$
V	V	V	V

La proposición $(p \wedge q) \longrightarrow p$ es, por lo tanto, una tautología ya que todos los demás casos son verdad por definición del valor de verdad del condicional.

– También podemos hacerlo partiendo de que la conclusión, p, es falsa. En tal caso veremos que la hipótesis, $p \wedge q$ no puede ser verdad. En efecto,

p	q	$p \wedge q$	$(p \wedge q) \longrightarrow p$
F			

Entonces, $p \wedge q$ es falsa, independientemente del valor de verdad que tenga q.

p	q	$p \wedge q$	$(p \wedge q) \longrightarrow p$
F		F	

Consecuentemente, el condicional $(p \wedge q) \longrightarrow p$ es verdad.

p	q	$p \wedge q$	$(p \wedge q) \longrightarrow p$
F		F	V

Al igual que antes, la proposición $(p \wedge q) \longrightarrow p$ es una tautología ya que todos los demás casos son verdad por definición del valor de verdad del condicional.

■

Ejemplo 1.14

Establecer si las siguientes proposiciones son tautologías, contingencias o contradicciones.

(a) $(p \longrightarrow q) \wedge (q \longrightarrow p)$

(b) $[p \wedge (q \vee r)] \longrightarrow [(p \wedge q) \vee (p \wedge r)]$

(c) $(p \vee \neg q) \longrightarrow q$

(d) $p \longrightarrow (p \vee q)$

(e) $(p \wedge q) \longrightarrow p$

(f) $[(p \wedge q) \longleftrightarrow p] \longrightarrow (p \longleftrightarrow q)$

(g) $[(p \longrightarrow q) \vee (r \longrightarrow s)] \longrightarrow [(p \wedge r) \longrightarrow (q \vee s)]$

Solución

Haremos, en todos los casos, una tabla de verdad.

(a) $(p \longrightarrow q) \wedge (q \longrightarrow p)$

p	q	$p \longrightarrow q$	$q \longrightarrow p$	$(p \longrightarrow q) \wedge (q \longrightarrow p)$
V	V	V	V	V
V	F	F	V	F
F	V	V	F	F
F	F	V	V	V

Luego es una *contingencia*.

(b) $[p \wedge (q \vee r)] \longrightarrow [(p \wedge q) \vee (p \wedge r)]$

Una proposición condicional sólo es falsa cuando la hipótesis es verdadera y la conclusión es falsa. Comprobaremos que esto no puede ocurrir.

- Veamos que si la hipótesis, $p \wedge (q \vee r)$, es verdad, la conclusión $(p \wedge q) \vee (p \wedge r)$ no puede ser falsa. En efecto, si la hipótesis, $p \wedge (q \vee r)$ es verdad, entonces p y $q \vee r$ serán, ambas, verdad y si $q \vee r$ es verdad, entonces una de las dos, al menos, q o r, ha de ser verdadera. Tenemos, pues, dos opciones:

  p es verdad y q es verdad. En tal caso, $p \wedge q$ será verdad y $(p \wedge q) \vee (p \wedge r)$ también, independientemente del valor de verdad que tenga r.

  o

  p es verdad y r es verdad. En este caso, será verdad $p \wedge r$ y, por lo tanto, también lo será $(p \wedge q) \vee (p \wedge r)$, independientemente del valor de verdad que tenga q.

  Una tabla de verdad que recoja, únicamente, estos casos sería:

p	q	r	$q \vee r$	$p \wedge (q \vee r)$	$p \wedge q$	$p \wedge r$	$(p \wedge q) \vee (p \wedge r)$	$[p \wedge (q \vee r)] \longrightarrow [(p \wedge q) \vee (p \wedge r)]$
V	V		V	V	V		V	V
V		V	V			V	V	V

– Ahora veremos que si la conclusión, $(p \wedge q) \vee (p \wedge r)$, es falsa, la hipótesis, $p \wedge (q \vee r)$, no puede ser verdadera.

En efecto, si $(p \wedge q) \vee (p \wedge r)$ es falsa, entonces por el valor de verdad de la disyunción (1.2.2), $p \wedge q$ será falsa y $p \wedge r$ también. Pues bien,

Si $p \wedge q$ es falsa, entonces por el valor de verdad de la conjunción (1.2.1), una de las dos proposiciones, p o q, al menos, ha de ser falsa.

– Si p es falsa, entonces la hipótesis, $p \wedge (q \vee r)$, es, por el valor de verdad de la conjunción, (1.2.1), falsa, independientemente de los valores de verdad que puedan tener q y r, por lo tanto hemos terminado.

– Si q es falsa, entonces como $p \wedge r$ es falsa, una de las dos proposiciones, p o r, al menos, ha de ser falsa.

– El caso en que p sea falsa ya lo hemos estudiado.

– Si r es falsa, entonces por el valor de verdad de la disyunción (1.2.2), $q \vee r$ será falsa y, por lo tanto, la hipótesis $p \wedge (q \vee r)$ será, por el valor de verdad de la conjunción (1.2.1), falsa, independientemente del valor de verdad de p.

Una *tabla de verdad abreviada* que recoge, únicamente, estos casos sería:

p	q	r	$q \vee r$	$p \wedge (q \vee r)$	$p \wedge q$	$p \wedge r$	$(p \wedge q) \vee (p \wedge r)$	$[p \wedge (q \vee r)] \longrightarrow [(p \wedge q) \vee (p \wedge r)]$
F				F	F	F	F	V
	F	F	F					V

La proposición será, por tanto, una *tautología*.

(c) $(p \vee \neg q) \longrightarrow q$

p	q	$\neg q$	$p \vee \neg q$	$(p \vee \neg q) \longrightarrow q$
V	V	F	V	V
V	F	V	V	F
F	V	F	F	V
F	F	V	V	F

luego la proposición es una *contingencia*.

(d) $p \longrightarrow (p \vee q)$

Un condicional es falso únicamente cuando la hipótesis es verdadera y la conclusión es falsa. Probaremos que esto no puede ocurrir, con lo cual quedará probado que la proposición es una tautología ya que en los demás casos será, por definición, verdadera.

– Veamos que si la hipótesis, p, es verdad, la conclusión, $p \vee q$ no puede ser falsa.

En efecto, si p es verdad, entonces, por el valor de verdad de la disyunción, $p \vee q$ será verdadera independientemente del valor de verdad de q.

– Ahora veremos que si la conclusión, $p \vee q$, es falsa, la hipótesis, p, no puede ser verdadera.

En efecto, si $p \vee q$ es falsa, entonces, por el valor de verdad de la disyunción, p y q serán, ambas, falsas.

una *tabla de verdad abreviada* será

p	$p \vee q$	$p \longrightarrow (p \vee q)$
V	V	V
F	F	V

y la proposición es una *tautología*.

(e) $(p \wedge q) \longrightarrow p$

Seguiremos un camino análogo al utilizado en el apartado anterior.

- Si la hipótesis, $p \wedge q$, es verdadera, la conclusión, p, no puede ser falsa.
  En efecto, si $p \wedge q$ es verdad, por el valor de verdad de la conjunción, p y q han de ser, ambas, verdaderas.
- Si la conclusión, p, es falsa, la hipótesis, $p \wedge q$ no puede ser verdadera.
  En efecto, si p es falsa, de nuevo por el valor de verdad de la conjunción, $p \wedge q$ es falsa.

La proposición es, por tanto, una tautología ya que el único caso posible de falsedad del condicional no puede darse.

Una *tabla de verdad abreviada* sería:

p	q	$p \wedge q$	$(p \wedge q) \longrightarrow p$
V	V	V	V
F		F	V

(f) $[(p \wedge q) \longleftrightarrow p] \longrightarrow (p \longleftrightarrow q)$.

Haremos una *tabla de verdad abreviada*. En efecto, $[(p \wedge q) \longleftrightarrow p] \longrightarrow (p \longleftrightarrow q)$ es falsa cuando $[(p \wedge q) \longleftrightarrow p]$ sea verdad y $(p \longleftrightarrow q)$ falsa. Pero ésta última es falsa cuando p y q tengan distintos valores de verdad.

p	q	$p \wedge q$	$(p \wedge q) \longleftrightarrow p$	$p \longleftrightarrow q$	$[(p \wedge q) \longleftrightarrow p] \longrightarrow (p \longleftrightarrow q)$
V	F	F	F	F	V
F	V	F	V	F	F

La proposición es, por tanto, una *contingencia*.

(g) $[(p \longrightarrow q) \vee (r \longrightarrow s)] \longrightarrow [(p \wedge r) \longrightarrow (q \vee s)]$

La proposición condicional únicamente es falsa cuando la hipótesis es verdad y la conclusión falsa. Veamos que es imposible que ocurra este caso.

- Si la hipótesis, $(p \longrightarrow q) \vee (r \longrightarrow s)$, es verdadera, la conclusión, $(p \wedge r) \longrightarrow (q \vee s)$, no puede ser falsa.
  Efectivamente, si $(p \longrightarrow q) \vee (r \longrightarrow s)$ es verdad, entonces, por el valor de verdad de la disyunción, uno de los dos condicionales, $p \longrightarrow q$ o $r \longrightarrow s$, al menos, ha de ser verdadero. Pues bien,
  - si $p \longrightarrow q$ es verdad, entonces p es falso o q es verdad.
    - Si p es falso, $p \wedge r$ también lo será y, por lo tanto, $(p \wedge r) \longrightarrow (q \vee s)$ será verdadera independientemente de los valores de verdad de r, q y s.
    - Si q es verdad, $q \vee s$ también será verdad y, consecuentemente, $(p \wedge r) \longrightarrow (q \vee s)$ será verdadera independientemente de los valores de verdad de p, r y s.
  - Si $r \longrightarrow s$ es verdad, entonces r es falso o s es verdad.
    - Si r es falso, $p \wedge r$ también lo será y, por lo tanto, $(p \wedge r) \longrightarrow (q \vee s)$ será verdadera independientemente de los valores de verdad de p, q y s.
    - Si s es verdad, $q \vee s$ también será verdad y, consecuentemente, $(p \wedge r) \longrightarrow (q \vee s)$ será verdadera independientemente de los valores de verdad de p, q y r.
- Si la conclusión, $(p \wedge r) \longrightarrow (q \vee s)$ es falsa, la hipótesis, $(p \longrightarrow q) \vee (r \longrightarrow s)$, no puede ser verdadera.
  En efecto, si la conclusión, $[(p \wedge r) \longrightarrow (q \vee s)]$ es falsa, entonces $(p \wedge r)$ es verdad y $(q \vee s)$ es falsa de donde se sigue que p y r son, ambas, verdad y q y s son, ambas, falsas. Por lo tanto, por el valor de verdad del condicional, (1.2.6), $p \longrightarrow q$ es falsa y $r \longrightarrow s$, también, de aquí que la disyunción de las dos, $(p \longrightarrow q) \vee (r \longrightarrow s)$, sea falsa.

Haremos una tabla de verdad que recoja únicamente estos casos.

p	q	r	s	$(p \longrightarrow q)$	$(r \longrightarrow s)$	$(p \wedge r)$	$(q \vee s)$
V	F	V	F	F	F	V	F
F				V		F	
	V						V
		F			V	F	
			V				V

$(p \longrightarrow q) \vee (r \longrightarrow s)$	$(p \wedge r) \longrightarrow (q \vee s)$
F	F
V	V
V	V
V	V
V	V

$[(p \longrightarrow q) \vee (r \longrightarrow s)] \longrightarrow [(p \wedge r) \longrightarrow (q \vee s)]$
V
V
V
V
V

■

1.3 Implicación

Estudiamos en este apartado la implicación lógica entre dos proposiciones.

1.3.1 Implicación lógica

Sean P y Q dos proposiciones cualesquiera. Diremos que P implica lógicamente Q, y escribiremos $P \Longrightarrow Q$, si Q es verdad cuando P lo sea.

Es por esto que suele decirse que P implica lógicamente Q si la veracidad de la conclusión se deduce o se infiere de la veracidad de la hipótesis.

■

Ejemplo 1.15

Probar que la proposición $p \wedge (p \longrightarrow q)$ implica lógicamente la proposición q, probando que la veracidad de q se sigue de la veracidad de $p \wedge (p \longrightarrow q)$.

Solución

En efecto, si $p \wedge (p \longrightarrow q)$ es verdad, entonces por el valor de verdad de la conjunción, (1.2.1), p y $p \longrightarrow q$ son, ambas, verdaderas, de aquí que por el valor de verdad del condicional, (1.2.6), q tenga que ser verdadera y, consecuentemente,

$$[p \wedge (p \longrightarrow q)] \Longrightarrow q$$

■

Ejemplo 1.16

Dadas las proposiciones p y q, demostrar que la negación de p ó q implica lógicamente la negación de p.

Solución

Veamos que $\neg(p \vee q) \Longrightarrow \neg p$.

En efecto, si $\neg(p \vee q)$ es verdad, entonces $p \vee q$ es falso y, por el valor de verdad de la disyunción, esto significa que p y q son, ambas, falsas. Pues bien, si p es falsa, su negación $\neg p$ será verdadera y según la definición (1.3.1) hay implicación lógica terminando la demostración.

■

Nota 1.7 Ahora podremos entender algo mejor lo que comentábamos en 1. de la nota 1.4. En efecto, de que "García Lorca fue un poeta" sea verdad no puede deducirse que Gauss fuera matemático, aunque lo fue y muy bueno.

De todas formas, es cierto que existe una semejanza entre el símbolo $\Longrightarrow$ para la implicación lógica y el símbolo $\longrightarrow$ para la proposición condicional. Esta semejanza es intencionada y debido a la manera en que se usa el término *implica*, en el lenguaje ordinario es natural leer $p \longrightarrow q$ como *"p implica q"*.

■

1.3.2 Implicaciones lógicas más comunes

La tabla siguiente presenta algunas implicaciones lógicas con los nombres que usualmente reciben.

Adición	$P \Longrightarrow (P \vee Q)$
Ley del Modus Ponendo Ponens (Modus Ponens)	$[(P \longrightarrow Q) \wedge P] \Longrightarrow Q$
Ley del Modus Tollendo Tollens (Modus Tollens)	$[(P \longrightarrow Q) \wedge \neg Q] \Longrightarrow \neg P$
Leyes de los Silogismos Hipotéticos	$[(P \longrightarrow Q) \wedge (Q \longrightarrow R)] \Longrightarrow (P \longrightarrow R)$ $[(P \longleftrightarrow Q) \wedge (Q \longleftrightarrow R)] \Longrightarrow (P \longleftrightarrow R)$
Leyes de los silogismos disyuntivos	$[\neg P \wedge (P \vee Q)] \Longrightarrow Q$ $[P \wedge (\neg P \vee \neg Q)] \Longrightarrow \neg Q$
Ley del Dilema Constructivo	$[(P \longrightarrow Q) \wedge (R \longrightarrow S) \wedge (P \vee R)] \Longrightarrow (Q \vee S)$
Contradicción	$(P \longrightarrow C) \Longrightarrow \neg P$

■

Ejemplo 1.17

Verificar la ley del Modus Tollendo Tollens, $[(P \longrightarrow Q) \wedge \neg Q] \Longrightarrow \neg P$.

Solución

En efecto, si $(P \longrightarrow Q) \wedge \neg Q$ es verdad, entonces $P \longrightarrow Q$ es verdad y $\neg Q$ es, también, verdad. Así pues, $P \longrightarrow Q$ es verdad y Q es falso, de aquí que por el valor de verdad del condicional, P tiene que ser falso y, consecuentemente, $\neg P$ es verdad. Por lo tanto, hemos llegado a que $\neg P$ es verdad partiendo de que $(P \longrightarrow Q) \wedge \neg Q$ es verdad, es decir,

$$[(P \longrightarrow Q) \wedge \neg Q] \Longrightarrow \neg P$$

y se verifica la ley del Modus Tollendo Tollens.

■

Ejemplo 1.18

Verificar las leyes de los silogismos hipotéticos.

(a) $(P \longrightarrow Q) \wedge (Q \longrightarrow R) \Longrightarrow (P \longrightarrow R)$

(b) $(P \longleftrightarrow Q) \wedge (Q \longleftrightarrow R) \Longrightarrow (P \longleftrightarrow R)$

Solución

(a) $(P \longrightarrow Q) \wedge (Q \longrightarrow R) \Longrightarrow (P \longrightarrow R)$

En efecto, si $(P \longrightarrow Q) \wedge (Q \longrightarrow R)$ es verdad, entonces por el valor de verdad de la conjunción (1.2.1), $P \longrightarrow Q$ es verdad y $Q \longrightarrow R$ también. Por el valor de verdad del condicional, (1.2.6), si $P \longrightarrow Q$ es verdad, entonces P es falsa o Q verdadera. Tendremos, pues, dos opciones:

- P es falsa y $Q \longrightarrow R$ es verdadera. En este caso, la conclusión, $P \longrightarrow R$, será verdadera independientemente de los valores de verdad de Q y R.
- Q es verdad y $Q \longrightarrow R$ es verdadera. En tal caso, por el valor de verdad del condicional, (1.2.6), R ha de ser verdadera y la conclusión $P \longrightarrow R$, será verdadera independientemente del valor de verdad que tenga P.

En todo caso la veracidad de la conclusión, $P \longrightarrow R$, se sigue de la veracidad de la hipótesis, $(P \longrightarrow Q) \wedge (Q \longrightarrow R)$, y por lo tanto,

$$(P \longrightarrow Q) \wedge (Q \longrightarrow R) \Longrightarrow (P \longrightarrow R)$$

(b) $(P \longleftrightarrow Q) \wedge (Q \longleftrightarrow R) \Longrightarrow (P \longleftrightarrow R)$

En efecto, si $(P \longleftrightarrow Q) \wedge (Q \longleftrightarrow R)$ es verdad, entonces $(P \longleftrightarrow Q)$ es verdad y $(Q \longleftrightarrow R)$ también. Pues bien, si $(P \longleftrightarrow Q)$ es verdad, entonces ambas proposiciones, P y Q, han de tener el mismo valor de verdad y como $(Q \longleftrightarrow R)$ es verdad, R ha de tener el mismo valor de verdad que Q, por lo tanto P y R tienen, ambas, los mismos valores de verdad y, consecuentemente, $(P \longleftrightarrow R)$ es verdad.

Como la veracidad de la conclusión, $(P \longleftrightarrow R)$, se sigue de la veracidad de la hipótesis, $(P \longleftrightarrow Q) \wedge (Q \longleftrightarrow R)$, tendremos que

$$(P \longleftrightarrow Q) \wedge (Q \longleftrightarrow R) \Longrightarrow (P \longleftrightarrow R)$$

■

Ejemplo 1.19

Obtener los valores de verdad de las proposiciones P y R que verifican el silogismo hipotético

$$(P \longrightarrow Q) \wedge (Q \longrightarrow R) \Longrightarrow (P \longrightarrow R)$$

en los casos en que

(a) Q sea verdadera.

(b) Q sea falsa.

Solución

Como ya sabemos para que se verifique la implicación lógica, la veracidad de la conclusión, $P \longrightarrow R$, ha de seguirse de la veracidad de la hipótesis, $(P \longrightarrow Q) \wedge (Q \longrightarrow R)$ y ésta es verdadera si los dos condicionales, $P \longrightarrow Q$ y $Q \longrightarrow R$ lo son.

(a) Q es verdadera. En este caso, al ser $Q \longrightarrow R$ verdadera, la proposición R no puede ser falsa, luego ha de ser verdadera y, consecuentemente, la conclusión $P \longrightarrow R$ es verdad independientemente del valor de verdad que tenga P.

Por lo tanto, R tiene que ser verdad y P puede tener cualquier valor de verdad.

(b) Q es falsa. La veracidad de $P \longrightarrow Q$ obliga a que P sea falsa y, en tal caso, $P \longrightarrow R$ es verdad, independientemente del valor de verdad que tenga R.

Por lo tanto, P tiene que ser falsa y el valor de verdad de R es indiferente.

■

Ejemplo 1.20

Verificar la Ley del Dilema Constructivo, $[(P \longrightarrow Q) \wedge (R \longrightarrow S) \wedge (P \vee R)] \Longrightarrow (Q \vee S)$.

Solución

En efecto, si la hipótesis $(P \longrightarrow Q) \wedge (R \longrightarrow S) \wedge (P \vee R)$ es verdad, entonces por el valor de verdad de la conjunción, (1.2.1), las tres proposiciones, $P \longrightarrow Q$, $R \longrightarrow S$ y $P \vee R$ han de ser verdad. Pues bien, si $P \vee R$ es verdad, una de las dos proposiciones, P ó R, al menos, ha de ser verdad.

- Si P es verdad, como $P \longrightarrow Q$ es verdad, Q tiene que ser verdad y, consecuentemente, $Q \vee S$ será verdadera independientemente del valor de verdad que tenga S.
- Si R es verdad, como $R \longrightarrow S$ es verdad, S tendrá que ser verdad y, por lo tanto, $Q \vee S$ es verdad independientemente del valor de verdad de Q.

En cualquier caso la veracidad de la conclusión, $Q \vee S$, se sigue de la veracidad de la hipótesis, $(P \longrightarrow Q) \wedge (R \longrightarrow S) \wedge (P \vee R)$, y, por lo tanto, se verifica la implicación lógica.

■

1.4 Equivalencia Lógica

1.4.1 Proposiciones lógicamente equivalentes

Sean P y Q dos proposiciones compuestas cualesquiera. Diremos que las proposiciones P y Q son lógicamente equivalentes, y se escribe $P \iff Q$, cuando se verifica al mismo tiempo que P implica lógicamente Q, $P \Longrightarrow Q$, y Q implica lógicamente P, $Q \Longrightarrow P$.

■

1.4.2 Implicación lógica y Condicional

La proposición P implica lógicamente la proposición Q si, y sólo si la proposición condicional $P \longrightarrow Q$ es una tautología.

Demostración

Probaremos la equivalencia,

$$(P \Longrightarrow Q) \iff (P \longrightarrow Q \text{ es una tautología})$$

(i) $(P \Longrightarrow Q) \Longrightarrow (P \longrightarrow Q$ es una tautología).

Supongamos que $P \Longrightarrow Q$ y comprobemos que, en tal caso, el condicional $P \longrightarrow Q$ no puede ser falso. La única posibilidad de que el condicional $P \longrightarrow Q$ sea falso es que P sea verdadera y Q sea falsa. Veremos que eso no puede ocurrir.

- Si P es verdad, Q no puede ser falsa.

  En efecto, si P es verdadera, como $P \Longrightarrow Q$, Q ha de ser verdadera.

- Si Q es falsa, P no puede ser verdad.

  En efecto, si Q es falsa, entonces P tiene que ser, también, falsa, ya que si P fuera verdadera, como $P \Longrightarrow Q$, Q sería verdadera.

Hemos visto, pues, que en ningún caso puede ocurrir que P sea verdad y Q falso, luego $P \longrightarrow Q$ es siempre verdadero, es decir es una tautología.

(ii) $(P \longrightarrow Q$ es una tautología$) \Longrightarrow (P \Longrightarrow Q)$.

Supongamos ahora que $P \longrightarrow Q$ es una tautología y comprobemos que, en tal caso, Q es verdad cuando P lo sea, es decir, $P \Longrightarrow Q$. En efecto, si P es verdad, como $P \longrightarrow Q$ es verdad, Q ha de ser verdad, por lo tanto, $P \Longrightarrow Q$.

■

El teorema anterior caracteriza las implicaciones lógicas y aporta un nuevo método para comprobar si una proposición implica lógicamente otra.

Ejemplo 1.21

Probar que la proposición $p \wedge (p \longrightarrow q)$ implica lógicamente la proposición q.

Solución

Veamos que la proposición condicional $[p \wedge (p \longrightarrow q)] \longrightarrow q$ es una tautología. En efecto, haciendo una tabla de verdad,

p	q	$p \longrightarrow q$	$p \wedge (p \longrightarrow q)$	$[p \wedge (p \longrightarrow q)] \longrightarrow q$
V	V	V	V	V
V	F	F	F	V
F	V	V	F	V
F	F	V	F	V

y, por por el teorema anterior, $p \wedge (p \longrightarrow q) \Longrightarrow q$.

■

Ejemplo 1.22

Verificar las leyes de los silogismos hipotéticos.

(a) $(P \longrightarrow Q) \wedge (Q \longrightarrow R) \Longrightarrow (P \longrightarrow R)$

(b) $(P \longleftrightarrow Q) \wedge (Q \longleftrightarrow R) \Longrightarrow (P \longleftrightarrow R)$

Solución

(a) Probaremos que el condicional,

$$(P \longrightarrow Q) \wedge (Q \longrightarrow R) \longrightarrow (P \longrightarrow R)$$

nunca puede ser falso para lo cual veremos que la única opción de falsedad de un condicional (hipótesis verdadera y conclusión falsa) no puede darse.

- Si la hipótesis es verdad, entonces la conclusión no puede ser falsa.
  En efecto, según hemos probado en el ejemplo 1.18 , si $(P \longrightarrow Q) \wedge (Q \longrightarrow R)$ es verdad, $(P \longrightarrow R)$ era, también, verdadera.
- Si la conclusión es falsa, entonces la hipótesis no puede ser verdadera.
  En efecto, si $(P \longrightarrow R)$ es falsa, entonces P ha de ser verdadera y R falsa. Ahora el valor de verdad de la hipótesis dependerá del que tenga Q, habrá, pues, dos opciones:
  - ⊛ Q es verdad. En este caso, $P \longrightarrow Q$ es verdad, $Q \longrightarrow R$ falso y, consecuentemente,
    $$(P \longrightarrow Q) \wedge (Q \longrightarrow R)$$
    es falso.
  - ⊛ Q es falso. En tal caso, $P \longrightarrow Q$ es falso, $Q \longrightarrow R$ verdad y, consecuentemente,
    $$(P \longrightarrow Q) \wedge (Q \longrightarrow R)$$
    es falso.

La siguiente tabla recoge estos casos.

P	Q	R	$P \longrightarrow Q$	$Q \longrightarrow R$	$(P \longrightarrow Q) \wedge (Q \longrightarrow R)$	$P \longrightarrow R$
V	V	F	V	F	F	F
V	F	F	F	V	F	F

$(P \longrightarrow Q) \wedge (Q \longrightarrow R) \longrightarrow (P \longrightarrow R)$
V
V

El condicional $(P \longrightarrow Q) \wedge (Q \longrightarrow R) \longrightarrow (P \longrightarrow R)$ es, por tanto, una tautología y por 1.4.2, se verifica la implicación lógica.

(b) $[(P \longleftrightarrow Q) \wedge (Q \longleftrightarrow R)] \Longrightarrow (P \longleftrightarrow R)$

Veamos, al igual que antes, que el condicional

$$[(P \longleftrightarrow Q) \wedge (Q \longleftrightarrow R)] \longrightarrow (P \longleftrightarrow R)$$

es una tautología probando que es imposible que sea falso.

- Si la hipótesis es verdadera, entonces la conclusión no puede ser falsa.

  En efecto, si $(P \longleftrightarrow Q) \wedge (Q \longleftrightarrow R)$ es verdad, entonces, según vimos en el ejemplo 1.18 , $P \longleftrightarrow R$, también lo es.

- Si la conclusión es falsa, entonces la hipótesis no puede ser verdadera.

  En efecto, si $(P \longleftrightarrow R)$ es falsa, entonces P y R han de tener valores de verdad distintos, con lo cual el valor de verdad de la hipótesis, $(P \longleftrightarrow Q) \wedge (Q \longleftrightarrow R)$ dependerá del valor de verdad que tenga Q. Habrá, pues, dos opciones:

  - Q tiene el mismo valor de verdad que P. En tal caso, $P \longleftrightarrow Q$ será verdad, R tendrá un valor de verdad distinto al de Q y, consecuentemente, $Q \longleftrightarrow R$ será falso. Por lo tanto, $(P \longleftrightarrow Q) \wedge (Q \longleftrightarrow R)$, es falsa.
  - Q tiene el mismo valor de verdad que R. En este caso, $Q \longleftrightarrow R$ es verdad, P tendrá un valor de verdad distinto al de Q y, consecuentemente, $P \longleftrightarrow Q$ será falso. Por lo tanto, $(P \longleftrightarrow Q) \wedge (Q \longleftrightarrow R)$, es falsa.

La siguiente tabla de verdad recoge estos casos.

P	Q	R	$P \longleftrightarrow Q$	$Q \longleftrightarrow R$	$(P \longleftrightarrow Q) \wedge (Q \longleftrightarrow R)$	$P \longleftrightarrow R$
V	V	V	V	V	V	V
F	F	F	V	V	V	V
V	V	F	V	F	F	F
V	F	F	F	V	F	F
F	V	V	F	V	F	F
F	F	V	V	F	F	F

$(P \longleftrightarrow Q) \wedge (Q \longleftrightarrow R) \longrightarrow (P \longleftrightarrow R)$
V
V
V
V
V
V

■

Ejemplo 1.23

Verificar la Ley del Dilema Constructivo, $[(P \longrightarrow Q) \wedge (R \longrightarrow S) \wedge (P \vee R)] \Longrightarrow (Q \vee S)$.

Solución

Probaremos ahora que $[(P \longrightarrow Q) \wedge (R \longrightarrow S) \wedge (P \vee R)] \longrightarrow (Q \vee S)$ es una tautología. La única posibilidad de que un condicional sea falso es que siendo verdad la hipótesis, la conclusión sea falsa. Veamos que esta posibilidad no puede darse.

- Si la hipótesis es verdadera, entonces la conclusión no puede ser falsa.

  En efecto, si la hipótesis, $[(P \longrightarrow Q) \wedge (R \longrightarrow S) \wedge (P \vee R)]$, es verdadera, entonces según vimos en el ejemplo 1.20 , la conclusión, $Q \vee S$, también lo es.

- Si la conclusión es falsa, entonces la hipótesis no puede ser verdadera.

  En efecto, si $Q \vee S$ es falsa, entonces Q y S han de ser, ambas, falsas. Veamos como es la hipótesis.

  - Si $P \vee R$ es falsa, entonces por el valor de verdad de la conjunción, (1.2.1), la hipótesis, $(P \longrightarrow Q) \wedge (R \longrightarrow S) \wedge (P \vee R)$, será falsa.
  - Si $P \vee R$ es verdadera, entonces por el valor de verdad de la disyunción, (1.2.2), una de las dos, P o R, al menos, ha de ser verdad. Tendremos, pues, dos opciones:
    - P es verdad. En tal caso, como Q es falsa, el condicional $P \longrightarrow Q$ también lo será y, consecuentemente, la hipótesis será falsa.
    - R es verdad. En este caso y razonando de forma análoga, el condicional $R \longrightarrow S$ será falso, con lo que la hipótesis será, también, falsa.

Una tabla que recoge este caso sería:

P	Q	R	S	$P \longrightarrow Q$	$R \longrightarrow S$	$P \vee R$	$Q \vee S$
	F		F			F	F
V	F		F	F		V	F
	F	V	F		F	V	F

$(P \longrightarrow Q) \wedge (R \longrightarrow S) \wedge (P \vee R)$
F
F
F

$[(P \longrightarrow Q) \wedge (R \longrightarrow S) \wedge (P \vee R)] \longrightarrow (Q \vee S)$
V
V
V

Por lo tanto,

$$[(P \longrightarrow Q) \wedge (R \longrightarrow S) \wedge (P \vee R)] \longrightarrow (Q \vee S)$$

es una tautología y, consecuentemente,

$$[(P \longrightarrow Q) \wedge (R \longrightarrow S) \wedge (P \vee R)] \Longrightarrow (Q \vee S)$$

verificándose, en consecuencia, la ley del dilema constructivo.

■

1.4.3 Equivalencia lógica y Bicondicional

Dos proposiciones son lógicamente equivalentes si el bicondicional entre ellas es una tautología.

Demostración

En efecto, sean P y Q proposiciones cualesquiera tales que $P \Longleftrightarrow Q$.

Entonces, $P \Longrightarrow Q$ y $Q \Longrightarrow P$ y por 1.4.2, tendremos que $P \longrightarrow Q$ y $Q \longrightarrow P$ son, ambas, tautologías y, consecuentemente, $P \longleftrightarrow Q$ también lo será.

■

1.4.4 Equivalencias lógicas más comunes

La tabla siguiente presenta algunas equivalencias lógicas con los nombres que usualmente reciben.

Idempotencia de la conjunción y la disyunción	$(P \wedge P) \Longleftrightarrow P$ $(P \vee P) \Longleftrightarrow P$
Conmutatividad de la conjunción y la disyunción	$(P \wedge Q) \Longleftrightarrow (Q \wedge P)$ $(P \vee Q) \Longleftrightarrow (Q \vee P)$
Asociatividad de la conjunción y la disyunción	$(P \wedge Q) \wedge R \Longleftrightarrow P \wedge (Q \wedge R)$ $(P \vee Q) \vee R \Longleftrightarrow P \vee (Q \vee R)$
Distributividad de la conjunción respecto de la disyunción	$[P \wedge (Q \vee R)] \Longleftrightarrow [(P \wedge Q) \vee (P \wedge R)]$
Distributividad de la disyunción respecto de la conjunción	$[P \vee (Q \wedge R)] \Longleftrightarrow [(P \vee Q) \wedge (P \vee R)]$
Leyes de De Morgan	$\neg (P \vee Q) \Longleftrightarrow \neg P \wedge \neg Q$ $\neg (P \wedge Q) \Longleftrightarrow \neg P \vee \neg Q$
Leyes de Dominación	$P \vee T \Longleftrightarrow T$ $P \wedge C \Longleftrightarrow C$
Leyes de Identidad	$P \wedge T \Longleftrightarrow P$ $P \vee C \Longleftrightarrow P$
Doble Negación	$\neg\neg P \Longleftrightarrow P$
Implicación	$(P \longrightarrow Q) \Longleftrightarrow (\neg P \vee Q)$
Exportación	$[P \longrightarrow (Q \longrightarrow R)] \Longleftrightarrow [(P \wedge Q) \longrightarrow R]$
Contrarrecíproca	$(P \longrightarrow Q) \Longleftrightarrow (\neg Q \longrightarrow \neg P)$
Reducción al absurdo	$(P \longrightarrow Q) \Longleftrightarrow [(P \wedge \neg Q) \longrightarrow C]$

■

Ejemplo 1.24

Probar las leyes de De Morgan.

(a) $\neg(P \vee Q) \iff (\neg P \wedge \neg Q)$

(b) $\neg(P \wedge Q) \iff (\neg P \vee \neg Q)$

Solución

Sean P y Q dos proposiciones cualesquiera.

(a) $\neg(P \vee Q) \iff (\neg P \wedge \neg Q)$.

1. Veamos que $\neg(P \vee Q) \Longrightarrow (\neg P \wedge \neg Q)$.
   En efecto, si $\neg(P \vee Q)$ es verdad, entonces por 1.2.4, $P \vee Q$ es falso, luego por 1.2.2, P y Q serán, ambas, falsas, de aquí que, de nuevo por 1.2.4, $\neg P$ y $\neg Q$ sean, las dos, verdaderas y, consecuentemente, $\neg P \wedge \neg Q$ es verdad (por 1.2.1).
   Como la veracidad de la conclusión, $\neg P \wedge \neg Q$, se ha seguido de la veracidad de la hipótesis, $\neg(P \vee Q)$, de acuerdo con la definición de implicación lógica (1.4.4), tendremos que
   $$\neg(P \vee Q) \Longrightarrow (\neg P \wedge \neg Q)$$
2. Recíprocamente, probemos ahora que $(\neg P \wedge \neg Q) \Longrightarrow \neg(P \vee Q)$.
   En efecto, si $\neg P \wedge \neg Q$ es verdad, entonces por 1.2.1 las dos proposiciones, $\neg P$ y $\neg Q$, han de ser verdad luego, por 1.2.4, P y Q tienen de ser, ambas, falsas y por 1.2.2 $P \vee Q$ es falsa y, consecuentemente, $\neg(P \vee Q)$ es verdad.
   Como la veracidad de la conclusión, $\neg(P \vee Q)$, se ha seguido de la veracidad de la hipótesis, $\neg P \wedge \neg Q$, de acuerdo con la definición de implicación lógica (1.4.4), tendremos que
   $$(\neg P \wedge \neg Q) \Longrightarrow \neg(P \vee Q)$$

De 1. y 2. se sigue que
$$\neg(P \vee Q) \iff (\neg P \wedge \neg Q)$$

Veremos ahora que se verifica la equivalencia lógica comprobando que el bicondicional
$$\neg(P \vee Q) \longleftrightarrow (\neg P \wedge \neg Q)$$
es una tautología.

1. El condicional,
   $$\neg(P \vee Q) \longrightarrow (\neg P \wedge \neg Q)$$
   es una tautología.
   Veamos que es imposible que sea falso.
   - Si la hipótesis es verdadera, entonces la conclusión no puede ser falsa.
     En efecto, si $\neg(P \vee Q)$ es verdad, entonces $P \vee Q$ es falsa, luego P y Q son, ambas, falsas, de aquí que $\neg P$ y $\neg Q$ sean, ambas, verdaderas y, consecuentemente, $\neg P \wedge \neg Q$ sea verdadera.
   - Si la conclusión es falsa, entonces la hipótesis no puede ser verdadera.
     En efecto, si $\neg P \wedge \neg Q$ es falsa, entonces una de las dos proposiciones, $\neg P$ o $\neg Q$, al menos, ha de ser falsa, con lo que una de las dos proposiciones P o Q, al menos, ha de ser verdadera y, por lo tanto, $P \vee Q$ es verdad siendo su negación, $\neg(P \vee Q)$, falsa.

2. El condicional,
$$(\neg P \wedge \neg Q) \longrightarrow \neg (P \vee Q)$$
también es una tautología.
Veamos que es imposible que sea falso.
   - Si la hipótesis es verdadera, entonces la conclusión no puede ser falsa.
   En efecto, si $\neg P \wedge \neg Q$ es verdad, entonces $\neg P$ y $\neg Q$ han de ser, ambas, verdaderas y, por lo tanto, sus negaciones P y Q serán, ambas, falsas, de aquí que $P \vee Q$ sea falsa y, consecuentemente, $\neg (P \vee Q)$ sea verdadera.
   - Si la conclusión es falsa, entonces la hipótesis no puede ser verdadera.
   En efecto, si $\neg (P \vee Q)$ es falsa, entonces $P \vee Q$ es verdad y, por lo tanto, una de las dos proposiciones, P o Q, al menos, ha de ser verdadera, luego una de las dos proposiciones, $\neg P$ o $\neg Q$, al menos, ha de ser falsa y, consecuentemente, su conjunción $\neg P \wedge \neg Q$ será falsa.

Ahora bastaría tener en cuenta 1., 2. y lo dicho en 1.4.3 para concluir que
$$\neg (P \vee Q) \Longleftrightarrow (\neg P \wedge \neg Q)$$

Probaremos ahora lo mismo haciendo una tabla de verdad para comprobar que el bicondicional,
$$\neg (P \vee Q) \longleftrightarrow (\neg P \wedge \neg Q)$$
es una tautología. En efecto,

P	Q	$P \vee Q$	$\neg (P \vee Q)$	$\neg P$	$\neg Q$	$\neg P \wedge \neg Q$	$\neg (P \vee Q) \longleftrightarrow (\neg P \wedge \neg Q)$
V	V	V	F	F	F	F	V
V	F	V	F	F	V	F	V
F	V	V	F	V	F	F	V
F	F	F	V	V	V	V	V

(c) $\neg (P \wedge Q) \Longleftrightarrow (\neg P \vee \neg Q)$

1. Veamos que $\neg (P \wedge Q) \Longrightarrow (\neg P \vee \neg Q)$.
   En efecto, si $\neg (P \wedge Q)$ es verdad, entonces por 1.2.4, $P \wedge Q$ es falso, luego por 1.2.2, una de las dos proposiciones, P o Q, al menos, ha de ser falsa, de aquí que, de nuevo por 1.2.4, una de las dos, $\neg P$ o $\neg Q$, ha de ser verdad y, consecuentemente, $\neg P \vee \neg Q$ es verdadera (por 1.2.2).
   Como la veracidad de la conclusión, $\neg P \vee \neg Q$, se ha seguido de la veracidad de la hipótesis, $\neg (P \wedge Q)$, de acuerdo con la definición de implicación lógica (1.4.4), tendremos que
$$\neg (P \wedge Q) \Longrightarrow (\neg P \vee \neg Q)$$

2. Recíprocamente, probemos ahora que $(\neg P \vee \neg Q) \Longrightarrow \neg (P \wedge Q)$.
   En efecto, si $\neg P \vee \neg Q$ es verdad, entonces por 1.2.2 una, al menos, de las dos proposiciones, $\neg P$ o $\neg Q$, han de ser verdad luego, por 1.2.4, al menos una de las dos, P o Q tiene que ser falsa y por 1.2.1 $P \wedge Q$ es falsa y, consecuentemente, $\neg (P \wedge Q)$ es verdad.
   Como la veracidad de la conclusión, $\neg (P \wedge Q)$, se ha seguido de la veracidad de la hipótesis, $\neg P \vee \neg Q$, de acuerdo con la definición de implicación lógica (1.4.4), tendremos que
$$(\neg P \vee \neg Q) \Longrightarrow \neg (P \wedge Q)$$

De 1. y 2. se sigue que
$$\neg (P \wedge Q) \Longleftrightarrow (\neg P \vee \neg Q)$$

Ahora veremos que se verifica la equivalencia lógica, comprobando que el bicondicional $\neg (P \wedge Q) \longleftrightarrow (\neg P \vee \neg Q)$ es una tautología.

1. El condicional $\neg(P \wedge Q) \longrightarrow (\neg P \vee \neg Q)$ es una tautología.
   Lo probaremos viendo que es imposible que sea falso.
   - Si la hipótesis es verdad, entonces la conclusión no puede ser falsa.
     En efecto, si $\neg(P \wedge Q)$ es verdad, entonces $P \wedge Q$ es falsa, luego una de las dos proposiciones, P o Q, al menos, ha de ser falsa y, por lo tanto, una de las dos negaciones, $\neg P$ o $\neg Q$, al menos, ha de ser verdadera y, consecuentemente, $\neg P \vee \neg Q$ es verdad.
   - Si la conclusión es falsa, entonces la hipótesis no puede ser verdadera.
     En efecto, si $\neg P \vee \neg Q$ es falsa, entonces tanto $\neg P$ como $\neg Q$ han de ser falsas, luego P y Q han de ser, ambas, verdaderas y, por lo tanto, $P \wedge Q$ es verdad, siendo su negación, $\neg(P \wedge Q)$, verdadera.
2. El condicional $(\neg P \vee \neg Q) \longrightarrow \neg(P \wedge Q)$ es una tautología.
   Al igual que antes veremos que es imposible que este condicional sea falso.
   - Si la hipótesis es verdadera, entonces la conclusión no puede ser falsa.
     En efecto, si $\neg P \vee \neg Q$ es verdadera, entonces una de las dos proposiciones, $\neg P$ o $\neg Q$, al menos, ha de ser verdad, con lo cual sus P o Q, una de la dos, al menos, ha de ser falsa. Por lo tanto, $P \wedge Q$ es falsa y, consecuentemente, su negación, $\neg(P \wedge Q)$, es verdadera.
   - Si la conclusión es falsa, entonces la hipótesis no puede ser verdadera.
     En efecto, si $\neg(P \wedge Q)$ es falsa, entonces $P \wedge Q$ es verdadera, luego P y Q han de ser, ambas, verdaderas, sus negaciones $\neg P$ y $\neg Q$, falsas y, consecuentemente, su disyunción, $\neg P \vee \neg Q$, será falsa.

Ahora bastaría tener en cuenta 1., 2. y lo dicho en 1.4.3 para concluir que

$$\neg(P \wedge Q) \Longleftrightarrow (\neg P \vee \neg Q)$$

Probaremos ahora lo mismo haciendo una tabla de verdad para comprobar que el bicondicional,

$$\neg(P \wedge Q) \longleftrightarrow (\neg P \vee \neg Q)$$

es una tautología. En efecto,

P	Q	$P \wedge Q$	$\neg(P \wedge Q)$	$\neg P$	$\neg Q$	$\neg P \vee \neg Q$	$\neg(P \wedge Q) \longleftrightarrow (\neg P \vee \neg Q)$
V	V	V	F	F	F	F	V
V	F	F	V	F	V	V	V
F	V	F	V	V	F	V	V
F	F	F	V	V	V	V	V

Ahora bastaría tener en cuenta lo dicho en 1.4.3 para concluir que

$$\neg(P \wedge Q) \Longleftrightarrow (\neg P \vee \neg Q)$$

■

Ejemplo 1.25

Probar la equivalencia lógica conocida como contrarrecíproca.

Solución

Sean P y Q dos proposiciones compuestas cualesquiera. Probaremos que $(P \longrightarrow Q) \Longleftrightarrow (\neg Q \longrightarrow \neg P)$.

$(P \longrightarrow Q) \Longrightarrow (\neg Q \longrightarrow \neg P)$. Como ya sabemos podemos hacerlo de dos formas:

⊛ Partiendo de la veracidad de $P \longrightarrow Q$, llegar a la veracidad de $\neg Q \longrightarrow \neg P$. En efecto, si $P \longrightarrow Q$ es verdad, entonces por el valor de verdad del condicional, pueden ocurrir dos cosas:

La hipótesis, P, es falsa, en cuyo caso $\neg P$ será verdadera y, consecuentemente, $\neg Q \longrightarrow \neg P$ será verdadera,

o

la conclusión, Q, es verdadera. En este caso, su negación, $\neg Q$, será falsa y, por lo tanto, $\neg Q \longrightarrow \neg P$ será verdadera.

Por lo tanto,

$$(P \longrightarrow Q) \Longrightarrow (\neg Q \longrightarrow \neg P)$$

⊛ Comprobando que el condicional $(P \longrightarrow Q) \longrightarrow (\neg Q \longrightarrow \neg P)$ es una tautología. Como ya sabemos la única posibilidad de que un condicional sea falso es que sea verdad la hipótesis y la conclusión falsa. Veamos que esta situación no es posible. Si partimos de que la hipótesis, $P \longrightarrow Q$, es verdad el camino sería idéntico al anterior, así que partiremos de la falsedad de la conclusión, $\neg Q \longrightarrow \neg P$.

En efecto, si $\neg Q \longrightarrow \neg P$ es falsa, entonces $\neg Q$ es verdad y $\neg P$ es falsa, luego P es verdad, Q falsa y, consecuentemente, $P \longrightarrow Q$ es falsa y, por tanto, $(P \longrightarrow Q) \longrightarrow (\neg Q \longrightarrow \neg P)$ es, siempre, verdad. También podemos hacer una tabla de verdad abreviada:

P	Q	$P \longrightarrow Q$	$\neg Q$	$\neg P$	$\neg Q \longrightarrow \neg P$	$(P \longrightarrow Q) \longrightarrow (\neg Q \longrightarrow \neg P)$
V	F	F	V	F	F	V

$(\neg Q \longrightarrow \neg P) \Longrightarrow (P \longrightarrow Q)$. Al igual que la implicación anterior, podemos hacerlo de dos formas.

⊛ Partiendo de que $\neg Q \longrightarrow \neg P$ es verdad y llegar a que $P \longrightarrow Q$ también lo es. En efecto, la veracidad de $\neg Q \longrightarrow \neg P$ puede ser por dos cosas:

$\neg Q$ es falsa. En este caso, Q será verdadera y, por lo tanto, $P \longrightarrow Q$ será verdadera.

o

$\neg P$ es verdad. En tal caso, P es falsa y el condicional $P \longrightarrow Q$ será verdadero.

Por lo tanto,

$$(\neg Q \longrightarrow \neg P) \Longrightarrow (P \longrightarrow Q)$$

⊛ Comprobando que el condicional $(\neg Q \longrightarrow \neg P) \longrightarrow (P \longrightarrow Q)$ es una tautología. Como ya sabemos la única posibilidad de que un condicional sea falso es que sea verdad la hipótesis y la conclusión falsa. Veamos que esta situación no es posible. Si partimos de que la hipótesis, $\neg Q \longrightarrow \neg P$, es verdad el camino sería idéntico al anterior, así que partiremos de que la conclusión, $P \longrightarrow Q$, es falsa.

En efecto, si $P \longrightarrow Q$ es falsa, entonces P es verdad y Q es falsa, luego $\neg Q$ es verdad, $\neg P$ falsa y, consecuentemente, $\neg Q \longrightarrow \neg P$ es falsa y, por tanto, $(\neg Q \longrightarrow \neg P) \longrightarrow (P \longrightarrow Q)$ es, siempre, verdad. También podemos hacer una tabla de verdad abreviada:

P	Q	$P \longrightarrow Q$	$\neg Q$	$\neg P$	$\neg Q \longrightarrow \neg P$	$(\neg Q \longrightarrow \neg P) \longrightarrow (P \longrightarrow Q)$
V	F	F	V	F	F	V

■

En los ejemplos siguientes utilizaremos las equivalencias lógicas para simplificar una expresión lógica.

Ejemplo 1.26

Demostrar que $(p \wedge \neg q) \vee (\neg p \wedge \neg q) \vee (\neg p \wedge q) \Longleftrightarrow \neg(p \wedge q)$.

Solución

En efecto,

$$\begin{array}{lcll}
(p \wedge \neg q) \vee (\neg p \wedge \neg q) \vee (\neg p \wedge q) & \iff & [(p \vee \neg p) \wedge \neg q] \vee (\neg p \wedge q) & \{\text{Distributividad}\} \\
& \iff & (T \wedge \neg q) \vee (\neg p \wedge q) & \{\text{Tautología}\} \\
& \iff & \neg q \vee (\neg p \wedge q) & \{\text{Dominación}\} \\
& \iff & (\neg q \vee \neg p) \wedge (\neg q \vee q) & \{\text{Distributividad}\} \\
& \iff & (\neg p \vee \neg q) \wedge T & \{\text{Commutatividad y Tautología}\} \\
& \iff & \neg p \vee \neg q & \{\text{Dominación}\} \\
& \iff & \neg\,(p \wedge q) & \{\text{De Morgan}\}
\end{array}$$

■

Ejemplo 1.27

Establecer las siguientes equivalencias simplificando las proposiciones del lado izquierdo.

(a) $[(p \wedge q) \longrightarrow p] \iff T$

(b) $\neg(\neg(p \vee q) \longrightarrow \neg p) \iff C$

(c) $[(q \longrightarrow p) \wedge (\neg p \longrightarrow q) \wedge (q \longrightarrow q)] \iff p$

(d) $[(p \longrightarrow \neg p) \wedge (\neg p \longrightarrow p)] \iff C$

siendo C una contradicción y T una tautología.

Solución

(a) $[(p \wedge q) \longrightarrow p] \iff T$

$$\begin{array}{lcll}
[(p \wedge q) \longrightarrow p] & \iff & \neg(p \wedge q) \vee p & \{\text{Implicación}\} \\
& \iff & (\neg p \vee \neg q) \vee p & \{\text{De Morgan}\} \\
& \iff & p \vee (\neg p \vee \neg q) & \{\text{Conmutatividad de } \vee\} \\
& \iff & (p \vee \neg p) \vee \neg q & \{\text{Asociatividad de } \vee\} \\
& \iff & T \vee \neg q & \{\text{Tautología}\} \\
& \iff & T & \{\text{Dominación}\}
\end{array}$$

(b) $\neg(\neg(p \vee q) \longrightarrow \neg p) \iff C$

$$\begin{array}{lcll}
\neg(\neg(p \vee q) \longrightarrow \neg p) & \iff & \neg(\neg\neg\,(p \vee q) \vee \neg p) & \{\text{Implicación}\} \\
& \iff & \neg((p \vee q) \vee \neg p) & \{\text{Doble negación}\} \\
& \iff & \neg(p \vee q) \wedge \neg\neg p & \{\text{De Morgan}\} \\
& \iff & (\neg p \wedge \neg q) \wedge p & \{\text{Doble Negación y De Morgan}\} \\
& \iff & (\neg q \wedge \neg p) \wedge p & \{\text{Conmutatividad de } \wedge\} \\
& \iff & \neg q \wedge (\neg p \wedge p) & \{\text{Asociatividad de } \wedge\} \\
& \iff & \neg q \wedge C & \{\text{Contradicción}\} \\
& \iff & C & \{\text{Dominación}\}
\end{array}$$

(c) $[(q \longrightarrow p) \wedge (\neg p \longrightarrow q) \wedge (q \longrightarrow q)] \Longleftrightarrow p$

$$\begin{array}{lll} [(q \longrightarrow p) \wedge (\neg p \longrightarrow q) \wedge (q \longrightarrow q)] & \Longleftrightarrow & (\neg q \vee p) \wedge (\neg\neg p \vee q) \wedge (\neg q \vee q) \quad \{\text{Implicación}\} \\ & \Longleftrightarrow & (\neg q \vee p) \wedge (p \vee q) \wedge T \quad \{\text{Tautología}\} \\ & \Longleftrightarrow & (p \vee \neg q) \wedge (p \vee q) \quad \{\text{Conmutatividad}\} \\ & \Longleftrightarrow & p \vee (\neg q \wedge q) \quad \{\text{Distributividad}\} \\ & \Longleftrightarrow & p \vee C \quad \{\text{Contradicción}\} \\ & \Longleftrightarrow & p \quad \{\text{Identidad}\} \end{array}$$

(d) $[(p \longrightarrow \neg p) \wedge (\neg p \longrightarrow p)] \Longleftrightarrow C$

$$\begin{array}{lll} [(p \longrightarrow \neg p) \wedge (\neg p \longrightarrow p)] & \Longleftrightarrow & (\neg p \vee \neg p) \wedge (\neg\neg p \vee p) \quad \{\text{Implicación}\} \\ & \Longleftrightarrow & \neg p \wedge p \quad \{\text{Idempotencia y doble negación}\} \\ & \Longleftrightarrow & C \quad \{\text{Contradicción}\} \end{array}$$

■

1.5 Razonamientos

Estudiamos en este apartado el significado formal del concepto de "razonamiento" y lo utilizamos para demostrar la veracidad de proposiciones a través de implicaciones y equivalencias lógicas.

Desde un punto de vista genérico, un razonamiento consta de una serie de proposiciones llamadas premisas y que son los "datos" y una proposición que es la conclusión o resultado del mismo. Probar que el razonamiento es válido significa demostrar que la conclusión se sigue lógicamente de las premisas dadas.

1.5.1 Razonamiento

Llamaremos de esta forma a cualquier proposición con la estructura

$$(p_1 \wedge p_2 \wedge \cdots \wedge p_n) \longrightarrow q$$

siendo n un entero positivo.

A las proposiciones $p_i, i = 1, 2, \ldots, n$ se les llama *premisas* del razonamiento y a la proposición q, *conclusión* del mismo.

■

1.5.2 Razonamiento Válido

Diremos que el razonamiento,

$$(p_1 \wedge p_2 \wedge \cdots \wedge p_n) \longrightarrow q$$

es válido si la conclusión q es verdadera cada vez que la hipótesis, $p_1 \wedge p_2 \wedge \cdots \wedge p_n$, lo sea.

Nota 1.8 Obsérvese que esto significa que la hipótesis *implica lógicamente* la conclusión, es decir, un razonamiento será válido cuando

$$(p_1 \wedge p_2 \wedge \cdots \wedge p_n) \Longrightarrow q$$

o lo que es igual, si el condicional,

$$(p_1 \wedge p_2 \wedge \cdots \wedge p_n) \longrightarrow q$$

es una tautología.

Esto, a su vez, nos permite aceptar como válido el razonamiento en el caso de que alguna de las premisas sea falsa. En efecto, si alguna de las $p_i, i = 1, 2, \ldots, n$ es falsa, entonces $p_1 \wedge p_2 \wedge \cdots \wedge p_n$ será falsa, luego el condicional $p_1 \wedge p_2 \wedge \cdots \wedge p_n \longrightarrow q$ es verdadero, independientemente del valor de verdad de la conclusión q.

■

Ejemplo 1.28

Estudiar la validez del siguiente razonamiento:

$$[p \wedge ((p \wedge q) \longrightarrow r)] \longrightarrow (q \longrightarrow r)$$

Solución

Veamos que la veracidad de la conclusión se sigue de la veracidad de la hipótesis, es decir, probemos que

$$[p \wedge ((p \wedge q) \longrightarrow r)] \Longrightarrow (q \longrightarrow r)$$

1 Lo haremos primero aplicando directamente la definición de implicación lógica.

En efecto, si $p \wedge ((p \wedge q) \longrightarrow r)$ es verdad, entonces p es verdad y $(p \wedge q) \longrightarrow r$ también lo es y la veracidad de ésta última proposición puede ser porque la hipótesis, $p \wedge q$, sea falsa o porque la conclusión, r, sea verdadera. Tenemos, pues, dos opciones:

- p es verdad y $p \wedge q$ es falsa. En este caso, por el valor de verdad de la conjunción, (1.2.1), q ha de ser falsa y, consecuentemente, la conclusión $q \longrightarrow r$ es verdadera independientemente del valor de verdad que tenga r.
- p es verdad y r es verdad. En tal caso, la conclusión, $q \longrightarrow r$ es verdadera, independientemente del valor de verdad que tenga q.

Por lo tanto, el razonamiento es válido.

2 Lo haremos ahora comprobando que el condicional,

$$[p \wedge ((p \wedge q) \longrightarrow r)] \longrightarrow (q \longrightarrow r)$$

es una tautología.

En efecto, como el único caso en que el condicional es falso es que siendo verdad la hipótesis, la conclusión sea falsa, y teniendo en cuenta que aplicando la definición hemos partido de que la hipótesis es verdadera, partiremos ahora de que la conclusión es falsa y veremos que es imposible que la hipótesis sea verdadera. En efecto, si $q \longrightarrow r$ es falsa, entonces q será verdadera y r falsa y ahora todo dependerá del valor de verdad de p, es decir, tendremos dos opciones:

⁕ Si p es verdad, entonces $p \wedge q$ es verdad y, al ser r falso, el condicional $(p \wedge q) \longrightarrow r$ es falso. Por lo tanto, $p \wedge ((p \wedge q) \longrightarrow r)$ será falso y, consecuentemente, $[p \wedge ((p \wedge q) \longrightarrow r)] \longrightarrow (q \longrightarrow r)$ será verdad.

⁕ Si p es falso, $p \wedge ((p \wedge q) \longrightarrow r)$ será falso y, consecuentemente, $[p \wedge ((p \wedge q) \longrightarrow r)] \longrightarrow (q \longrightarrow r)$ será verdad.

La siguiente tabla de verdad *abreviada* recoge los casos anteriores,

p	q	r	$p \wedge q$	$(p \wedge q) \longrightarrow r$	$p \wedge ((p \wedge q) \longrightarrow r)$	$q \longrightarrow r$
V	V	F	V	F	F	F
F					F	F

$[p \wedge ((p \wedge q) \longrightarrow r)] \longrightarrow (q \longrightarrow r)$
V
V

3 Comprobaremos, finalmente, que el razonamiento es válido simplificando la hipótesis mediante implicaciones y equivalencias lógicas.

$$\begin{aligned}
p \wedge ((p \wedge q) \longrightarrow r) &\iff p \wedge (\neg (p \wedge q) \vee r) && \{\text{Implicación}\}\\
&\iff p \wedge (\neg p \vee \neg q \vee r) && \{\text{De Morgan}\}\\
&\iff p \wedge (\neg p \vee (q \longrightarrow r)) && \{\text{Implicación}\}\\
&\iff p \wedge (p \longrightarrow (q \longrightarrow r)) && \{\text{Implicación}\}\\
&\Longrightarrow q \longrightarrow r && \{\text{Modus Ponendo Ponens}\}
\end{aligned}$$

■

1.5.3 Demostración por Contradicción o Reducción al Absurdo

Este método de demostración de la validez de un razonamiento se basa en la equivalencia lógica conocida como "Reducción al absurdo" (1.4.4),

$$(P \longrightarrow Q) \Longrightarrow [(P \wedge \neg Q) \longrightarrow C]$$

Demostración

Pues bien, si queremos demostrar la validez del razonamiento, $P \longrightarrow Q$, podemos demostrar, en su lugar, la validez del razonamiento $(P \wedge \neg Q) \longrightarrow C$ que como hemos visto en 1.4.4, es equivalente al primero.

En efecto, para establecer que $P \Longrightarrow Q$, tenemos que probar que la veracidad de Q se deduce de la veracidad de P. Supongamos, pues, que P es verdad y supongamos, también, que la conclusión Q es falsa. Entonces, $P \wedge \neg Q$ será verdadera.

Si ahora partimos de que $P \wedge \neg Q$ es verdad y llegamos a una contradicción, C, para que $(P \wedge \neg Q) \longrightarrow C$ sea una tautología y, por tanto, un razonamiento valido, $P \wedge \neg Q$ ha de ser falsa y como P es verdadera, es $\neg Q$ la que tiene que ser falsa y, consecuentemente, Q será verdadera.

Obsérvese que en realidad hemos probado que

$$[(P \wedge \neg Q) \longrightarrow C] \Longrightarrow Q$$

es decir, la veracidad de Q se sigue de la veracidad de $(P \wedge \neg Q) \longrightarrow C$, de aquí que, como decíamos al principio, el nombre de método de demostración por contradicción o reducción al absurdo.

■

Ejemplo 1.29

Estudiar la validez del razonamiento:

$$[p \wedge ((p \wedge q) \longrightarrow r)] \longrightarrow (q \longrightarrow r)$$

por contradicción.

Solución

Probaremos que

$$[p \wedge ((p \wedge q) \longrightarrow r) \wedge \neg (q \longrightarrow r)] \longrightarrow C$$

es una tautología.

En efecto, si la hipótesis,

$$p \wedge ((p \wedge q) \longrightarrow r) \wedge \neg (q \longrightarrow r)$$

es verdad, por el valor de verdad de la conjunción, (1.2.1), las tres proposiciones han de ser verdaderas, es decir,

- p es verdad.
- $(p \wedge q) \longrightarrow r$ es verdad.
- $\neg (q \longrightarrow r)$ es verdad.

o lo que es igual,

- p es verdad.
- $(p \wedge q) \longrightarrow r$ es verdad.
- $q \longrightarrow r$ es falsa.

Por lo tanto, q es verdad y r es falsa y como $(p \wedge q) \longrightarrow r$ es verdad, siendo falsa la conclusión, r, la hipótesis, $p \wedge q$, ha de ser, también, falsa, y al ser q verdadera, p deberá ser falsa, es decir $\neg p$ es verdadera. Tendremos, pues, que $p \wedge \neg p$ es verdad.

Partiendo, pues, de la veracidad de

$$p \wedge ((p \wedge q) \longrightarrow r) \wedge \neg (q \longrightarrow r)$$

hemos llegado a la veracidad de $p \wedge \neg p$, es decir,

$$[p \wedge ((p \wedge q) \longrightarrow r) \wedge \neg (q \longrightarrow r)] \Longrightarrow (p \wedge \neg p)$$

o lo que es igual,

$$[p \wedge ((p \wedge q) \longrightarrow r) \wedge \neg (q \longrightarrow r)] \longrightarrow (p \wedge \neg p)$$

es una tautología. Como $p \wedge \neg p \Longleftrightarrow C$,

$$[p \wedge ((p \wedge q) \longrightarrow r) \wedge \neg (q \longrightarrow r)] \longrightarrow C$$

será, también, una tautología. Bastaría aplicar la equivalencia lógica conocida como "*reducción al absurdo*", (1.4.4), y tendríamos que

$$[p \wedge ((p \wedge q) \longrightarrow r)] \longrightarrow (q \longrightarrow r)$$

es, también, una tautología y el razonamiento, por lo tanto, es válido.

■

1.5.4 Demostración por la Contrarrecíproca

Este método de demostración de la validez de un razonamiento se basa en la equivalencia lógica conocida como "Contrarrecíproca" (1.4.4),

$$(P \longrightarrow Q) \Longleftrightarrow (\neg Q \longrightarrow \neg P)$$

Demostración

En efecto, supongamos que queremos establecer la validez de un razonamiento de hipótesis P y conclusión Q, es decir probar que $P \Longrightarrow Q$.

Una de las formas de hacerlo es comprobar que $P \longrightarrow Q$ es una tautología y como

$$(P \longrightarrow Q) \Longleftrightarrow (\neg Q \longrightarrow \neg P)$$

lo podremos hacer también comprobando que su contrarrecíproca, $\neg Q \longrightarrow \neg P$, lo es.

■

Ejemplo 1.30

Estudiar la validez del razonamiento:

$$[p \wedge ((p \wedge q) \longrightarrow r)] \longrightarrow (q \longrightarrow r)$$

por la contrarrecíproca.

Solución

Probaremos que

$$\neg (q \longrightarrow r) \Longrightarrow \neg [p \wedge ((p \wedge q) \longrightarrow r)]$$

Aplicando las equivalencias lógicas correspondientes,

$$\begin{aligned} \neg (q \longrightarrow r) &\Longleftrightarrow \neg (\neg q \vee r) && \{\text{Implicación}\} \\ &\Longleftrightarrow \neg\neg \wedge \neg r && \{\text{De Morgan}\} \\ &\Longleftrightarrow q \wedge \neg r && \{\text{Doble negación}\} \end{aligned}$$

y

$$\begin{aligned} \neg [p \wedge ((p \wedge q) \longrightarrow r)] &\Longleftrightarrow \neg p \vee \neg [(p \wedge q) \longrightarrow r] && \{\text{De Morgan}\} \\ &\Longleftrightarrow \neg p \vee \neg [\neg (p \wedge q) \vee r] && \{\text{Implicación}\} \\ &\Longleftrightarrow \neg p \vee \neg\neg (p \wedge q) \wedge \neg r && \{\text{De Morgan}\} \\ &\Longleftrightarrow \neg p \vee (p \wedge q \wedge \neg r) && \{\text{Doble Negación}\} \end{aligned}$$

Probaremos, pues, que

$$(q \wedge \neg r) \Longrightarrow [\neg p \vee (p \wedge q \wedge \neg r)]$$

En efecto, si $q \wedge \neg r$ es verdad, entonces el valor de verdad de la conclusión, $\neg p \vee (p \wedge q \wedge \neg r)$, dependerá del valor de verdad de p y, por tanto, habrá dos opciones:

- Si p es verdad, entonces $p \wedge q \wedge \neg r$ será verdad y, consecuentemente, la conclusión, $\neg p \vee (p \wedge q \wedge \neg r)$ también lo será.

⁎ Si p es falsa, entonces $\neg p$ será verdadera y, por lo tanto, la conclusión, $\neg p \vee (p \wedge q \wedge \neg r)$ será verdad.

Como la veracidad de la conclusión se deduce de la veracidad de la hipótesis habremos probado que el razonamiento (el contrarrecíproco) es válido o lo que es igual el condicional,

$$(q \wedge \neg r) \Longrightarrow [\neg p \vee (p \wedge q \wedge \neg r)]$$

es una tautología. Esto equivale a decir, por 1.4.4, que

$$[p \wedge ((p \wedge q) \longrightarrow r)] \longrightarrow (q \longrightarrow r)$$

es, también, una tautología y, por lo tanto, el razonamiento propuesto es válido, es decir,

$$[p \wedge ((p \wedge q) \longrightarrow r)] \Longrightarrow (q \longrightarrow r)$$

■

Ejemplo 1.31

Sean p, q y r las proposiciones,

p : *Torcuato se casa.*

q : *Florinda se tira al tren.*

r : *Torcuato se hace cura.*

Estudiar la validez del siguiente razonamiento:

$$[(p \longrightarrow q) \wedge (q \longleftrightarrow \neg r)] \longrightarrow (p \longrightarrow \neg r)$$

Solución

Tenemos que comprobar que la veracidad de la conclusión se sigue de la veracidad de la hipótesis, es decir,

$$[(p \longrightarrow q) \wedge (q \longleftrightarrow \neg r)] \Longrightarrow (p \longrightarrow \neg r)\,.$$

Lo haremos de varias formas.

1 Aplicando directamente la definición de implicación lógica.

En efecto, si $(p \longrightarrow q) \wedge (q \longleftrightarrow \neg r)$ es verdad, entonces $p \longrightarrow q$ ha de ser verdad y $q \longleftrightarrow \neg r$ también. Ahora bien, la veracidad del condicional $p \longrightarrow q$ puede deberse a que p sea falsa o a que q sea verdadera. Así pues, tendremos dos opciones:

⁎ p es falsa y $q \longleftrightarrow \neg r$ verdadera. En este caso, la conclusión $p \longrightarrow \neg r$ es verdadera, independientemente del valor de verdad que tenga r.

⁎ q es verdadera y $q \longleftrightarrow \neg r$ también. En tal caso, $\neg r$ ha de ser verdad y, consecuentemente, $p \longrightarrow \neg r$ es verdadera sin importar el valor de verdad de p.

Así pues, y en cualquier caso, la veracidad de la conclusión, $p \longrightarrow \neg r$ se sigue de la veracidad de la hipótesis, $(p \longrightarrow q) \wedge (q \longleftrightarrow \neg r)$, lo cual significa que

$$[(p \longrightarrow q) \wedge (q \longleftrightarrow \neg r)] \Longrightarrow (p \longrightarrow \neg r)$$

y el razonamiento es válido.

2 Comprobando que el condicional $[(p \longrightarrow q) \wedge (q \longleftrightarrow \neg r)] \longrightarrow (p \longrightarrow \neg r)$ es una tautología.

Tendremos en cuenta que la única opción en la que un condicional puede ser falso es que siendo verdad la hipótesis, la conclusión, sea falsa. Veamos que esta opción no puede darse.

- Si la hipótesis, $(p \longrightarrow q) \wedge (q \longleftrightarrow \neg r)$, es verdadera, la conclusión, $p \longrightarrow \neg r$, no puede ser falsa.
  En efecto, según hemos visto en la demostración anterior, si la hipótesis es verdad, entonces la conclusión también lo es.
- Si la conclusión, $p \longrightarrow \neg r$, es falsa, la hipótesis, $(p \longrightarrow q) \wedge (q \longleftrightarrow \neg r)$, no puede ser verdadera.
  En efecto, si la conclusión, $p \longrightarrow \neg r$, es falsa, entonces p es verdad y $\neg r$ es falso y el valor de verdad de $p \longrightarrow q$ y $q \longleftrightarrow \neg r$ dependerá del valor de verdad que tenga q. Habrá pues dos opciones:
  - q es verdad. En tal caso, $p \longrightarrow q$ será verdad y $q \longleftrightarrow \neg r$ falso.
  - q es falso. En este caso, $p \longrightarrow q$ será falso y $q \longleftrightarrow \neg r$ verdad.

  Por lo tanto y en ambos casos, la hipótesis, $(p \longrightarrow q) \wedge (p \longleftrightarrow \neg r)$, es falsa.
  La tabla de verdad siguiente refleja los pasos que hemos dado.

p	q	$\neg r$	$p \longrightarrow q$	$q \longleftrightarrow \neg r$	$(p \longrightarrow q) \wedge (p \longleftrightarrow \neg r)$	$p \longrightarrow \neg r$
V	V	F	V	F	F	F
V	F	F	F	V	F	F

$[(p \longrightarrow q) \wedge (q \longleftrightarrow \neg r)] \longrightarrow (p \longrightarrow \neg r)$
V
V

Consecuentemente, el condicional,

$$[(p \longrightarrow q) \wedge (q \longleftrightarrow \neg r)] \longrightarrow (p \longrightarrow \neg r)$$

es verdadero y, por lo tanto, el razonamiento es válido.

3 Utilizaremos, ahora, el método de demostración por contradicción (1.5.3).

Probaremos que

$$[(p \longrightarrow q) \wedge (q \longleftrightarrow \neg r) \wedge \neg (p \longrightarrow \neg r)] \longrightarrow C$$

es una tautología.

En efecto, si la hipótesis, $(p \longrightarrow q) \wedge (q \longleftrightarrow \neg r) \wedge \neg (p \longrightarrow \neg r)$ es verdad, por el valor de verdad de la conjunción, (1.2.1), las tres proposiciones que la integran han de ser verdaderas, es decir,

$p \longrightarrow q$ es verdad.

$q \longleftrightarrow \neg r$ es verdad.

$\neg (p \longrightarrow \neg r)$ es verdad, o sea $p \longrightarrow \neg r$ es falsa.

Pues bien, si $p \longrightarrow \neg r$ es falsa, entonces, por el valor de verdad del condicional, (1.2.6), p ha de ser verdad y $\neg r$, falsa. Como $q \longleftrightarrow \neg r$ es verdad, por el valor de verdad del bicondicional, (1.2.9), q ha de ser falsa y, al ser $p \longrightarrow q$ verdadera, nuevamente por el valor de verdad del condicional, p ha de ser falsa y, por lo tanto, $\neg p$ es verdadera. Tendremos, pues, que $p \wedge \neg p$ es verdadera.

Partiendo de la veracidad de

$$(p \longrightarrow q) \wedge (q \longleftrightarrow \neg r) \wedge \neg (p \longrightarrow \neg r)$$

hemos llegado a que $p \wedge \neg p$ es verdad, luego,

$$[(p \longrightarrow q) \wedge (q \longleftrightarrow \neg r) \wedge \neg (p \longrightarrow \neg r)] \Longrightarrow (p \wedge \neg p)$$

o lo que es igual,

$$[(p \longrightarrow q) \wedge (q \longleftrightarrow \neg r) \wedge \neg (p \longrightarrow \neg r)] \longrightarrow (p \wedge \neg p)$$

es una tautología. Como $p \wedge \neg p$ es una contradicción, tendremos que

$$[(p \longrightarrow q) \wedge (q \longleftrightarrow \neg r) \wedge \neg (p \longrightarrow \neg r)] \longrightarrow C$$

también será una tautología. Aplicamos la equivalencia lógica conocida como "*reducción al absurdo*", (1.4.4), y

$$[(p \longrightarrow q) \wedge (q \longleftrightarrow \neg r) \wedge \neg (p \longrightarrow \neg r)] \longrightarrow (p \longrightarrow \neg r)$$

es una tautología y, consecuentemente, el razonamiento es válido.

4 Probaremos, una vez más, que el razonamiento es válido utilizando el método de demostración por la contrarrecíproca, (1.5.4).

Veamos que

$$\neg (p \longrightarrow \neg r) \Longrightarrow \neg [(p \longrightarrow q) \wedge (q \longleftrightarrow \neg r)]$$

Utilizando las equivalencias lógicas correspondientes,

$$\begin{array}{lll} \neg (p \longrightarrow \neg r) & \Longleftrightarrow & \neg (\neg p \vee \neg r) \quad \{\text{Implicación}\} \\ & \Longleftrightarrow & \neg\neg p \wedge \neg\neg r \quad \{\text{De Morgan}\} \\ & \Longleftrightarrow & p \wedge r \quad \{\text{Doble negación}\} \end{array}$$

y

$$\begin{array}{lll} \neg [(p \longrightarrow q) \wedge (q \longleftrightarrow \neg r)] & \Longleftrightarrow & \neg (p \longrightarrow q) \vee \neg (q \longleftrightarrow \neg r) \quad \{\text{De Morgan}\} \\ & \Longleftrightarrow & \neg (p \longrightarrow q) \vee \neg [(q \longrightarrow \neg r) \wedge (\neg r \longrightarrow q)] \quad \{\text{Def. Bicondicional}\} \\ & \Longleftrightarrow & \neg (p \longrightarrow q) \vee \neg (q \longrightarrow \neg r) \vee \neg (\neg r \longrightarrow q) \quad \{\text{De Morgan}\} \\ & \Longleftrightarrow & \neg (\neg p \vee q) \vee \neg (\neg q \vee \neg r) \vee \neg (\neg\neg r \vee q) \quad \{\text{Implicación}\} \\ & \Longleftrightarrow & (\neg\neg p \wedge \neg q) \vee (\neg\neg q \wedge \neg\neg r) \vee (\neg\neg\neg r \wedge \neg q) \quad \{\text{De Morgan}\} \\ & \Longleftrightarrow & (p \wedge \neg q) \vee (q \wedge r) \vee (\neg r \wedge \neg q) \quad \{\text{Doble Negación}\} \end{array}$$

Probaremos, pues, que

$$(p \wedge r) \Longrightarrow [(p \wedge \neg q) \vee (q \wedge r) \vee (\neg r \wedge \neg q)]$$

En efecto, si la hipótesis, $p \wedge r$ es verdad, entonces por el valor de verdad de la conjunción, (1.2.1), p y r serán, ambas, verdaderas. El valor de verdad de la conclusión dependerá, por tanto, de q y tendremos, pues, dos opciones:

- q es verdad. En este caso, la proposición $q \wedge r$ será verdadera y, por el valor de verdad de la disyunción, (1.2.2), la conclusión, $(p \wedge \neg q) \vee (q \wedge r) \vee (\neg r \wedge \neg q)$, será verdadera.
- q es falsa. En tal caso, $\neg q$ será verdad, la proposición $p \wedge \neg q$ también y, nuevamente, por el valor de verdad de la disyunción, (1.2.2), la conclusión, $(p \wedge \neg q) \vee (q \wedge r) \vee (\neg r \wedge \neg q)$, será verdadera.

Como la veracidad de la conclusión se sigue de la veracidad de la hipótesis hemos comprobado la implicación lógica y por lo tanto el condicional,

$$(p \wedge r) \longrightarrow [(p \wedge \neg q) \vee (q \wedge r) \vee (\neg r \wedge \neg q)]$$

será una tautología, es decir,

$$\neg (p \longrightarrow \neg r) \Longrightarrow \neg [(p \longrightarrow q) \wedge (q \longleftrightarrow \neg r)]$$

es una tautología. Utilizando la equivalencia lógica "*contrarrecíproca*", 1.4.4,

$$[(p \longrightarrow q) \wedge (q \longleftrightarrow \neg r)] \longrightarrow (p \longrightarrow \neg r)$$

será, también, tautología y, consecuentemente, el razonamiento es válido.

Finalmente, escribimos el razonamiento con palabras,

> Si Torcuato se casa, entonces Florinda se tira al tren.
> Florinda se tira al tren siempre y cuando Torcuato no se haga cura.
> Por lo tanto, si Torcuato se casa, entonces no se hace cura.

■

Ejemplo 1.32

Estudiar la validez del siguiente razonamiento:

> *Si Florinda resuelve los ejercicios, entonces aprobará Lógica Matemática.*
> *Si Florinda no se va de fiesta, entonces resolverá los ejercicios.*
> *Florinda no aprobó Lógica Matemática.*
> *Por lo tanto, Florinda se fue de fiesta.*

Solución

Llamando,

p : Florinda resuelve los ejercicios.

q : Florinda aprueba Lógica Matemática.

r : Florinda se va de fiesta.

El razonamiento escrito en notación simbólica será:

$$[(p \longrightarrow q) \wedge (\neg r \longrightarrow p) \wedge \neg q] \longrightarrow r$$

Veamos si la veracidad de la conclusión se sigue de la veracidad de la hipótesis, es decir, si

$$[(p \longrightarrow q) \wedge (\neg r \longrightarrow p) \wedge \neg q] \Longrightarrow r$$

Lo haremos de varias formas.

1 Aplicando directamente la definición de implicación lógica.

En efecto, si $(p \longrightarrow q) \wedge (\neg r \longrightarrow p) \wedge \neg q$ es verdad, entonces, las tres proposiciones que la componen han de ser verdaderas. Pues bien, si $\neg q$ es verdad, entonces q ha de ser falsa, y como $p \longrightarrow q$ es verdad, la proposición p tendrá que ser falsa. Por otra parte, si $\neg r \longrightarrow p$ es verdad, al ser p falsa, la proposición $\neg r$ tendrá que ser falsa también y, consecuentemente, r será verdad.

La siguiente tabla de verdad recoge los pasos anteriores en el orden en que se producen.

p	q	r	$\neg r$	$p \longrightarrow q$	$\neg r \longrightarrow p$	$\neg q$	$(p \longrightarrow q) \wedge (\neg r \longrightarrow p) \wedge \neg q$
							V
				V	V	V	
	F			V	V		
F					V		
			F				
		V					

El razonamiento propuesto es, por tanto, válido.

2 Comprobando que el condicional $[(p \longrightarrow q) \wedge (\neg r \longrightarrow p) \wedge \neg q] \longrightarrow r$ es una tautología.

Sabemos que un condicional es falso únicamente cuando siendo verdad la hipótesis, la conclusión es falsa. Veamos que esta situación no puede ocurrir.

- Si la hipótesis, $(p \longrightarrow q) \wedge (\neg r \longrightarrow p) \wedge \neg q$ es verdadera, la conclusión r no puede ser falsa.
  En efecto, si la hipótesis es verdad, hemos visto en la demostración anterior que la conclusión también lo es.
- Si la conclusión, r, es falsa, entonces $\neg r$ es verdadera, luego el valor de verdad de $\neg r \longrightarrow p$ dependerá del de p.
  - Si p es verdad, entonces $\neg r \longrightarrow p$ es verdad y el valor de verdad de $p \longrightarrow q$ dependerá del valor de verdad que tenga q.
    - Si q es verdad, entonces $\neg q$ es falsa y, por lo tanto, la hipótesis, $(p \longrightarrow q) \wedge (\neg r \longrightarrow p) \wedge \neg q$, es falsa.
    - Si q es falsa, entonces $p \longrightarrow q$ es falsa y, consecuentemente, la hipótesis también lo es.
  - Si p es falsa, entonces el condicional $\neg r \longrightarrow p$ es falso y, por lo tanto, la hipótesis es falsa.

  Hemos visto, pues, que la falsedad de la conclusión nos conduce, en cualquier caso, a la falsedad de la hipótesis.

La tabla de verdad siguiente recoge los pasos dados.

p	q	r	$\neg q$	$\neg r$	$p \longrightarrow q$	$\neg r \longrightarrow p$	$(p \longrightarrow q) \wedge (\neg r \longrightarrow p) \wedge \neg q$
V	V	F	F	V		V	F
V	F	F			F		F
F		F		V		F	F

$[(p \longrightarrow q) \wedge (\neg r \longrightarrow p) \wedge \neg q] \longrightarrow r$
V
V
V

Consecuentemente, el condicional

$$[(p \longrightarrow q) \wedge (\neg r \longrightarrow p) \wedge \neg q] \longrightarrow r$$

es una tautología siendo, por lo tanto, válido el razonamiento.

3 Simplificando la hipótesis mediante implicaciones y equivalencias lógicas.

$$\begin{aligned}
(p \longrightarrow q) \wedge (\neg r \longrightarrow p) \wedge \neg q &\iff [(p \longrightarrow q) \wedge \neg q] \wedge (\neg r \longrightarrow p) && \{\text{Conmutatividad}\}\\
&\implies \neg p \wedge (\neg r \longrightarrow p) && \{\text{Modus tollendo tollens}\}\\
&\iff (\neg r \longrightarrow p) \wedge \neg p && \{\text{Conmutatividad}\}\\
&\implies \neg\neg r && \{\text{Modus tollendo tollens}\}\\
&\iff r && \{\text{Doble negación}\}
\end{aligned}$$

Con lo cual hemos probado, también, que el razonamiento es válido.

4 Demostración por contradicción.

Probaremos que

$$[(p \longrightarrow q) \wedge (\neg r \longrightarrow p) \wedge \neg q \wedge \neg r] \longrightarrow C$$

es una tautología.

En efecto, si la hipótesis, $(p \longrightarrow q) \wedge (\neg r \longrightarrow p) \wedge \neg q \wedge \neg r$ es verdad, entonces por el valor de verdad de la conjunción, (1.2.1), las cuatro proposiciones que la integran han de ser verdaderas, es decir,

- $p \longrightarrow q$ es verdad.
- $\neg r \longrightarrow p$ es verdad.
- $\neg q$ es verdad, o sea q es falsa.
- $\neg r$ es verdad.

Pues bien, si q es falsa, al ser verdad $p \longrightarrow q$, por el valor de verdad del condicional, (1.2.6), p ha de ser falsa, es decir $\neg p$ es verdadera.

Por otra parte, si $\neg r$ es verdad y $\neg r \longrightarrow p$ también, nuevamente por el valor de verdad del condicional, (1.2.6), tendremos que p ha de ser verdad.

Hemos llegado, por tanto, a que $p \wedge \neg p$ es verdad, luego,

$$[(p \longrightarrow q) \wedge (\neg r \longrightarrow p) \wedge \neg q \wedge \neg r] \Longrightarrow (p \wedge \neg p)$$

es decir, el condicional,

$$[(p \longrightarrow q) \wedge (\neg r \longrightarrow p) \wedge \neg q \wedge \neg r] \longrightarrow (p \wedge \neg p)$$

es una tautología y, como $p \wedge \neg p$ es una contradicción,

$$[(p \longrightarrow q) \wedge (\neg r \longrightarrow p) \wedge \neg q \wedge \neg r] \longrightarrow C$$

también lo será.

Aplicamos "*reducción al absurdo*", (1.4.4), y

$$[(p \longrightarrow q) \wedge (\neg r \longrightarrow p) \wedge \neg q] \longrightarrow r$$

es una tautología y, consecuentemente, el razonamiento propuesto es válido.

5 Demostración por la contrarrecíproca.

Probaremos que

$$\neg r \Longrightarrow \neg\,[(p \longrightarrow q) \wedge (\neg r \longrightarrow p) \wedge \neg q]$$

Utilizando las equivalencias lógicas correspondientes,

$$\begin{aligned}
\neg\,[(p \longrightarrow q) \wedge (\neg r \longrightarrow p) \wedge \neg q] &\iff \neg\,(p \longrightarrow q) \vee \neg\,(\neg r \longrightarrow p) \vee \neg\neg q && \{\text{De Morgan}\}\\
&\iff \neg\,(\neg p \vee q) \vee \neg\,(\neg\neg r \vee p) \vee \neg\neg q && \{\text{Implicación}\}\\
&\iff (\neg\neg p \wedge \neg q) \vee (\neg\neg\neg r \wedge \neg p) \vee \neg\neg q && \{\text{De Morgan}\}\\
&\iff (p \wedge \neg q) \vee (\neg r \wedge \neg p) \vee q && \{\text{Doble Negación}\}
\end{aligned}$$

Probaremos, pues, que

$$\neg r \Longrightarrow [(p \wedge \neg q) \vee (\neg r \wedge \neg p) \vee q]$$

En efecto, si $\neg r$ es verdad, entonces el valor de verdad de $\neg r \wedge \neg p$ dependerá de $\neg p$. Habrá, por tanto, dos opciones:

1. $\neg p$ es verdad. En este caso, $\neg r \wedge \neg p$ será verdadera y, por el valor de verdad de la disyunción, (1.2.2), la conclusión, $(p \wedge \neg q) \vee (\neg r \wedge \neg p) \vee q$ será verdadera.
2. $\neg p$ es falsa. p será verdad y el valor de verdad de $p \wedge \neg q$ dependerá de $\neg q$. Tendremos, pues, dos opciones:
   - 2.1 $\neg q$ es verdad. En este caso, $p \wedge \neg q$ será verdad y, al igual que antes, la conclusión será verdadera.
   - 2.2 $\neg q$ es falsa. En tal caso, q será verdad y, nuevamente, por el valor de verdad de la disyunción, (1.2.2), la conclusión será verdadera.

Por lo tanto, y en cualquier caso, la veracidad de la conclusión se sigue de la veracidad de la hipótesis, es decir se verifica la implicación lógica y, por tanto, el condicional,

$$\neg r \longrightarrow [(p \wedge \neg q) \vee (\neg r \wedge \neg p) \vee q]$$

será una tautología, luego

$$\neg r \longrightarrow \neg\,[(p \longrightarrow q) \wedge (\neg r \longrightarrow p) \wedge \neg q]$$

también lo será y en virtud de la equivalencia entre un condicional y su contrarrecíproco, (1.4.4),

$$[(p \longrightarrow q) \wedge (\neg r \longrightarrow p) \wedge \neg q] \longrightarrow r$$

también será una tautología y, consecuentemente, el razonamiento propuesto será válido.

■

Ejemplo 1.33

Consideremos el siguiente razonamiento:

Florinda está en una fiesta.
Si Florinda está en una fiesta, entonces no está resolviendo los ejercicios de Lógica.
Si Florinda no está resolviendo los ejercicios de Lógica, entonces no aprobará Lógica.

¿Cuál es la conclusión (distinta de las premisas) para que el razonamiento sea válido?

Solución

Sean:

p : Florinda está en una fiesta.

q : Florinda está haciendo los ejercicios de Lógica.

r : Florinda aprueba lógica.

La hipótesis será:

$$p \wedge (p \longrightarrow \neg q) \wedge (\neg q \longrightarrow \neg r)$$

Pues bien,

$$\begin{array}{lcll} p \wedge (p \longrightarrow \neg q) \wedge (\neg q \longrightarrow \neg r) & \Longrightarrow & p \wedge (p \longrightarrow \neg r) & \{\text{Silogismo Hipótetico}\} \\ & \Longrightarrow & \neg r & \{\text{Modus Ponendo Ponens}\} \end{array}$$

Por lo tanto, para que el razonamiento sea válido la conclusión debe ser "Florinda no aprobará Lógica".

■

1.5.5 Falacia

Llamaremos de esta forma a un razonamiento que no es válido

Ejemplo 1.34

Estudiar la validez del siguiente razonamiento:

> *Si el mayordomo es el asesino, se pondrá nervioso cuando lo interroguen.*
> *El mayordomo se puso muy nervioso cuando lo interrogaron.*
> *Por lo tanto, el mayordomo es el asesino.*

Solución

Sean:

> p : El mayordomo es el asesino.
> q : El mayordomo se puso muy nervioso cuando lo interrogaron.

El razonamiento escrito en forma simbólica sería:

$$[(p \longrightarrow q) \wedge q] \longrightarrow p$$

Veamos si es una tautología.

La proposición anterior es falsa, únicamente si siendo verdad la hipótesis, $(p \longrightarrow q) \wedge q$, es falsa la conclusión p. Pero, si $(p \longrightarrow q) \wedge q$ es verdad, entonces $p \longrightarrow q$ es verdad y q también lo es, de aquí que p pueda ser verdadero o falso, luego una de las líneas de su *tabla de verdad* sería:

p	q	$p \longrightarrow q$	$(p \longrightarrow q) \wedge q$	$[(p \longrightarrow q) \wedge q] \longrightarrow p$
F	V	V	V	F

Por tanto, $[(p \longrightarrow q) \wedge q] \longrightarrow p$ no es una tautología y el argumento no sería válido, es decir, es una *falacia.*

El nerviosismo del mayordomo pudo estar no en su culpabilidad sino en cualquier otra causa.

■

Ejemplo 1.35

Estudiar la validez del siguiente razonamiento:

> *Si las manos del mayordomo están manchadas de sangre, entonces es culpable.*
> *El mayordomo está impecablemente limpio.*
> *Por lo tanto, el mayordomo es inocente.*

Solución

Sean

> p : El mayordomo tiene las manos manchadas de sangre.
> q : El mayordomo es culpable.

En forma simbólica, el razonamiento puede representarse en la forma:

$$[(p \longrightarrow q) \wedge \neg p] \longrightarrow \neg q$$

Veamos si es una tautología.

Razonando igual que en el ejercicio anterior, una *tabla de verdad abreviada* sería:

p	q	$p \longrightarrow q$	$\neg p$	$(p \longrightarrow q) \wedge \neg p$	$\neg q$	$[(p \longrightarrow q) \wedge \neg p] \longrightarrow \neg q$
F	V	V	V	V	F	F

Luego no es una tautología y, consecuentemente, el razonamiento no es válido.

El razonamiento ignora la obsesión compulsiva del mayordomo por la limpieza, lo cual le lleva siempre a lavarse las manos inmediatamente después de cometer un crimen.

■

Lección 2

Lógica de Predicados

2.1 Definiciones

Cualquier teoría científica aspira a enunciar leyes, postulados, definiciones, teoremas, etc... con una validez más o menos universal y, en cualquier caso, bien precisada. A menudo interesa afirmar que todos los individuos de un cierto campo tienen la propiedad p o que algunos la tienen.

El cálculo proposicional no es suficientemente fuerte para hacer todas las afirmaciones que se necesitan en cualquier disciplina científica. Por ejemplo, afirmaciones como "x es par" ó "$x \geqslant y$" no son proposiciones ya que no son necesariamente verdaderas o falsas. Sin embargo, asignando valores concretos a las variables x e y, las afirmaciones anteriores son susceptibles de ser verdaderas o falsas, es decir, se convierten en proposiciones.

En castellano también ocurren situaciones similares, por ejemplo,

Ella es alta y rubia.

Él vive en el campo.

Ella, él y el campo se utilizan como variables,

x es alta y rubia.

x vive en y

2.1.1 Predicado

Es una afirmación que expresa una propiedad de un objeto o una relación entre objetos. Estas afirmaciones se hacen verdaderas o falsas cuando se reemplazan los objetos (variables) por valores específicos.

Notaremos los predicados por $p(x)$, $q(x)$, $r(x)\ldots$, *o bien* $p(x,y)$, $q(x,y)$, $r(x,y,z)$ *si tienen más de una variable.*

■

Ejemplo 2.1

La afirmación "$p(x)$: x es alta y rubia" es un predicado que expresa la propiedad del objeto x de ser "alta y rubia". Si sustituimos la variable x por un valor determinado, por ejemplo Florinda, entonces el predicado se transforma en la afirmación "Florinda es alta y rubia" que podrá ser verdadera o falsa y, consecuentemente, es una proposición.

El predicado "$q(x)$: x vive en y" expresa una relación entre los objetos x e y. Si sustituimos x por Torcuato e y por Cádiz, obtendremos la afirmación "Torcuato vive en Cádiz". Ésta podrá ser verdadera o falsa, es decir, es una proposición.

■

Nota 2.1 Cuando analizamos la frase "x es un número par" vemos que es un predicado, ya que es una afirmación que expresa la propiedad de ser par del objeto x. En este caso parece obvio que el objeto ha de ser, al menos, numérico y más concretamente un número entero.

■

2.1.2 Universo del discurso

Llamaremos de esta forma al conjunto al cual pertenecen todos los valores que puedan tomar las variables. Lo notaremos por $\mathscr{U}$ y lo nombraremos por universo del discurso, conjunto universal o, simplemente, universo. Debe contener, al menos, un elemento.

■

Ejemplo 2.2

En una posible evaluación del predicado "$p(x) : x > 5$", elegiríamos probablemente un conjunto numérico, por ejemplo los números enteros, como universo del discurso. No tendría sentido elegir, por ejemplo, el conjunto de los colores del arco iris ya que podríamos encontrarnos con situaciones tales como "azul > 5".

■

2.1.3 Predicados y Proposiciones

Si $p(x_1, x_2, \ldots, x_n)$ es un predicado con n variables y asignamos los valores $c_1, c_2, \ldots, c_n$ a cada una de ellas, el resultado es la proposición $p(c_1, c_2, \ldots, c_n)$.

■

Para transformar un predicado en proposición, cada variable del predicado debe estar "ligada".

Ejemplo 2.3

Consideremos el predicado $p(x, y) : x + y = 5$ *en el universo de los números enteros. En principio las variables* x *e* y *pueden tomar cualquier valor entero, es decir están "libres".*

> *Si asignamos a* x *el valor* 2 *y a la* y *el valor* 3*, entonces el predicado* $p(x, y)$ *se transforma en la proposición* $p(2, 3) : 2 + 3 = 5$ *que es* verdad.
>
> *Si hubiéramos asignado los valores* 1 *y* 2 *a las variables* x *e* y*, respectivamente, entonces resultaría la proposición* $p(1, 2) : 1 + 2 = 5$ *que es* falsa.

En ambos casos, las variables x *e* y *han pasado de estar* libres *a estar* ligadas*. Hemos ligado las variables asignándoles unos valores concretos del universo del discurso.*

■

2.2 Cuantificadores

Supongamos que el Universo del Discurso es un conjunto de animales como, por ejemplo,

$$\mathscr{U} = \{avestruces, caballos, gallinas, leones\}$$

y veamos si la afirmación "*todos los animales de* $\mathscr{U}$ *tienen cuatro patas*" es, o no, una proposición. En efecto, observemos que la afirmación propuesta equivale a esta otra, "*los avestruces tienen cuatro patas y los caballos tienen cuatro patas y las gallinas tienen cuatro patas y los leones tienen cuatro patas*", es decir, la afirmación inicial es equivalente a cuatro afirmaciones unidas por el conectivo "y ", siendo cada una de ellas una proposición.

La respuesta, por tanto, será que la afirmación "*todos los animales de* $\mathscr{U}$ *tienen cuatro patas*" es, efectivamente, una proposición.

Si llamamos x a cualquier elemento de $\mathscr{U}$, consideramos el predicado,

$$p(x) : x \text{ tiene cuatro patas}$$

y utilizamos el símbolo $\forall$ para indicar "todos" o "cada uno de los" o "cualquiera de los", podemos escribir todo esto en lenguaje simbólico,

$$\begin{aligned} \text{Todos los animales de } \mathscr{U} \text{ tienen cuatro patas} &\iff \forall x \in \mathscr{U},\ p(x) \\ &\iff p(\text{avestruces}) \wedge p(\text{caballos}) \wedge p(\text{gallinas}) \wedge p(\text{leones}) \end{aligned}$$

es decir, *todos los animales de* $\mathscr{U}$ *tienen cuatro patas* es una proposición compuesta de cuatro proposiciones simples unidas por el conectivo "y".

Obsérvese que si en el universo del discurso, $\mathscr{U}$, hubiera, por ejemplo, 50, 100, 500 o un número indeterminado de animales no sería posible escribir todas y cada una de las proposiciones simples que componen la proposición compuesta "*todos los animales de* $\mathscr{U}$ *tienen cuatro patas*", por lo que, en tal caso, tendríamos que utilizar siempre la notación $\forall x, p(x)$.

Observemos, también, que está proposición será verdad, únicamente cuando todas las proposiciones simples que la componen sean verdaderas ya que están unidas por el conectivo $\wedge$ y para que sea falsa bastará que lo sea, al menos, una de ellas.

Planteemos ahora la misma cuestión respecto de la afirmación "*hay, al menos, un animal en $\mathscr{U}$ que tiene cuatro patas*", ¿es, o no es, una proposición? En efecto, observemos que esta afirmación es equivalente a, "*los avestruces tienen cuatro patas o los caballos tienen cuatro patas o las gallinas tienen cuatro patas o los leones tienen cuatro patas*", o sea, la afirmación es equivalente, al igual que antes, a cuatro afirmaciones unidas, en este caso, por el conectivo "*o*", siendo cada una de ellas una proposición.

Siguiendo un razonamiento idéntico al anterior y utilizando el símbolo $\exists$ para indicar "hay, al menos un" o "existe, al menos, un", podremos escribir en lenguaje simbólico,

$$\begin{aligned} \text{Hay, al menos, un animal en } \mathscr{U} \text{ con 4 } patas &\iff \exists x \in \mathscr{U} : p(x) \\ &\iff p(\text{avestruces}) \vee p(\text{caballos}) \vee p(\text{gallinas}) \vee p(\text{leones}) \end{aligned}$$

es decir, *hay, al menos, un animal en $\mathscr{U}$ que tiene cuatro patas* es una proposición compuesta de cuatro proposiciones simples unidas por el conectivo "*o*".

Obsérvese que esta proposición será falsa únicamente cuando todas las proposiciones simples que la componen lo sean ya que están unidas por el conectivo $\vee$ y para que sea verdadera bastará que lo sea, al menos, una de ellas.

2.2.1 Cuantificador universal

Si $p(x)$ es un predicado cuya variable es x, entonces la afirmación

$$\textit{"para todo } x,\ p(x)\textit{"}$$

es una proposición en la cual se dice que la variable x está universalmente cuantificada.

La frase "para todo" se simboliza con $\forall$, símbolo que recibe el nombre de *"cuantificador universal"*.

Así pues, "para todo x, $p(x)$" se escribe " $\forall x, p(x)$". El símbolo $\forall x$ puede interpretarse también como "para cada x", "para cualquier x" y "para x arbitrario".

■

Ejemplo 2.4

Escribir, en el universo de los enteros positivos, la proposición "todo número es estrictamente menor que el siguiente".

Solución

Sea $\mathscr{U} = \mathbb{Z}^+$. Observemos que la proposición propuesta equivale a decir que,

$$1 < 2 \text{ y } 2 < 3 \text{ y } 3 < 4 \text{ y } 4 < 5 \text{ y} \ldots\ldots$$

Naturalmente, es imposible escribir todas las proposiciones simples que la integran, aunque si utilizamos el predicado $p(a) : a < a + 1$, será equivalente a:

$$p(1) \wedge p(2) \wedge p(3) \wedge p(4) \wedge \ldots\ldots$$

que, a su vez, equivale a la proposición universalmente cuantificada,

$$\forall n, p(n)$$

o

$$\forall n, (n < n + 1)$$

es decir, la frase "todo número es estrictamente menor que el siguiente" equivale a escribir con notación lógica, $\forall n, (n < n + 1)$.

■

Ejemplo 2.5

En el conjunto de los números enteros consideremos los siguientes predicados:

$p(n_1, n_2, n_3) : n_1 n_2 = n_3$

$q(n_1, n_2) : n_1 = n_2$

$r(n_1, n_2) : n_1 > n_2$

Transcribir las siguientes proposiciones a notación lógica.

(a) Dado cualquier par de números enteros, si su producto es distinto de cero, entonces ambos han de ser, también, distintos de cero.

(b) Dados dos números enteros cualesquiera, es necesario que uno de los dos sea cero para que su producto lo sea.

(c) Para que cualquier par de enteros a y b sean iguales es suficiente que $a \leqslant b$ y $b \leqslant a$.

(d) Para cualquier terna de enteros, a, b y c, si $a < b$ y $c < 0$, entonces $ac > bc$.

Solución

(a) Dado cualquier par de números enteros, si su producto es distinto de cero, entonces ambos han de ser, también, distintos de cero.

La forma simbólica de la proposición utilizando el cuantificador universal sería,

$$\forall a, \forall b, (ab \neq 0 \longrightarrow a \neq 0 \text{ y } b \neq 0)$$

la cual, utilizando los predicados del enunciado, se escribiría

$$\forall a, \forall b, [\neg p(a, b, 0) \longrightarrow (\neg q(a, 0) \wedge \neg q(b, 0))]$$

(b) Dados dos números enteros cualesquiera, es necesario que uno de los dos sea cero para que su producto lo sea.

En efecto, utilizando el cuantificador universal y teniendo en cuenta que la condición propuesta es necesaria, la proposición será:

$$\forall a, \forall b, (ab = 0 \longrightarrow a = 0 \text{ ó } b = 0)$$

y utilizando los predicados,

$$\forall a, \forall b, [p(a, b, 0) \longrightarrow (q(a, 0) \vee q(b, 0))]$$

(c) Para que cualquier par de enteros a y b sean iguales es suficiente que $a \leqslant b$ y $b \leqslant a$.

Utilizando el cuantificador universal y recordando cual era la condición suficiente en un condicional, la proposición es:

$$\forall a, \forall b, (a \leqslant b \text{ y } b \leqslant a \longrightarrow a = b)$$

y con los predicados,

$$\forall a, \forall b, [(\neg r(a, b) \wedge \neg r(b, a)) \longrightarrow a = b]$$

(d) Para cualquier terna de enteros, a, b y c, si $a < b$ y $c < 0$, entonces $ac > bc$.

Utilizando el cuantificador universal, $\forall$,

$$\forall a, \forall b, \forall c\, (a < b \text{ y } c < 0 \longrightarrow ac > bc)$$

Para escribir la proposición con los predicados propuestos utilizaremos las variables auxiliares, d y e. En efecto,

$$\forall a, \forall b, \forall c\, [(r(b, a) \wedge r(0, c)) \longrightarrow \forall d, \forall e\, ((p(a, c, d) \wedge p(b, c, e)) \longrightarrow r(d, e))]$$

■

2.2.2 Valor de verdad del cuantificador universal

Sea $p(x)$ un predicado cuya variable x toma valores en un universo del discurso $\mathscr{U}$.

- ⁕ *$\forall x, p(x)$ es verdad si el predicado $p(x)$ se transforma en una proposición verdadera para todos los valores de x en el universo $\mathscr{U}$.*
- ⁕ *$\forall x, p(x)$ es falsa si hay, al menos, un valor de x en $\mathscr{U}$ para el cual el predicado $p(x)$ se transforme en una proposición falsa.*

■

Ejemplo 2.6

Estudiar en el universo de los números enteros, el valor de verdad de las siguientes afirmaciones:

(a) Todo número es estrictamente menor que el siguiente.

(b) Todos los números enteros son iguales a 5.

Solución

(a) Todo número es estrictamente menor que el siguiente.

Probaremos que la proposición $\forall n, (n < n+1)$ es verdad en, $\mathbb{Z}$, universo de los números enteros.

Por la relación de orden estricto definida en $\mathbb{Z}$, sabemos que dados dos enteros cualesquiera, a y b,

$$a < b \iff \exists q \in \mathbb{Z}^+ : b = a + q$$

Pues bien, dado a cualquiera, tomando $b = a + 1$, tendremos que b es entero y

$$a < b$$

es decir,

$$a < a + 1$$

Si ahora tenemos en cuenta que a es cualquier entero, podemos decir que el predicado $n < n + 1$ se transforma en una proposición verdadera para todos y cada uno de los elementos del universo, luego por 2.2.2,

$$\forall n, (n < n + 1)$$

es una proposición verdadera.

(b) Todos los números enteros son iguales a 5.

Probaremos que la proposición $\forall n, (n = 5)$ es falsa.

En efecto, bastaría encontrar, al menos, un número entero que transformara el predicado $n = 5$ en una proposición falsa. En este caso, valdría cualquier entero, $a \neq 5$, es decir hay infinitos ejemplos.

Aplicando de nuevo, 2.2.2, la proposición

$$\forall n, (n = 5)$$

es falsa.

■

2.2.3 Cuantificador existencial

Si $p(x)$ es un predicado cuya variable es x, entonces la afirmación

$$\text{“existe un } x \text{ tal que } p(x)\text{”}$$

es una proposición en la que diremos que la variable x está existencialmente cuantificada.

La frase “existe [al menos]” se simboliza con $\exists$, símbolo que recibe el nombre de *cuantificador existencial.*

Por tanto, “existe un x, tal que $p(x)$” se escribe “$\exists x : p(x)$” y puede leerse también como “para algún $x, p(x)$” o “existe, al menos, un x, tal que $p(x)$”.

■

Ejemplo 2.7

Sea el universo del discurso $\mathscr{U} = \{0, 1\}$. Encontrar conjunciones y disyunciones finitas de proposiciones que no usen cuantif icadores y que sean equivalentes a las siguientes:

(a) $\forall x, p(0, x)$

(b) $\forall x, [\forall y, p(x, y)]$

(c) $\forall x, [\exists y : p(x, y)]$

(d) $\exists x : [\forall y, p(x, y)]$

(e) $\exists y\, [\exists x : p(x, y)]$

Solución

(a) $\forall x, p(0, x)$

La forma equivalente pedida es

$$p(0, 0) \wedge p(0, 1)$$

(b) La proposición cuantificada $\forall x, [\forall y, (p(x, y))]$ puede expandirse en la forma:

$$[\forall y, p(0, y)] \wedge [\forall y, p(1, y)]$$

la cual puede interpretarse como

$$[p(0, 0) \wedge p(0, 1)] \wedge [p(1, 0) \wedge p(1, 1)]$$

que por la asociatividad de $\wedge$ equivale a

$$p(0, 0) \wedge p(0, 1) \wedge p(1, 0) \wedge p(1, 1)$$

(c) Expandimos la proposición $\forall x, [\exists y : p(x, y)]$ a

$$[\exists y : p(0, y)] \wedge [\exists y : p(1, y)]$$

la cual equivale a

$$[p(0, 0) \vee p(0, 1)] \wedge [p(1, 0) \vee p(1, 1)]$$

y aplicando la distributividad de $\wedge$ respecto de $\vee$,

$$[(p(0, 0) \vee p(0, 1)) \wedge p(1, 0)] \vee [(p(0, 0) \vee p(0, 1)) \wedge p(1, 1)]$$

es decir,

$$(p(0, 0) \wedge p(1, 0)) \vee (p(0, 1) \wedge p(1, 0)) \vee (p(0, 0) \wedge p(1, 1)) \vee (p(0, 1) \wedge p(1, 1))$$

(d) $\exists x : [\forall y, p(x, y)]$ se expande en la forma:

$$[\forall y, p(0, y)] \vee [\forall y, p(1, y)]$$

la cual equivale a la proposición

$$[p(0, 0) \wedge p(0, 1)] \vee [p(1, 0) \wedge p(1, 1)]$$

y por la distributividad de $\vee$ respecto de $\wedge$,

$$[(p(0, 0) \wedge p(0, 1)) \vee p(1, 0)] \wedge [(p(0, 0) \wedge p(0, 1)) \vee p(1, 1)]$$

es decir,

$$(p(0, 0) \vee p(0, 1)) \wedge (p(0, 1) \vee p(1, 0)) \wedge (p(0, 0) \vee p(1, 1)) \wedge (p(0, 1) \vee p(1, 1))$$

(e) La proposición con cuantificadores $\exists y\, [\exists x : p(x, y)]$ puede expandirse a:

$$[\exists x : p(x, 0)] \vee [\exists x : p(x, 1)]$$

que es equivalente a la proposición,

$$p(0, 0) \vee p(1, 0) \vee p(0, 1) \vee p(1, 1)$$

■

2.2.4 Valor de verdad del cuantificador existencial

Sea $p(x)$ un predicado de variable x que toma valores en un universo del discurso $\mathscr{U}$.

- ⁕ *$\exists x : p(x)$ es verdadera, si el predicado $p(x)$ se transforma en una proposición verdadera para, al menos, uno de los valores de x en $\mathscr{U}$.*
- ⁕ *$\exists x : p(x)$ es falsa, si el predicado $p(x)$ se transforma en una proposición falsa para todos los valores de x en $\mathscr{U}$.*

Ejemplo 2.8

Estudiar en el conjunto de los números enteros, el valor de verdad de las afirmaciones siguientes:

(a) $\exists n : n = 5$

(b) $\exists n : n = n + 1$

Solución

(a) $\exists n : n = 5$

En efecto, en el universo de los números enteros, uno de los elementos es el 5, luego tomando $a = 5$, tendremos que hay, al menos, un valor de n en $\mathbb{Z}$ que hace que el predicado $n = 5$ se transforme en una proposición verdadera, luego por 2.2.4, la proposición

$$\exists n : n = 5$$

es verdadera.

(b) Probaremos que la proposición $\exists n : n = n + 1$ es falsa.

En efecto, sea a cualquier número entero. La ecuación $a = a+1$ no tiene solución, ya que eso significaría que $0 = 1$ lo que, obviamente, no es cierto.

Por tanto, el predicado $n = n + 1$ se transforma en una proposición falsa para todos y cada uno de los números enteros y, consecuentemente, por 2.2.4,

$$\exists n : n + 1$$

es una proposición falsa.

■

2.2.5 Valores de verdad. Resumen

El siguiente cuadro resume los valores de verdad de las proposiciones con cuantificadores. $\mathscr{U}$ será un universo del discurso cualquiera, x cualquiera de $\mathscr{U}$ y $p(x)$ cualquier predicado.

$\forall x, p(x)$	Es **verdad**, si $p(x)$ se transforma en una proposición verdadera para todos y cada uno de los valores de x en $\mathscr{U}$.	Es **falsa**, si $p(x)$ se transforma en una proposición falsa para, al menos, un valor de x en $\mathscr{U}$.
$\exists x : p(x)$	Es **verdad**, si $p(x)$ se transforma en una proposición verdadera para, al menos, un valor de x en $\mathscr{U}$.	Es **falsa**, si $p(x)$ se transforma en una proposición falsa para todos y cada uno de los valores de x en $\mathscr{U}$.

■

Ejemplo 2.9

Estudiar el valor de verdad de las siguientes proposiciones:

(a) Dado cualquier número entero, siempre puede encontrarse otro tal que el producto de ambos sea cero.

(b) ¿Puede encontrarse un número entero tal que su producto por todos los demás sea 1*?*

(c) ¿Existe, al menos, un número entero que al multiplicarlo por todos los demás, los deje igual?

Solución

Sea $\mathscr{U}$ el conjunto, $\mathbb{Z}$, de los números enteros.

(a) Dado cualquier número entero, siempre puede encontrarse otro tal que el producto de ambos sea cero.

Primero escribimos la proposición en lenguaje simbólico,

$$\forall n_1, [\exists n_2 : (n_1 \cdot n_2 = 0)]$$

y ahora estudiamos su valor de verdad.

Según el valor de verdad del cuantificador universal, $\forall n_1, [\exists n_2 : (n_1 \cdot n_2 = 0)]$ es verdad si la proposición $\exists n_2 : (n_1 \cdot n_2 = 0)$ es verdadera para todos y cada uno de los valores que n_1 pueda tomar en $\mathbb{Z}$. Pues bien, sea a cualquiera de esos valores, es decir cualquier número entero. Entonces, por el valor de verdad del cuantificador existencial, $\exists n_2 : (a \cdot n_2 = 0)$ es verdad si existe, al menos, un valor de n_2 en $\mathbb{Z}$ para el cual el predicado $a \cdot n_2 = 0$ se transforme en una proposición verdadera.

Obviamente, este valor existe ya que bastaría tomar $n_2 = 0$ y, por lo tanto, $\exists n_2 : (a \cdot n_2 = 0)$ sería una proposición verdadera para todos y cada uno de los números enteros y, consecuentemente, la proposición propuesta, $\forall n_1, [\exists n_2 : (n_1 \cdot n_2 = 0)]$, es verdadera.

(b) ¿Puede encontrarse un número entero tal que su producto por todos los demás sea 1?

Cuantificamos la proposición,

$$\exists n_1 : [\forall n_2, (n_1 \cdot n_2 = 1)]$$

y estudiamos su valor de verdad.

Por el valor de verdad del cuantificador existencial, $\exists n_1 : [\forall n_2, (n_1 \cdot n_2 = 1)]$ será falsa si la proposición $\forall n_2 \, (n_1 \cdot n_2 = 1)$ es falsa para todos y cada uno de los valores que n_1 pueda tomar en $\mathbb{Z}$. Pues bien, sea a cualquier número entero. Por el valor de verdad del cuantificador universal, $\forall n_2, (a \cdot n_2 = 1)$ es falsa si podemos encontrar, al menos, un valor de n_2 en $\mathbb{Z}$ para el que el predicado $a \cdot n_2 = 1$ se transforme en una proposición falsa.

Bastaría tomar n_2 como cualquier entero distinto de 1 para que la proposición $\forall n_2, (a \cdot n_2 = 1)$ fuera falsa para todos y cada uno de los números enteros y, consecuentemente, la proposición propuesta $\exists n_1 : [\forall n_2, (n_1 \cdot n_2 = 1)]$ será falsa.

(c) ¿Existe, al menos, un número entero que al multiplicarlo por todos los demás, los deje igual?

Escribiendo la proposición en notación simbólica,

$$\exists n_1 : [\forall n_2, (n_2 \cdot n_1 = n_2)]$$

Esta proposición será verdadera si hay, al menos, un valor de n_1 en $\mathbb{Z}$ que transforme el predicado $n_2 \cdot n_1 = n_2$ en una proposición verdadera para todos y cada uno de los valores que n_2 pueda tomar en $\mathbb{Z}$.

Pues bien, sea a cualquier número entero, como $a \cdot 1 = a$, la proposición $\forall n_2, (n_2 \cdot 1 = n_2)$ es verdadera y ahora bastaría tomar $n_1 = 1$ para que la proposición propuesta, $\exists n_1 : [\forall n_2, (n_2 \cdot n_1 = n_2)]$ también lo sea.

■

En el ejemplo siguiente veremos como el orden en que se ligan las variables es vital y puede afectar profundamente el significado de una afirmación.

Ejemplo 2.10

Evaluar las siguientes proposiciones en el universo de los números enteros:

(a) $\forall n_1, [\exists n_2 : (n_1 + n_2 = 0)]$

(b) $\exists n_2 : [\forall n_1, (n_1 + n_2 = 0)]$

Solución

(a) $\forall n_1, [\exists n_2 : (n_1 + n_2 = 0)]$.

Esta proposición será verdadera si $\exists n_2 : (n_1 + n_2 = 0)$ es verdad para cualquier valor que n_1 pueda tomar en $\mathbb{Z}$.

Pues bien, sea a cualquier entero, entonces $\exists n_2 : (a + n_2 = 0)$ es verdad, si podemos encontrar un número entero, n_2, que transforme el predicado $a + n_2 = 0$ en una proposición verdadera.

Obviamente, bastaría tomar $n_2 = -a$ para que $a + n_2 = 0$, luego $\exists n_2 : (a + n_2 = 0)$ es verdad para cualquier entero y, consecuentemente, $\forall n_1, [\exists n_2 : (n_1 + n_2 = 0)]$ es verdad.

(b) $\exists n_2 : [\forall n_1, (n_1 + n_2 = 0)]$.

Esta proposición dice que hay, al menos, un número entero que al sumarlo con todos los demás da cero, lo cual, obviamente, es falso. Analicemos en profundidad por qué.

La proposición $\exists n_2 : [\forall n_1, (n_1 + n_2 = 0)]$ es falsa si $\forall n_1, (n_1 + n_2 = 0)$ es falsa para cualquier valor que n_2 pueda tomar en $\mathbb{Z}$.

Pues bien, sea a cualquier número entero, entonces $\forall n_1, (n_1 + a = 0)$ es falsa si podemos encontrar, al menos, un valor de n_1 en $\mathbb{Z}$ que transforme el predicado $n_1 + a = 0$ en una proposición falsa, para lo cual bastaría con tomar n_1 como cualquier entero distinto de $-a$. Por lo tanto, $\forall n_1, (n_1 + a = 0)$ es falsa para cualquier entero, a, y, consecuentemente, $\exists n_2 : [\forall n_1, (n_1 + n_2 = 0)]$ es falsa.

■

Ejemplo 2.11

En el universo, $\mathbb{R}$*, de los números reales, consideramos los predicados:*

$p(x) : x \geqslant 0$

$q(x) : (x - 2)(x + 3) = 0$

$r(x) : x^2 - 5 > 0$

Estudiar el valor de verdad de las siguientes proposiciones:

(a) $\exists x : [p(x) \wedge q(x)]$

(b) $\forall x, [q(x) \vee r(x)]$

Solución

(a) $\exists x : [p(x) \wedge q(x)]$

Esta proposición será verdadera si encontramos, al menos, un número real, a, que transforme el predicado $p(x) \wedge q(x)$ en una proposición verdadera.

Pues bien, si $p(a) \wedge r(a)$ es verdad, entonces por el valor de verdad de la conjunción tendremos que

$$p(a) \text{ es verdad } \wedge q(a) \text{ es verdad}$$

es decir,

$$a \geqslant 0 \wedge [(a-2)(a+3) = 0]$$

o sea,

$$a \geqslant 0 \wedge [(a-2=0) \vee (a+3=0)]$$

de donde, por la distributividad de la conjunción respecto a la disyunción, se sigue que

$$(a \geqslant 0 \wedge a = 2) \vee (a \geqslant 0 \wedge a = -3)$$

y como el segundo de los paréntesis es una contradicción, por las leyes de identidad, resulta

$$a = 2$$

Luego, en efecto, hay al menos un valor de x en $\mathbb{R}$, $x = 2$, que transforma el predicado $p(x) \wedge q(x)$ en una proposición, $p(2) \wedge q(2)$, verdadera y, consecuentemente, la proposición $\exists x : [p(x) \wedge q(x)]$ es verdad.

(b) $\forall x, [q(x) \vee r(x)]$

Esta proposición será verdadera si el predicado $q(x) \vee r(x)$ se transforma en una proposición verdadera para cualquier número real y será falsa si hay, al menos, un valor de x en $\mathbb{R}$ que haga que los predicados $q(x)$ y $r(x)$ se transformen, ambos, en proposiciones falsas.

Sea a, pues, un número real arbitrario. Entonces, $q(a) \vee r(a)$ es verdad si al menos una de las dos proposiciones, $q(a)$ o $r(a)$, es verdadera. Pues bien,

$$\begin{aligned} q(a) \text{ es verdadera} &\iff (a-2)(a+3) = 0 \\ &\iff a-2=0 \text{ ó } a+3=0 \\ &\iff a = 2 \text{ o } a = -3 \end{aligned}$$

$$\begin{aligned} r(a) \text{ es verdadera} &\iff a^2 - 5 > 0 \\ &\iff a > \pm\sqrt{5} \\ &\iff a < -\sqrt{5} \text{ o } a > \sqrt{5} \end{aligned}$$

Pero, si tomamos un valor de x en $\mathbb{R}$ que sea

$$x \neq 2 \text{ y } x \neq -3 \text{ y } -\sqrt{5} \leqslant x \leqslant \sqrt{5}$$

tendríamos que tanto $p(x)$ como $r(x)$ serían falsas para ese x.

Por ejemplo, si x es igual a 1, tendremos que $p(1)$ es falsa y $r(1)$ también, por lo tanto, hemos encontrado un valor de x en $\mathbb{R}$ (hay muchos más) que transforma el predicado $p(x) \vee r(x)$ en una proposición falsa y, consecuentemente, la proposición $\forall x, [q(x) \vee r(x)]$ es falsa.

■

2.3 Cálculo de Predicados

La versión de la lógica que trata con proposiciones cuantificadas se llama *lógica de predicados.* La introducción de cuantificadores no sólo amplía la fuerza expresiva de las proposiciones que se pueden construir, sino que también permite elaborar principios lógicos que explican el razonamiento seguido en casi todas las demostraciones matemáticas.

Una transcripción cuidadosa de los desarrollos matemáticos incluyen, a menudo, cuantificadores, predicados y operadores lógicos.

Ejemplo 2.12

Consideremos como universo del discurso el conjunto de los números enteros y sean los predicados,

$p(n)$: *n es no negativo.*

$q(n)$: *n es par.*

$r(n)$: *n es impar.*

$s(n)$: *n es primo.*

Expresar en notación lógica las siguientes afirmaciones:

(a) Existe un entero par.

(b) Todo número entero es par o impar.

(c) Todos los números primos son no negativos.

(d) El único número primo par es el 2.

(e) No todos los enteros son pares.

(f) No todos los primos son impares.

(g) Si un entero no es impar, entonces es par.

Solución

(a) Existe un entero par.

$$\exists n : q(n)$$

(b) Todo número entero es par o impar.

$$\forall n, [q(n) \vee r(n)]$$

(c) Todos los números primos son no negativos.

$$\forall n, [s(n) \longrightarrow p(n)]$$

(d) El único número primo par es el 2.

$$\forall n, [s(n) \wedge q(n) \longrightarrow n = 2]$$

(e) No todos los enteros son pares.

$$\neg\,[\forall n, q(n)]$$

(f) No todos los primos son impares.

$$\neg\forall n, [s(n) \longrightarrow r(n)]$$

(g) Si un entero no es impar, entonces es par.

$$\forall n, [\neg r(n) \longrightarrow q(n)]$$

Obsérvese que en el ejemplo anterior, los cuantificadores están al comienzo de cada afirmación. Sin embargo, no siempre es así, los cuantificadores pueden ir en cualquier parte y su situación es importante. Los ejemplos anteriores ilustran la gran variedad de formas en las que pueden hacerse afirmaciones que contengan predicados, cuantificadores y operadores lógicos.

Nota 2.2 El valor de verdad de una proposición compuesta depende, generalmente, del conjunto universal donde las variables ligadas están cuantificadas. Sin embargo, existen ejemplos importantes donde el valor de verdad no depende ni del universo del discurso ni de los valores que las variables tomen en el mismo.

2.3.1 Leyes de De Morgan generalizadas

Constituyen una clase importante de equivalencias lógicas y son las siguientes:

$\boxed{1}$ $\neg\forall x, p(x) \Longleftrightarrow \exists x : \neg p(x)$

$\boxed{2}$ $\neg\exists x : p(x) \Longleftrightarrow \forall x, \neg p(x)$

$\boxed{3}$ $\forall x, p(x) \Longleftrightarrow \neg\exists x : \neg p(x)$

$\boxed{4}$ $\exists x : p(x) \Longleftrightarrow \neg\forall x, \neg p(x)$

Demostración

Sea $\mathscr{U}$ un universo del discurso arbitrario, $p(x)$ un predicado cualquiera, y x cualquiera de $\mathscr{U}$.

Veamos que en todos los casos las dos proposiciones tienen los mismos valores de verdad.

$\boxed{1}$ $\neg\forall x, p(x) \Longleftrightarrow \exists x : \neg p(x)$

$\Rightarrow$) $\neg\forall x, p(x) \Longrightarrow \exists x : \neg p(x)$

En efecto, si $\neg\forall x, p(x)$ es verdad, entonces $\forall x, p(x)$ es falso, luego habrá, al menos, un valor de x en $\mathscr{U}$, digamos a, tal que la proposición $p(a)$ sea falsa, o lo que es igual para el que $\neg p(a)$ sea verdadera.

Hemos encontrado, pues, un valor de x en $\mathscr{U}$ que hace que el predicado $\neg p(x)$ se transforme en una proposición verdadera, luego entonces la proposición $\exists x : \neg p(x)$ es verdad.

$\Leftarrow$) $\exists x : \neg p(x) \Longrightarrow \neg\forall x, p(x)$

Recíprocamente, si $\exists x : \neg p(x)$ es verdad, entonces hay, al menos, un valor de x en $\mathscr{U}$, digamos a, tal que $\neg p(a)$ es verdad y, por lo tanto, $p(a)$ falsa.

Existe, pues, al menos, un valor de x en $\mathscr{U}$ que hace que el predicado $p(x)$ se transforme en una proposición falsa, luego $\forall x, p(x)$ es falsa y, consecuentemente, su negación, $\neg\forall x, p(x)$, verdadera.

2 $\neg\exists x : p(x) \Longleftrightarrow \forall x, \neg p(x)$

$\Rightarrow$) $\neg\exists x : p(x) \Longrightarrow \forall x, \neg p(x)$

Si $\neg\exists x : p(x)$ es verdad, entonces $\exists x : p(x)$ es falsa, luego $p(x)$ se transforma en una proposición falsa para todos y cada uno de los valores de x en $\mathscr{U}$ y, consecuentemente, $\neg p(x)$ se transformará en una proposición verdadera para esos mismos valores y, por lo tanto, $\forall x, \neg p(x)$ es verdad.

$\Leftarrow$) $\forall x, \neg p(x) \Longrightarrow \neg\exists x : p(x)$

Recíprocamente, si $\forall x, \neg p(x)$ es verdad, entonces $\neg p(x)$ se transforma en una proposición verdadera para todos los valores que x pueda tomar en $\mathscr{U}$ y, por lo tanto, $p(x)$ se transformará en una proposición falsa para esos valores.

Pues bien, como el predicado $p(x)$ se transforma en una proposición falsa para todos y cada uno de los valores de x en $\mathscr{U}$, tendremos que $\exists x : p(x)$ es falsa y, consecuentemente, $\neg\exists x : p(x)$ es verdad.

3 $\forall x, p(x) \Longleftrightarrow \neg\exists x : \neg p(x)$

$\Rightarrow$) $\forall x, p(x) \Longrightarrow \neg\exists x : \neg p(x)$

Si $\forall x, p(x)$ es verdad, entonces $p(x)$ se transforma en una proposición verdadera para cualquier valor de x en $\mathscr{U}$ y, por lo tanto, $\neg p(x)$ se transformará en una proposición falsa para esos mismos valores de x.

Pues bien, si $\neg p(x)$ se transforma en una proposición falsa para todos y cada uno de los valores de x en $\mathscr{U}$, entonces $\exists x : \neg p(x)$ será falsa y, consecuentemente, su negación, $\neg\exists x : \neg p(x)$, verdadera.

$\Leftarrow$) $\neg\exists x : \neg p(x) \Longrightarrow \forall x, p(x)$

Recíprocamente, si $\neg\exists x : \neg p(x)$ es verdad, entonces $\exists x : \neg p(x)$ es falsa y, por lo tanto, el predicado $\neg p(x)$ se transforma en una proposición falsa para todos y cada uno de los valores de x en $\mathscr{U}$ y $p(x)$ en una proposición verdadera para esos mismos valores.

Como el predicado $p(x)$ se transforma en una proposición verdadera para todos los valores que pueda tomar x en $\mathscr{U}$, tendremos que $\forall x, p(x)$ será verdadera.

4 $\exists x : p(x) \Longleftrightarrow \neg\forall x, \neg p(x)$

$\Rightarrow$) $\exists x : p(x) \Longrightarrow \neg\forall x, \neg p(x)$

En efecto, si $\exists x : p(x)$ es verdad, entonces $p(x)$ se transforma en una proposición verdadera para algún valor de x, digamos a, en $\mathscr{U}$. Entonces, $\neg p(a)$ será una proposición falsa y, por tanto, habrá, al menos, un valor de x en $\mathscr{U}$ que transforma el predicado $\neg p(x)$ en una proposición falsa. Consecuentemente, $\forall x, \neg p(x)$ es falsa y, por lo tanto, su negación, $\neg\forall x, \neg p(x)$, verdadera.

$\Leftarrow$) $\neg\forall x, \neg p(x) \Longrightarrow \exists x : p(x)$

Recíprocamente, si $\neg\forall x, \neg p(x)$ es verdad, entonces $\forall x, \neg p(x)$ será falsa y, por lo tanto, habrá, al menos, un valor de x, digamos a, en $\mathscr{U}$ que transforme el predicado $\neg p(x)$ en una proposición falsa y su negación, $p(a)$, en verdadera.

Hemos encontrado, pues, un valor de x en $\mathscr{U}$ $(x = a)$ que hace al predicado $p(x)$ una proposición verdadera lo cual significa que $\exists x : p(x)$ es verdad.

■

Nota 2.3 Obsérvese que según lo que acabamos de probar, la primera de las leyes de De Morgan generalizadas es cierta para cualquier predicado luego, en particular, será cierta para su negación, $\neg p(x)$. Entonces,

$$\neg\forall x, \neg p(x) \Longleftrightarrow \exists x : \neg\neg p(x)$$

y si sustituimos $\neg\neg p(x)$ por $p(x)$, resulta

$$\neg\forall x, \neg p(x) \Longleftrightarrow \exists x : p(x)$$

que es la cuarta ley de De Morgan, de la cual, negando ambos miembros, y en virtud de la equivalencia lógica entre una proposición y su contrarrecíproca, obtenemos,

$$\neg\neg\forall x, \neg p(x) \Longleftrightarrow \neg\exists x : p(x)$$

es decir,

$$\forall x, \neg p(x) \Longleftrightarrow \neg\exists x : p(x)$$

que es la segunda ley de De Morgan. Si ahora se la aplicamos a $\neg p(x)$, obtendremos

$$\forall x, \neg\neg p(x) \Longleftrightarrow \neg\exists x : \neg p(x)$$

o sea,

$$\forall x, p(x) \Longleftrightarrow \neg\exists x : \neg p(x)$$

que es la tercera ley de De Morgan.

■

Nota 2.4 Las leyes de De Morgan generalizadas pueden utilizarse repetidamente para negar cualquier proposición con cuantificadores.

Por ejemplo, podemos utilizarlas para negar la proposición

$$\exists w : [\forall x, (\exists y : (\exists z : p(w, x, y, z)))]$$

En efecto,

$$\begin{aligned}
\neg\exists w : [\forall x, (\exists y : (\exists z : p(w, x, y, z)))] &\Longleftrightarrow \forall w, [\neg\forall x, (\exists y : (\exists z : p(w, x, y, z)))] && \{\text{Segunda ley}\} \\
&\Longleftrightarrow \forall w, [\exists x : (\neg\exists y : (\exists z : p(w, x, y, z)] && \{\text{Primera ley}\} \\
&\Longleftrightarrow \forall w, [\exists x : (\forall y, (\neg\exists z : p(w, x, y, z)))] && \{\text{Segunda ley}\} \\
&\Longleftrightarrow \forall w, [\exists x : (\forall y, (\forall z, \neg p(w, x, y, z)))] && \{\text{Segunda ley}\}
\end{aligned}$$

■

De lo dicho en la nota anterior podemos extraer una regla general para negar cualquier proposición con cuantificadores.

2.3.2 Regla general

La negación de una proposición con cuantificadores es lógicamente equivalente a la proposición que se obtiene sustituyendo cada $\forall$ por $\exists$, cada $\exists$ por $\forall$ y reemplazando el predicado por su negación.

■

2.3.3 Proposiciones al alcance de un cuantificador

Si una proposición está dentro del alcance de un cuantificador mediante una conjunción o una disyunción, entonces puede situarse fuera del alcance del mismo.

1. $\forall x, [p(x) \vee q] \iff [\forall x, p(x)] \vee q$
2. $\exists x : [p(x) \vee q] \iff [\exists x : p(x)] \vee q$
3. $\exists x : [p(x) \wedge q] \iff [\exists x : p(x)] \wedge q$
4. $\forall x, [p(x) \wedge q] \iff [\forall x, p(x)] \wedge q$

Demostración

Supondremos que $\mathscr{U}$ es un universo del discurso arbitrario, $p(x)$ será cualquier predicado, x un elemento cualquiera de $\mathscr{U}$ y q una proposición cualquiera.

1.– $\forall x, [p(x) \vee q] \iff [\forall x, p(x)] \vee q$.

$\Rightarrow$) $\forall x, [p(x) \vee q] \Longrightarrow [\forall x, p(x)] \vee q$
Si la proposición $\forall x\, [p(x) \vee q]$ es verdad, entonces el predicado $p(x) \vee q$ se transforma en una proposición verdadera para todos los valores de x en $\mathscr{U}$ luego una de las dos proposiciones ha ser verdad para todo x.

- Si el predicado $p(x)$ se transforma en una proposición verdadera para todos los valores de x en $\mathscr{U}$, entonces $\forall x, p(x)$ es verdad y, consecuentemente $[\forall x, p(x)] \vee q$ es verdad.
- Si q es verdad, entonces $[\forall x, p(x)] \vee q$ es verdad independientemente del valor de verdad de la proposición $\forall x, p(x)$.

luego $[\forall x, p(x)] \vee q$ es verdad en cualquier caso.

$\Leftarrow$) $[\forall x, p(x)] \vee q \Longrightarrow \forall x, [p(x) \vee q]$
Si $[\forall x, p(x)] \vee q$ es verdad, entonces una de las dos proposiciones, al menos, ha de ser verdad.

- Si $\forall x, p(x)$ es verdad, entonces $p(x)$ se transforma en una proposición verdadera para cualquier x que tomemos en $\mathscr{U}$ y, por lo tanto, $p(x) \vee q$ será una proposición verdadera para todos esos x.
- Si q es verdad, entonces el predicado $p(x) \vee q$ será una proposición verdadera independientemente de quien sea x.

Por lo tanto, en ambos casos $p(x) \vee q$ se transforma en proposición verdadera para cualquier x en $\mathscr{U}$ y, consecuentemente, $\forall x, [p(x) \vee q]$ es verdad.

2.– $\exists x : [p(x) \vee q] \iff [\exists x : p(x)] \vee q$.

$\Rightarrow$) $\exists x : [p(x) \vee q] \Longrightarrow [\exists x : p(x)] \vee q$
Si la proposición $\exists x : [p(x) \vee q]$ es verdad, entonces existirá, al menos, un valor de x, digamos a, en $\mathscr{U}$, para el cual la proposición $p(a) \vee q$ sea verdad, luego una de las dos proposiciones, al menos, ha de ser verdad.

- Si $p(a)$ es verdad, entonces hay, al menos, un valor de x ($x = a$) en $\mathscr{U}$ que hace del predicado $p(x)$ una proposición verdadera, luego $\exists x : p(x)$ es verdad y, consecuentemente, $[\exists x : p(x)] \vee q$ también lo es.
- Si q es verdad, entonces la proposición $[\exists x : p(x)] \vee q$ también es verdad independientemente del valor de verdad de $\exists x : p(x)$.

Por lo tanto, en cualquier caso, $[\exists x : p(x)] \vee q$ es verdad.

$\Leftarrow$) $[\exists x : p(x)] \vee q \Longrightarrow \exists x : [p(x) \vee q]$

Si $[\exists x : p(x)] \vee q$ es verdad, entonces una de las dos proposiciones, al menos, ha de ser verdadera.

- Si $\exists x : p(x)$ es verdad, entonces podremos encontrar un a en $\mathscr{U}$ que transforme el predicado $p(x)$ en una proposición verdadera y, consecuentemente, $p(a) \vee q$ será verdad independientemente del valor de verdad que tenga q. Así pues, existe al menos un valor de x en $\mathscr{U}$ que hace que el predicado $p(x) \vee q$ sea una proposición verdadera, es decir, $\exists x : [p(x) \vee q]$ es verdad.
- Si q es verdad, entonces el predicado $p(x) \vee q$ será una proposición verdadera para cualquier valor de x que tomemos en $\mathscr{U}$, por lo tanto, $\exists x : [p(x) \vee q]$ es verdad.

Consecuentemente $\exists x : [p(x) \vee q]$ es verdad en cualquier caso.

3.– $\exists x : [p(x) \wedge q] \Longleftrightarrow [\exists x : p(x)] \wedge q$.

Para probar esta equivalencia podemos seguir un método similar al utilizado en los apartados anteriores, aunque lo haremos de otra forma.

En efecto, según hemos visto en 1.–, la equivalencia,

$$\forall x, [p(x) \vee q] \Longleftrightarrow [\forall x, p(x)] \vee q$$

es cierta para cualquier predicado $p(x)$ y cualquier proposición q, por tanto también será cierta para sus negaciones, es decir,

$$\forall x, [\neg p(x) \vee \neg q] \Longleftrightarrow [\forall x, \neg p(x)] \vee \neg q$$

Si ahora negamos ambos miembros,

$$\neg \forall x, [\neg p(x) \vee \neg q] \Longleftrightarrow \neg \left([\forall x, \neg p(x)] \vee \neg q \right)$$

aplicamos las leyes de De Morgan en el segundo miembro

$$\neg \forall x, [\neg p(x) \vee \neg q] \Longleftrightarrow [\neg \forall x, \neg p(x)] \wedge q$$

y las leyes de De Morgan generalizadas,

$$\exists x : \neg \left[\neg (p(x) \vee \neg q] \Longleftrightarrow [\exists x : \neg \neg p(x)] \wedge q \right.$$

es decir,

$$\exists x : [\neg \neg p(x) \wedge \neg \neg q] \Longleftrightarrow [\exists x : p(x)] \wedge q$$

y, consecuentemente,

$$\exists x : [p(x) \wedge q] \Longleftrightarrow [\exists x : p(x)] \wedge q$$

4.– $\forall x, [p(x) \wedge q] \Longleftrightarrow [\forall x, p(x)] \wedge q$.

Lo haremos utilizando el mismo método que en el apartado anterior, aunque partiremos de la equivalencia probada en 2. En efecto,

$$\exists x : [p(x) \vee q] \Longleftrightarrow [\exists x : p(x)] \vee q$$

y al ser esto cierto para cualquier predicado $p(x)$ y cualquier proposición q también lo será para sus negaciones, es decir,

$$\exists x : [\neg p(x) \vee \neg q] \Longleftrightarrow [\exists x : \neg p(x)] \vee \neg q$$

y si negamos ambos miembros,

$$\neg \exists x : [\neg p(x) \vee \neg q] \Longleftrightarrow \neg \left([\exists x : \neg p(x)] \vee \neg q \right)$$

aplicamos De Morgan al segundo,

$$\neg \exists x : [\neg p(x) \vee \neg q] \Longleftrightarrow [\neg \exists x : \neg p(x)] \wedge q$$

las Leyes de De Morgan generalizadas,

$$\forall x, \neg\left[\neg p(x) \vee \neg q\right] \Longleftrightarrow \left[\forall x, \neg\neg p(x)\right] \wedge q$$

y, nuevamente, De Morgan,

$$\forall x, \left[\neg\neg p(x) \wedge \neg\neg q\right] \Longleftrightarrow \left[\forall x, p(x)\right] \wedge q$$

obtendremos,

$$\forall x, \left[p(x) \wedge q\right] \Longleftrightarrow \left[\forall x, p(x)\right] \wedge q$$

■

2.3.4 Asociatividad y Distributividad

1. $\forall x, [p(x) \wedge q(x)] \Longleftrightarrow [\forall x, p(x)] \wedge [\forall x, q(x)]$
2. $\exists x : [p(x) \wedge q(x)] \Longrightarrow [\exists x : p(x)] \wedge [\exists x : q(x)]$
3. $\exists x : [p(x) \vee q(x)] \Longleftrightarrow [\exists x : p(x)] \vee [\exists x : q(x)]$
4. $[\forall x, p(x)] \vee [\forall x, q(x)] \Longrightarrow \forall x, [p(x) \vee q(x)]$

Demostración

Sea $\mathscr{U}$ un universo del discurso cualquiera y $p(x), q(x)$ dos predicados arbitrarios, siendo x cualquier elemento de $\mathscr{U}$

1. $\forall x, [p(x) \wedge q(x)] \Longleftrightarrow [\forall x, p(x)] \wedge [\forall x, q(x)]$

   $\Rightarrow$) $\forall x, [p(x) \wedge q(x)] \Longrightarrow [\forall x, p(x)] \wedge [\forall x, q(x)]$

   En efecto, si la proposición $\forall x\,[p(x) \wedge q(x)]$ es verdad, entonces el predicado $p(x) \wedge q(x)$ se transforma en una proposición verdadera para todos y cada uno de los valores de x en $\mathscr{U}$ luego, tanto $p(x)$ como $q(x)$ se transformarán en proposiciones verdaderas para todos esos valores de x y, consecuentemente, las proposiciones $\forall x, p(x)$ y $\forall x, q(x)$ serán, ambas, verdaderas y, por lo tanto, su conjunción, $[\forall x, p(x)] \wedge [\forall x, p(x)]$, también.

   $\Leftarrow$) $[\forall x, p(x)] \wedge [\forall x, q(x)] \Longrightarrow \forall x\,[p(x) \wedge q(x)]$

   Recíprocamente, si la proposición $[\forall x, p(x)] \wedge [\forall x, q(x)]$ es verdadera, entonces las proposiciones $[\forall x, p(x)]$ y $[\forall x, q(x)]$ han de ser, ambas, verdaderas. Pues bien,

   - si $[\forall x, p(x)]$ es verdad, entonces el predicado $p(x)$ se transforma en proposición verdadera para todos y cada uno de los valores de x en $\mathscr{U}$.
   - Si $[\forall x, q(x)]$ es verdad, el predicado $q(x)$ se transforma en proposición verdadera para cualquier valor de x en $\mathscr{U}$.

   Por lo tanto, el predicado $p(x) \wedge q(x)$ se transforma en proposición verdadera para todos y cada uno de los valores de x en $\mathscr{U}$ y, consecuentemente, $\forall x\,[p(x) \wedge q(x)]$ es verdadera.

La relación anterior suele enunciarse informalmente diciendo que "*el cuantificador universal es asociativo respecto del conectivo lógico conjunción.*"

2. $\exists x : [p(x) \wedge q(x)] \Longrightarrow [\exists x : p(x)] \wedge [\exists x : q(x)]$

   Veamos que si la primera de las proposiciones es verdad, entonces la segunda también lo es. En efecto si la proposición $\exists x : [p(x) \wedge q(x)]$ es verdadera, entonces ha de existir, al menos, un valor de x, digamos a, en $\mathscr{U}$ tal que el predicado $p(x) \wedge q(x)$ se convierta en una proposición verdadera para ese valor de x, es decir, $p(a) \wedge q(a)$ es verdadera.

   Entonces, ambas proposiciones, $p(a)$ y $q(a)$ han de ser verdaderas y habremos encontrado un valor de x $(x = a)$ en $\mathscr{U}$ para el cual tanto $p(x)$ como $q(x)$ se transforman, ambos, en proposiciones verdaderas. Por lo tanto, $\exists x : p(x)$ es verdad y $\exists x : q(x)$ también lo es, de aquí que la conjunción de ambas proposiciones, $[\exists x : p(x)] \wedge [\exists x : q(x)]$, también lo sea.

   Veamos que, sin embargo, no se da la equivalencia lógica como en el apartado anterior, es decir, el recíproco no es cierto o lo que es igual,

   $$[\exists x : p(x)] \wedge [\exists x : q(x)] \not\Longrightarrow \exists x : [p(x) \wedge q(x)]$$

   En efecto, si la proposición $[\exists x : p(x)] \wedge [\exists x : q(x)]$ es verdad, entonces $[\exists x : p(x)]$ es verdad y $[\exists x : q(x)]$ también lo es. Ahora bien,

   - si $\exists x : p(x)$ es verdad, entonces existe, al menos, un valor de x, digamos a, en $\mathscr{U}$ que transforma al predicado $p(x)$ en una proposición, $p(a)$, verdadera.
   - Si $\exists x : q(x)$ es verdad, entonces existe, al menos, un valor de x, digamos b, en $\mathscr{U}$ que transforma al predicado $q(x)$ en una proposición, $q(b)$, verdadera.

   Pero el hecho de que $p(a)$ sea verdadera no significa que $q(a)$ lo sea, es decir no sabemos que valor de verdad tiene $p(a) \wedge q(a)$ y lo mismo pasaría con $p(b) \wedge q(b)$. Por lo tanto, no podemos asegurar que exista, al menos, un valor de x, sea a o sea b, en $\mathscr{U}$ que haga que el predicado $p(x) \wedge q(x)$ se transforme en una proposición verdadera, de aquí que no podemos deducir nada sobre el valor de verdad de la proposición $\exists x : [p(x) \wedge q(x)]$ y, consecuentemente, no haya implicación lógica.

   Veamos un contraejemplo que pone de manifiesto lo que decimos. Supongamos que $\mathscr{U}$ es el conjunto de los números enteros y sean los predicados,

   $p(x) : x$ *es un número par*

   $q(x) : x$ *es un número impar*

   Entonces, la proposición,

   $$[\exists x : p(x)] \wedge [\exists x : q(x)]$$

   significaría que existe, al menos, un número entero que es par y también existe, al menos, un entero que es impar, lo cual, evidentemente, es verdad. Por otra parte, la proposición,

   $$\exists x : [p(x) \wedge q(x)]$$

   significa que hay, al menos, un número entero que es, al mismo tiempo, par e impar, lo cual es falso. Por lo tanto, la veracidad de la conclusión no se sigue de la veracidad de la hipótesis y no habría, consecuentemente, implicación lógica, es decir,

   $$[\exists x : p(x)] \wedge [\exists x : q(x)] \not\Longrightarrow \exists x : [p(x) \wedge q(x)]$$

3. $\exists x : [p(x) \vee q(x)] \Longleftrightarrow [\exists x : p(x)] \vee [\exists x : q(x)]$

   Aunque podemos probarlo con un método similar al utilizado en primer apartado, lo haremos de otra forma. En efecto, en el apartado 1., hemos visto que

   $$\forall x, [p(x) \wedge q(x)] \Longleftrightarrow [\forall x, p(x)] \wedge [\forall x, q(x)]$$

   siendo cierto este resultado para cualquier predicado, luego también lo será para sus negaciones, es decir,

   $$\forall x, [\neg p(x) \wedge \neg q(x)] \Longleftrightarrow [\forall x, \neg p(x)] \wedge [\forall x, \neg q(x)]$$

negando ahora ambos miembros, resulta

$$\neg\forall x, [\neg p(x) \wedge \neg q(x)] \Longleftrightarrow \neg\left[(\forall x, \neg p(x)) \wedge (\forall x, \neg q(x))\right]$$

así pues,

$$\exists x : \neg([\neg p(x) \wedge \neg q(x)]] \Longleftrightarrow [\neg\forall x, \neg p(x)] \vee [\neg\forall x, \neg q(x)]$$

es decir,

$$\exists x : [\neg\neg p(x) \vee \neg\neg q(x)] \Longleftrightarrow [\exists x : \neg\neg p(x)] \vee [\exists x : \neg\neg q(x)]$$

de aquí que

$$\exists x : [p(x) \vee q(x)] \Longleftrightarrow [\exists x : p(x)] \vee (\exists x : \ q(x)]$$

La relación anterior suele enunciarse informalmente diciendo que "*el cuantificador existencial es asociativo respecto del conectivo lógico disyunción*"

4. $[\forall x, p(x)] \vee [\forall x, q(x)] \Longrightarrow \forall x, [p(x) \vee q(x)]$

   Lo probaremos de forma similar al apartado anterior. En el apartado 2. vimos que

$$\exists x : [p(x) \wedge q(x)] \Longrightarrow [\exists x : p(x)] \wedge [\exists x : \ q(x)]$$

   Sustituyendo los predicados por sus negaciones,

$$\exists x : [\neg p(x) \wedge \neg q(x)] \Longrightarrow [\exists x : \neg p(x)] \wedge [\exists x : \neg q(x)]$$

   y aplicando la "contrarrecíproca", resulta

$$\neg\left([\exists x : \neg p(x)] \wedge [\exists x : \neg q(x)]\right) \Longrightarrow \neg\exists x : [\neg p(x) \wedge \neg q(x)]$$

   luego,

$$[\neg\exists x : \neg p(x)] \vee [\neg\exists x : \neg q(x)] \Longrightarrow \forall x \neg\left[\neg p(x) \wedge \neg q(x)\right]$$

   es decir,

$$[\forall x, \neg\neg p(x)] \vee [\forall x, \neg\neg q(x)] \Longrightarrow \forall x, [\neg\neg p(x) \vee \neg\neg q(x)]$$

   de donde se sigue que

$$[\forall x, p(x)] \vee [\forall x, q(x)] \Longrightarrow \forall x, [p(x) \vee q(x)]$$

   Por razones análogas a las del apartado 2. no se da la equivalencia lógica.

■

Ejemplo 2.13

Si $p(x)$ y $q(x)$ son dos predicados arbitrarios, siendo x cualquiera de un universo $\mathscr{U}$, probar que

$$\neg\forall x, (p(x) \longrightarrow q(x)) \Longleftrightarrow \exists x : (p(x) \wedge \neg q(x))$$

Solución

Veamos, primero, que $\neg\forall x, (p(x) \longrightarrow q(x)) \Longrightarrow \exists x : (p(x) \wedge \neg q(x))$.

En efecto, si $\neg\forall x, (p(x) \longrightarrow q(x))$ es verdad, entonces $\forall x, (p(x) \longrightarrow q(x))$ es falsa, lo cual significa por el valor de verdad del cuantificador universal que hay, al menos, un valor de x en $\mathscr{U}$ que transforma el predicado $p(x) \longrightarrow q(x)$ en una proposición falsa. A este valor concreto lo llamaremos a, es decir, $p(a) \longrightarrow q(a)$ es una proposición falsa. Entonces, por el valor de verdad del condicional, $p(a)$ será verdadera y $q(a)$ falsa, es decir, $\neg q(a)$ verdadera y, por lo tanto, $p(a) \wedge \neg q(a)$ será verdadera.

Hemos encontrado, pues, un valor de x en $\mathscr{U}$ que transforma el predicado $p(x) \wedge \neg q(x)$ en una proposición verdadera y eso significa, por el valor de verdad del cuantificador existencial, que $\exists x : (p(x) \wedge \neg q(x))$ es verdad.

Recíprocamente, si $\exists x : (p(x) \wedge \neg q(x))$ es verdad, entonces, por el valor de verdad del cuantificador existencial, hay, al menos, un valor de x en $\mathscr{U}$ que transforma el predicado $p(x) \wedge \neg q(x)$ en una proposición verdadera. A ese valor concreto de x lo llamaremos a, es decir, la proposición $p(a) \wedge \neg q(a)$ es verdad, de aquí que por el valor de verdad de la conjunción, $p(a)$ sea verdad $\neg q(a)$ también, es decir, $p(a)$ es verdad y $q(a)$ falsa, luego el valor de verdad del condicional asegura que la proposición $p(a) \longrightarrow q(a)$ es falsa.

Por lo tanto, hemos encontrado, al menos, un valor de x en el universo del discurso, $\mathscr{U}$, que transforma el predicado $p(x) \longrightarrow q(x)$ en una proposición falsa, es decir, la proposición $\forall x, (p(x) \longrightarrow q(x))$ es falsa y, consecuentemente, su negación, $\neg\forall x, (p(x) \longrightarrow q(x))$, será verdadera.

■

2.4 Razonamientos y Cuantificadores

En este apartado veremos algunos ejemplos de razonamientos con proposiciones cuantificadas. Los métodos de demostración de los mismos serán los que ya hemos estudiado en la lección anterior (1.5).

Ejemplo 2.14

Estudiar, en el universo de todos los alumnos de la Universidad de Cádiz, la validez del siguiente razonamiento.

> *Todos los alumnos de Informática estudian Matemática Discreta.*
> *Florinda es alumna de Informática.*
> *Por lo tanto, Florinda estudia Matemática Discreta.*

Solución

Sean

> $p(x)$: x es alumno de Informática.
> $q(x)$: x estudia Matemática Discreta.

y llamemos f a Florinda.

El razonamiento en forma simbólica sería:

$$[\forall x, (p(x) \longrightarrow q(x)) \wedge p(f)] \longrightarrow q(f)$$

Comprobaremos si es válido de varias formas.

1 Aplicando directamente la definición de implicación lógica.

En efecto, si la hipótesis, $[\forall x, (p(x) \longrightarrow q(x)) \wedge p(f)]$, es verdad, entonces, por el *valor de verdad de la conjunción*, las proposiciones $\forall x, (p(x) \longrightarrow q(x))$ y $p(f)$ serán, ambas, verdaderas.

Pues bien, si $\forall x, (p(x) \longrightarrow q(x))$ es verdad, por el *valor de verdad del cuantificador universal*, el condicional $p(x) \longrightarrow q(x)$ se transformará en una proposición verdadera para todos y cada uno de los elementos del universo y, en particular, será verdad para Florinda. Así pues, tendremos que la proposición $p(f) \longrightarrow q(f)$ es verdad y, como $p(f)$ es verdad, el *valor de verdad del condicional* asegura que $q(f)$ también tiene que serlo. La veracidad de la conclusión se sigue, pues, de la veracidad de la hipótesis, luego por la definición de *implicación lógica*,

$$[\forall x, (p(x) \longrightarrow q(x)) \wedge p(f)] \Longrightarrow q(f)$$

y, consecuentemente, el razonamiento es válido.

2 Comprobando que el condicional entre las dos proposiciones es una tautología.

Por 1.4.2 sabemos que si el condicional,

$$[\forall x, (p(x) \longrightarrow q(x)) \wedge p(f)] \longrightarrow q(f)$$

es una tautología, entonces

$$[\forall x, (p(x) \longrightarrow q(x)) \wedge p(f)] \Longrightarrow q(f)$$

Comprobemos, pues, que el condicional es tautología.

Por el valor de verdad del *condicional* será falso, únicamente, cuando siendo verdad la hipótesis, la conclusión sea falsa, por lo tanto si comprobamos que este caso no puede darse, concluiremos que es una tautología.

Podemos partir de que la hipótesis es verdadera y comprobar que la conclusión no puede ser falsa, algo que ya hemos hecho en el apartado anterior, así que lo haremos partiendo de que la conclusión es falsa y comprobando que, en tal caso, la hipótesis no puede ser verdadera.

Si la conclusión, $q(f)$, es falsa, entonces el valor de verdad de la hipótesis dependerá de las diferentes opciones que pueden presentarse para el predicado $p(x)$.

- $p(x)$ se transforma en proposición verdadera para cada x de $\mathscr{U}$, o sea $\forall x, p(x)$ es verdad.
  En este caso, y en particular, $p(f)$ sería verdad y, al ser falsa $q(f)$, el condicional $p(f) \longrightarrow q(f)$ sería falso. Hemos encontrado, pues, un valor de x en $\mathscr{U}$ que transforma el predicado $p(x) \longrightarrow q(x)$ en una proposición falsa luego $\forall x, (p(x) \longrightarrow q(x))$ es falsa.
- $\forall x, p(x)$ es falso. En tal caso, habrá, al menos, un valor de x en $\mathscr{U}$ que transforma $p(x)$ en una proposición falsa y tendríamos dos opciones:
  - si x es Florinda, entonces $p(f)$ sería falsa.
  - Si x no es Florinda, entonces $p(f)$ sería verdad y, razonando igual que en el caso anterior, la proposición $\forall x, (p(x) \longrightarrow q(x))$ sería falsa.
- $p(x)$ se transforma en proposición verdadera para, al menos, un valor de x en $\mathscr{U}$, es decir $\exists x : p(x)$ es verdad. Habría dos opciones:
  - si x es Florinda, entonces $p(f)$ es verdad y, al igual que en los casos anteriores, la proposición $\forall x, (p(x) \longrightarrow q(x))$ es falsa.
  - Si x no es Florinda, $p(f)$ ha de ser falsa.
- $\exists x : p(x)$ es falsa. En este caso, $p(x)$ se transforma en una proposición falsa para cada x de $\mathscr{U}$ y, en particular, $p(f)$ será falsa.

Por el valor de verdad de la conjunción, tendremos que la hipótesis, en cualquier caso, es falsa y, consecuentemente, el condicional

$$[\forall x, (p(x) \longrightarrow q(x)) \wedge p(f)] \longrightarrow q(f)$$

es una tautología y el razonamiento es válido.

3 Utilizando el método de demostración por reducción al absurdo o contradicción (1.5.3).

En efecto, supongamos que la hipótesis, $(\forall x, (p(x) \longrightarrow q(x))) \wedge p(f)$ es verdad y que la conclusión $q(f)$ es falsa.

Por ser verdad la hipótesis, el valor de verdad de la conjunción asegura que $\forall x, (p(x) \longrightarrow q(x))$ es verdad y $p(f)$ también lo es. Además, la veracidad de $\forall x, (p(x) \longrightarrow q(x))$ significa, por el valor de verdad del cuantificador universal, que el predicado $p(x) \longrightarrow q(x)$ se transforma en una proposición verdadera para cada x de $\mathscr{U}$, por lo tanto, y en particular, $p(f) \longrightarrow q(f)$ es verdad.

Pues bien, si $p(f) \longrightarrow q(f)$ es verdad y $q(f)$ es falsa, por el valor de verdad del condicional, $p(f)$ ha de ser falsa y su negación $\neg p(f)$ será verdadera con lo cual, al ser $p(f)$ verdadera, tendremos que $p(f) \wedge \neg p(f)$ es verdad.

De la veracidad de $(\forall x, (p(x) \longrightarrow q(x))) \wedge p(f) \wedge \neg q(f)$ hemos deducido la veracidad de $p(f) \wedge \neg p(f)$, luego el condicional

$$[(\forall x, (p(x) \longrightarrow q(x))) \wedge p(f) \wedge \neg q(f)] \longrightarrow (p(f) \wedge \neg p(f))$$

es una tautología y, al ser falsa la proposición $p(f) \wedge \neg p(f)$, esto significa que la proposición

$$(\forall x, (p(x) \longrightarrow q(x))) \wedge p(f) \wedge \neg q(f)$$

es falsa y, por tanto, su negación

$$[(\forall x, (p(x) \longrightarrow q(x))) \wedge p(f)] \longrightarrow q(f)$$

es verdadera y el razonamiento es válido.

4 Utilizando el método de demostración por la contrarrecíproca (1.5.4).

$$\begin{aligned}
[(\forall x, (p(x) \longrightarrow q(x))) \wedge p(f)] \longrightarrow q(f) &\iff \neg q(f) \longrightarrow \neg\,[(\forall x, (p(x) \longrightarrow q(x))) \wedge p(f)] \\
&\iff \neg q(f) \longrightarrow \neg \forall x, (p(x) \longrightarrow q(x)) \vee \neg p(f) \qquad (1.4.4) \\
&\iff \neg q(f) \longrightarrow (\exists x, (p(x) \wedge \neg q(x))) \vee \neg p(f) \qquad (2.13)
\end{aligned}$$

Probaremos, pues, que esta última proposición es una tautología. En efecto, si $\neg q(f)$ es verdad, el valor de verdad de la conclusión dependerá de los distintos casos que puedan presentarse para el predicado $p(x)$.

- $p(x)$ se transforma en proposición verdadera para cada x de $\mathscr{U}$ o lo que es igual $\forall x, p(x)$ es verdad. En este caso, y en particular, $p(f)$ sería verdad y, al ser $\neg q(f)$ verdadera, habríamos encontrado un valor de x en $\mathscr{U}$ que transforma el predicado $p(x) \wedge \neg q(x)$ en proposición verdadera y, por el valor de verdad del cuantificador existencial, esto significa que $\exists x : p(x) \wedge \neg q(x)$ es verdad.
- $p(x)$ se transforma en proposición falsa para, al menos, un valor de x en $\mathscr{U}$ es decir, $\forall x, p(x)$ es falsa. Habría dos opciones:
  - x es Florinda. En este caso, $p(f)$ sería falsa y su negación, $\neg p(f)$, verdadera.
  - x no es Florinda. En tal caso, $p(f)$ debería ser verdadera y, al ser $\neg q(f)$ verdad, la conjunción $p(f) \wedge \neg q(f)$ también lo sería y, por lo tanto, habríamos encontrado, al menos, un valor de x en $\mathscr{U}$ que transforma $p(x) \wedge \neg q(x)$ en proposición verdadera, o sea $\exists x : (p(x) \wedge \neg q(x))$ es verdad.
- $p(x)$ se transforma en proposición verdadera para, al menos, un valor de x en $\mathscr{U}$ es decir, $\exists x : p(x)$ es verdadera. Al igual que en el caso anterior, habría dos opciones:
  - si x es Florinda, entonces $p(f)$ es verdad y, razonando como lo hicimos en el caso anterior, $\exists x : (p(x) \wedge \neg q(x))$ sería verdad.
  - Si x no es Florinda, entonces $p(f)$ ha de ser falsa y su negación, $\neg p(f)$, verdadera.
- $p(x)$ se transforma en proposición falsa para cada x de $\mathscr{U}$ o sea $\exists x : p(x)$ es falsa.
  En este caso, y en particular, $p(f)$ sería falsa y, por lo tanto, su negación, $\neg p(f)$, verdadera.

Hemos probado que en cualquier caso, al menos una de las dos proposiciones $(\exists x, (p(x) \wedge \neg q(x)))$ o $\neg p(f)$ es verdadera, luego

$$(\exists x, (p(x) \wedge \neg q(x))) \vee \neg p(f)$$

es verdadera y, consecuentemente,

$$\neg q(f) \longrightarrow (\exists x, (p(x) \wedge \neg q(x))) \vee \neg p(f)$$

también lo es y, por la equivalencia del principio, esto significa que

$$[(\forall x, (p(x) \longrightarrow q(x))) \wedge p(f)] \longrightarrow q(f)$$

es una tautología y el razonamiento propuesto es válido.

■

Ejemplo 2.15

Consideremos el universo de los números enteros, elijamos un número a que no sea múltiplo de 2 *y estudiemos la validez del siguiente razonamiento.*

El número a no es múltiplo de 2.
Si un número es par, entonces es divisible por 2.
Si un número es divisible por 2*, entonces es múltiplo de* 2.
Por lo tanto, el número a no es par.

Solución

Sean

$p(x)$: x es par.
$q(x)$: x es divisible por 2.
$r(x)$: x es múltiplo de 2.

El razonamiento escrito en forma simbólica sería:

$$[\neg r(a) \wedge (\forall x, (p(x) \longrightarrow q(x))) \wedge (\forall x, (q(x) \longrightarrow r(x)))] \longrightarrow \neg p(a)$$

Al igual que en el ejercicio anterior, comprobaremos si el razonamiento es válido de varias formas.

1 Aplicando directamente la definición de implicación lógica.

Veremos, como siempre, que la veracidad de la conclusión se deduce de la veracidad de la hipótesis.

En efecto, si la hipótesis, $\neg r(a) \wedge (\forall x, (p(x) \longrightarrow q(x))) \wedge (\forall x, (q(x) \longrightarrow r(x)))$, es verdad, por el *valor de verdad de la conjunción*, (1.2.1), tendremos que

- $\neg r(a)$ es verdad.
- $\forall x, (p(x) \longrightarrow q(x))$ es verdad.
- $\forall x, (q(x) \longrightarrow r(x))$ es verdad.

De lo que se deduce,

- $r(a)$ es falsa.

- ⊛ Por el *valor de verdad del cuantificador universal*, (2.2.2), el predicado $p(x) \longrightarrow q(x)$ se transforma en una proposición verdadera para todos y cada uno de los elementos del universo y, al ser a uno de ellos, la proposición $p(a) \longrightarrow q(a)$ es verdad.
- ⊛ Por el *valor de verdad del cuantificador universal*, (2.2.2), el predicado $q(x) \longrightarrow r(x)$ se transforma en una proposición verdadera para todos y cada uno de los elementos del universo y, al ser a uno de ellos, la proposición $q(a) \longrightarrow r(a)$ es verdad.

Pues bien, como $r(a)$ es falsa y $q(a) \longrightarrow r(a)$ verdad, por el *valor de verdad del condicional*, (1.2.6), $q(a)$ ha de ser falsa y, al ser verdad $p(a) \longrightarrow q(a)$, $p(a)$, por el mismo motivo, deberá ser falsa y, consecuentemente, $\neg p(a)$ es verdadera, es decir, a no es par.

Como la veracidad de la conclusión se sigue de la veracidad de la hipótesis, tendremos que

$$[\neg r(a) \wedge (\forall x, (p(x) \longrightarrow q(x))) \wedge (\forall x, (q(x) \longrightarrow r(x)))] \Longrightarrow \neg p(a)$$

y, por lo tanto, el razonamiento es válido.

2 Comprobando que el razonamiento,

$$[\neg r(a) \wedge (\forall x, (p(x) \longrightarrow q(x))) \wedge (\forall x, (q(x) \longrightarrow r(x)))] \longrightarrow \neg p(a)$$

es una tautología.

Este condicional será falso, por el *valor de verdad del condicional*, únicamente, si siendo verdad la hipótesis, la conclusión fuera falsa. Veamos que este caso no puede darse.

En efecto, si la conclusión, $\neg p(a)$ es falsa, entonces $p(a)$ será verdadera y habría dos opciones:

- ⊛ $\neg r(a)$ es falsa. Por el valor de verdad de la conjunción, la hipótesis sería falsa.
- ⊛ $\neg r(a)$ es verdadera y, por tanto, $r(a)$ es falsa. En este caso, el valor de verdad de la hipótesis dependerá de los distintos casos que puedan presentarse para el predicado $q(x)$.
  - ⊛⊛ $q(x)$ se transforma en proposición verdadera para cada x de $\mathscr{U}$, es decir, $\forall x, q(x)$ es verdad. En este caso, y en particular, $q(a)$ sería verdadera, el condicional $q(a) \longrightarrow r(a)$ sería falso y habríamos encontrado, al menos, un valor de x en $\mathscr{U}$ que transformaría el predicado $q(x) \longrightarrow r(x)$ en una proposición falsa. Por el valor de verdad del cuantificador universal, la proposición $\forall x, (q(x) \longrightarrow r(x))$, y con ella toda la hipótesis, sería falsa.
  - ⊛⊛ $q(x)$ se transforma en una proposición falsa para, al menos, un valor de x en $\mathscr{U}$, es decir $\forall x, q(x)$ es falsa. En este caso tendríamos dos opciones:
    - si $x = a$, la proposición $q(a)$ sería falsa y, al ser $p(a)$ verdadera, el condicional $p(a) \longrightarrow q(a)$ sería falso con lo cual habríamos encontrado en $\mathscr{U}$ un valor de x que transforma el predicado $p(x) \longrightarrow q(x)$ en una proposición falsa y, consecuentemente, la proposición $\forall x, (p(x) \longrightarrow q(x))$, y con ella toda la hipótesis, sería falsa.
    - si $x \neq a$, entonces $q(a)$ debería ser verdadera y podríamos aplicar el razonamiento del caso anterior.
  - ⊛⊛ $q(x)$ se transforma en una proposición verdadera para al menos un valor de x en $\mathscr{U}$. Habría, de nuevo, dos opciones:
    - si $x = a$, entonces $q(a)$ es verdadera y estaríamos en el primer caso.
    - Si $x \neq a$, entonces $q(a)$ debería ser falsa con lo que estaríamos en el caso anterior.
  - ⊛⊛ $q(x)$ se transforma en una proposición falsa para cualquier valor de x en $\mathscr{U}$, es decir $\exists x : q(x)$ es falsa.
    En tal caso, y en particular, $q(a)$ será falsa y, por lo tanto, el condicional $p(a) \longrightarrow q(a)$ sería falso y habríamos encontrado, al menos, un valor de x en $\mathscr{U}$ que transforma el predicado $p(x) \longrightarrow q(x)$ en una proposición falsa. Por el valor de verdad del cuantificador universal, la proposición $\forall x, (p(x) \longrightarrow q(x))$, y con ella toda la hipótesis, sería falsa.

Por lo tanto, y en cualquier caso, si la conclusión es falsa, la hipótesis también lo es, es decir la única opción de que el condicional fuera falso no es posible de aquí que

$$[\neg r(a) \wedge (\forall x, (p(x) \longrightarrow q(x))) \wedge (\forall x, (q(x) \longrightarrow r(x)))] \longrightarrow \neg p(a)$$

sea una tautología y, consecuentemente, el razonamiento propuesto es válido.

3 Utilizando el método de demostración por reducción al absurdo o contradicción, (1.5.3).

En efecto, supongamos que la hipótesis,

$$\neg r(a) \wedge (\forall x, (p(x) \longrightarrow q(x))) \wedge (\forall x, (q(x) \longrightarrow r(x)))$$

es verdad y que la conclusión $\neg p(a)$ es falsa.

Entonces, $p(a)$ será verdadera y por el valor de verdad de la conjunción,

$\neg r(a)$ es verdad.

$\forall x, (p(x) \longrightarrow q(x))$ es verdad.

$\forall x, (q(x) \longrightarrow r(x))$ es verdad.

Pues bien, si $\forall x, (p(x) \longrightarrow q(x))$ y $\forall x\, (q(x) \longrightarrow r(x))$ son verdaderas, entonces por el valor de verdad del cuantificador universal, (2.2.2), los predicados, $p(x) \longrightarrow q(x)$ y $q(x) \longrightarrow r(x)$ se transformarán en proposiciones verdaderas para cualquier elemento del universo y en particular para a, es decir, $p(a) \longrightarrow q(a)$ y $q(a) \longrightarrow r(a)$ son, ambas, verdaderas.

Además, si $p(a) \longrightarrow q(a)$ es verdad y $p(a)$ también lo es, entonces por el *valor de verdad del condicional*, (1.2.6), $q(a)$ tiene que ser verdad y, al ser verdad $q(a) \longrightarrow r(a)$, por el mismo motivo, la proposición $r(a)$ tiene que ser verdadera. Como $\neg r(a)$ es verdad, hemos llegado a que $r(a) \wedge \neg r(a)$ es verdadera, es decir,

$$[\neg r(a) \wedge (\forall x, (p(x) \longrightarrow q(x))) \wedge (\forall x, (q(x) \longrightarrow r(x))) \wedge p(a)] \longrightarrow (\neg r(a) \wedge r(a))$$

es una tautología y, como $\neg r(a) \wedge r(a)$ es falsa, la hipótesis

$$\neg r(a) \wedge (\forall x, (p(x) \longrightarrow q(x))) \wedge (\forall x, (q(x) \longrightarrow r(x))) \wedge p(a)$$

también ha de ser falsa. Su negación

$$[\neg r(a) \wedge (\forall x, (p(x) \longrightarrow q(x))) \wedge (\forall x, (q(x) \longrightarrow r(x)))] \longrightarrow \neg p(a)$$

será verdadera y, consecuentemente, el razonamiento propuesto es válido.

4 Utilizando el método de demostración por la contrarrecíproca (1.5.4).

$$[\neg r(a) \wedge (\forall x, (p(x) \longrightarrow q(x))) \wedge (\forall x, (q(x) \longrightarrow r(x)))] \longrightarrow \neg p(a)$$

$\Longleftrightarrow$ {Contrarrecíproca}

$$\neg\neg p(a) \longrightarrow \neg\, [\neg r(a) \wedge (\forall x, (p(x) \longrightarrow q(x))) \wedge (\forall x, (q(x) \longrightarrow r(x)))]$$

$\Longleftrightarrow$ {De Morgan}

$$p(a) \longrightarrow r(a) \vee (\neg\forall x, (p(x) \longrightarrow q(x))) \vee (\neg\forall x, (q(x) \longrightarrow r(x)))$$

$\Longleftrightarrow$ {Ejemplo 2.13}

$$p(a) \longrightarrow r(a) \vee (\exists x : (p(x) \wedge \neg q(x))) \vee (\exists x : (q(x) \wedge \neg r(x)))$$

Probaremos, pues, que este último condicional es una tautología.

En efecto, si $p(a)$ es verdad, tendremos dos opciones:

- $r(a)$ es verdad. Por el valor de verdad de la disyunción, la conclusión sería verdadera.

- $r(a)$ es falsa. En esta opción el valor de verdad de la conclusión dependerá de las proposiciones cuantificadas existencialmente y, al ser $p(a)$ verdadero, los valores de verdad de las mismas dependerán, a su vez, de los diferentes casos que puedan presentarse para el predicado $q(x)$.
  - $q(x)$ se transforma en proposición verdadera para cada x de $\mathscr{U}$, o sea $\forall x, q(x)$ es verdadera. En este caso, y en particular, la proposición $q(a)$ será verdadera. Como $\neg r(a)$ es verdad, la proposición $q(a) \wedge \neg r(a)$ es verdadera y esto significa que hemos encontrado, al menos, un valor de x en $\mathscr{U}$ que transforma el predicado $q(x) \wedge \neg r(x)$ en una proposición verdadera lo cual, a su vez, significa, por el valor de verdad del cuantificador existencial, que $\exists x : (q(x) \wedge \neg r(x))$, y con ella la conclusión, es verdad.
  - $q(x)$ se transforma en proposición falsa para cada x de $\mathscr{U}$, o sea $\exists x : q(x)$ es falsa.
    En tal caso, y en particular, la proposición $q(a)$ será falsa, su negación, $\neg q(a)$ verdadera y, al ser verdad $p(a)$, la conjunción $p(a) \wedge \neg q(a)$ será verdadera y esto significa que hemos encontrado, al menos, un valor de x en $\mathscr{U}$ que transforma el predicado $p(x) \wedge \neg q(x)$ en una proposición verdadera lo cual, por el valor de verdad del cuantificador existencial, quiere decir que $\exists x : (p(x) \wedge \neg q(x))$, y con ella la conclusión, es verdad.
  - $q(x)$ se transforma en proposición verdadera para, al menos, un valor de x en $\mathscr{U}$, es decir $\exists x, q(x)$ es verdad.
    En este caso, habrá, al menos, un valor de x en $\mathscr{U}$ que transforma el predicado $q(x)$ en una proposición verdadera y tendremos, por tanto, dos opciones:
    - si $x = a$, entonces $q(a)$ es verdadera y estaríamos en el primer caso.
    - Si $x \neq a$, entonces $q(a)$ debería ser falsa y estaríamos en el segundo caso.
  - $q(x)$ se transforma en proposición falsa para, al menos, un valor de x en $\mathscr{U}$, es decir $\forall x, q(x)$ es falsa.
    En este caso, habrá, al menos, un valor de x en $\mathscr{U}$ que transforma el predicado $q(x)$ en una proposición falsa y tendremos, por tanto, dos opciones:
    - si $x = a$, entonces $q(a)$ es falsa y estaríamos en el segundo caso.
    - Si $x \neq a$, entonces $q(a)$ debería ser verdadera y estaríamos en el primer caso.

Por lo tanto, y en cualquier caso, la conclusión es verdad, es decir la proposición

$$p(a) \longrightarrow r(a) \vee (\exists x : (p(x) \wedge \neg q(x))) \vee (\exists x : (q(x) \wedge \neg r(x)))$$

es una tautología lo cual, por las equivalencias del principio, equivale a decir que

$$[\neg r(a) \wedge (\forall x, (p(x) \longrightarrow q(x))) \wedge (\forall x, (q(x) \longrightarrow r(x)))] \longrightarrow \neg p(a)$$

también es una tautología y, consecuentemente, el razonamiento propuesto es válido.

■

Nota 2.5 En los ejemplos anteriores, hemos deducido conclusiones particulares partiendo de premisas o hipótesis generales. Sin embargo, en la inmensa mayoría de los teoremas matemáticos hay que llegar a conclusiones generales. Por ejemplo, tendremos que probar que $p(x)$ es verdad para todos los valores de un cierto universo del discurso, es decir probar que $\forall x, p(x)$ es verdad, para lo cual habrá que establecer la veracidad de la proposición $p(a)$ para cada elemento a del universo y, como ya hemos comentado anteriormente, en la mayor parte de los universos esto no es factible. Lo que haremos para solventar esta cuestión es probar que $p(a)$ es verdad pero no para el caso en que a sea un elemento particular y concreto sino para el caso en que a denote un elemento arbitrario o genérico del universo.

■

Ejemplo 2.16

Estudiar, en el universo de los estudiantes de la Universidad de Cádiz, la validez del siguiente razonamiento:

> *Todos los alumnos de Informática estudian Lógica Matemática.*
> *Todos los alumnos que estudian Lógica, saben analizar la validez de un razonamiento.*
> *Por lo tanto, todos los alumnos de informática saben analizar la validez de un razonamiento.*

Solución

Sean los predicados,

$p(x)$: x es alumno de Informática.

$q(x)$: x estudia Lógica Matemática.

$r(x)$: x sabe analizar la validez de un razonamiento.

El razonamiento escrito en forma simbólica sería:

$$[(\forall x, (p(x) \longrightarrow q(x))) \wedge (\forall x, (q(x) \longrightarrow r(x)))] \longrightarrow [\forall x, (p(x) \longrightarrow r(x))]$$

Comprobaremos su validez por varios métodos.

1 Directamente por la definición de implicación lógica.

Comprobaremos que la veracidad de la conclusión se deduce de la veracidad de la hipótesis.

En efecto, si la proposición $(\forall x, (p(x) \longrightarrow q(x))) \wedge (\forall x, (q(x) \longrightarrow r(x)))$ es verdadera, entonces por el *valor de verdad de la conjunción*, $\forall x, (p(x) \longrightarrow q(x))$ será verdadera y $\forall x, (q(x) \longrightarrow r(x))$ también.

Pues bien, si $\forall x, (p(x) \longrightarrow q(x))$ es verdad, entonces por el *valor de verdad del cuantificador universal*, el predicado $p(x) \longrightarrow q(x)$ se transforma en una proposición verdadera para todos y cada uno de los valores de x en $\mathscr{U}$. En cada una de dichas proposiciones, y por el valor de verdad del condicional, la hipótesis es falsa o la conclusión es verdadera y habrá, por tanto, dos opciones:

- Todas las hipótesis son falsas, es decir el predicado $p(x)$ se transforma en proposición falsa para cada x de $\mathscr{U}$ o lo que es igual $\exists x : p(x)$ es falso.
  En tal caso, el predicado $p(x) \longrightarrow r(x)$ se transformará en proposición verdadera para todos los x, sin importar lo que ocurra con $r(x)$ y, por lo tanto, por el valor de verdad del cuantificador universal, $\forall x, (p(x) \longrightarrow r(x))$ es verdad.
- Las conclusiones, todas, son verdaderas, o sea $q(x)$ se transforma en proposición verdadera para cada x de $\mathscr{U}$, es decir, $\forall x, q(x)$ es verdad.
  En este caso y teniendo en cuenta que $\forall x, (q(x) \longrightarrow r(x))$ es verdad, el predicado $r(x)$ deberá transformarse en una proposición verdadera para todos los x de $\mathscr{U}$ y, por lo tanto, $p(x) \longrightarrow r(x)$ se transforma en verdadera para todos y cada uno de los valores de x en $\mathscr{U}$ lo cual significa, por el valor de verdad del cuantificador universal, que $\forall x, (p(x) \longrightarrow r(x))$ es verdad.

La veracidad de la conclusión se sigue de la veracidad de la hipótesis, luego,

$$[\forall x, (p(x) \longrightarrow q(x)) \wedge \forall x, (q(x) \longrightarrow r(x))] \Longrightarrow [\forall x, (p(x) \longrightarrow r(x))]$$

y, por tanto, el condicional,

$$[\forall x, (p(x) \longrightarrow q(x)) \wedge \forall x, (q(x) \longrightarrow r(x))] \longrightarrow [\forall x, (p(x) \longrightarrow r(x))]$$

es una tautología, es decir, el razonamiento propuesto es válido.

2 Comprobando que el razonamiento es una tautología.

Veamos, como siempre, que el único caso de falsedad del condicional no puede darse. Probaremos que si la conclusión es falsa, la hipótesis también lo es.

Si $\forall x, (p(x) \longrightarrow r(x))$ es falsa, entonces tiene que haber, al menos, un valor de x en $\mathscr{U}$ que transforme el predicado $p(x) \longrightarrow r(x)$ en una proposición falsa. A ese valor concreto de x lo llamaremos a, es decir la proposición $p(a) \longrightarrow r(a)$ es falsa. Entonces, $p(a)$ será verdadera, $r(a)$ falsa y el valor de verdad de la hipótesis dependerá, por tanto, del predicado $q(x)$ y habrá las siguientes opciones:

- $q(x)$ se transforma en proposición verdadera para cada x de $\mathscr{U}$, es decir, $\forall x, q(x)$ es verdad.
  En este caso, y en particular, $q(a)$ será verdad y al ser $r(a)$ falsa, el valor de verdad del condicional asegura que $q(a) \longrightarrow r(a)$ es falso.
- $q(x)$ se transforma en proposición falsa para, al menos, un valor de x en $\mathscr{U}$, es decir, $\forall x, q(x)$ es falsa. En este caso pueden ocurrir dos cosas:
  - Si $x = a$, entonces $q(a)$ es falsa y, al ser $p(a)$ verdadera, el condicional $p(a) \longrightarrow q(a)$ será falso.
  - Si $x \neq a$, entonces $q(a)$ ha de ser verdadera y como $r(a)$ es falsa, el condicional $q(a) \longrightarrow r(a)$ es falso.
- $q(x)$ se transforma en proposición verdadera para, al menos, un valor de x en $\mathscr{U}$, es decir, $\exists x, q(x)$ es verdad. En tal caso pueden ocurrir, también, dos cosas:
  - Si $x = a$, entonces $q(a)$ es verdad y, al ser $r(a)$ falsa, el condicional $q(a) \longrightarrow r(a)$ será falso.
  - Si $x \neq a$, entonces $q(a)$ ha de ser falsa y, como $p(a)$ es verdad, el condicional $p(a) \longrightarrow q(a)$ es falso.
- $q(x)$ se transforma en proposición falsa para cada x de $\mathscr{U}$, es decir, $\exists x, q(x)$ es falsa.
  En tal caso, y en particular, $q(a)$ sería falsa y, al ser verdad $p(a)$, el condicional $p(a) \longrightarrow q(a)$ sería falso.

Por lo tanto, y en cualquier caso, siempre existe, al menos, un valor de x en $\mathscr{U}$ que transforma el predicado $p(x) \longrightarrow q(x)$ o el $q(x) \longrightarrow r(x)$ en una proposición falsa y, por lo tanto, por el valor de verdad del cuantificador universal, $\forall x, (p(x) \longrightarrow q(x))$ o $\forall x, (q(x) \longrightarrow r(x))$ son falsos.

Como si la conclusión es falsa, la hipótesis también lo es, el condicional,

$$[(\forall x, (p(x) \longrightarrow q(x))) \wedge (\forall x, (q(x) \longrightarrow r(x)))] \longrightarrow [\forall x, (p(x) \longrightarrow r(x))]$$

será una tautología y el razonamiento, en consecuencia, es válido.

3 Utilizando el método de demostración por reducción al absurdo o contradicción (1.5.3).

Supongamos que la hipótesis, $(\forall x, (p(x) \longrightarrow q(x))) \wedge (\forall x, (q(x) \longrightarrow r(x)))$ es verdad y que, sin embargo, la conclusión $\forall x, (p(x) \longrightarrow r(x))$ no lo es, es decir, $\forall x, (p(x) \longrightarrow r(x))$ es falsa.

Entonces, por el valor de verdad del cuantificador universal ha de existir, al menos, un valor de x en $\mathscr{U}$ que transforme el predicado $p(x) \longrightarrow r(x)$ en una proposición falsa. Si a este valor concreto lo llamamos a, tendremos que $p(a) \longrightarrow q(a)$ es falsa lo que, por el valor de verdad del condicional, significa que $p(a)$ es verdad y $r(a)$ falsa.

Por otra parte, las proposiciones $\forall x, (p(x) \longrightarrow q(x))$ y $\forall x, (q(x) \longrightarrow r(x))$ son, por el valor de verdad de la conjunción, verdaderas luego por el valor de verdad del cuantificador universal, los predicados $p(x) \longrightarrow q(x)$ y $q(x) \longrightarrow r(x)$ se transformarán en proposiciones verdaderas para cada x de $\mathscr{U}$. En particular, $p(a) \longrightarrow q(a)$ será verdad y $q(a) \longrightarrow r(a)$ también.

Pues bien, si $p(a) \longrightarrow q(a)$ es verdad y $p(a)$ también, por el valor de verdad del condicional, $q(a)$ ha de ser verdad y si $q(a) \longrightarrow r(a)$ es verdad y $r(a)$ es falsa, entonces, por la misma razón, $q(a)$ ha de ser falsa, es decir, $\neg q(a)$ es verdad y, consecuentemente, $q(a) \wedge \neg q(a)$ es verdad. Hemos encontrado, pues, un valor de x en $\mathscr{U}$ que transforma el predicado $q(x) \wedge \neg q(x)$ en una proposición verdadera, es decir, $\exists x : (q(x) \wedge \neg q(x))$ es verdad.

Como de la veracidad de $(\forall x, (p(x) \longrightarrow q(x))) \wedge (\forall x, (q(x) \longrightarrow r(x))) \wedge \neg\forall x, (p(x) \longrightarrow r(x))$ hemos llegado a la de $\exists x : (q(x) \wedge \neg q(x))$, tendremos que

$$[(\forall x, (p(x) \longrightarrow q(x))) \wedge (\forall x, (q(x) \longrightarrow r(x))) \wedge \neg (\forall x, (p(x) \longrightarrow r(x)))] \longrightarrow \exists x : (q(x) \wedge \neg q(x))$$

es una tautología.

Ahora bien, el predicado $q(x) \wedge \neg q(x)$ se transforma en una proposición falsa para todos y cada uno de los valores de x en $\mathscr{U}$, por lo tanto, $\exists x : (q(x) \wedge \neg q(x))$ es, siempre, falsa y, por el valor de verdad del condicional,

$$(\forall x, (p(x) \longrightarrow q(x))) \wedge (\forall x, (q(x) \longrightarrow r(x))) \wedge \neg (\forall x, (p(x) \longrightarrow r(x)))$$

ha de ser, también, falsa y, por lo tanto, su negación

$$[(\forall x, (p(x) \longrightarrow q(x))) \wedge (\forall x, (q(x) \longrightarrow r(x)))] \longrightarrow (\forall x, (p(x) \longrightarrow r(x)))$$

ha de ser verdadera. Este condicional será, por tanto, una tautología y, consecuentemente, el razonamiento propuesto es válido.

4 Utilizando el método de demostración por la contrarrecíproca (1.5.4).

Probaremos que

$$\neg\forall x, (p(x) \longrightarrow r(x)) \longrightarrow \neg [(\forall x, (p(x) \longrightarrow q(x))) \wedge (\forall x, (q(x) \longrightarrow r(x)))]$$

es una tautología, lo cual, utilizando las leyes de De Morgan, equivale a probar que

$$\neg\forall x, (p(x) \longrightarrow r(x)) \longrightarrow \neg\forall x, (p(x) \longrightarrow q(x)) \vee \neg\forall x, (q(x) \longrightarrow r(x))$$

también lo es y que, a su vez, utilizando el resultado del ejemplo 2.13 , equivale a probar que

$$\exists x : (p(x) \wedge \neg r(x)) \longrightarrow (\exists x : (p(x) \wedge \neg q(x))) \vee (\exists x : (q(x) \wedge \neg r(x)))$$

es una tautología.

En efecto, si $\exists x : (p(x) \wedge \neg r(x))$ es verdad, entonces existirá, al menos, un valor de x en $\mathscr{U}$ que transforma el predicado $p(x) \wedge \neg r(x)$ en una proposición verdadera. Si a ese valor concreto lo llamamos a, tendremos que la proposición $p(a) \wedge \neg r(a)$ es verdadera luego, por el valor de verdad de la conjunción, $p(a)$ es verdad y $\neg r(a)$ también.

El valor de verdad de la conclusión dependerá, por tanto, de las distintas opciones que puedan presentarse para el predicado $q(x)$ cuando x sea igual a a, es decir, dependerá del valor de verdad de la proposición $q(a)$.

- Si $q(a)$ es verdad, como $\neg r(a)$ es verdadera, la proposición $q(a) \wedge \neg r(a)$ es verdad.
- Si $q(a)$ es falsa, entonces $\neg q(a)$ será verdadera y, al ser $p(a)$ verdad, tendremos que $p(a) \wedge \neg q(a)$ es una proposición verdadera.

Por lo tanto, y en cualquier caso, siempre existe, al menos, un valor de x en $\mathscr{U}$ que transforma el predicado $p(x) \wedge \neg q(x)$ o el $q(x) \wedge \neg r(x)$ en una proposición verdadera y, por lo tanto, por el valor de verdad del cuantificador existencial, (2.2.4), $\exists x : (p(x) \wedge \neg q(x))$ o $\exists x : (q(x) \wedge \neg r(x))$ son verdaderas lo cual significa, por el valor de verdad de la disyunción, (1.2.2), que la conclusión es verdadera, luego el condicional es una tautología y, consecuentemente, el razonamiento propuesto es válido.

■

Unidad Temática II

Teoría de Conjuntos

Lección 3

Conjuntos y Subconjuntos

Un conjunto es la reunión en un todo de objetos de nuestra intuición o de nuestro pensar, bien determinados y diferenciables los unos de los otros.

Georg Cantor (1845-1918)

3.1 Introducción

El concepto de conjunto es de fundamental importancia en las matemáticas modernas. La mayoría de los matemáticos creen que es posible expresar todas las matemáticas en el lenguaje de la teoría de conjuntos. Nuestro interés en los conjuntos se debe tanto al papel que representan en las matemáticas como a su utilidad en la modelización e investigación de problemas en la informática.

Los conjuntos fueron estudiados formalmente por primera vez por Georg Cantor[1]. Después de que la teoría de conjuntos se estableciera como un área bien definida de las matemáticas, aparecieron contradicciones o paradojas en la misma. Para eliminar tales paradojas, se desarrollaron aproximaciones más sofisticadas que las que hizo Cantor. Un tratamiento introductorio de la teoría de conjuntos se ocupa, generalmente, de la teoría elemental, la cual es bastante similar al trabajo original de Cantor. Utilizaremos esta aproximación más simple y desarrollaremos una teoría de conjuntos de la cual es posible derivar contradicciones. Parece extraño el proponerse tal cosa deliberadamente, pero las contradicciones no son un problema si, como es nuestro caso, el universo del discurso se define convenientemente. Aún más, la existencia de las paradojas en la teoría elemental no afecta a la validez de nuestros resultados ya que los teoremas que presentaremos pueden demostrarse mediante sistemas alternativos en los que las paradojas no ocurren.

■

3.2 Generalidades

Definimos los conceptos fundamentales del tema como conjunto, elemento, determinación de un conjunto por extensión, por comprensión y estudiamos la igualdad de dos conjuntos.

[1]Georg Cantor. Matemático alemán de origen ruso (San Petesburgo 1845-Halle 1918). Después de estudiar en Alemania, fue profesor de la universidad de Halle (1879). Escribió numerosas memorias, pero es especialmente conocido por ser el creador de la *Teoría de los conjuntos*.

3.2.1 Conjuntos y Elementos

Intuitivamente, un conjunto es cualquier colección de objetos que pueda tratarse como una entidad. A cada objeto de la colección lo llamaremos elemento o miembro del conjunto.

A los conjuntos los designaremos con letras mayúsculas y a sus elementos con letras minúsculas. La afirmación "*el elemento a pertenece al conjunto A*" se escribe

$$a \in A$$

y la negación de este hecho se escribe

$$a \notin A$$

La definición de un conjunto no debe ser ambigua en el sentido de que pueda decidirse cuando un objeto particular pertenece, o no, a un conjunto.

La forma más usual de escribir un conjunto es encerrar entre llaves los elementos que lo integran separados por comas. Por ejemplo,

$$A = \{a, b, c, d\}$$

es el conjunto formado las letras a, b, c y d.

■

3.2.2 Diagramas de Venn

Una forma muy útil de representar gráficamente un conjunto es utilizar una región cerrada en la que pueden especificarse, si así se quiere, los elementos.

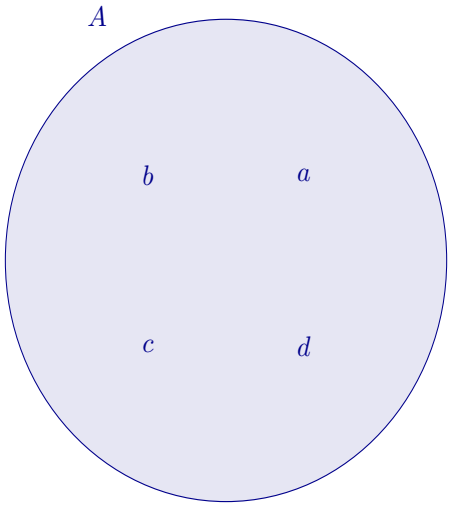


Diagrama de Venn del Conjunto $A = \{a, b, c, d\}$

■

3.2.3 Determinación por Extensión

Un conjunto está definido por extensión cuando se especifican todos y cada uno de los elementos que forman el mismo.

Ejemplo 3.1

Los siguientes conjuntos están definidos por extensión.

(a) El conjunto de las vocales del alfabeto.

$$A = \{a, e, i, o, u\}$$

(b) El conjunto formado por los números enteros pares no negativos y menores que diez.

$$B = \{0, 2, 4, 6, 8\}$$

Obsérvese que los elementos del conjunto están separados por comas y encerrados entre llaves.

■

Ejemplo 3.2

Definir por extensión los siguientes conjuntos.

(a) El conjunto de los enteros no negativos menores que cinco.

(b) El conjunto de las letras de mi nombre.

(c) El conjunto cuyo único elemento es el primer Presidente de Gobierno de la democracia.

(d) El conjunto de los números primos entre 10 y 20.

(e) El conjunto de los múltiplos de 12 que son menores que 65.

Solución

(a) $A = \{0, 1, 2, 3, 4\}$

(b) $B = \{p, a, c, o\}$

(c) $C = \{\text{Adolfo Suárez}\}$

(d) $D = \{11, 13, 17, 19\}$

(e) $E = \{12, 24, 36, 48, 60\}$

■

Ejemplo 3.3

Definir, por extensión, los conjuntos siguientes:

(a) $A = \{x : x \in \mathbb{Z} \text{ y } 3 < x < 12\}$

(b) $B = \{x : x \text{ es un número de un dígito}\}$

(c) $B = \{x : x = 2 \text{ ó } x = 5\}$

Solución

(a) $A = \{4, 5, 6, 7, 8, 9, 10, 11\}$

(b) $B = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$

(c) $C = \{2, 5\}$

■

Nota 3.1 Los elementos de un conjunto infinito no pueden especificarse de una forma explícita; consecuentemente necesitaremos una forma alternativa de describir tales conjuntos implícitamente.

3.2.4 Determinación por Comprensión

Se dice que un conjunto está definido por comprensión cuando se especifica una propiedad que caracteriza a todos los elementos del mismo.

Esta propiedad o especificación implícita se hace a menudo mediante un predicado con una variable libre. El conjunto estará formado por aquellos elementos del universo que hacen del predicado una proposición verdadera. De aquí que si $p(x)$ es un predicado con una variable libre, el conjunto

$$A = \{x : p(x)\}$$

denota al conjunto A tal que $a \in A$ si, y sólo si $p(a)$ es verdad.

■

Ejemplo 3.4

Definir por comprensión los siguientes conjuntos:

(a) El conjunto de los enteros mayores que diez.

(b) El conjunto de los enteros pares.

(c) El conjunto $\{1, 2, 3, 4, 5\}$

(d) El conjunto formado por todos los enteros positivos pares menores o iguales que 100.

(e) El conjunto formado por todos los enteros positivos impares menores que 100.

Solución

(a) $A = \{n \in \mathbb{Z} \text{ y } n > 10\}$

(b) $B = \{n : n = 2q,\ q \in \mathbb{Z}\}$

(c) $C = \{n \in \mathbb{Z} \text{ y } 1 \leqslant n \leqslant 5\}$

(d) $D = \{n \in \mathbb{Z}^+ : n = 2q,\ 1 \leqslant q \leqslant 50\}$

(e) $E = \{n \in \mathbb{Z}^+ : n = 2q + 1,\ 0 \leqslant q \leqslant 49\}$

■

Ejemplo 3.5

Definir por comprensión y por extensión el conjunto formado por todos los números reales cuyo cuadrado menos su quíntuplo más seis es cero.

Solución

Si llamamos A al conjunto pedido,

- Definición por comprensión.
$$A = \left\{x \in \mathbb{R} : x^2 - 5x + 6 = 0\right\}$$

- Definición por extensión.
Sea a cualquier número real. Entonces,
$$\begin{aligned} a \in A &\iff a^2 - 5a + 6 = 0 \\ &\iff a = \frac{5 \pm \sqrt{25 - 4 \cdot 1 \cdot 6}}{2 \cdot 1} \\ &\iff a = \frac{5 \pm 1}{2} \\ &\iff \begin{cases} a = 2 \\ \text{ó} \\ a = 3 \end{cases} \end{aligned}$$
Por lo tanto,
$$A = \{2, 3\}$$

■

Nota 3.2 Muchas veces se utilizan significados algo menos formales para describir conjuntos. Por ejemplo, el conjunto de los números enteros mayores que diez, suele escribirse:

$$A = \{x \in \mathbb{Z} : x > 10\}$$

y el conjunto de los enteros pares,

$$B = \{x = 2k,\ k \in \mathbb{Z}\}$$

A veces tanto en conjuntos finitos demasiado grandes, como en conjuntos infinitos, se utiliza la elipsis matemática para caracterizar a los elementos de un conjunto. Por ejemplo, el conjunto de los números enteros del 1 al 100,

$$C = \{1, 2, 3, \ldots, 100\}$$

o el conjunto de los enteros pares no negativos,

$$D = \{0, 2, 4, 6, \ldots\}$$

Algunos conjuntos aparecerán muy frecuentemente a lo largo del curso y se usan símbolos especiales para designarlos.

$\mathbb{Z}$: Conjunto de los números enteros.

$\mathbb{N} = \mathbb{Z}^+$: Conjunto de los números naturales o enteros positivos.

$\mathbb{Z}_0^+$: Conjunto de los enteros no negativos.

$\mathbb{Q}$: Conjunto de los números racionales.

$\mathbb{R}$: Conjunto de los números reales.

$\mathbb{C}$: Conjunto de los números complejos.

Incluso si podemos especificar todos los elementos de un conjunto puede que no sea práctico hacerlo. Por ejemplo, no definiríamos por extensión el conjunto de los estudiantes de la Universidad de Cádiz que estudien Informática, aunque teóricamente es posible definirlo. Así pues, describiremos un conjunto mediante un listado exhaustivo de sus elementos sólo si contiene unos pocos elementos, en caso contrario describiremos un conjunto mediante una propiedad que caracterice a los mismos.

■

3.2.5 Conjunto Universal

En cualquier aplicación de la teoría de conjuntos, los elementos de todos los conjuntos en consideración pertenecen a un gran conjunto fijo llamado conjunto universal. Lo notaremos por $\mathscr{U}$. Normalmente, lo representaremos por un rectángulo donde estén incluidos todos los demás conjuntos.

■

Ejemplo 3.6

Escribir cada uno de los conjuntos siguientes especificando el conjunto universal correspondiente.

(a) El conjunto de los enteros entre 0 *y* 100*.*

(b) El conjunto de los enteros positivos impares.

(c) El conjunto de los múltiplos de 10*.*

Solución

(a) $A = \{n : n \in \mathbb{Z} \text{ y } n > 0 \text{ y } n < 100\}$ ó $A = \{n \in \mathbb{Z} : 0 < n < 100\}$

(b) $B = \left\{n : \exists q \in \mathbb{Z}_0^+,\ n = 2q + 1\right\}$ ó $B = \left\{n : n = 2q + 1,\ q \in \mathbb{Z}_0^+\right\}$

(c) $C = \{n : \exists q \in \mathbb{Z},\ n = 10q\}$ ó $C = \{n : n = 10q,\ q \in \mathbb{Z}\}$

■

3.2.6 Conjunto Vacío

Al conjunto único que no contiene elementos, lo llamaremos conjunto vacío. Lo notaremos con el símbolo $\emptyset$ *que proviene del alfabeto noruego. A veces, también se nota* $\{\}$*.*

■

3.2.7 Axioma de Extensión

Dos conjuntos A *y* B *son iguales si tienen los mismos elementos.*

Obsérvese que esto quiere decir lo siguiente:

$$
\begin{aligned}
A = B &\iff A \text{ y } B \text{ tienen lo mismos elementos} \\
&\iff A \text{ tiene los mismos elementos que } B \text{ y } B \text{ tiene los mismos elementos que } A \\
&\iff \text{Todos los elementos de } A \text{ pertenecen a } B \text{ y todos los elementos de } B \text{ pertenecen a } A \\
&\iff [\forall x, (x \in A \longrightarrow x \in B)] \wedge [\forall x, (x \in B \longrightarrow x \in A)] \\
&\iff \forall x, [(x \in A \longrightarrow x \in B) \wedge (x \in B \longrightarrow x \in A)] \\
&\iff \forall x, (x \in A \longleftrightarrow x \in B)
\end{aligned}
$$

■

Nota 3.3 El axioma de extensión asegura que si dos conjuntos tienen los mismos elementos, ambos son iguales, independientemente de como estén definidos.

Como todo conjunto tiene los mismos elementos que él mismo, se sigue que si un conjunto está definido por extensión, el orden en el que los elementos figuren en él es intrascendente. Así pues, los conjuntos $\{a, b, c\}$, $\{b, c, a\}$ y $\{c, b, a\}$ son iguales.

También se sigue del axioma de extensión que la aparición de un elemento más de una vez en un conjunto, es igualmente intrascendente. Por ejemplo, los conjuntos $\{a, b\}$, $\{a, b, b\}$ y $\{a, a, a, b\}$ son iguales ya que todo elemento de cualquiera de ellos está en los demás, por tanto, son especificaciones diferentes del mismo conjunto.

■

Ejemplo 3.7

Determinar, en el conjunto de los números enteros, cuáles de los siguientes conjuntos son iguales.

$A = \{n : n \text{ es par y } n^2 \text{ es impar}\}$

$B = \{n : \exists q \in \mathbb{Z} \text{ y } n = 2q\}$

$C = \{1, 2, 3\}$

$D = \{\ldots, -6, -4, -2, 0, 2, 4, 6, \ldots\}$

$E = \{3, 3, 2, 1, 2\}$

$F = \{n : n^3 - 6n^2 - 7n - 6 = 0\}$

Solución

⁎ $A = \{n : n \text{ es par y } n^2 \text{ es impar}\}$. Comprobaremos que A es el conjunto vacío, procediendo por contradicción. En efecto, supongamos que $A \neq \emptyset$. Entonces, A tendrá, al menos, un elemento, es decir, existirá, al menos, un número entero a que estará en A. Pues bien,

$$\begin{aligned}
\exists a : a \in A \iff & \begin{cases} a \text{ es par} \\ \text{y} \\ a^2 \text{ es impar} \end{cases} \\
\iff & \begin{cases} a = 2q_1, \text{ con } q_1 \in \mathbb{Z} \\ \text{y} \\ a^2 = 2q_2 + 1 \text{ con } q_2 \in \mathbb{Z} \end{cases} \\
\implies & 2q_1 = 2q_2 + 1 \\
\iff & 1 = 2(q_1 - q_2), \text{ con } q_1 - q_2 \in \mathbb{Z} \\
\implies & 1 \text{ es par}
\end{aligned}$$

Lo cual, obviamente, es una contradicción. Por lo tanto, la hipótesis $\exists a : a \in A$ es falsa y, consecuentemente, su negación verdadera, es decir, ningún número entero pertenece al conjunto A, o lo que es igual $A = \emptyset$.

⁎ $B = \{n : \exists q \in \mathbb{Z} \text{ y } n = 2q\}$. Sea a cualquier número entero. Entonces,

$$\begin{aligned} a \in B &\iff \exists q \in \mathbb{Z} : a = 2q \\ &\iff \begin{cases} a = 0 \\ \text{ó} \\ a = -2 \\ \text{ó} \\ a = 2 \\ \text{ó} \\ a = -4 \\ \text{ó} \\ a = 4 \\ \text{ó} \\ \vdots \end{cases} \\ &\iff a \in D \end{aligned}$$

Por lo tanto,

$$\forall n, (n \in B \longleftrightarrow n \in D)$$

de aquí que por el Axioma de Extensión, (3.2.7), $B = D$.

⁎ $C = \{1, 2, 3\}$. Sea a cualquier número entero. Entonces,

$$\begin{aligned} a \in C &\iff \begin{cases} a = 1 \\ \text{ó} \\ a = 2 \\ \text{ó} \\ a = 3 \end{cases} \\ &\iff a \in E \end{aligned}$$

Por lo tanto,

$$\forall n, (n \in C \longleftrightarrow n \in E)$$

y por el Axioma de Extensión, (3.2.7), $C = E$.

⁎ $F = \left\{n : n^3 - 6n^2 - 7n - 6 = 0\right\}$. Ninguno de los divisores del término independiente, -6, satisface la ecuación, por lo tanto ningún número entero verifica la ecuación y, consecuentemente, el conjunto F es vacío, es decir, $F = A$.

■

Ejemplo 3.8

Dar una condición necesaria y suficiente para que dos conjuntos sean distintos.

Solución

Sean A y B dos conjuntos cualesquiera de un universal arbitrario $\mathscr{U}$. Por el Axioma de Extensión, (3.2.7),

$$A = B \iff \forall x, [(x \in A \longrightarrow x \in B) \wedge (x \in B \longrightarrow x \in A)]$$

de aquí que por la asociatividad del cuantificador universal,

$$A = B \iff [\forall x, (x \in A \longrightarrow x \in B) \wedge \forall x, (x \in B \longrightarrow x \in A)]$$

y, negando ambos miembros,

$$\neg(A = B) \Longleftrightarrow \neg\left[\forall x, (x \in A \longrightarrow x \in B) \wedge \forall x, (x \in B \longrightarrow x \in A)\right]$$

por lo tanto, aplicando De Morgan,

$$A \neq B \Longleftrightarrow (\neg\forall x, (x \in A \longrightarrow x \in B)) \vee (\neg\forall x, (x \in B \longrightarrow x \in A))$$

Veamos a que proposición es equivalente,

$$(\neg\forall x, (x \in A \longrightarrow x \in B)) \vee (\neg\forall x, (x \in B \longrightarrow x \in A))$$

En efecto, si esta proposición es verdadera, entonces una de las dos ha de ser verdad. Pues bien,

- Si $\neg\forall x, (x \in A \longrightarrow x \in B)$ es verdad, entonces $\forall x, (x \in A \longrightarrow x \in B)$ será falsa, luego ha de existir, al menos, un elemento en $\mathscr{U}$, llamémosle a, que transforme el predicado al alcance del cuantificador en una proposición falsa, es decir,

  $$a \in A \longrightarrow a \in B$$

  es falsa, luego,

  $$\neg\left(a \in A \longrightarrow a \in B\right)$$

  es verdadera, es decir,

  $$a \in A \wedge a \notin B$$

  es verdad.

  Hemos encontrado, pues, un elemento en $\mathscr{U}$ que transforma el predicado $x \in A \wedge x \notin B$ en una proposición verdadera, luego,

  $$\exists x : (x \in A \wedge x \notin B)$$

  es verdad.

- Si $\neg\forall x, (x \in B \longrightarrow x \in A)$ es verdad, razonando exactamente igual llegaríamos a que

  $$\exists x : (x \in B \wedge x \notin A)$$

  es verdadera.

Tendremos, pues, que

$$(\exists x : (x \in A \wedge x \notin B)) \vee (\exists x : (x \in B \wedge x \notin A))$$

es verdadera y, consecuentemente,

$$(\neg\forall x, (x \in A \longrightarrow x \in B)) \vee (\neg\forall x, (x \in B \longrightarrow x \in A)) \Longrightarrow (\exists x : (x \in A \wedge x \notin B)) \vee (\exists x : (x \in B \wedge x \notin A)) \tag{3.1}$$

Recíprocamente, si $(\exists x : (x \in A \wedge x \notin B)) \vee (\exists x : (x \in B \wedge x \notin A))$ es verdad, entonces una de las dos ha de ser verdadera.

- Si $(\exists x : (x \in A \wedge x \notin B))$ es verdadera, entonces tiene que haber, al menos, un elemento, que llamaremos a, en $\mathscr{U}$, que transforme $(x \in A \wedge x \notin B)$ en una proposición verdadera, es decir,

  $$a \in A \wedge a \notin B$$

  es verdad, y su negación

  $$a \notin A \vee a \in B$$

  debe ser falsa, o sea la proposición

  $$a \in A \longrightarrow a \in B$$

es falsa.

Hemos encontrado, por tanto, un elemento en $\mathscr{U}$ que transforma el predicado $x \in A \longrightarrow x \in B$ en una proposición falsa, es decir,

$$\forall x, (x \in A \longrightarrow x \in B)$$

es falsa y, consecuentemente, su negación

$$\neg\forall x, (x \in A \longrightarrow x \in B)$$

será verdadera.

⁕ Si $(\exists x : (x \in B \wedge x \notin A))$ es verdadera, haciendo un razonamiento idéntico al anterior, llegaríamos a que la proposición

$$\neg\forall x, (x \in A \longrightarrow x \in B)$$

es verdadera.

Tendremos, por tanto, que

$$(\neg\forall x, (x \in A \longrightarrow x \in B)) \vee (\neg\forall x, (x \in A \longrightarrow x \in B))$$

es verdad y, en consecuencia,

$$(\exists x : (x \in A \wedge x \notin B)) \vee (\exists x : (x \in B \wedge x \notin A)) \Longrightarrow (\neg\forall x, (x \in A \longrightarrow x \in B)) \vee (\neg\forall x, (x \in A \longrightarrow x \in B)) \tag{3.2}$$

De (3.1) y (3.2) se sigue que

$$(\neg\forall x, (x \in A \longrightarrow x \in B)) \vee (\neg\forall x, (x \in B \longrightarrow x \in A)) \Longleftrightarrow (\exists x : (x \in A \wedge x \notin B)) \vee (\exists x : (x \in B \wedge x \notin A))$$

y por lo tanto,

$$A \neq B \Longleftrightarrow (\exists x : (x \in A \wedge x \notin B)) \vee (\exists x : (x \in B \wedge x \notin A))$$

es decir una condición necesaria y suficiente para que dos conjuntos A y B sean distintos es que exista, al menos, un elemento en $\mathscr{U}$ que esté en A y no esté en B o que haya, al menos, un elemento en $\mathscr{U}$ que esté en B y no esté en A.

■

3.3 Inclusión de Conjuntos

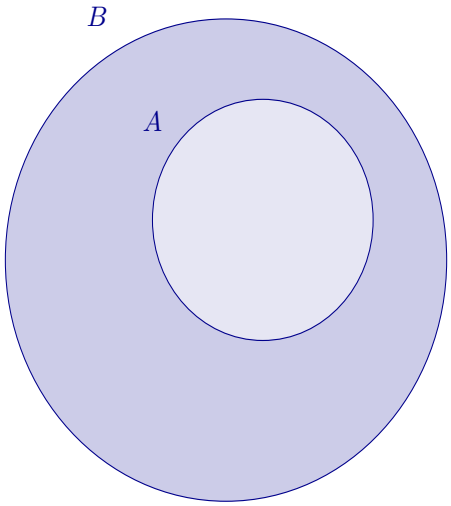
3.3.1 Subconjuntos

Sean A y B dos conjuntos. Diremos que A está contenido en B o que es un subconjunto de B, y lo notaremos por $A \subseteq B$, si cada elemento de A es un elemento de B, es decir,

$$A \subseteq B \Longleftrightarrow \forall x, (x \in A \longrightarrow x \in B)$$

También puede decirse que B contiene a A, en cuyo caso escribiremos $B \supseteq A$.

Un Diagrama de Venn que expresa gráficamente la inclusión es el siguiente:



El conjunto A está incluido en el B. $A \subseteq B$

■

Ejemplo 3.9

Probar que el conjunto $A = \{x \in \mathbb{R} : x^2 - 3x + 2 = 0\}$ *es subconjunto de* $B = \{1, 2, 3\}$

Solución

En efecto, sea a cualquier número real. Entonces,

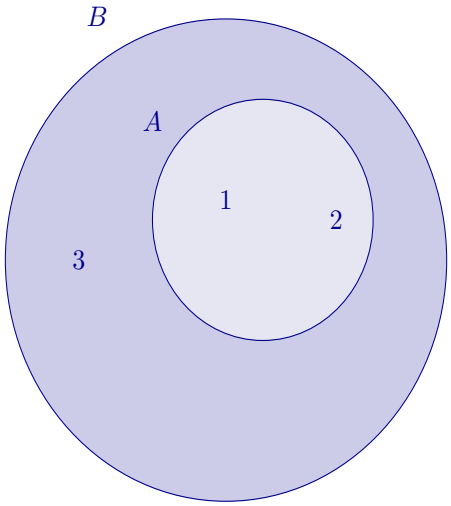
$$\begin{aligned} a \in A &\implies a^2 - 3a + 2 = 0 \\ &\implies a = \frac{3 \pm \sqrt{9 - 4 \cdot 1 \cdot 2}}{2} \\ &\implies a = \frac{3 \pm 1}{2} \\ &\implies \begin{cases} a = 1 \\ \text{ó} \\ a = 2 \end{cases} \\ &\implies a \in B \end{aligned}$$

Como a es un número real arbitrario,

$$\forall x, (x \in A \longrightarrow x \in B)$$

de aquí que, de acuerdo con la definición de subconjunto, (3.3.1), tengamos que $A \subseteq B$.

Un diagrama de Venn representativo de la situación es:



El conjunto A está incluido en el B. $A \subseteq B$

■

Ejemplo 3.10

Obtener una condición necesaria y suficiente para un conjunto A no esté contenido en otro conjunto B.

Solución

Sean A y B dos conjuntos cualesquiera de un universal arbitrario $\mathscr{U}$. Entonces, aplicando el mismo razonamiento que en el ejemplo 3.8

$$\begin{aligned} A \nsubseteq B &\iff \neg\,(A \subseteq B) \\ &\iff \neg\,[\forall x, (x \in A \longrightarrow x \in B)] \\ &\iff \exists x : (x \in A \wedge x \notin B) \end{aligned}$$

es decir, una condición necesaria y suficiente para que A no esté contenido en B es que exista, al menos, un elemento en A que no esté en B.

■

Ejemplo 3.11

¿Es $B = \{1, 2, 3\}$ un subconjunto de $A = \left\{x \in \mathbb{R} : x^2 - 3x + 2 = 0\right\}$?

Solución

No, ya que $3 \in B$ y, sin embargo, $3^2 - 3 \cdot 3 + 2 = 2 \neq 0$, luego $3 \notin A$, es decir, hemos encontrado un elemento en B que no está en A, por tanto, $B \nsubseteq A$.

■

3.3.2 Inclusión Estricta

Si $A \subseteq B$ y además B tiene, al menos, un elemento que no está en A, diremos que A está estrictamente incluido en B o que A es un subconjunto propio de B y lo notaremos por $A \subset B$ o por $A \subsetneq B$, es decir,

$$A \subset B \Longleftrightarrow A \subseteq B \ y \ [\exists x : (x \in B \ y \ x \notin A)]$$

■

Ejemplo 3.12

En el conjunto universal de los enteros positivos, $\mathbb{Z}^+$, se consideran los conjuntos:

A: Conjunto formado por todos los múltiplos de 3 *más* 3.

B: Conjunto formado por todos los múltiplos de 3.

Probar que A está incluido estrictamente en B.

Solución

La definición, por comprensión de los conjuntos A y B es:

$$A = \{n : n = 3q + 3\}$$
$$B = \{n : n = 3q\}$$

siendo q, naturalmente, un entero positivo.

Pues bien, sea a cualquier entero positivo. Entonces,

$$\begin{aligned} a \in A &\iff a = 3q_1 + 3, \ q_1 \in \mathbb{Z}^+ \\ &\iff a = 3(q_1 + 1), \ q_1 \in \mathbb{Z}^+ \\ &\Longrightarrow a = 3q, \ q \in \mathbb{Z}^+ \qquad \{\text{Tomando } q = q_1 + 1\} \\ &\iff a \in B \end{aligned}$$

Por lo tanto, se verifica que

$$a \in A \longrightarrow a \in B$$

siendo a cualquiera de $\mathbb{Z}^+$, lo cual significa que la proposición

$$\forall n, (n \in A \longrightarrow n \in B)$$

es verdadera, de aquí que por la definición de inclusión, (3.3.1), tengamos que $A \subseteq B$.

Por otra parte, tomando $a = 3$, tendremos que

- $a = 3 \cdot 1, \ 1 \in \mathbb{Z}^+$, es decir, $a \in B$.
- a no se puede escribir en la forma $3q + 3$ ya que, en tal caso, q debería ser 0 lo cual, siendo $q \geqslant 1$, es imposible, por lo tanto,
$$a \neq 3q + 3, \ \forall q \in \mathbb{Z}^+$$
y, consecuentemente, $a \notin A$.

Hemos encontrado, pues, un entero positivo, a, que pertenece a A y que no pertenece a B, por lo tanto es verdad la proposición,

$$\exists n : (n \in B \wedge n \notin A)$$

Resumiendo tenemos que

$$A \subseteq B \ \wedge \ \exists n : (n \in B \wedge n \notin A)$$

lo cual, por (3.3.2), equivale a decir que

$$A \subset B$$

o sea, A está incluido estrictamente en B.

■

Ejemplo 3.13

Obtener una condición necesaria y suficiente para que un conjunto A esté estrictamente contenido en otro B.

Solución

Sean A y B dos conjuntos cualesquiera de un universal arbitrario $\mathscr{U}$. Según la definición anterior,

$$A \subset B \Longleftrightarrow A \subseteq B \text{ y } [\exists x : (x \in B \text{ y } x \notin A)]$$

y según lo que vimos en el ejemplo 3.8 , esto significa que

$$A \subset B \Longleftrightarrow A \subseteq B \text{ y } A \neq B$$

Por lo tanto, una condición necesaria y suficiente para que un conjunto esté contenido en otro es que la inclusión sea estricta y que sean distintos.

■

Nota 3.4 Los conjuntos también son objetos, luego pueden ser elementos de otros conjuntos, por ejemplo, el conjunto

$$A = \{\{a, b\}, \{a, c\}, \{b\}, \{c\}\}$$

tiene cuatro elementos que son los conjuntos $\{a, b\}, \{a, c\}, \{b\}$ y $\{c\}$.

Si tuviéramos una caja con tres paquetes de caramelos, la consideraríamos como una caja con paquetes antes que una caja con caramelos, por lo que se trataría de un conjunto (la caja) con tres elementos (los paquetes).

En general, si A es un conjunto, entonces $\{A\}$ es un conjunto con un único elemento, A, sin importarnos cuantos elementos tenga A.

Un caso curioso ocurre con el conjunto vacío, $\emptyset$. Una caja con un paquete vacío de caramelos no es una caja vacía ya que contiene algo, un paquete. De la misma forma $\{\emptyset\}$ es un conjunto con un elemento mientras que $\emptyset$ no contiene elementos, así que $\emptyset$ y $\{\emptyset\}$ son conjuntos distintos. Tendremos que $\emptyset \in \{\emptyset\}$ e incluso $\emptyset \subseteq \{\emptyset\}$, pero $\emptyset \neq \{\emptyset\}$.

■

Ejemplo 3.14

Describir brevemente la diferencia entre los conjuntos $\{a\}$ *y* $\{\{a\}\}$ *y entre los conjuntos* $\emptyset$, $\{\emptyset\}$ *y* $\{\emptyset, \{\emptyset\}\}$.

Solución

- $\{a\}$ es un conjunto cuyo único elemento es el a.
- $\{\{a\}\}$ es un conjunto cuyo único elemento es el conjunto $\{a\}$.
- $\emptyset$. Conjunto único que no tiene elementos (3.2.6).
- $\{\emptyset\}$. Conjunto con un único elemento que es el $\emptyset$.
- $\{\emptyset, \{\emptyset\}\}$. Conjunto con dos elementos, el $\emptyset$ y el $\{\emptyset\}$.

■

3.3.3 Proposición

Sea $\mathscr{U}$ *el conjunto universal y* A *un conjunto cualquiera. Entonces* $A \subseteq \mathscr{U}$.

Demostración

La demostración es un ejemplo de *demostración trivial* basada en la definición de conjunto universal, (3.2.5), que nos permite afirmar que la proposición $\forall x, x \in \mathscr{U}$ es una tautología, es decir es verdadera siempre.

Pues bien, sea a cualquiera de $\mathscr{U}$. Como $a \in \mathscr{U}$ es verdad, la proposición condicional,

$$a \in A \longrightarrow a \in \mathscr{U}$$

es verdadera independientemente de que $a \in A$ sea verdadera o falsa, y como a estaba arbitrariamente elegido en $\mathscr{U}$,

$$\forall x, (x \in A \longrightarrow x \in \mathscr{U})$$

es decir,

$$A \subseteq \mathscr{U}$$

■

3.3.4 Proposición

Sea A *un conjunto cualquiera, entonces* $\emptyset \subseteq A$

Demostración

La demostración es un ejemplo de *demostración vacía* basada en la definición de conjunto vacío, (3.2.6), que nos permite afirmar que la proposición $\exists x : x \in \emptyset$ es falsa siempre.

Pues bien, sea a cualquiera de $\mathscr{U}$. Como $a \in \emptyset$ es falsa, la proposición condicional,

$$a \in \emptyset \longrightarrow a \in A$$

es verdadera independientemente de que $a \in A$ sea verdadera o falsa, y como a estaba arbitrariamente elegido en $\mathscr{U}$,

$$\forall x, (x \in \emptyset \longrightarrow x \in A)$$

es decir,

$$\emptyset \subseteq A$$

■

Ejemplo 3.15

Obtener los subconjuntos de los siguientes conjuntos:

(a) $\{a, b\}$

(b) $\{\{a\}\}$

Solución

(a) Veamos cuáles son los subconjuntos del conjunto $\{a, b\}$.

De la proposición 3.3.4 se sigue que el conjunto vacío, $\emptyset$, es uno de ellos. Por otra parte, $a \in \{a, b\}$ y $b \in \{a, b\}$ luego por la definición de subconjunto, (3.3.1), $\{a\}$, $\{b\}$ y $\{a, b\}$ son subconjuntos de $\{a, b\}$. Por lo tanto, el conjunto propuesto tiene cuatro subconjuntos,

$$\emptyset,\ \{a\},\ \{b\}\ \text{ y }\ \{a, b\}$$

Obsérvese que $\{a\} \subseteq \{a, b\}$ y $a \in \{a, b\}$ pero $a \not\subseteq \{a, b\}$ y $\{a\} \notin \{a, b\}$, es decir, a es un elemento pero no un subconjunto de $\{a, b\}$ y $\{a\}$ es un subconjunto, pero no un elemento de $\{a, b\}$.

(b) Veamos ahora los subconjuntos de $\{\{a\}\}$.

Este conjunto es un conjunto unitario ya que tiene un único elemento que es el conjunto $\{a\}$. Sus subconjuntos son, pues, el $\emptyset$ y el propio $\{\{a\}\}$.

■

Ejemplo 3.16

Determinar todos los subconjuntos de los siguientes conjuntos:

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

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

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

(d) $\{\emptyset\}$

(e) $\{\emptyset, \{\emptyset\}\}$

(f) $\{\{1, 2\}, \{2, 1, 1\}, \{2, 1, 1, 2\}\}$

(g) $\{\{\emptyset, 2\}, \{2\}\}$

Solución

Utilizaremos la definición de subconjunto, 3.3.1,

$$A \subseteq B \Longleftrightarrow \forall x, (x \in A \longrightarrow x \in B)$$

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

$\emptyset \subseteq \{1,2,3\}$ (3.3.4).

$1 \in \{1,2,3\}$, luego $\{1\} \subseteq \{1,2,3\}$.

$2 \in \{1,2,3\}$, luego $\{2\} \subseteq \{1,2,3\}$.

$3 \in \{1,2,3\}$, luego $\{3\} \subseteq \{1,2,3\}$.

$1 \in \{1,2,3\}$ y $2 \in \{1,2,3\}$, luego $\{1,2\} \subseteq \{1,2,3\}$.

$1 \in \{1,2,3\}$ y $3 \in \{1,2,3\}$, luego $\{1,3\} \subseteq \{1,2,3\}$.

$2 \in \{1,2,3\}$ y $3 \in \{1,2,3\}$, luego $\{2,3\} \subseteq \{1,2,3\}$.

$1 \in \{1,2,3\}$, $2 \in \{1,2,3\}$ y $3 \in \{1,2,3\}$, luego $\{1,2,3\} \subseteq \{1,2,3\}$.

por lo tanto, los subconjuntos de $\{1,2,3\}$ son

$$\emptyset, \{1\}, \{2\}, \{3\}, \{1,2\}, \{1,3\}, \{2,3\} \text{ y } \{1,2,3\}$$

(b) $\{1,\{2,3\}\}$. Aquí tenemos que 1 y $\{2,3\}$ son los dos elementos que tiene este conjunto, luego razonando igual que en el apartado anterior, sus subconjuntos son:

$$\emptyset, \{1\}, \{\{2,3\}\} \text{ y } \{1,\{2,3\}\}$$

(c) $\{\{1,\{2,3\}\}\}$. Este conjunto tiene un único elemento que es $\{1,\{2,3\}\}$, por lo tanto sus subconjuntos son:

$$\emptyset \text{ y } \{\{1,\{2,3\}\}\}$$

(d) $\{\emptyset\}$. Este conjunto tiene un elemento que es $\emptyset$, por lo tanto tiene dos subconjuntos,

$$\emptyset \text{ (3.3.4) y } \{\emptyset\} \text{ (3.3.1)}$$

(e) $\{\emptyset,\{\emptyset\}\}$. Este conjunto tiene dos elementos, $\emptyset$ y $\{\emptyset\}$, por lo tanto sus subconjuntos son

$$\emptyset \text{ (3.3.4) y } \{\emptyset\}, \{\{\emptyset\}\} \text{ y } \{\emptyset,\{\emptyset\}\} \text{ (3.3.1)}$$

(f) $\{\{1,2\},\{2,1,1\},\{2,1,1,2\}\}$. Obsérvese que

$$\{1,2\} = \{2,1,1\} = \{2,1,1,2\}$$

luego el conjunto propuesto es

$$\{\{1,2\}\}$$

y, por lo tanto, sus subconjuntos son

$$\emptyset \text{ y } \{\{1,2\}\}$$

(g) $\{\{\emptyset,2\},\{2\}\}$. Siguiendo un razonamiento idéntico a los anteriores apartados, sus subconjuntos son

$$\emptyset, \{\{\emptyset,2\}\}, \{\{2\}\} \text{ y } \{\{\emptyset,2\},\{2\}\}$$

■

3.3.5 Caracterización de la Igualdad

Sean A y B dos conjuntos cualesquiera de un universal arbitrario $\mathscr{U}$. Entonces $A = B$ si, y sólo si $A \subseteq B$ y $B \subseteq A$.

Demostración

"Sólo si." $A = B \Longrightarrow A \subseteq B$ y $B \subseteq A$

En efecto, supongamos que $A = B$. Entonces por el axioma de extensión, (3.2.7), cada elemento de A es un elemento de B luego por definición de subconjunto, (3.3.1), $A \subseteq B$. Así pues, si $A = B$, entonces $A \subseteq B$. Utilizando los mismos argumentos, aunque intercambiando los papeles de A y B, tendremos que si $A = B$, entonces $B \subseteq A$. De aquí que

$$(A = B \Longrightarrow A \subseteq B) \text{ y } (A = B \Longrightarrow B \subseteq A)$$

lo cual equivale a

$$A = B \Longrightarrow A \subseteq B \text{ y } \ B \subseteq A$$

"Si." $A \subseteq B$ y $B \subseteq A \Longrightarrow A = B$

En efecto,

$$(A \subseteq B) \text{ y } (B \subseteq A) \Longrightarrow [(\forall x, (x \in A \longrightarrow x \in B)] \ \text{ y } \ [(\forall x, (x \in B \longrightarrow x \in A)]$$

consecuentemente, por el axioma de extensión, (3.2.7),

$$A = B$$

Este teorema lo utilizaremos con mucha frecuencia para comprobar que dos conjuntos son iguales, es decir, para probar que $A = B$, probaremos que $A \subseteq B$ y $B \subseteq A$.

■

3.3.6 Corolario

De la caracterización anterior se sigue que para cualquier conjunto A, se verifica que $A \subseteq A$.

■

3.3.7 Transitividad de la inclusión

Sean A, B y C tres conjuntos cualesquiera de un universal arbitrario $\mathscr{U}$. Si $A \subseteq B$ y $B \subseteq C$, entonces $A \subseteq C$.

Demostración

En efecto, sea a un elemento cualquiera de $\mathscr{U}$. Entonces,

$$\begin{aligned} a \in A &\Longrightarrow a \in B \quad \{\text{por hipótesis } A \subseteq B\} \\ &\Longrightarrow a \in C \quad \{\text{por hipótesis } B \subseteq C\} \end{aligned}$$

y, por la arbitrariedad de la elección de a, esto quiere decir que

$$\forall x, (x \in A \longrightarrow x \in C)$$

por lo tanto,

$$A \subseteq C$$

■

Ejemplo 3.17

Estudiar la relación que existe entre los siguientes conjuntos:

$A = \{1, 2\}$

$B = \{1, 3\}$

$C = \{x \in \mathbb{R} : x^2 - 4x + 3 = 0\}$

$D = \{x \in \mathbb{R} : x^2 - 3x + 2 = 0\}$

$E = \{x \in \mathbb{Z}^+ : x < 3\}$

$F = \{x \in \mathbb{Z}^+ : x \text{ es impar y } x < 5\}$

Solución

A y B son distintos, ya que $2 \in A$ y $2 \notin B$ y $3 \in B$ y $3 \notin A$. Así pues, hemos encontrado un elemento en A que no está en B y un elemento en B que no está en A. Por tanto, por el ejemplo 3.8 $A \neq B$.

Ahora observemos lo siguiente:

Sea a un número real arbitrario. Entonces,

$$a \in C \iff a^2 - 4a + 3 = 0 \iff a = 1 \text{ ó } a = 3 \iff a \in B$$

y, como a es cualquiera, esto significa que

$$\forall x, (x \in C \longleftrightarrow x \in B)$$

aplicamos el axioma de extensión, (3.2.7) y $C = B$.

Aplicando idéntico razonamiento,

$$a \in D \iff a^2 - 3a + 2 = 0 \iff a = 1 \text{ ó } a = 2 \iff a \in A$$

es decir, $A = D$.

Sea a un entero positivo cualquiera. Entonces,

$$a \in E \iff a < 3 \iff a = 1 \text{ ó } a = 2 \iff a \in A$$

como a es cualquiera, esto significa que

$$\forall n, (n \in E \longleftrightarrow n \in A)$$

aplicamos el axioma de extensión, (3.2.7) y $A = E$.

Sea a un entero positivo cualquiera. Entonces,

$$a \in F \iff a \text{ es impar y } a < 5 \iff a = 1 \text{ ó } a = 3 \iff a \in B$$

y, aplicando el mismo razonamiento que en el anterior, $F = B$.

Consecuentemente,

$A \neq B$				
$A \neq C$	$B = C$			
$A = D$	$B \neq D$	$C \neq D$		
$A = E$	$B \neq E$	$C \neq E$	$D = E$	
$A \neq F$	$B = F$	$C = F$	$D \neq F$	$E \neq F$

■

Nota 3.5 Con el conjunto vacío puede construirse una sucesión infinita de conjuntos distintos.

- Por ejemplo, en la sucesión,
$$\emptyset, \{\emptyset\}, \{\{\emptyset\}\}, \{\{\{\emptyset\}\}\}, \ldots$$
el primer conjunto no tiene ningún elemento y cada uno de los restantes tiene, exactamente, un elemento que es el conjunto que le precede en la sucesión.

- En la sucesión,
$$\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\}, \{\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\}\}, \{\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\}, \{\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\}\}\}, \ldots$$
cada conjunto tiene como elementos todos los conjuntos que le preceden en la sucesión. Así, contando desde cero, el conjunto que ocupa el lugar k tiene k elementos.

■

3.4 Conjunto de las Partes de un Conjunto

Dado un conjunto A, si nos referimos a algunos de sus subconjuntos estaríamos considerando un conjunto de conjuntos. En tales casos hablaremos de una clase de conjuntos o colección de conjuntos en vez de un conjunto de conjuntos. Si quisiéramos considerar algunos de los conjuntos de una clase dada de conjuntos, entonces hablaremos de una subclase o de una subcolección.

Ejemplo 3.18

Sea $A = \{a, b, c, d, e\}$. Obtener, $\mathscr{A}$, clase de subconjuntos de A que contienen exactamente tres elementos de A.

Solución

$$\mathscr{A} = \{\{a, b, c\}, \{a, b, d\}, \{a, b, e\}, \{a, c, d\}, \{a, c, e\}, \{a, d, e\}, \{b, c, d\}, \{b, c, e\}, \{c, d, e\}\}$$

siendo los elementos de $\mathscr{A}$ los conjuntos:

$$\{a, b, c\}, \{a, b, d\}, \{a, b, e\}, \{a, c, d\}, \{a, c, e\}, \{a, d, e\}, \{b, c, d\}, \{b, c, e\} \text{ y } \{c, d, e\}$$

■

3.4.1 Definición

Dado un conjunto A, llamaremos conjunto de las partes de A a la clase o colección de todos los subconjuntos de A y se nota por $\mathscr{P}(A)$. Es decir, si X es un conjunto cualquiera de $\mathscr{U}$, entonces

$$X \in \mathscr{P}(A) \longleftrightarrow X \subseteq A$$

Ejemplo 3.19

Sea $A = \{1, 2, 3\}$. Obtener el conjunto de las partes de A.

Solución

$$\mathscr{P}(A) = \{\emptyset, \{1\}, \{2\}, \{3\}, \{1, 2\}, \{1, 3\}, \{2, 3\}, \{1, 2, 3\}\}$$

■

Ejemplo 3.20

Especificar el conjunto de las partes para cada uno de los conjuntos siguientes:

(a) $\{a, b, c\}$

(b) $\{\{a, b\}, \{c\}\}$

(c) $\{\{a, b\}, \{b, a\}, \{a, b, b\}\}$

Solución

(a) $\{a, b, c\}$

$$\mathscr{P}(\{a, b, c\}) = \{\emptyset, \{a\}, \{b\}, \{c\}, \{a, b\}, \{a, c\}, \{b, c\}, \{a, b, c\}\}$$

(b) $\{\{a, b\}, \{c\}\}$

$$\mathscr{P}(\{\{a, b\}, \{c\}\}) = \{\emptyset, \{\{a, b\}\}, \{\{c\}\}\{\{a, b\}, \{c\}\}\}$$

(c) $\{\{a, b\}, \{b, a\}, \{a, b, b\}\}$

$$\mathscr{P}(\{\{a, b\}, \{b, a\}, \{a, b, b\}\}) = \mathscr{P}(\{a, b\}) = \{\emptyset, \{a, b\}\{\{a, b\}\}\}$$

■

Lección 4

Operaciones con Conjuntos

4.1 Definiciones

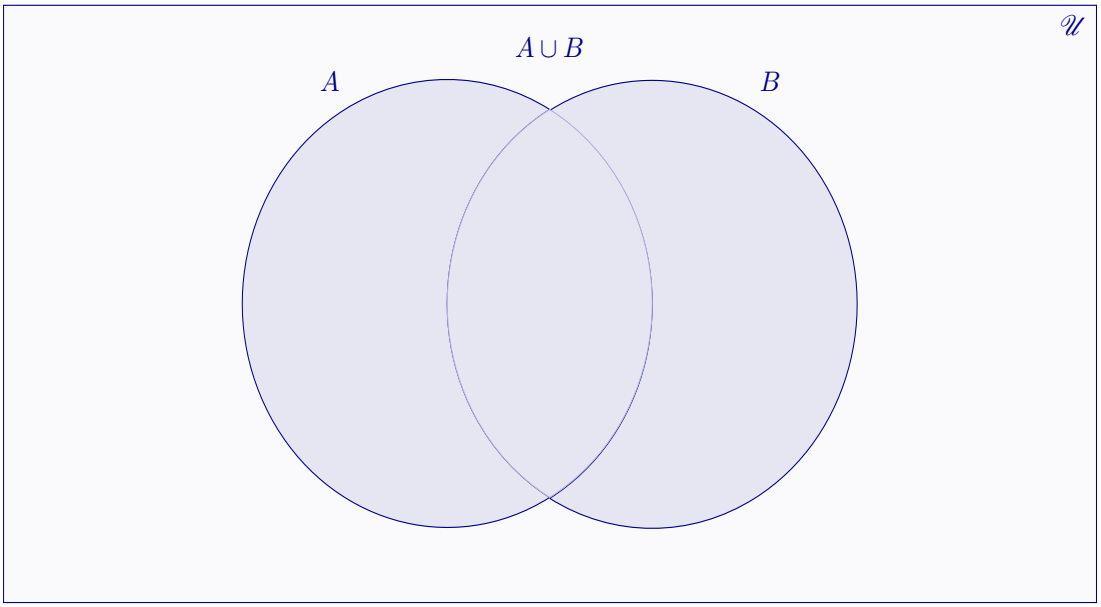
Introduciremos las operaciones con conjuntos que nos van a permitir obtener nuevos conjuntos, partiendo de conjuntos ya conocidos. A y B serán dos conjuntos cualesquiera de un universal arbitrario $\mathscr{U}$.

4.1.1 Unión

La unión de dos conjuntos A y B es el conjunto formado por todos los elementos que pertenecen a A o a B. Se nota $A \cup B$.

$$A \cup B = \{x : x \in A \text{ ó } x \in B\}.$$

La disyunción se utiliza en el sentido inclusivo, es decir, significa "y/o".



■

Ejemplo 4.1

Hallar la unión de los conjuntos $A = \{a, b, c, d, e\}$ *y* $B = \{b, d, f, g\}$

Solución

En efecto, sea n un elemento arbitrario del universal que contiene a los dos conjuntos. Según la definición de unión,

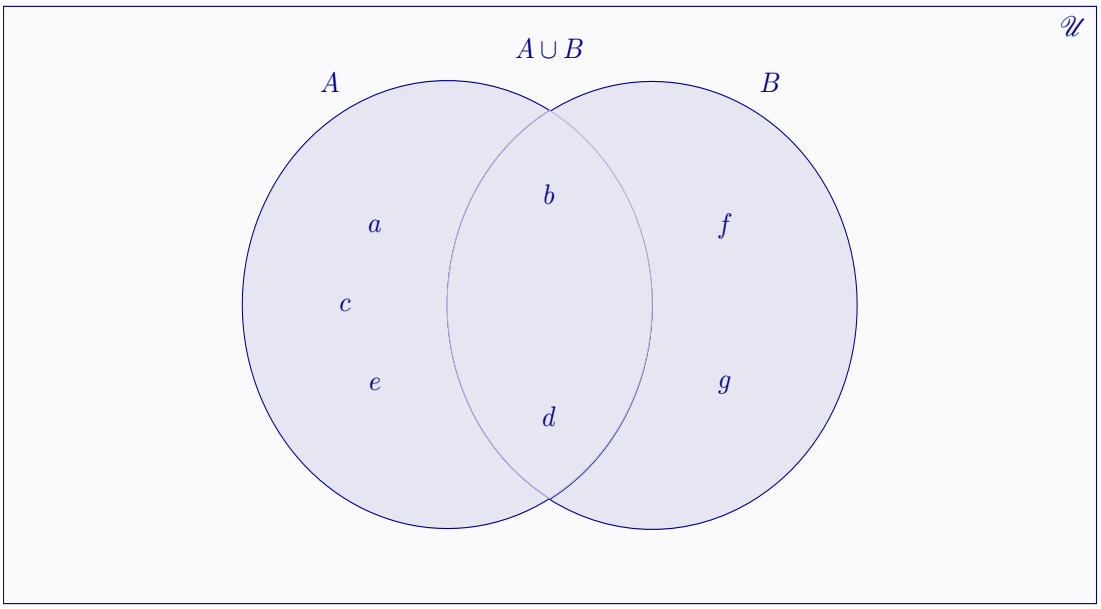
$$\begin{aligned} n \in A \cup B &\iff n \in A \text{ ó } n \in B \\ &\iff (n = a \text{ ó } n = b \text{ ó } n = c \text{ ó } n = d \text{ ó } n = e) \text{ ó } (n = b \text{ ó } n = d \text{ ó } n = f \text{ ó } n = g) \\ &\iff n = a \text{ ó } n = b \text{ ó } n = c \text{ ó } n = d \text{ ó } n = e \text{ ó } n = f \text{ ó } n = g \\ &\iff n \in \{a, b, c, d, e, f, g\} \end{aligned}$$

Como n es cualquiera del universal, hemos probado que

$$\forall x, (x \in A \cup B \longleftrightarrow x \in \{a, b, c, d, e, f, g\})$$

y por el axioma de extensión, (3.2.7),

$$A \cup B = \{a, b, c, d, e, f, g\}$$



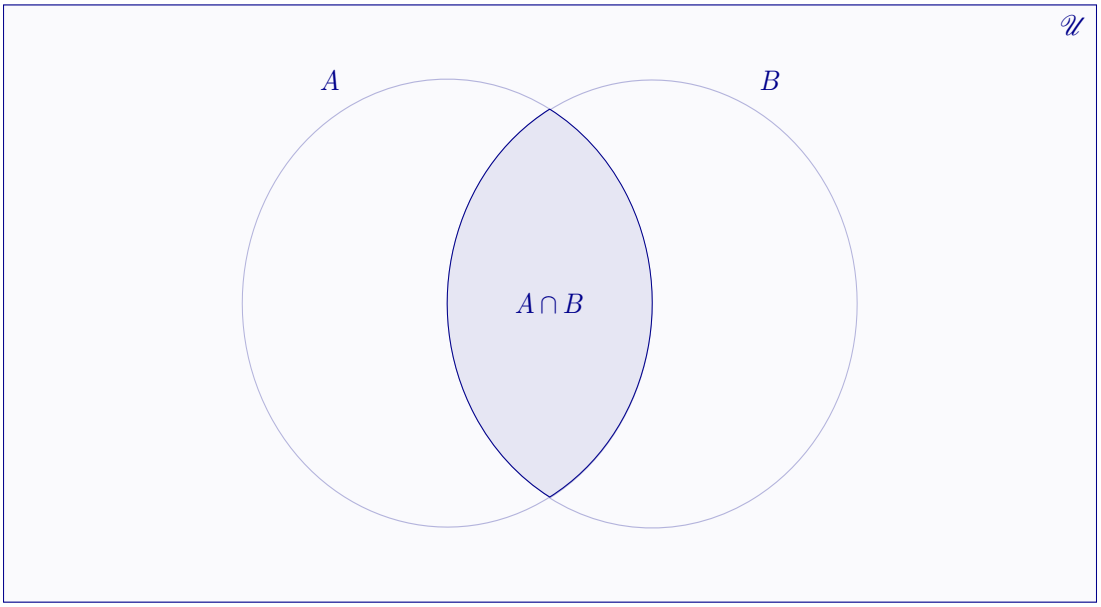
■

4.1.2 Intersección

La intersección de dos conjuntos A *y* B *es el conjunto formado por todos los elementos que pertenecen a* A *y a* B*. Se nota* $A \cap B$*.*

$$A \cap B = \{x : x \in A \text{ y } x \in B\}$$

Si A *y* B *no tienen elementos en común, es decir, si* $A \cap B = \emptyset$*, entonces diremos que* A *y* B *son conjuntos disjuntos.*



■

Ejemplo 4.2

Hallar la intersección de los conjuntos $A = \{a, b, c, d, e\}$ *y* $B = \{b, d, f, g\}$

Solución

Sea n un elemento arbitrario del universal que contiene ambos conjuntos. Por la definición de intersección,

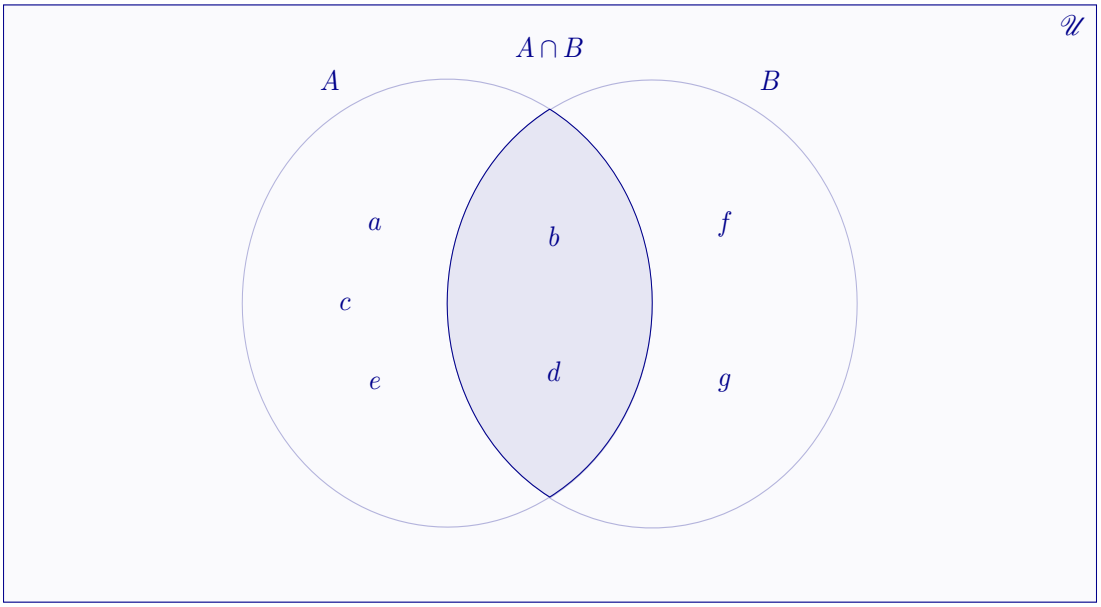
$$\begin{aligned} n \in A \cap B &\iff n \in A \text{ y } n \in B \\ &\iff n \in \{a, b, c, d, e\} \text{ y } n \in \{b, d, f, g\} \\ &\iff n = b \text{ ó } n = d \\ &\iff n \in \{b, d\} \end{aligned}$$

Como n es cualquiera del universal,

$$\forall x, (x \in A \cap B \longleftrightarrow x \in \{b, d, \})$$

y por el axioma de extensión, (3.2.7),

$$A \cap B = \{b, d\}$$



■

4.1.3 Diferencia

La diferencia entre dos conjuntos A y B es el conjunto formado por todos los elementos que pertenecen a A y no pertenecen a B. Se nota por $A \setminus B$.

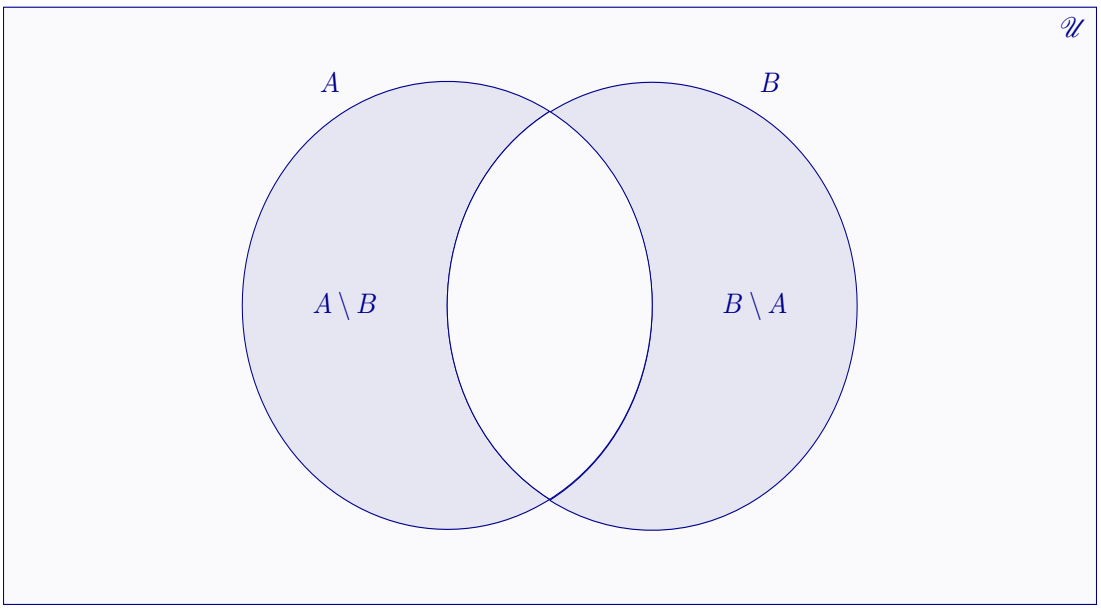
$$A \setminus B = \{x : x \in A \text{ y } x \notin B\}$$

El conjunto $A \setminus B$ se lee "A menos B" y también recibe el nombre de complementario relativo del conjunto B respecto del conjunto A.

De la misma forma se define la diferencia entre B y A, es decir el conjunto formado todos los elementos que pertenecen a B y no pertenecen a A.

$$B \setminus A = \{x : x \in B \text{ y } x \notin A\}$$

En general, $A \setminus B \neq B \setminus A$.



Ejemplo 4.3

Hallar la diferencia entre los conjuntos A y B y la diferencia entre B y A, siendo, $A = \{a, b, c, d, e\}$ y $B = \{b, d, f, g\}$

Solución

Sea t un elemento arbitrario del universal que contiene ambos conjuntos. Por la definición de diferencia,

$$\begin{aligned} t \in A \setminus B &\iff t \in A \text{ y } t \notin B \\ &\iff t \in \{a, b, c, d, e\} \text{ y } t \notin \{b, d, f, g\} \\ &\iff t = a \text{ ó } t = c \text{ ó } t = e \\ &\iff t \in \{a, c, e\} \end{aligned}$$

Como t es cualquiera del universal, hemos probado que

$$\forall x, (x \in A \setminus B \longleftrightarrow x \in \{a, c, e\})$$

y por el axioma de extensión, (3.2.7),

$$A \setminus B = \{a, c, e\}$$

Análogamente, sea t un elemento arbitrario del universal que contiene ambos conjuntos. Por la definición de diferencia,

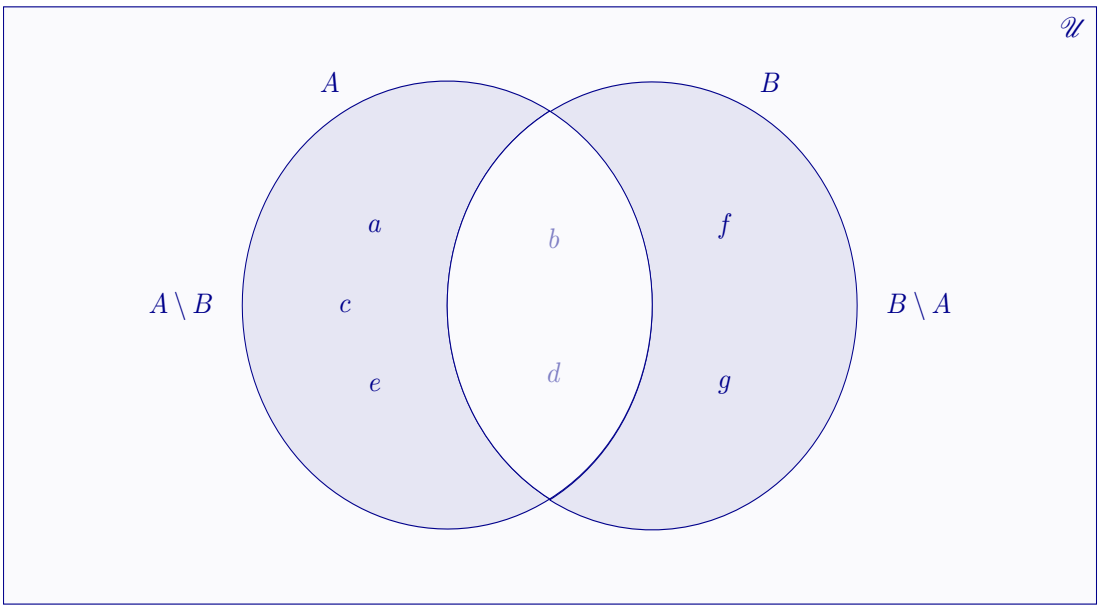
$$\begin{aligned} t \in B \setminus A &\iff t \in B \text{ y } x \notin A \\ &\iff t \in \{b, d, f, g\} \text{ y } t \notin \{a, b, c, d, e\} \\ &\iff t = f \text{ ó } t = g \\ &\iff t \in \{f, g\} \end{aligned}$$

Por lo tanto,

$$\forall x, (x \in B \setminus A \longleftrightarrow x \in \{f, g\})$$

y por el axioma de extensión, (3.2.7),

$$B \setminus A = \{f, g\}$$



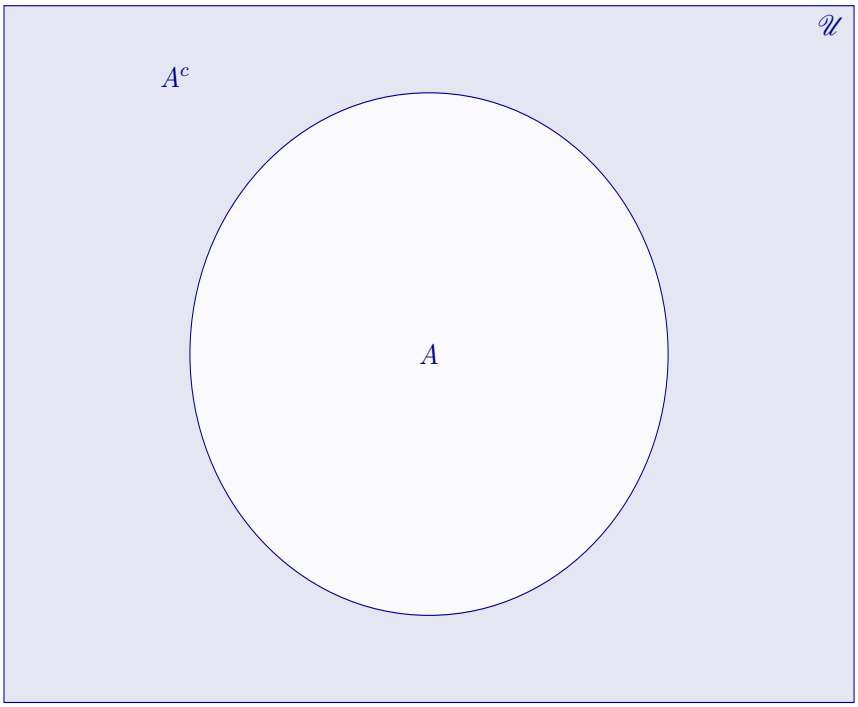
■

4.1.4 Complementario

El complementario de un conjunto A es el conjunto formado por todos los elementos del conjunto universal que no pertenecen a A. Se nota A^c.

$$A^c = \{x : x \in \mathscr{U} \text{ y } x \notin A\}$$

Obsérvese que el complementario de A es igual a la diferencia entre $\mathscr{U}$ y A, es decir, $A^c = \mathscr{U} \setminus A$.



■

Ejemplo 4.4

Sea $\mathscr{U}$ el conjunto de los números enteros positivos menores o iguales que 10 y sea A el conjunto formado por los números primos de $\mathscr{U}$. Obtener el complementario de A.

Solución

Sea a cualquiera de $\mathscr{U}$. Entonces, por definición de complementario,

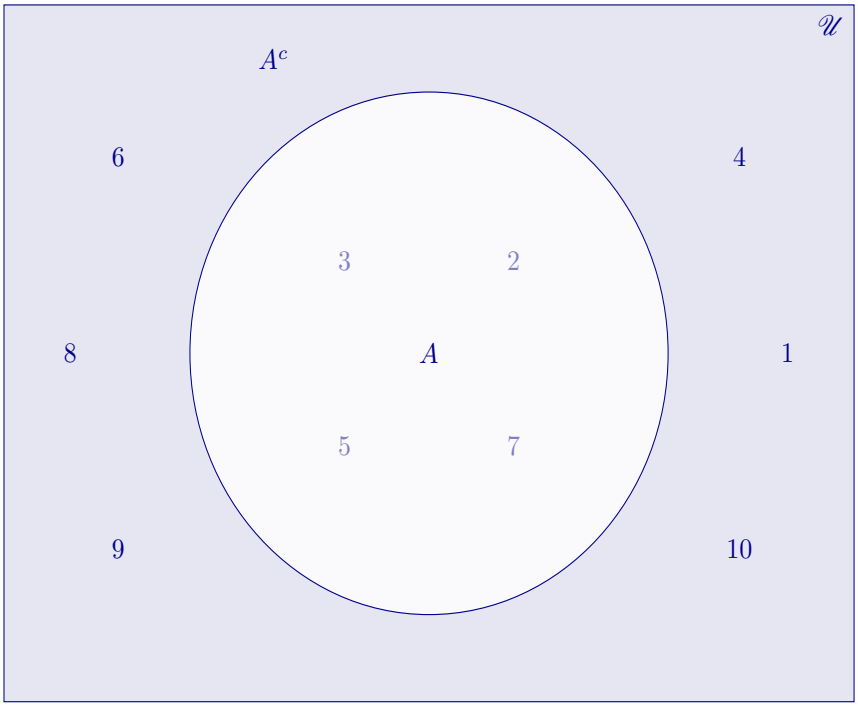
$$\begin{aligned} a \in A^c &\iff a \in \mathscr{U} \text{ y } a \notin A \\ &\iff a \leqslant 10 \text{ y } a \text{ no es primo} \\ &\iff a \leqslant 10 \text{ y } a \neq 2 \text{ y } a \neq 3 \text{ y } a \neq 5 \text{ y } a \neq 7 \\ &\iff a = 1 \text{ ó } a = 4 \text{ ó } a = 6 \text{ ó } a = 8 \text{ ó } a = 9 \text{ ó } a = 10 \\ &\iff a \in \{1, 4, 6, 8, 9, 10\} \end{aligned}$$

Por lo tanto,

$$\forall n, (n \in A^c \longleftrightarrow n \in \{1, 4, 6, 8, 9, 10\})$$

y por el axioma de extensión, (3.2.7),

$$A^c = \{1, 4, 6, 8, 9, 10\}$$



■

4.1.5 Diferencia simétrica

La diferencia simétrica entre dos conjuntos A y B es el conjunto formado por todos los elementos que pertenecen a A o a B, pero no ambos. Se nota por Se nota por $A \triangle B$.

$$A \triangle B = (A \setminus B) \cup (B \setminus A)$$

■

Ejemplo 4.5

En el conjunto universal, $\mathscr{U}$, formado por todos los números enteros positivos menores o iguales que 40, se consideran los conjuntos:

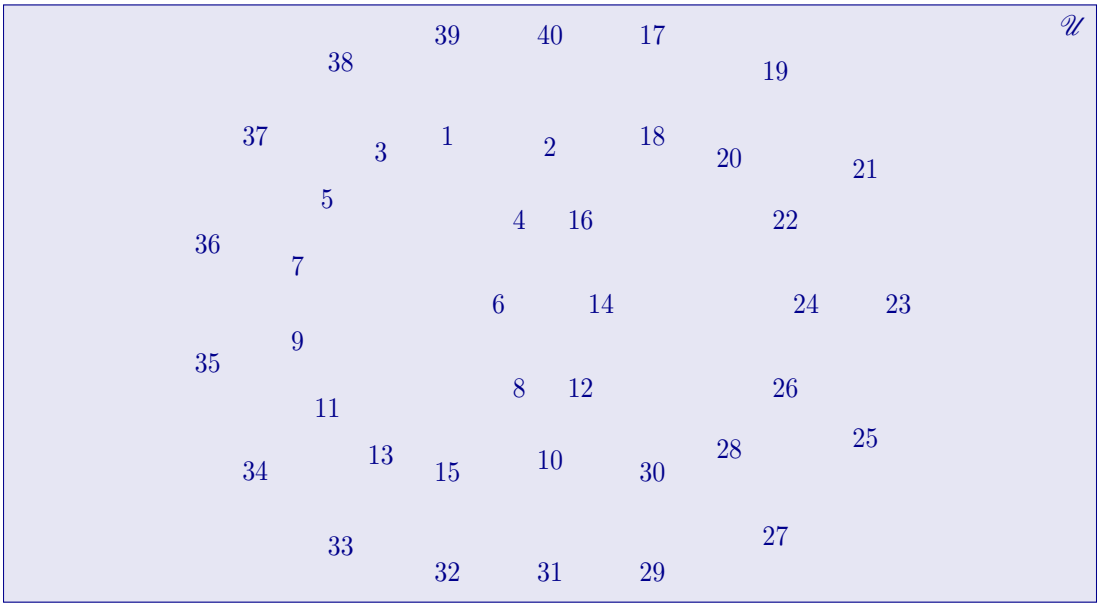
$$A = \{n : n \leqslant 16\}$$

$$B = \{n : n \text{ es par y } n \leqslant 30\}$$

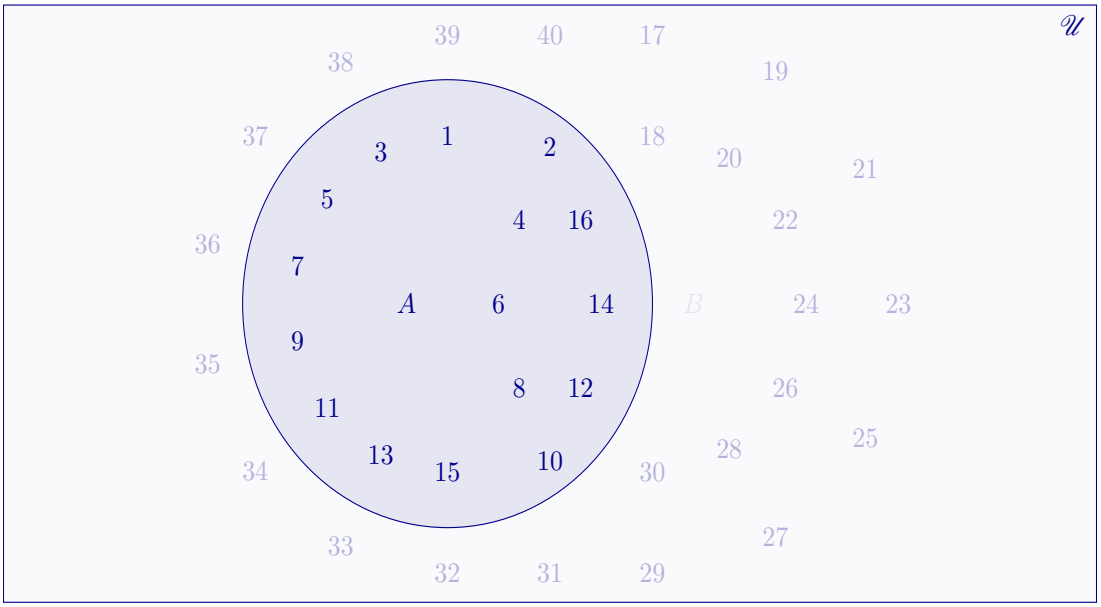
Representar gráficamente, $\mathscr{U}$, A y B y calcular $A \cup B$, $A \cap B$, $A \setminus B$, $B \setminus A$, A^c, B^c dibujando, además, sus correspondientes representaciones gráficas.

Solución

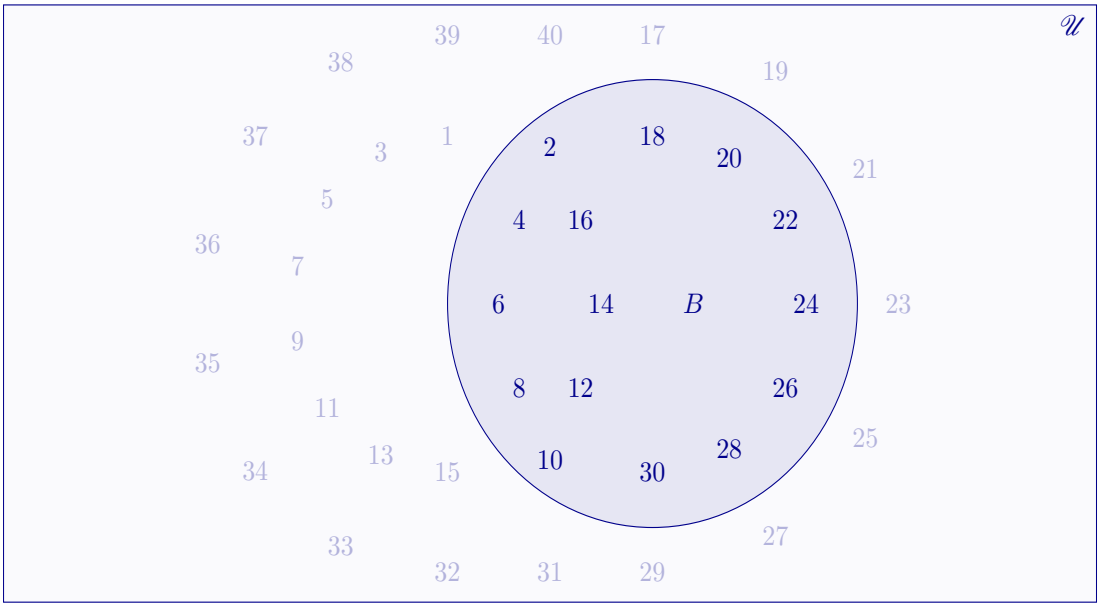
Una representación del conjunto universal, $\mathscr{U}$, podría ser la siguiente:



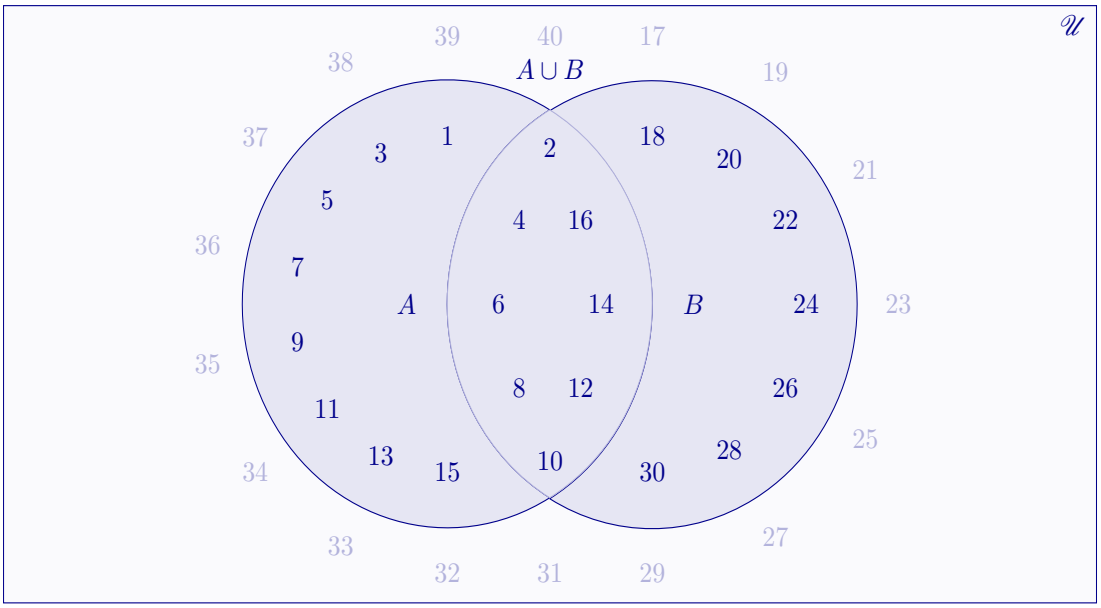
Un diagrama de Venn representativo del conjunto A, es:



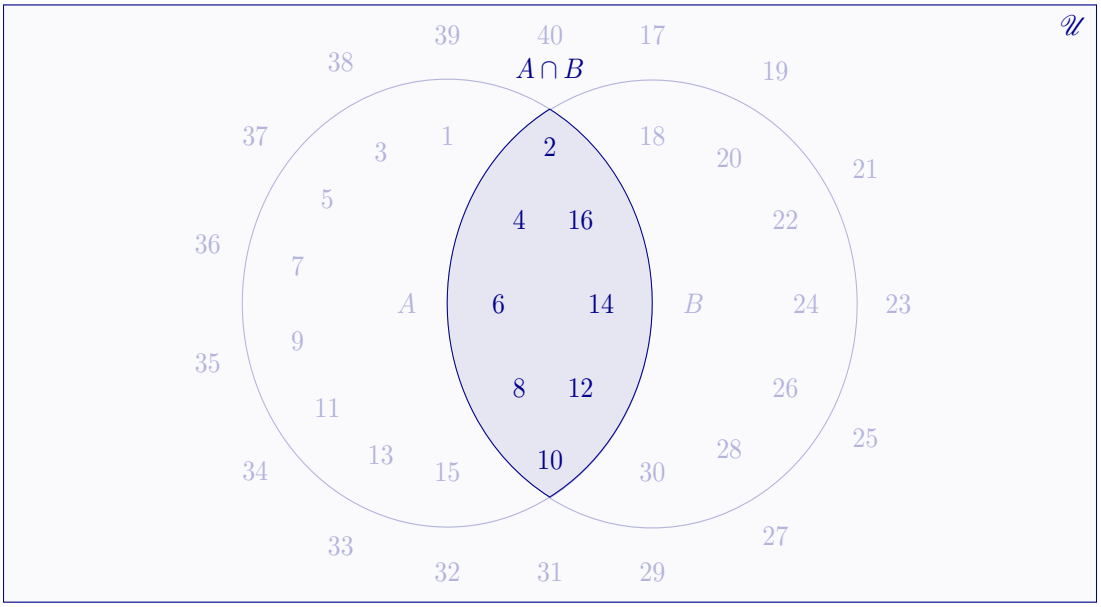
La representación gráfica del conjunto B, sería:



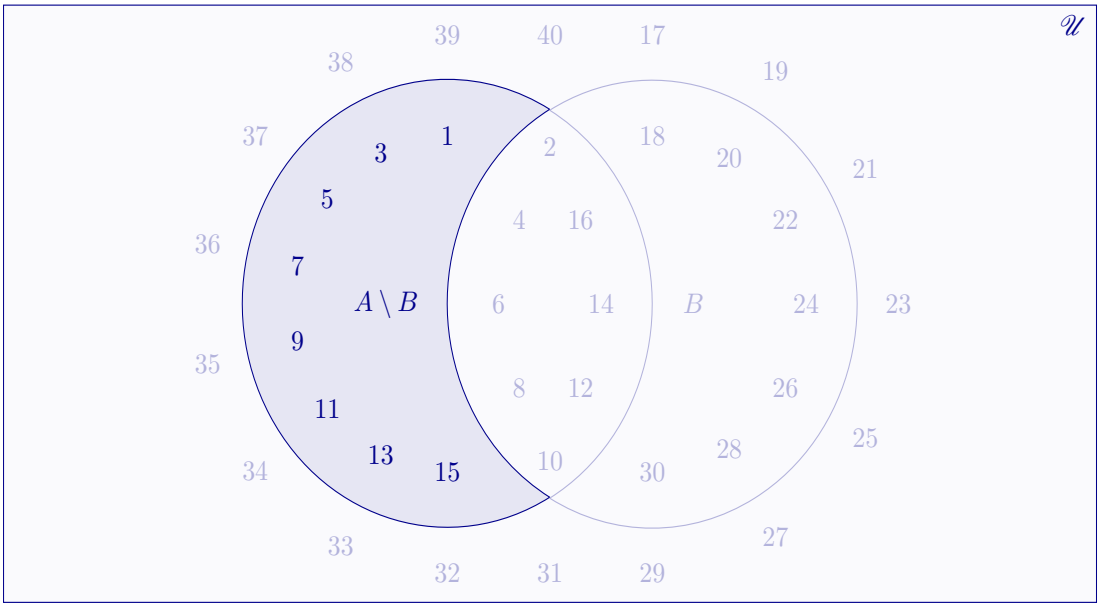
$$\begin{aligned} A \cup B &= \{n : n \leqslant 16\} \cup \{n : n \text{ es par y } n \leqslant 30\} \\ &= \{1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16\} \cup \{2,4,6,8,10,12,14,16,18,20,22,24,26,28,30\} \\ &= \{1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,18,20,22,24,26,28,30\} \end{aligned}$$



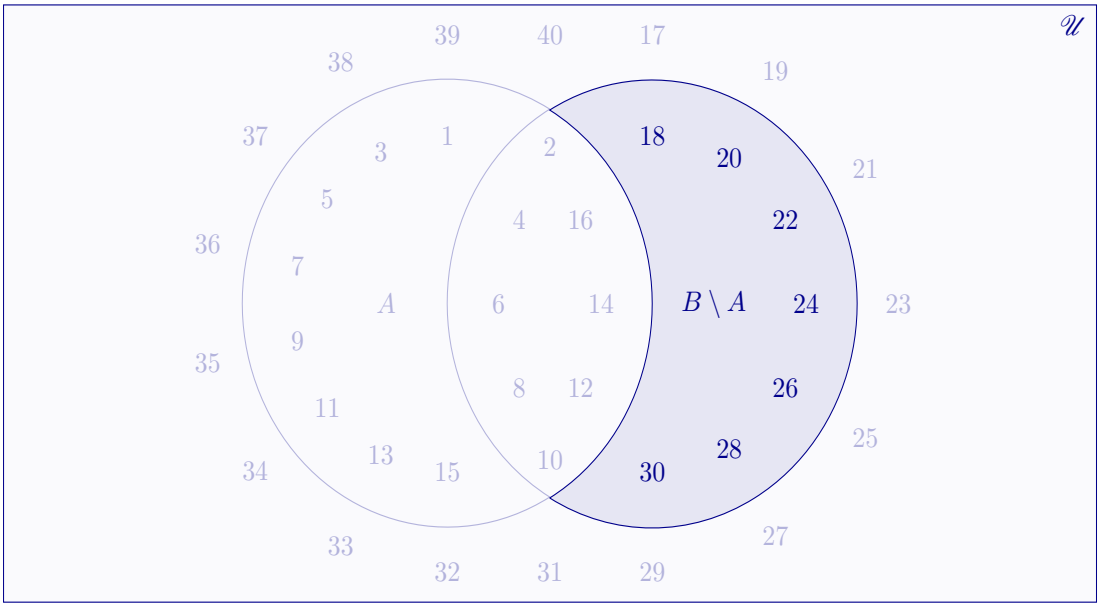
$$\begin{aligned} A \cap B &= \{n : n \leqslant 16\} \cap \{n : n \text{ es par y } n \leqslant 30\} \\ &= \{1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16\} \cap \{2,4,6,8,10,12,14,16,18,20,22,24,26,28,30\} \\ &= \{2,4,6,8,10,12,14,16\} \end{aligned}$$



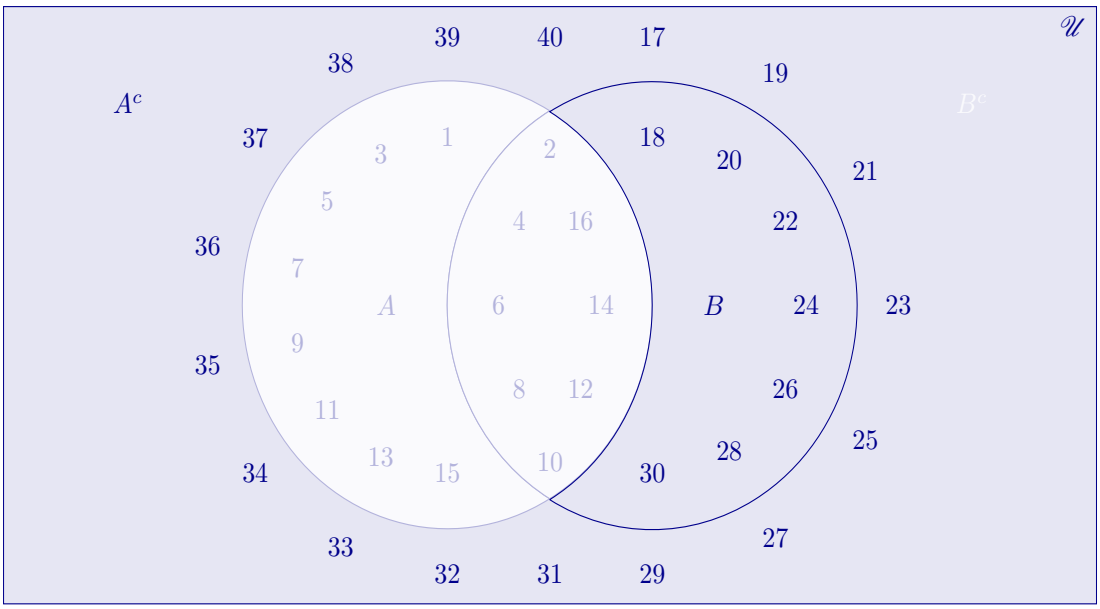
$$
\begin{aligned}
A \setminus B &= \{n : n \in A \text{ y } n \notin B\} \\
&= \{n : n \leqslant 16 \text{ y } \neg (n \text{ es par y } n \leqslant 30)\} \\
&= \{n : n \leqslant 16 \text{ y } (n \text{ no es par ó } n > 30)\} \\
&= \{n : (n \leqslant 16 \text{ y } n \text{ no es par}) \text{ ó } (n \leqslant 16 \text{ y } n > 30)\} \\
&= \{n : n \leqslant 16 \text{ y } n \text{ no es par}\} \\
&= \{1, 3, 5, 7, 9, 11, 13, 15\}
\end{aligned}
$$



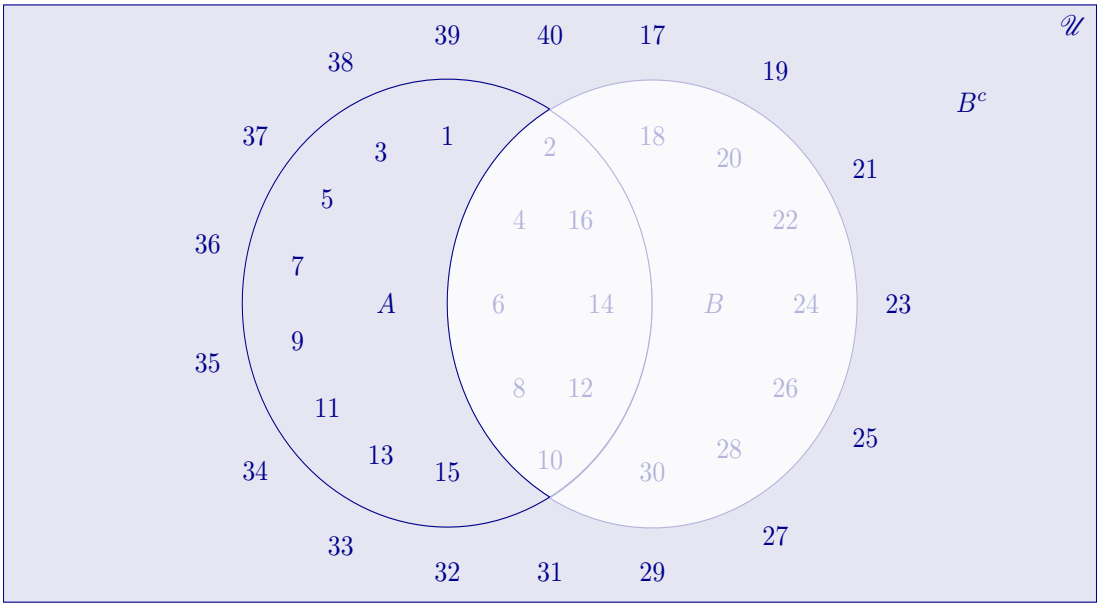
$$
\begin{aligned}
B \setminus A &= \{n : n \in B \text{ y } n \notin A\} \\
&= \{n : n \text{ es par y } n \leqslant 30 \text{ y } n > 16\} \\
&= \{n : n \text{ es par y } 16 < n \leqslant 30\} \\
&= \{18, 20, 22, 24, 26, 28, 30\}
\end{aligned}
$$



$$\begin{aligned} A^c &= \{n : n \notin A\} \\ &= \{n : n > 16\} \\ &= \{17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40\} \end{aligned}$$



$$\begin{aligned} B^c &= \{n : n \notin B\} \\ &= \{n : \neg(n \text{ es par y } n \leqslant 30)\} \\ &= \{n : \neg(n \text{ es par}) \text{ ó } \neg(n \leqslant 30)\} \\ &= \{n : n \text{ no es par ó } n > 30\} \\ &= \{1, 3, 5, 7, 9, 11, 13, 15, 17, 19, 21, 23, 25, 27, 29, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40\} \end{aligned}$$



■

4.2 Álgebra de conjuntos. Dualidad

Bajo las operaciones definidas en los apartados anteriores, los conjuntos satisfacen varias leyes o identidades. Observaremos que existe una dualidad entre las leyes que utilizan la intersección y las que utilizan la unión.

4.2.1 Leyes Idempotentes

Dado cualquier conjunto A en un universal arbitrario $\mathscr{U}$, se verifica:

1. $A \cup A = A$
2. $A \cap A = A$

Demostración

En efecto, sea a un elemento arbitrario del universal $\mathscr{U}$. Entonces,

1. $$\begin{aligned} a \in (A \cup A) &\iff a \in A \text{ ó } a \in A && \{\text{Definición de unión}\} \\ &\iff a \in A && \{\text{Idempotencia de la disyunción}\} \end{aligned}$$

   De la arbitrariedad de a se sigue que

   $$\forall x, [x \in (A \cup A) \longleftrightarrow x \in A]$$

   de aquí que por el axioma de extensión, (3.2.7),

   $$A \cup A = A$$

2. Análogamente se prueba que $A \cap A = A$.

■

4.2.2 Leyes Conmutativas

Dados dos conjuntos A y B de un universal arbitrario $\mathscr{U}$, se verifica:

1. $A \cup B = B \cup A$
2. $A \cap B = B \cap A$

Demostración

En efecto,

1. Sea a cualquier elemento de $\mathscr{U}$. Entonces,

$$\begin{aligned} a \in (A \cup B) &\iff a \in A \text{ ó } a \in B && \{\text{Definición de unión}\} \\ &\iff a \in B \text{ ó } a \in A && \{\text{Conmutatividad de la disyunción}\} \\ &\iff a \in (B \cup A) && \{\text{Definición de unión}\} \end{aligned}$$

   Como a es cualquiera de $\mathscr{U}$, se sigue que

$$\forall x, [x \in A \cup B \longleftrightarrow x \in B \cup A]$$

   por lo tanto, el axioma de extensión, (3.2.7), asegura que

$$A \cup B = B \cup A$$

2. De forma idéntica se prueba que $A \cap B = B \cap A$.

■

4.2.3 Leyes Asociativas

Dados tres conjuntos A, B y C cualesquiera de un universal, $\mathscr{U}$, se verifica:

1. $A \cup (B \cup C) = (A \cup B) \cup C$
2. $A \cap (B \cap C) = (A \cap B) \cap C$

Demostración

En efecto, sea a es un elemento arbitrario de $\mathscr{U}$. Entonces,

1.

$$\begin{aligned} a \in A \cup (B \cup C) &\iff a \in A \text{ ó } [a \in (B \cup C)] && \{\text{Definición de unión}\} \\ &\iff a \in A \text{ ó } (a \in B \text{ ó } a \in C) && \{\text{Definición de unión}\} \\ &\iff (a \in A \text{ ó } a \in B) \text{ ó } a \in C && \{\text{Asociatividad de la disyunción}\} \\ &\iff (a \in A \cup B) \text{ ó } a \in C && \{\text{Definición de unión}\} \\ &\iff a \in (A \cup B) \cup C && \{\text{Definición de unión}\} \end{aligned}$$

   De la arbitrariedad de a se sigue que

$$\forall x, [x \in A \cup (B \cup C) \longleftrightarrow x \in (A \cup B) \cup C]$$

   y de nuevo, el axioma de extensión, (3.2.7), asegura que

$$A \cup (B \cup C) = (A \cup B) \cup C$$

2. Análogamente se demuestra que
$$A \cap (B \cap C) = (A \cap B) \cap C$$

■

4.2.4 Leyes Distributivas

Dados tres conjuntos A, B y C cualesquiera de un conjunto universal, $\mathscr{U}$, se verifica:

1. $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$
2. $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$

Demostración

En efecto,

1. En efecto, sea a cualquier elemento del conjunto universal $\mathscr{U}$, entonces

$$\begin{aligned}
a \in A \cup (B \cap C) &\iff a \in A \text{ ó } [a \in (B \cap C)] && \{\text{Definición de unión}\} \\
&\iff a \in A \text{ ó } (a \in B \text{ y } a \in C) && \{\text{Definición de intersección}\} \\
&\iff (a \in A \text{ ó } a \in B) \text{ y } (a \in A \text{ ó } a \in C) && \{\text{Distributividad } \vee \text{ respecto } \wedge\} \\
&\iff a \in (A \cup B) \text{ y } a \in (A \cup C) && \{\text{Definición de unión}\} \\
&\iff a \in (A \cup B) \cap (A \cup C) && \{\text{Definición de intersección}\}
\end{aligned}$$

   Al ser a cualquier elemento de $\mathscr{U}$, se sigue que
$$\forall x, [x \in A \cup (B \cap C) \longleftrightarrow x \in (A \cup B) \cap (A \cup C)]$$
   y por el axioma de extensión, (3.2.7),
$$A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$$

2. De una forma similar se prueba que
$$A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$$

■

4.2.5 Leyes de Dominación

Dado un conjunto cualquiera, A, de un universal $\mathscr{U}$, se verifica:

1. $A \cup \mathscr{U} = \mathscr{U}$
2. $A \cap \emptyset = \emptyset$

Demostración

1. $A \cup \mathscr{U} = \mathscr{U}$. En efecto, sea a un elemento cualquiera de $\mathscr{U}$. Entonces,

$$\begin{aligned} a \in (A \cup \mathscr{U}) &\iff a \in A \text{ ó } a \in \mathscr{U} && \{\text{Definición de unión}\} \\ &\iff a \in \mathscr{U} \text{ ó } a \in \mathscr{U} && \{A \subseteq \mathscr{U} \ (3.3.3)\} \\ &\iff a \in \mathscr{U} && \{\text{Idempotencia de la unión}, (4.2.1)\} \end{aligned}$$

   luego,

$$\forall x, [x \in (A \cup \mathscr{U}) \longleftrightarrow x \in \mathscr{U}]$$

   de aquí que por el axioma de extensión, (3.2.7),

$$A \cup \mathscr{U} = \mathscr{U}$$

2. $A \cap \emptyset = \emptyset$. En efecto, sea a cualquiera de $\mathscr{U}$. Entonces,

$$\begin{aligned} a \in (A \cap \emptyset) &\iff a \in A \text{ y } a \in \emptyset && \{\text{Definición de intersección}\} \\ &\iff a \in \emptyset && \{a \in \emptyset \text{ es falso siempre. } (1.4.4)\} \end{aligned}$$

   luego,

$$\forall x, [x \in (A \cap \emptyset) \longleftrightarrow x \in \emptyset]$$

   de aquí que por el axioma de extensión, (3.2.7),

$$A \cap \emptyset = \emptyset$$

■

4.2.6 Leyes de Identidad

Dado un conjunto cualquiera, A, de un universal, $\mathscr{U}$, se verifica:

1. $A \cup \emptyset = A$
2. $A \cap \mathscr{U} = A$

Demostración

1. $A \cup \emptyset = A$. En efecto, sea a es un elemento arbitrario de $\mathscr{U}$. Entonces,

$$\begin{aligned} a \in (A \cup \emptyset) &\iff a \in A \text{ ó } a \in \emptyset && \{\text{Definición de unión}\} \\ &\iff a \in A \text{ ó } a \in A && \{\emptyset \subseteq A \ (3.3.4)\} \\ &\iff a \in A \cup A && \{\text{Definición de unión}\} \\ &\iff a \in A && \{\text{Idempotencia de la unión}, (4.2.1)\} \end{aligned}$$

   luego,

$$\forall x, [x \in (A \cup \emptyset) \longleftrightarrow x \in A]$$

   de aquí que por el axioma de extensión, (3.2.7),

$$A \cup \emptyset = A$$

2. $A \cap \mathscr{U} = A$. En efecto, sea a cualquiera de $\mathscr{U}$. Entonces,

$$\begin{array}{rcll} a \in (A \cap \mathscr{U}) & \iff & a \in A \text{ y } a \in \mathscr{U} & \{\text{Definición de intersección}\} \\ & \iff & a \in A & \{a \in \mathscr{U} \text{ es verdad siempre. (1.4.4)}\} \end{array}$$

luego,

$$\forall x, [x \in (A \cap \mathscr{U}) \longleftrightarrow x \in A]$$

de aquí que por el axioma de extensión, (3.2.7),

$$A \cap \mathscr{U} = A$$

■

4.2.7 Ley Involutiva

Dado un conjunto cualquiera A de un universal $\mathscr{U}$, se verifica:

$$(A^c)^c = A$$

Demostración

Sea a cualquiera de $\mathscr{U}$. Entonces,

$$\begin{array}{rcll} a \in (A^c)^c & \iff & a \notin A^c & \{\text{Definición de complementario}\} \\ & \iff & \neg\,(a \in A^c) & \{\text{Negación}\} \\ & \iff & \neg\,(a \notin A) & \{\text{Definición de complementario}\} \\ & \iff & \neg\neg\,(a \in A) & \{\text{Negación}\} \\ & \iff & a \in A & \{\text{Doble negación (1.4.4)}\} \end{array}$$

luego,

$$\forall x, [x \in (A^c)^c \longleftrightarrow x \in A]$$

de aquí que por el axioma de extensión, (3.2.7),

$$(A^c)^c = A$$

■

4.2.8 Leyes del Complementario

Dado un conjunto cualquiera A de un universal arbitrario $\mathscr{U}$, se verifica:

1. $A \cup A^c = \mathscr{U}$
2. $\mathscr{U}^c = \emptyset$
3. $A \cap A^c = \emptyset$
4. $\emptyset^c = \mathscr{U}$

Demostración

1. $A \cup A^c = \mathscr{U}$. En efecto, sea a cualquier elemento de $\mathscr{U}$. Entonces,

$$\begin{aligned} a \in (A \cup A^c) &\iff a \in A \text{ ó } a \in A^c && \{\text{Definición de unión}\} \\ &\iff a \in A \text{ ó } a \notin A && \{\text{Complementario}\} \\ &\iff a \in A \text{ ó } \neg(a \in A) && \{\text{Negación (1.2.4)}\} \\ &\iff a \in \mathscr{U} && \{\text{Tautología (1.2.5)}\} \end{aligned}$$

   luego,

$$\forall x, [x \in (A \cup A^c) \longleftrightarrow x \in \mathscr{U}]$$

   de aquí que por el axioma de extensión, (3.2.7),

$$A \cup A^c = \mathscr{U}$$

2. $\mathscr{U}^c = \emptyset$. En efecto,

$$\mathscr{U}^c = \{x \in \mathscr{U} : x \in \mathscr{U}^c\} = \{x \in \mathscr{U} \text{ y } x \notin \mathscr{U}\} = \emptyset$$

3. $A \cap A^c = \emptyset$. En efecto,

$$A \cap A^c = \{x \in \mathscr{U} : x \in A \text{ y } x \in A^c\} = \{x \in \mathscr{U} : x \in A \text{ y } x \notin A\} = \emptyset$$

4. $\emptyset^c = \mathscr{U}$. En efecto, de 2.,

$$\begin{aligned} \mathscr{U}^c = \emptyset &\iff (\mathscr{U}^c)^c = \emptyset^c && \text{Complementario} \\ &\iff \mathscr{U} = \emptyset^c && \{\text{Ley involutiva (4.2.7)}\} \end{aligned}$$

■

4.2.9 Leyes de De Morgan

Dados dos conjuntos A y B en un universal $\mathscr{U}$, se verifica:

1. $(A \cup B)^c = A^c \cap B^c$
2. $(A \cap B)^c = A^c \cup B^c$

Demostración

1. $(A \cup B)^c = A^c \cap B^c$. En efecto, sea a un elemento arbitrario del conjunto universal $\mathscr{U}$. Entonces,

$$\begin{aligned} a \in (A \cup B)^c &\iff a \notin (A \cup B) && \{\text{Definición de complementario}\} \\ &\iff \neg[a \in (A \cup B)] && \{\text{Negación (1.2.4)}\} \\ &\iff \neg(a \in A \text{ ó } a \in B) && \{\text{Definición de unión}\} \\ &\iff \neg(a \in A) \text{ y } \neg(a \in B) && \{\text{De Morgan (1.4.4)}\} \\ &\iff a \notin A \text{ y } a \notin B && \{\text{Negación (1.2.4)}\} \\ &\iff a \in A^c \text{ y } a \in B^c && \{\text{Definición de complementario}\} \\ &\iff a \in (A^c \cap B^c) && \{\text{Definición de intersección}\} \end{aligned}$$

y al ser a un elemento arbitrario de $\mathscr{U}$, se sigue que

$$\forall x, [x \in (A \cup B)^c \longleftrightarrow x \in (A^c \cap B^c)]$$

luego por el axioma de extensión, (3.2.7),

$$(A \cup B)^c = A^c \cap B^c$$

2. $(A \cap B)^c = A^c \cup B^c$. En efecto, sea a un elemento arbitrario del conjunto universal $\mathscr{U}$. Entonces,

$$\begin{array}{rcll} a \in (A \cap B)^c & \iff & a \notin (A \cap B) & \{\text{Definición de complementario}\} \\ & \iff & \neg [a \in (A \cap B)] & \{\text{Negación (1.2.4)}\} \\ & \iff & \neg (a \in A \text{ y } a \in B) & \{\text{Definición de intersección}\} \\ & \iff & \neg (a \in A) \text{ ó } \neg (a \in B) & \{\text{De Morgan (1.4.4)}\} \\ & \iff & a \notin A \text{ ó } a \notin B & \{\text{Negación (1.2.4)}\} \\ & \iff & a \in A^c \text{ ó } a \in B^c & \{\text{Definición de complementario}\} \\ & \iff & a \in (A^c \cup B^c) & \{\text{Definición de unión}\} \end{array}$$

y al ser a un elemento arbitrario de $\mathscr{U}$, se sigue que

$$\forall x, [x \in (A \cap B)^c \iff x \in (A^c \cup B^c)]$$

luego por el axioma de extensión, (3.2.7),

$$(A \cap B)^c = A^c \cup B^c$$

■

Ejemplo 4.6

Sean A, B, C y D subconjuntos arbitrarios de un conjunto universal arbitrario, $\mathscr{U}$. Se verifica:

(a) $A \setminus B \subseteq A$

(b) *Si* $A \subseteq B$ *y* $C \subseteq D$, *entonces* $(A \cup C) \subseteq (B \cup D)$

(c) *Si* $A \subseteq B$ *y* $C \subseteq D$, *entonces* $(A \cap C) \subseteq (B \cap D)$

(d) $A \cap B \subseteq A$

(e) $A \setminus \emptyset = A$

(f) $A \setminus B = A \cap B^c$

(g) $A \cap (B \setminus A) = \emptyset$

(h) $A \cup (B \setminus A) = A \cup B$

(i) $A \setminus (B \cup C) = (A \setminus B) \cap (A \setminus C)$

(j) $A \setminus (B \cap C) = (A \setminus B) \cup (A \setminus C)$

(k) $A \cup (A^c \cap B) = A \cup B$

(l) $A \cap (A^c \cup B) = A \cap B$

(m) $(A \setminus B) \cup (A \cap B) \cup (B \setminus A) = A \cup B$

Solución

(a) $A \setminus B \subseteq A$

En efecto, sea a un elemento arbitrario de $\mathscr{U}$,

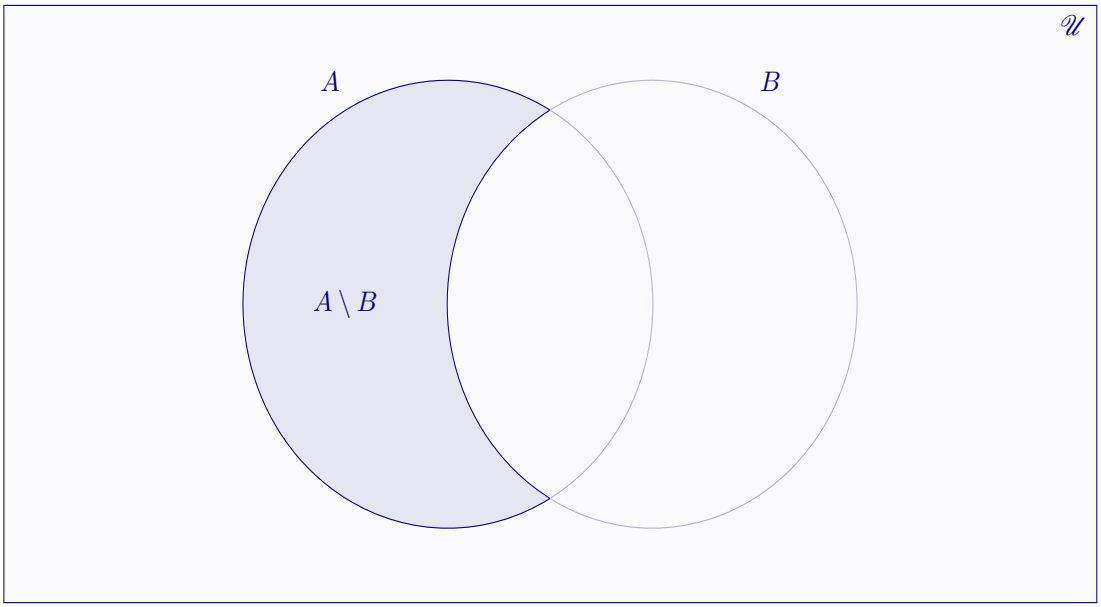
$$\begin{aligned} a \in A \setminus B &\iff a \in A \text{ y } a \notin B \quad \{\text{Definición de diferencia}\} \\ &\implies a \in A \end{aligned}$$

luego,

$$\forall x, [x \in A \setminus B \longrightarrow x \in A]$$

consecuentemente, y por definición de subconjunto (3.3.1),

$$A \setminus B \subseteq A$$



(b) Si $A \subseteq B$ y $C \subseteq D$, entonces $(A \cup C) \subseteq (B \cup D)$

En efecto, supongamos que $A \subseteq B$ y $C \subseteq D$ y sea a un elemento arbitrario de $\mathscr{U}$, entonces

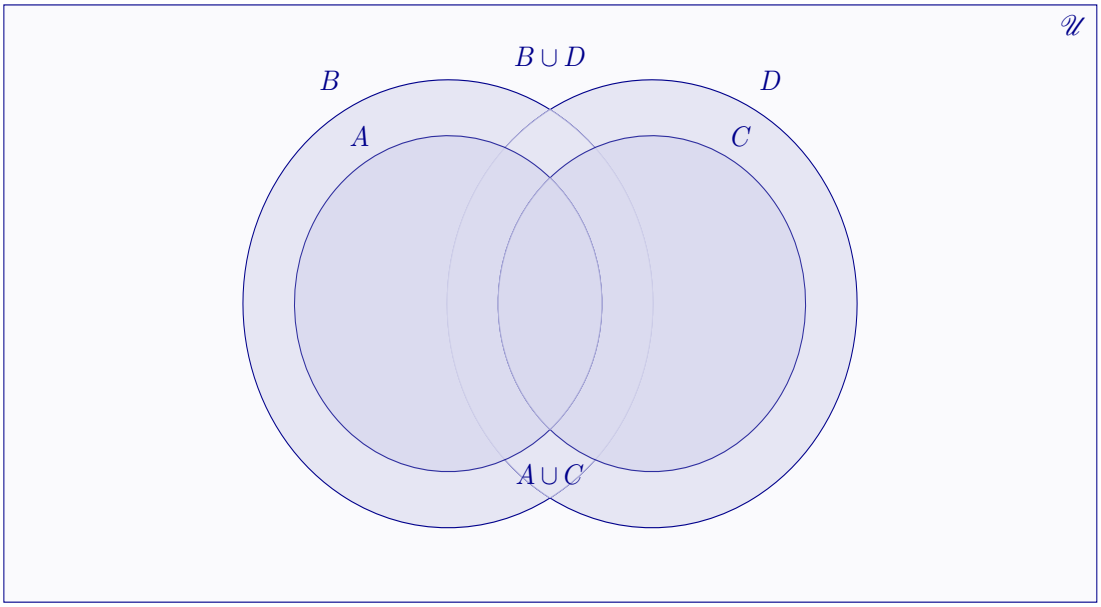
$$\begin{aligned} a \in A \cup C &\iff a \in A \text{ ó } a \in C \quad \{\text{Definición de unión}\} \\ &\implies a \in B \text{ ó } a \in D \quad \{\text{Hipótesis } A \subseteq B,\ C \subseteq D\} \\ &\iff a \in (B \cup D) \quad \{\text{Definición de unión}\} \end{aligned}$$

luego,

$$\forall x, [x \in (A \cup C) \longrightarrow x \in (B \cup D)]$$

por lo tanto, la definición de subconjunto, (3.3.1), nos lleva a que

$$A \cup C \subseteq B \cup D$$



(c) Si $A \subseteq B$ y $C \subseteq D$, entonces $(A \cap C) \subseteq (B \cap D)$

En efecto, supongamos que $A \subseteq B$ y $C \subseteq D$ y sea a un elemento arbitrario de $\mathscr{U}$, entonces

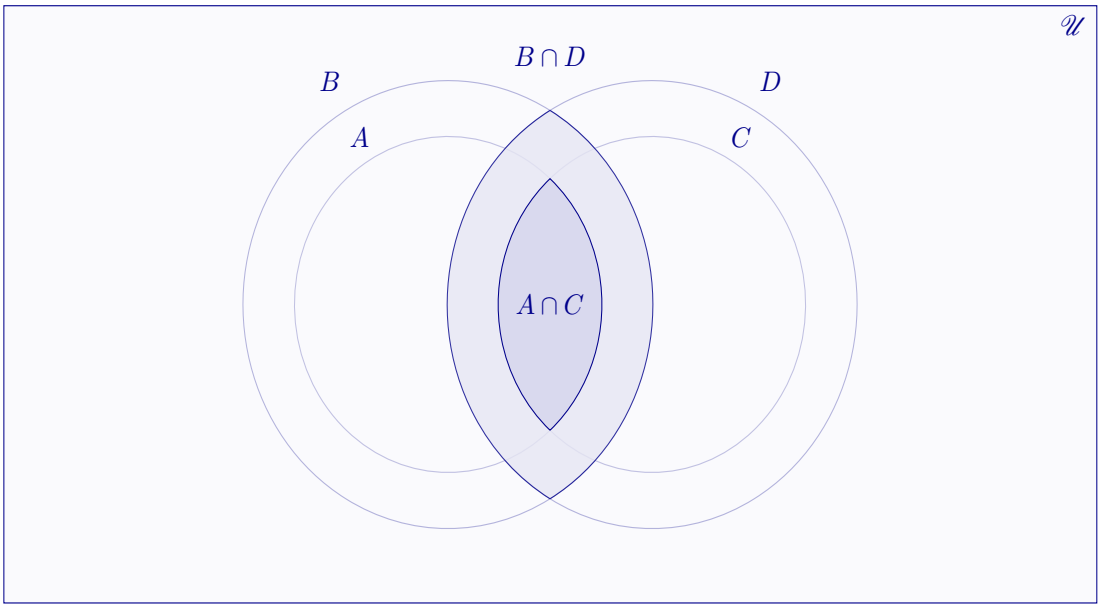
$$\begin{aligned} a \in A \cap C &\iff a \in A \text{ y } a \in C && \{\text{Definición de intersección}\} \\ &\implies a \in B \text{ y } a \in D && \{\text{Hipótesis } A \subseteq B,\ C \subseteq D\} \\ &\iff a \in (B \cap D) && \{\text{Definición de intersección}\} \end{aligned}$$

luego,

$$\forall x, [x \in (A \cap C) \longrightarrow x \in (B \cap D)]$$

por lo tanto, la definición de subconjunto, (3.3.1), nos lleva a que

$$A \cap C \subseteq B \cap D$$



(d) $A \cap B \subseteq A$

En efecto, sea a un elemento cualquiera de $\mathscr{U}$. Entonces,

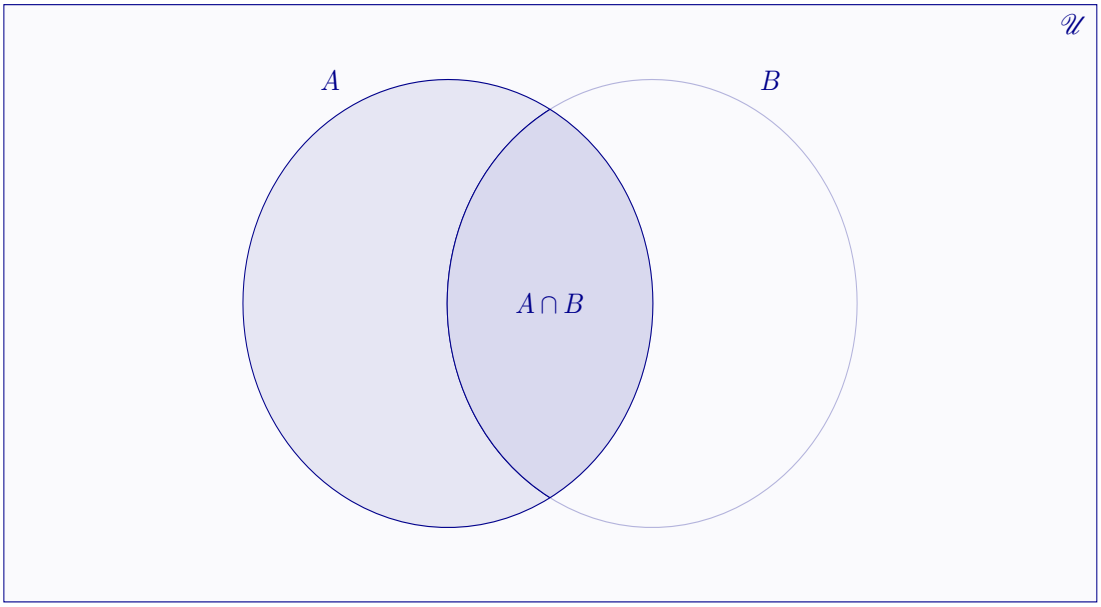
$$\begin{aligned} a \in A \cap B &\iff a \in A \text{ y } a \in B \quad \{\text{Definición de intersección}\} \\ &\implies a \in A \end{aligned}$$

luego por definición de subconjunto, (3.3.1),

$$\forall x, [x \in (A \cap B) \longrightarrow x \in A]$$

de donde se sigue

$$A \cap B \subseteq A$$



(e) $A \setminus \emptyset = A$

Sea a cualquiera de $\mathscr{U}$. Entonces,

$$\begin{aligned} a \in A \setminus \emptyset &\iff a \in A \text{ y } a \notin \emptyset \quad \{\text{Definición de diferencia}\} \\ &\iff a \in A \qquad\qquad\quad \{a \notin \emptyset \text{ es verdad siempre}\} \end{aligned}$$

luego,

$$\forall x, [x \in A \setminus \emptyset \longleftrightarrow x \in A]$$

de aquí que por el axioma de extensión, (3.2.7),

$$A \setminus \emptyset = A$$

(f) $A \setminus B = A \cap B^c$

En efecto, sea a cualquiera del conjunto universal $\mathscr{U}$. Entonces,

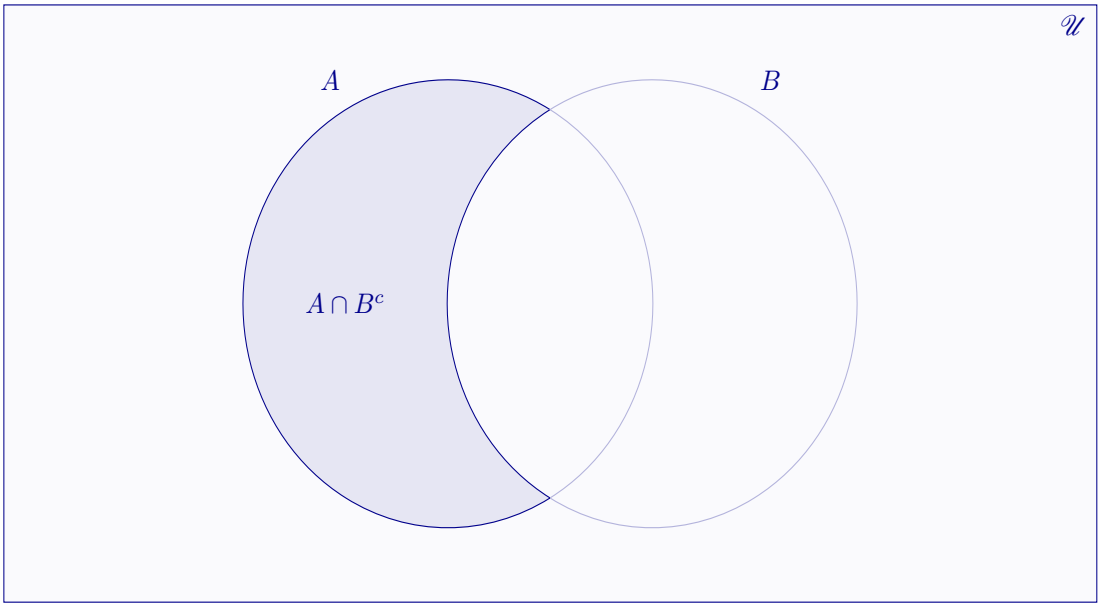
$$\begin{aligned} a \in A \setminus B &\iff a \in A \text{ y } a \notin B \quad \{\text{Definición de diferencia}\} \\ &\iff a \in A \text{ y } a \in B^c \quad \{\text{Definición de complementario}\} \\ &\iff a \in (A \cap B^c) \quad \{\text{Definición de intersección}\} \end{aligned}$$

luego,

$$\forall x, [x \in A \setminus B \iff x \in (A \cap B^c)]$$

de aquí que por el axioma de extensión, (3.2.7),

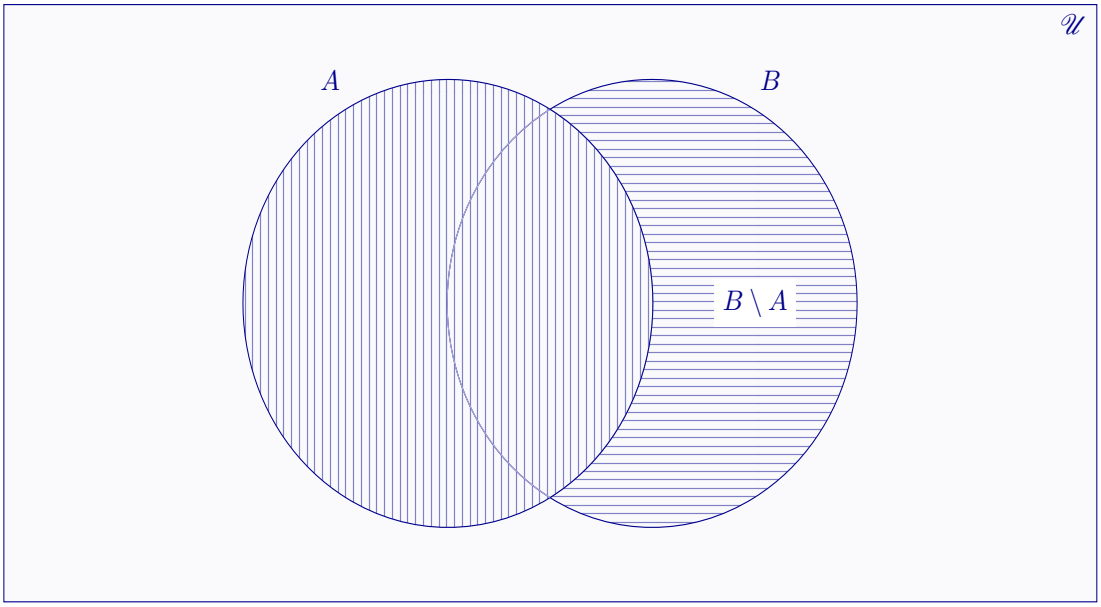
$$A \setminus B = A \cap B^c$$



(g) $A \cap (B \setminus A) = \emptyset$

En efecto,

$$\begin{aligned} A \cap (B \setminus A) &= A \cap (B \cap A^c) && \{\text{Apartado anterior}\} \\ &= A \cap (A^c \cap B) && \{\text{Conmutatividad de la intersección}\} \\ &= (A \cap A^c) \cap B && \{\text{Asociatividad de la intersección}\} \\ &= \emptyset \cap B && \{\text{Leyes del complementario}\} \\ &= \emptyset && \{\text{Leyes de identidad}\} \end{aligned}$$



(h) $A \cup (B \setminus A) = A \cup B$

En efecto,

$$\begin{aligned} A \cup (B \setminus A) &= A \cup (B \cap A^c) && \{\text{Diferencia de conjuntos}\} \\ &= (A \cup B) \cap (A \cup A^c) && \{\text{Distributividad}\} \\ &= (A \cup B) \cap \mathscr{U} && \{\text{Leyes del complementario}\} \\ &= A \cup B && \{\text{Leyes de identidad}\} \end{aligned}$$

(i) $A \setminus (B \cup C) = (A \setminus B) \cap (A \setminus C)$

En efecto,

$$\begin{aligned} A \setminus (B \cup C) &= A \cap (B \cup C)^c && \{\text{Diferencia de conjuntos}\} \\ &= A \cap (B^c \cap C^c) && \{\text{Leyes de De Morgan}\} \\ &= (A \cap A) \cap (B^c \cap C^c) && \{\text{Idempotencia de la intersección}\} \\ &= (A \cap B^c) \cap (A \cap C^c) && \{\text{Commutatividad y asociatividad}\} \\ &= (A \setminus B) \cap (A \setminus C) && \{\text{Diferencia de conjuntos}\} \end{aligned}$$

(j) $A \setminus (B \cap C) = (A \setminus B) \cup (A \setminus C)$

En efecto,

$$\begin{aligned} A \setminus (B \cap C) &= A \cap (B \cap C)^c && \{\text{Diferencia de conjuntos}\} \\ &= A \cap (B^c \cup C^c) && \{\text{Leyes de De Morgan}\} \\ &= (A \cap B^c) \cup (A \cap C^c) && \{\text{Distributividad}\} \\ &= (A \setminus B) \cup (A \setminus C) && \{\text{Diferencia de conjuntos}\} \end{aligned}$$

(k) $A \cup (A^c \cap B) = A \cup B$ En efecto,

$$\begin{aligned} A \cup (A^c \cap B) &= (A \cup A^c) \cap (A \cup B) && \{\text{Distributividad}\} \\ &= \mathscr{U} \cap (A \cup B) && \{\text{Leyes del complementario}\} \\ &= A \cup B && \{\text{Leyes de identidad}\} \end{aligned}$$

(l) $A \cap (A^c \cup B) = A \cap B$

$$\begin{aligned} A \cap (A^c \cup B) &= (A \cap A^c) \cup (A \cap B) && \{\text{Distributividad}\} \\ &= \emptyset \cup (A \cap B) && \{\text{Leyes del complementario}\} \\ &= A \cap B && \{\text{Leyes de identidad}\} \end{aligned}$$

(m) $(A \setminus B) \cup (A \cap B) \cup (B \setminus A) = A \cup B$

$$\begin{aligned} (A \setminus B) \cup (A \cap B) \cup (B \setminus A) &= (A \cap B^c) \cup (A \cap B) \cup (B \cap A^c) && \{\text{Diferencia (4.1.3)}\} \\ &= [A \cap (B^c \cup B)] \cup (B \cap A^c) && \{\text{Leyes distributivas (4.2.4)}\} \\ &= (A \cap \mathscr{U}) \cup (B \cap A^c) && \{\text{Leyes complementario (4.2.8)}\} \\ &= A \cup (B \cap A^c) && \{\text{Leyes de identidad (4.2.6)}\} \\ &= (A \cup B) \cap (A \cup A^c) && \{\text{Leyes distributivas (4.2.4)}\} \\ &= (A \cup B) \cap \mathscr{U} && \{\text{Leyes complementario (4.2.8)}\} \\ &= A \cup B && \{\text{Leyes de identidad (4.2.6)}\} \end{aligned}$$

■

4.3 Partición de un conjunto

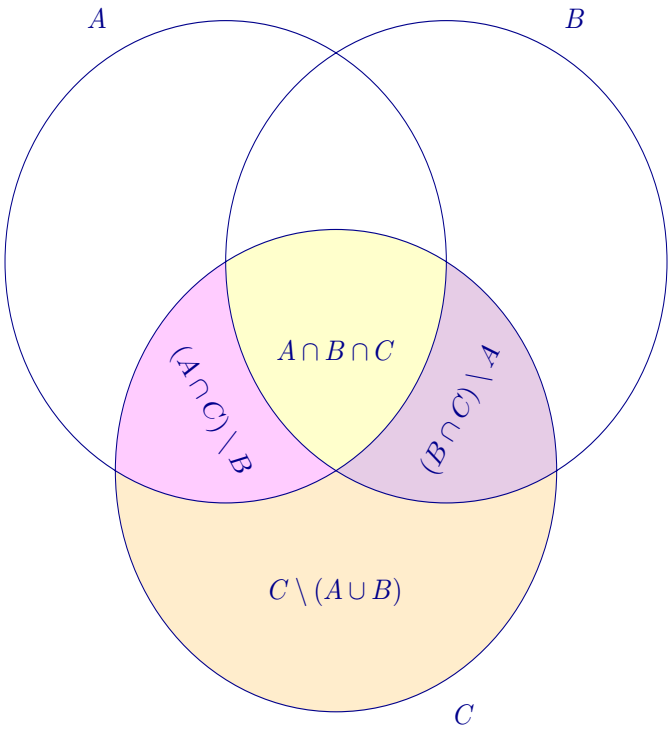
4.3.1 Definición

Dado un conjunto cualquiera A contenido en un conjunto universal $\mathscr{U}$, se dice que $A_1, A_2, \ldots, A_n$, subconjuntos de A, constituyen una partición de A, y lo notaremos $\mathscr{P} = \{A_1, A_2, \ldots A_n\}$ si se cumplen las condiciones siguientes:

1. *Todos los subconjuntos de la partición tienen algún elemento, es decir, $A_i \neq \emptyset$, $\forall i = 1, 2, \ldots, n$.*
2. *Los conjuntos de la partición son dos a dos disjuntos, o sea, $A_i \neq A_j \Longrightarrow A_i \cap A_j = \emptyset$.*
3. *La unión de todos los subconjuntos que conforman la partición es igual al conjunto A, $\bigcup_{i=1}^{n} A_i = A$.*

Ejemplo 4.7

En un conjunto universal cualquiera, $\mathscr{U}$, se consideran los conjuntos A, B y C, intersecados entre ellos según la figura siguiente:



Probar que

$$\mathscr{P} = \{(A \cap C) \setminus B, A \cap B \cap C, (B \cap C) \setminus A, C \setminus (A \cup B)\}$$

es una partición del conjunto C.

Solución

Veamos que se cumplen las tres condiciones de partición.

1 Según se aprecia en la figura ninguno de los subconjuntos de C que conforman la partición es vacío, es decir,

$(A \cap C) \setminus B \neq \emptyset$.
$A \cap B \cap C \neq \emptyset$.
$(B \cap C) \setminus A \neq \emptyset$.
$C \setminus (A \cup B) \neq \emptyset$.

2 Los subconjuntos de C que integran la partición son dos a dos disjuntos.

En efecto,

$$\begin{aligned}
[(A \cap C) \setminus B] \cap (A \cap B \cap C) &= A \cap C \cap B^c \cap A \cap B \cap C && \{\text{Diferencia de conjuntos (4.1.3)}\}\\
&= A \cap C \cap A \cap C \cap B^c \cap B && \{\text{Leyes conmutativas (4.2.2)}\}\\
&= A \cap C \cap B^c \cap B && \{\text{Leyes de idempotencia (4.2.1)}\}\\
&= A \cap C \cap \emptyset && \{\text{Leyes del complementario (4.2.8)}\}\\
&= \emptyset && \{\text{Leyes de dominación (4.2.5)}\}
\end{aligned}$$

$$\begin{aligned}
[(A \cap C) \setminus B] \cap [(B \cap C) \setminus A] &= A \cap C \cap B^c \cap B \cap C \cap A^c && \{\text{Diferencia de conjuntos (4.1.3)}\}\\
&= A \cap A^c \cap C \cap C \cap B^c \cap B && \{\text{Leyes conmutativas (4.2.2)}\}\\
&= A \cap A^c \cap C \cap B^c \cap B && \{\text{Leyes de idempotencia (4.2.1)}\}\\
&= \emptyset \cap C \cap \emptyset && \{\text{Leyes del complementario (4.2.8)}\}\\
&= \emptyset && \{\text{Leyes de dominación (4.2.5)}\}
\end{aligned}$$

$$\begin{aligned}
[(A \cap C) \setminus B] \cap [C \setminus (A \cup B)] &= A \cap C \cap B^c \cap C \cap (A \cup B)^c && \{\text{Diferencia de conjuntos (4.1.3)}\}\\
&= A \cap C \cap B^c \cap C \cap A^c \cap B^c && \{\text{Leyes de De Morgan (4.2.9)}\}\\
&= A \cap A^c \cap C \cap C \cap B^c \cap B^c && \{\text{Leyes conmutativas (4.2.2)}\}\\
&= A \cap A^c \cap C \cap B^c && \{\text{Leyes de idempotencia (4.2.1)}\}\\
&= \emptyset \cap C \cap B^c && \{\text{Leyes del complementario (4.2.8)}\}\\
&= \emptyset && \{\text{Leyes de dominación (4.2.5)}\}
\end{aligned}$$

$$\begin{aligned}
(A \cap B \cap C) \cap [(B \cap C) \setminus A] &= A \cap B \cap C \cap B \cap C \cap A^c && \{\text{Diferencia de conjuntos (4.1.3)}\}\\
&= A \cap A^c \cap B \cap B \cap C \cap C && \{\text{Leyes conmutativas (4.2.2)}\}\\
&= A \cap A^c \cap B \cap C && \{\text{Leyes de idempotencia (4.2.1)}\}\\
&= \emptyset \cap B \cap C && \{\text{Leyes del complementario (4.2.8)}\}\\
&= \emptyset && \{\text{Leyes de dominación (4.2.5)}\}
\end{aligned}$$

$$\begin{aligned}
(A \cap B \cap C) \cap [C \setminus (A \cup B)] &= A \cap B \cap C \cap C \cap (A \cup B)^c && \{\text{Diferencia de conjuntos (4.1.3)}\}\\
&= A \cap B \cap C \cap C \cap A^c \cap B^c && \{\text{Leyes de De Morgan (4.2.9)}\}\\
&= A \cap A^c \cap B \cap B^c \cap C \cap C && \{\text{Leyes conmutativas (4.2.2)}\}\\
&= A \cap A^c \cap B \cap B^c \cap C && \{\text{Leyes de idempotencia (4.2.1)}\}\\
&= \emptyset \cap \emptyset \cap C && \{\text{Leyes del complementario (4.2.8)}\}\\
&= \emptyset && \{\text{Leyes de dominación (4.2.5)}\}
\end{aligned}$$

$$
\begin{aligned}
[(B\cap C)\setminus A]\cap[C\setminus(A\cup B)] &= B\cap C\cap A^c\cap C\cap(A\cup B)^c && \{\text{Diferencia de conjuntos (4.1.3)}\}\\
&= B\cap C\cap A^c\cap C\cap A^c\cap B^c && \{\text{Leyes de De Morgan (4.2.9)}\}\\
&= B\cap B^c\cap C\cap C\cap A^c\cap A^c && \{\text{Leyes conmutativas (4.2.2)}\}\\
&= B\cap B^c\cap C\cap A^c && \{\text{Leyes de idempotencia (4.2.1)}\}\\
&= \emptyset\cap C\cap A^c && \{\text{Leyes del complementario (4.2.8)}\}\\
&= \emptyset && \{\text{Leyes de dominación (4.2.5)}\}
\end{aligned}
$$

3 Veremos, finalmente, que C es igual a la unión de todos los subconjuntos que integran la partición. En efecto,

$$
\begin{aligned}
&[(A\cap C)\setminus B]\cup(A\cap B\cap C)\cup[(B\cap C)\setminus A]\cup[C\setminus(A\cup B)]\\
&=\\
&(A\cap C\cap B^c)\cup(A\cap B\cap C)\cup(B\cap C\cap A^c)\cup[C\cap(A\cup B)^c] && \{\text{Diferencia de conjuntos (4.1.3)}\}\\
&=\\
&(A\cap C\cap B^c)\cup(A\cap B\cap C)\cup(B\cap C\cap A^c)\cup(C\cap A^c\cap B^c) && \{\text{Leyes de De Morgan (4.2.9)}\}\\
&=\\
&(C\cap A\cap B)\cup(C\cap A\cap B^c)\cup(C\cap A^c\cap B)\cup(C\cap A^c\cap B^c) && \{\text{Leyes conmutativas (4.2.2)}\}\\
&=\\
&[(C\cap A)\cap(B\cup B^c)]\cup[(C\cap A^c)\cap(B\cup B^c)] && \{\text{Leyes distributivas (4.2.4)}\}\\
&=\\
&[(C\cap A)\cup(C\cap A^c)]\cap(B\cup B^c) && \{\text{Leyes distributivas (4.2.4)}\}\\
&=\\
&C\cap(A\cup A^c)\cap(B\cup B^c) && \{\text{Leyes distributivas (4.2.4)}\}\\
&=\\
&C\cap\mathscr{U}\cap\mathscr{U} && \{\text{Leyes del complementario (4.2.8)}\}\\
&=\\
&C && \{\text{Leyes de identidad (4.2.6)}\}
\end{aligned}
$$

■

Ejemplo 4.8

En el conjunto $\mathbb{Z}$ de los números enteros se consideran los conjuntos A, formado por todos los números pares y B, integrado por los múltiplos de 3. Se pide:

a) $A\cap B$

b) $A\setminus B$

c) $B\setminus A$

d) $A^c\cap B^c$

e) Probar que los cuatro conjuntos anteriores forman una partición del conjunto de los números enteros.

f) Probar, aplicando los resultados obtenidos en los apartados anteriores, que cualquier entero es múltiplo de 6 o da resto par al dividirlo entre 6 o da resto 3 al dividirlo entre 6 o da resto impar al dividirlo entre 6.

Solución

Las definiciones, por comprensión, de los conjuntos A y B son:

$$A = \{n : n = 2q,\ q \in \mathbb{Z}\}$$

$$B = \{n : n = 3q,\ q \in \mathbb{Z}\}$$

a) $A \cap B$

Sea a cualquier número entero. Entonces,

$$\begin{aligned}
a \in (A \cap B) &\iff a \in A \wedge a \in B \ \{\text{Definición de intersección. (4.1.2)}\} \\
&\iff \begin{cases} \exists q_1 \in \mathbb{Z} : a = 2q_1 & \{\text{Definición de } A\} \\ \wedge & \\ \exists q_2 \in \mathbb{Z} : a = 3q_2 & \{\text{Definición de } B\} \end{cases} \\
&\iff 2q_1 = 3q_2 \\
&\iff \frac{q_1}{q_2} = \frac{3}{2} \\
&\iff \frac{\frac{q_1}{q}}{\frac{q_2}{q}} = \frac{3}{2} \ \{q = \text{m.c.d.}(q_1, q_2)\} \\
&\iff \begin{cases} \frac{q_1}{q} = 3 & \\ \wedge & \{\text{Las dos fracciones son irreducibles}\} \\ \frac{q_2}{q} = 2 & \end{cases} \\
&\iff \begin{cases} q_1 = 3q & \\ \wedge & \\ q_2 = 2q & \end{cases} \\
&\implies \begin{cases} a = 6q,\ q \in \mathbb{Z} & \\ \wedge & \{\text{Sustituyendo en los valores de } a\} \\ a = 6q,\ q \in \mathbb{Z} & \end{cases} \\
&\iff a = 6q,\ q \in \mathbb{Z} \\
&\iff a \in \{n : n = 6q,\ q \in \mathbb{Z}\}
\end{aligned}$$

Como a era un número entero elegido de forma arbitraria, hemos probado que la proposición,

$$\forall x, (x \in (A \cap B) \longrightarrow x \in \{n : n = 6q,\ q \in \mathbb{Z}\})$$

es verdadera y, consecuentemente, por definición de inclusión de conjuntos, (3.3.1),

$$(A \cap B) \subseteq \{n : n = 6q,\ q \in \mathbb{Z}\}$$

Recíprocamente,

$$\begin{aligned}
a \in \{n : n = 6q,\ q \in \mathbb{Z}\} &\iff \exists q \in \mathbb{Z} : a = 6q \\
&\iff \exists q \in \mathbb{Z} : \begin{cases} a = 2 \cdot 3q \\ \wedge \\ a = 3 \cdot 2q \end{cases} \\
&\implies \begin{cases} \exists q_1 \in \mathbb{Z} : a = 2q_1 \quad \{\text{Tomando } q_1 = 3q\} \\ \wedge \\ \exists q_2 \in \mathbb{Z} : a = 3q_2 \quad \{\text{Tomando } q_2 = 2q\} \end{cases} \\
&\iff \begin{cases} a \in A \quad \{\text{Definición de } A\} \\ \wedge \\ a \in B \quad \{\text{Definición de } B\} \end{cases} \\
&\iff a \in (A \cap B) \ \{\text{Definición de intersección. (4.1.2)}\}
\end{aligned}$$

Como a era cualquiera, la proposición,

$$\forall x, (x \in \{n : n = 6q,\ q \in \mathbb{Z}\} \longrightarrow x \in (A \cap B))$$

es verdadera y, de nuevo, por la definición de inclusión de conjuntos, (3.3.1),

$$\{n : n = 6q,\ q \in \mathbb{Z}\} \subseteq (A \cap B)$$

Finalmente, por la doble inclusión, tendremos, (3.3.5), que

$$A \cap B = \{n : n = 6q,\ q \in \mathbb{Z}\}$$

es decir, $A \cap B$ es el conjunto formado por todos los múltiplos de 6.

b) $A \setminus B$

Sea a un número elegido arbitrariamente en $\mathbb{Z}$. Entonces,

$$
\begin{aligned}
a \in A \setminus B \iff & \left\{ \begin{array}{l} a \in A \\ \wedge \qquad \{\text{Definición de Diferencia. (4.1.3)}\} \\ a \notin B \end{array} \right. \\
\iff & \left\{ \begin{array}{l} \exists q_1 \in \mathbb{Z} : a = 2q_1 \\ \wedge \\ a \neq 3q_2,\ \forall q_2 \in \mathbb{Z} \end{array} \right. \\
\iff & \left\{ \begin{array}{l} \exists q_1 \in \mathbb{Z} : a = 2q_1 \\ \wedge \\ \exists q_2, r_2 \in \mathbb{Z} : a = 3q_2 + r_2,\ r_2 \neq 0 \quad \{\text{T.E.U.C.R. (13.2.1)}\} \end{array} \right. \\
& \left\{ \begin{array}{l} \text{Dividiendo } q_1 \text{ por 3, } q_1 = 3q + r, \text{ con } q, r \in \mathbb{Z}, \text{ y } r = 0, 1 \text{ o } 2 \\ \text{Dividiendo } q_2 \text{ por 2, } q_2 = 2q_3 + r_3, \text{ con } q_3, r_3 \in \mathbb{Z}, \text{ y } r_3 = 0 \text{ o } 1 \end{array} \right\} \\
\Longrightarrow & \left\{ \begin{array}{l} a = 2(3q + r), \text{ con } q, r \in \mathbb{Z}, \text{ y } r = 0, 1 \text{ o } 2 \\ \wedge \\ a = 3(2q_3 + r_3) + r_2, \text{ con } q_3, r_3, r_2 \in \mathbb{Z}, \text{ y } r_3 = 0 \text{ o } 1 \text{ y } r_2 \neq 0 \end{array} \right. \\
\iff & \left\{ \begin{array}{l} a = 6q + 2r, \text{ con } q, r \in \mathbb{Z}, \text{ y } r = 0, 1 \text{ o } 2 \\ \wedge \\ a = 6q_3 + 3r_3 + r_2, \text{ con } q_3, r_3, r_2 \in \mathbb{Z}, \text{ y } r_3 = 0 \text{ o } 1 \text{ y } r_2 = 1 \text{ o } 2 \end{array} \right. \\
\iff & \left\{ \begin{array}{l} a = 6q + 2r, \text{ con } q, r \in \mathbb{Z}, \text{ y } 2r = 0, 2 \text{ o } 4 \\ \wedge \\ a = 6q_3 + 3r_3 + r_2, \text{ con } q_3, r_3, r_2 \in \mathbb{Z}, \text{ y } 3r_3 + r_2 = 1, 2, 4 \text{ o } 5 \end{array} \right. \\
\iff & \left\{ \begin{array}{l} a = 6q,\ a = 6q + 2 \text{ o } a = 6q + 4, \text{ con } q \in \mathbb{Z} \\ \wedge \\ a = 6q_3 + 1,\ a = 6q_3 + 2,\ a = 6q_3 + 4, \text{ o } a = 6q_3 + 5, \text{ con } q_3 \in \mathbb{Z} \end{array} \right. \\
\Longrightarrow & \ \exists q \in \mathbb{Z}\ a = 6q + 2 \text{ o } a = 6q + 4 \ \{\text{Unicidad de cociente y resto. (13.2.1)}\} \\
\iff & \ a \in \{n : n = 6q + 2 \ \vee \ n = 6q + 4,\ q \in \mathbb{Z}\}
\end{aligned}
$$

De la arbitrariedad de a se sigue que la proposición,

$$\forall x, (x \in A \setminus B \longrightarrow x \in \{n : n = 6q + 2 \ \vee \ n = 6q + 4,\ q \in \mathbb{Z}\})$$

es verdadera y por la definición de inclusión de conjuntos, (3.3.1),

$$(A \setminus B) \subseteq \{n : n = 6q + 2 \ \vee \ n = 6q + 4,\ q \in \mathbb{Z}\}$$

Recíprocamente,

$$
\begin{aligned}
a \in \{n : n = 6q+2 \ \vee \ n = 6q+4, \ q \in \mathbb{Z}\} \iff & \begin{cases} \exists q_1 \in \mathbb{Z} : a = 6q_1 + 2 \\ \vee \\ \exists q_2 \in \mathbb{Z} : a = 6q_2 + 4 \end{cases} \\
\iff & \begin{cases} \exists q_1 \in \mathbb{Z} : a = 2(3q_1+1) \ \wedge \ a = 3(2q_1) + 2 \\ \vee \\ \exists q_2 \in \mathbb{Z} : a = 2(3q_2+2) \ \wedge \ a = 3(2q_2+1) + 1 \end{cases} \\
& \left\{ \begin{array}{l} a \text{ da resto 0 al dividir por 2} \\ \wedge \\ a \text{ da resto 1 o 2 al dividir por 3} \end{array} \right\} \\
\implies & \begin{cases} \exists q_3 \in \mathbb{Z} : a = 2q_3 \\ \wedge \\ \exists q_4, r \in \mathbb{Z} : a = 3q_4 + r, \text{ con } r \neq 0 \end{cases} \\
\iff & \begin{cases} a \in A \\ \wedge \\ a \notin B \end{cases} \\
\iff & a \in (A \setminus B)
\end{aligned}
$$

Como a era cualquiera, la proposición,

$$\forall x, (x \in \{n : n = 6q+2 \ \vee \ n = 6q+4, \ q \in \mathbb{Z}\} \longrightarrow x \in (A \setminus B))$$

es verdadera y, de nuevo, por la definición de inclusión de conjuntos, (3.3.1),

$$\{n : n = 6q+2 \ \vee \ n = 6q+4, \ q \in \mathbb{Z}\} \subseteq (A \setminus B)$$

Finalmente, por la doble inclusión, tendremos, (3.3.5), que

$$A \setminus B = \{n : n = 6q+2 \ \vee \ n = 6q+4, \ q \in \mathbb{Z}\}$$

es decir, $A \setminus B$ es el conjunto formado por todos los enteros que dan resto par al dividirlos por 6.

c) $B \setminus A$

Sea a cualquier número entero. Entonces,

$$
\begin{aligned}
a \in B \setminus A \iff & \left\{ \begin{array}{l} a \in B \\ \wedge \\ a \notin A \end{array} \right. \\
\iff & \left\{ \begin{array}{l} \exists q_1 \in \mathbb{Z} : a = 3q_1 \\ \wedge \\ \exists q_2 \in \mathbb{Z} : a = 2q_2 + 1 \end{array} \right. \\
& \left\{ \begin{array}{l} \text{Dividiendo } q_1 \text{ por 2, } q_1 = 2q + r, \text{ con } q, r \in \mathbb{Z} \text{ y } r = 0 \text{ o } 1 \\ \text{Dividiendo } q_2 \text{ por 3, } q_2 = 3q_3 + r_3, \text{ con } q_3, r_3 \in \mathbb{Z} \text{ y } r_3 = 0, 1 \text{ o } 2 \end{array} \right\} \\
\Longrightarrow & \left\{ \begin{array}{l} \exists q, r \in \mathbb{Z} : a = 3(2q + r), \text{ con } r = 0 \text{ o } 1 \\ \wedge \\ \exists q_3, r_3 \in \mathbb{Z} : a = 2(3q_3 + r_3) + 1, \text{ con } r_3 = 0, 1 \text{ o } 2 \end{array} \right. \\
\iff & \left\{ \begin{array}{l} \exists q, r \in \mathbb{Z} : a = 6q + 3r, \text{ con } r = 0 \text{ o } 1 \\ \wedge \\ \exists q_3, r_3 \in \mathbb{Z} : a = 6q_3 + 2r_3 + 1, \text{ con } r_3 = 0, 1 \text{ o } 2 \end{array} \right. \\
\iff & \left\{ \begin{array}{l} \exists q, r \in \mathbb{Z} : a = 6q + 3r, \text{ con } 3r = 0 \text{ o } 3 \\ \wedge \\ \exists q_3, r_3 \in \mathbb{Z} : a = 6q_3 + 2r_3 + 1, \text{ con } 2r_3 + 1 = 1, 3 \text{ o } 5 \end{array} \right. \\
\iff & \left\{ \begin{array}{l} \exists q \in \mathbb{Z} : a = 6q \text{ o } a = 6q + 3 \\ \wedge \\ \exists q_3 \in \mathbb{Z} : a = 6q_3 + 1, \ a = 6q_3 + 3 \text{ o } a = 6q_3 + 5 \end{array} \right. \\
\Longrightarrow & \ \exists q \in \mathbb{Z} : a = 6q + 3 \ \{\text{Unicidad de cociente y resto. (13.2.1)}\} \\
\iff & \ a \in \{n : n = 6q + 3, \ q \in \mathbb{Z}\}
\end{aligned}
$$

De la arbitrariedad de a se sigue que la proposición,

$$\forall x, (x \in B \setminus A \longrightarrow x \in \{n : n = 6q + 3, \ q \in \mathbb{Z}\})$$

es verdadera y por la definición de inclusión de conjuntos, (3.3.1),

$$(B \setminus A) \subseteq \{n : n = 6q + 3, \ q \in \mathbb{Z}\}$$

Recíprocamente,

$$
\begin{aligned}
a \in \{n : n = 6q + 3,\ q \in \mathbb{Z}\} &\iff \exists q_1 \in \mathbb{Z} : a = 6q_1 + 3 \\
&\iff \begin{cases} \exists q_1 \in \mathbb{Z} : a = 3(2q_1 + 1) \\ \wedge \\ \exists q_1 \in \mathbb{Z} : a = 2(3q_1 + 1) + 1 \end{cases} \\
&\implies \begin{cases} \exists q_2 \in \mathbb{Z} : a = 3q_2 & \{\text{Tomando } q_2 = 2q_1 + 1\} \\ \wedge \\ \exists q_3 \in \mathbb{Z} : a = 2q_3 + 1 & \{\text{Tomando } q_3 = 3q_1 + 1\} \end{cases} \\
&\iff \begin{cases} a \in B \\ \wedge \\ a \notin A \end{cases} \\
&\iff a \in (B \setminus A)
\end{aligned}
$$

Como a era cualquiera, la proposición,

$$\forall x, (x \in \{n : n = 6q + 3,\ q \in \mathbb{Z}\} \longrightarrow x \in (B \setminus A))$$

es verdadera y, de nuevo, por la definición de inclusión de conjuntos, (3.3.1),

$$\{n : n = 6q + 3,\ q \in \mathbb{Z}\} \subseteq (B \setminus A)$$

Finalmente, por la doble inclusión, tendremos, (3.3.5), que

$$B \setminus A = \{n : n = 6q + 3,\ q \in \mathbb{Z}\}$$

es decir, $B \setminus A$ es el conjunto formado por todos los enteros que dan resto 3 al dividirlos por 6.

d) $A^c \cap B^c$

Sea a cualquier número entero. Entonces,

$$
\begin{aligned}
a \in (A^c \cap B^c) &\iff \left\{ \begin{array}{l} a \in A^c \\ \wedge \\ a \in B^c \end{array} \right. \\
&\iff \left\{ \begin{array}{l} a \notin A \\ \wedge \\ a \notin B \end{array} \right. \\
&\iff \left\{ \begin{array}{l} \exists q_1, r_1 \in \mathbb{Z} : a = 2q_1 + r_1, \text{ con } r_1 \neq 0 \\ \wedge \\ \exists q_2, r_2 \in \mathbb{Z} : a = 3q_2 + r_2, \text{ con } r_2 \neq 0 \end{array} \right. \\
&\iff \left\{ \begin{array}{l} \exists q_1 \in \mathbb{Z} : a = 2q_1 + 1 \\ \wedge \\ \exists q_2, r_2 \in \mathbb{Z} : a = 3q_2 + r_2, \text{ con } r_2 = 1 \text{ o } 2 \end{array} \right. \\
&\qquad \left\{ \begin{array}{l} \text{Dividiendo } q_1 \text{ por } 3,\ q_1 = 3q + r, \text{ con } q, r \in \mathbb{Z} \text{ y } r = 0, 1 \text{ o } 2 \\ \text{Dividiendo } q_2 \text{ por } 2,\ q_2 = 2q_3 + r_3, \text{ con } q_3, r_3 \in \mathbb{Z} \text{ y } r_3 = 0 \text{ o } 1 \end{array} \right\} \\
&\iff \left\{ \begin{array}{l} \exists q, r \in \mathbb{Z} : a = 6q + 2r + 1, \text{ con } r = 0, 1 \text{ o } 2 \\ \wedge \\ \exists q_2, r_2 \in \mathbb{Z} : a = 6q_3 + 3r_3 + r_2, \text{ con } r_3 = 0 \text{ o } 1 \text{ y } r_2 = 1 \text{ o } 2 \end{array} \right. \\
&\iff \left\{ \begin{array}{l} \exists q, r \in \mathbb{Z} : a = 6q + 2r + 1, \text{ con } 2r + 1 = 1, 3 \text{ o } 5 \\ \wedge \\ \exists q_2, r_2 \in \mathbb{Z} : a = 6q_3 + 3r_3 + r_2, \text{ con } 3r_3 + r_2 = 1, 2, 4, 5 \end{array} \right. \\
&\iff \left\{ \begin{array}{l} \exists q \in \mathbb{Z} : a = 6q + 1 \text{ o } a = 6q + 5 \\ \wedge \\ \exists q_2 \in \mathbb{Z} : a = 6q_3 + 1,\ a = 6q_3 + 2,\ a = 6q_3 + 4, \text{ o } a = 6q_5 + 5 \end{array} \right. \\
&\implies \exists q \in \mathbb{Z} : a = 6q + 1 \text{ o } a = 6q + 5 \ \{\text{Unicidad de cociente y resto. (13.2.1)}\} \\
&\iff a \in \{n : n = 6q + 1 \ \vee \ n = 6q + 5,\ q \in \mathbb{Z}\}
\end{aligned}
$$

De la arbitrariedad de a se sigue que la proposición,

$$\forall x, (x \in A^c \cap B^c \longrightarrow x \in \{n : n = 6q + 1 \ \vee \ n = 6q + 5,\ q \in \mathbb{Z}\})$$

es verdadera y por la definición de inclusión de conjuntos, (3.3.1),

$$(A^c \cap B^c) \subseteq \{n : n = 6q + 1 \ \vee \ n = 6q + 5,\ q \in \mathbb{Z}\}$$

Recíprocamente,

$$
\begin{aligned}
a \in \{n : n = 6q+1 \ \vee \ n = 6q+5, \ q \in \mathbb{Z}\} &\iff \begin{cases} \exists q_1 \in \mathbb{Z} : a = 6q_1 + 1 \\ \vee \\ \exists q_2 \in \mathbb{Z} : a = 6q_2 + 5 \end{cases} \\
&\iff \begin{cases} \exists q_1 \in \mathbb{Z} : a = 2(3q_1) + 1 \ \wedge \ a = 3(2q_1) + 1 \\ \vee \\ \exists q_2 \in \mathbb{Z} : a = 2(3q_2 + 2) + 1 \ \wedge \ a = 3(2q_2 + 1) + 2 \end{cases} \\
&\quad \begin{cases} a \text{ da resto 1 al dividir por 2} \\ \wedge \\ a \text{ da resto 1 o 2 al dividir por 3} \end{cases} \\
&\implies \begin{cases} \exists q_3 \in \mathbb{Z} : a = 2q_3 + 1 \\ \wedge \\ \exists q_4, r \in \mathbb{Z} : a = 3q_4 + r, \text{ con } r \neq 0 \end{cases} \\
&\iff \begin{cases} a \notin A \\ \wedge \\ a \notin B \end{cases} \\
&\iff \begin{cases} a \in A^c \\ \wedge \\ a \in B^c \end{cases} \\
&\iff a \in (A^c \cap B^c)
\end{aligned}
$$

Como a era cualquiera, la proposición,

$$\forall x, (x \in \{n : n = 6q+1 \ \vee \ n = 6q+5, \ q \in \mathbb{Z}\} \longrightarrow x \in (B \setminus A))$$

es verdadera y, de nuevo, por la definición de inclusión de conjuntos, (3.3.1),

$$\{n : n = 6q+1 \ \vee \ n = 6q+5, \ q \in \mathbb{Z}\} \subseteq (A^c \cap B^c)$$

Finalmente, por la doble inclusión, tendremos, (3.3.5), que

$$A^c \cap B^c = \{n : n = 6q+1 \ \vee \ n = 6q+5, \ q \in \mathbb{Z}\}$$

es decir, $A^c \cap B^c$ es el conjunto formado por todos los enteros que dan resto 1 o 5 al dividirlos por 6.

e) Probar que los cuatro conjuntos anteriores forman una partición del conjunto de los números enteros.
Sea $\mathscr{P} = \{A \cap B, A \setminus B, B \setminus A, A^c \cap B^c\}$. Veamos si $\mathscr{P}$ cumple las tres condiciones de partición.

1 Ninguno de los conjuntos que integran $\mathscr{P}$ es vacío.

⁕ $A \cap B \neq \emptyset$

En efecto, supongamos que $A \cap B$ fuera vacío. Entonces, ningún entero que sea par puede múltiplo de 3, es decir, la proposición,

$$\forall n, (n \in A \longrightarrow n \notin B)$$

sería verdadera. Esto no es cierto ya que, por ejemplo, el 6 es par y múltiplo de 3, es decir, la proposición,

$$\exists n : (n \in A \wedge n \in B)$$

es verdadera, la anterior sería falsa y, consecuentemente, $A \cap B \neq \emptyset$.

⁎ $A \setminus B \neq \emptyset$
En efecto, supongamos que $A \setminus B$ fuera el conjunto vacío. Esto querría decir que todos los enteros pares son múltiplos de 3, o sea, es verdadera la proposición,

$$\forall n, (n \in A \longrightarrow n \in B)$$

Esto, obviamente, no es cierto ya que, por ejemplo, el 2 es par y no es múltiplo de 3, es decir, la proposición,

$$\exists n : (n \in A \wedge n \notin B)$$

es verdadera, por lo tanto, la anterior sería falsa y, consecuentemente, $A \setminus B \neq \emptyset$.

⁎ $B \setminus A \neq \emptyset$
En efecto, supongamos que $B \setminus A$ fuera el conjunto vacío. Esto querría decir que todos los múltiplos de 3 son pares, o sea, es verdadera la proposición,

$$\forall n, (n \in B \longrightarrow n \in A)$$

Esto, obviamente, no es cierto ya que, por ejemplo, el 3 es múltiplo de 3 y no es par, es decir, la proposición,

$$\exists n : (n \in B \wedge n \notin A)$$

es verdadera, por lo tanto, la anterior sería falsa y, consecuentemente, $B \setminus A \neq \emptyset$.

⁎ $A^c \cap B^c \neq \emptyset$
En efecto, supongamos que $A^c \cap B^c \neq \emptyset$. Esto significaría que todos los números impares son múltiplos de 3, es decir, la proposición,

$$\forall n, (n \notin A \longrightarrow n \in B)$$

es verdadera, lo cual, obviamente, no es cierto ya que el 1 es impar y no es múltiplo de 3, es decir, la proposición

$$\exists n : (n \in A^c \wedge n \in B^c)$$

es verdadera, la anterior sería falsa y, consecuentemente, $A^c \cap B^c \neq \emptyset$.

2 Los conjuntos que conforman $\mathscr{P}$ son dos a dos disjuntos.
En efecto,

$$\begin{aligned}
(A \cap B) \cap (A \setminus B) &= A \cap B \cap A \cap B^c && \{\text{Diferencia de conjuntos. (4.1.3)}\}\\
&= A \cap A \cap B \cap B^c && \{\text{Leyes conmutativas. (4.2.2)}\}\\
&= A \cap B \cap B^c && \{\text{Leyes de idempotencia. (4.2.1)}\}\\
&= A \cap \emptyset && \{\text{Leyes del complementario. (4.2.8)}\}\\
&= \emptyset && \{\text{Leyes de dominación (4.2.5)}\}
\end{aligned}$$

$$\begin{aligned}
(A \cap B) \cap (B \setminus A) &= A \cap B \cap B \cap A^c && \{\text{Diferencia de conjuntos. (4.1.3)}\}\\
&= A \cap A^c \cap B \cap B && \{\text{Leyes conmutativas. (4.2.2)}\}\\
&= A \cap A^c \cap B && \{\text{Leyes de idempotencia. (4.2.1)}\}\\
&= \emptyset \cap B && \{\text{Leyes del complementario. (4.2.8)}\}\\
&= \emptyset && \{\text{Leyes de dominación (4.2.5)}\}
\end{aligned}$$

$$\begin{aligned}
(A \cap B) \cap (A^c \cap B^c) &= A \cap A^c \cap B \cap B^c && \{\text{Leyes conmutativas. (4.2.2)}\}\\
&= \emptyset \cap \emptyset && \{\text{Leyes del complementario. (4.2.8)}\}\\
&= \emptyset && \{\text{Leyes de idempotencia. (4.2.1)}\}
\end{aligned}$$

$$\begin{aligned}
(A \setminus B) \cap (B \setminus A) &= A \cap B^c \cap B \cap A^c && \{\text{Diferencia de conjuntos. (4.1.3)}\} \\
&= A \cap A^c \cap B \cap B^c && \{\text{Leyes conmutativas. (4.2.2)}\} \\
&= \emptyset \cap \emptyset && \{\text{Leyes del complementario. (4.2.8)}\} \\
&= \emptyset && \{\text{Leyes de idempotencia. (4.2.1)}\}
\end{aligned}$$

$$\begin{aligned}
(A \setminus B) \cap (A^c \cap B^c) &= A \cap B^c \cap A^c \cap B^c && \{\text{Diferencia de conjuntos. (4.1.3)}\} \\
&= A \cap A^c \cap B^c \cap B^c && \{\text{Leyes conmutativas. (4.2.2)}\} \\
&= A \cap A^c \cap B^c && \{\text{Leyes de idempotencia. (4.2.1)}\} \\
&= \emptyset \cap B^c && \{\text{Leyes del complementario. (4.2.8)}\} \\
&= \emptyset && \{\text{Leyes de dominación (4.2.5)}\}
\end{aligned}$$

$$\begin{aligned}
(B \setminus A) \cap (A^c \cap B^c) &= B \cap A^c \cap A^c \cap B^c && \{\text{Diferencia de conjuntos. (4.1.3)}\} \\
&= A^c \cap A^c \cap B \cap B^c && \{\text{Leyes conmutativas. (4.2.2)}\} \\
&= A^c \cap B \cap B^c && \{\text{Leyes de idempotencia. (4.2.1)}\} \\
&= A^c \cap \emptyset && \{\text{Leyes del complementario. (4.2.8)}\} \\
&= \emptyset && \{\text{Leyes de dominación (4.2.5)}\}
\end{aligned}$$

3 El conjunto de los enteros es igual a la unión de todos los conjuntos que integran la partición. En efecto,

$$\begin{aligned}
&(A \cap B) \cup (A \setminus B) \cup (B \setminus A) \cup (A^c \cap B^c) \\
&= \\
&(A \cap B) \cup (A \cap B^c) \cup (B \cap A^c) \cup (A^c \cap B^c) && \{\text{Diferencia de conjuntos. (4.1.3)}\} \\
&= \\
&(A \cap B) \cup (A \cap B^c) \cup (A^c \cap B) \cup (A^c \cap B^c) && \{\text{Leyes conmutativas. (4.2.2)}\} \\
&= \\
&[A \cap (B \cup B^c)] \cup [A^c \cap (B \cup B^c)] && \{\text{Leyes distributivas. (4.2.4)}\} \\
&= \\
&(A \cap \mathbb{Z}) \cup (A^c \cap \mathbb{Z}) && \{\text{Leyes del complementario. (4.2.8)}\} \\
&= \\
&A \cup A^c && \{\text{Leyes de identidad. (4.2.6)}\} \\
&= \\
&\mathbb{Z} && \{\text{Leyes del complementario. (4.2.8)}\}
\end{aligned}$$

d) Probar, aplicando los resultados obtenidos en los apartados anteriores, que cualquier entero es múltiplo de 6 o da resto par al dividirlo entre 6 o da resto 3 al dividirlo entre 6 o da resto impar al dividirlo entre 6.

En efecto, directamente del apartado anterior,

$$\mathbb{Z} = (A \cap B) \cup (A \setminus B) \cup (B \setminus A) \cup (A^c \cap B^c)$$

Entonces, si a es un entero cualquiera,

$$
\begin{aligned}
a \in \mathbb{Z} \iff & \begin{cases} a \in (A \cap B) \\ \vee \\ a \in (A \setminus B) \\ \vee \\ a \in (B \setminus A) \\ \vee \\ a \in (A^c \cap B^c) \end{cases} \\
\iff & \begin{cases} a \in \{n : n = 6q,\ q \in \mathbb{Z}\} \\ \vee \\ a \in \{n : n = 6q+2 \ \vee \ n = 6q+4,\ q \in \mathbb{Z}\} \\ \vee \\ a \in \{n : n = 6q+3,\ q \in \mathbb{Z}\} \\ \vee \\ a \in \{n : n = 6q+1 \ \vee \ n = 6q+5,\ q \in \mathbb{Z}\} \end{cases} \\
\iff & \begin{cases} \exists q \in \mathbb{Z} : a = 6q \\ \vee \\ \exists q \in \mathbb{Z} : a = 6q+2 \ \vee \ a = 6q+4 \\ \vee \\ \exists q \in \mathbb{Z} : a = 6q+3 \\ \vee \\ \exists q \in \mathbb{Z} : a = 6q+1 \ \vee \ a = 6q+5 \end{cases} \\
\iff & \begin{cases} a \text{ es múltiplo de } 6 \\ \vee \\ a \text{ da resto par al dividirlo por } 6 \\ \vee \\ a \text{ da resto } 3 \text{ al dividirlo por } 6 \\ \vee \\ a \text{ da resto impar al dividirlo por } 6 \end{cases}
\end{aligned}
$$

■

4.4 Producto cartesiano de conjuntos

El concepto matemático de relación está basado en la noción de relación entre objetos. Algunas relaciones describen comparaciones entre elementos de un conjunto: Una caja es más pesada que otra, un hombre es

más rico que otro, etc. Otras relaciones involucran elementos de conjuntos diferentes, tal como "x vive en y", donde x es una persona e y es una ciudad, "x es propiedad de y" donde x es un edificio e y es una empresa, ó "x nació en el país y en el año z".

Todos los ejemplos anteriores son de relaciones entre dos o tres objetos, sin embargo, en principio, podemos describir relaciones que abarquen n objetos, donde n es cualquier entero positivo. Cuando hagamos una afirmación que relacione n objetos, será necesario no solamente especificar los objetos en sí mismos sino también una ordenación de los mismos. Por ejemplo, la posición relativa de 3 y 5 da lugar únicamente a dos afirmaciones "$5 < 3$" y "$3 < 5$", siendo una de ellas falsa y la otra verdadera.

Usaremos las *n-tuplas ordenadas de elementos* para especificar una sucesión finita de objetos no necesariamente distintos; la posición relativa de los objetos en la sucesión nos dará la ordenación necesaria de los mismos.

4.4.1 n-tupla ordenada

Llamaremos n-tupla ordenada a una sucesión de n objetos $a_1, a_2, \ldots, a_n$ dados en un cierto orden y la notaremos por $(a_1, a_2, \ldots, a_n)$.

Obsérvese que es fundamental el orden en que escribamos los elementos de la n-tupla, así

$$(a_1, a_2, \ldots, a_n) \neq (a_2, a_1, \ldots, a_n)$$

Si $n = 2$, una n-tupla ordenada se llama "par ordenado" y si $n = 3$, "terna ordenada".

■

4.4.2 Igualdad de n-tuplas

Diremos que dos n-tuplas ordenadas son iguales si, y sólo si, sus i-ésimas componentes son iguales para todo $i,\ 1 \leqslant i \leqslant n$, es decir,

$$(a_1, a_2, \ldots, a_n) = (b_1, b_2, \ldots, b_n) \Longleftrightarrow a_i = b_i,\ \forall i, 1 \leqslant i \leqslant n$$

Muchas veces trataremos con colecciones de n-tuplas donde la componente i-ésima de cada n-tupla es un elemento de un conjunto A_i. Definimos el conjunto de todas las n-tuplas ordenadas.

■

4.4.3 Producto cartesiano

Dada una colección arbitraria de conjuntos $A_1, A_2, \ldots, A_n$, llamaremos producto cartesiano de los mismos y lo notaremos por $A_1 \times A_2 \times \cdots \times A_n$, al conjunto formado por todas las n-tuplas ordenadas, $(a_1, a_2, \ldots, a_n)$, donde $a_i \in A_i,\ 1 \leqslant i \leqslant n$, es decir,

$$A_1 \times A_2 \times \cdots \times A_n = \{(a_1, a_2, \ldots, a_n) : a_i \in A_i\ 1 \leqslant i \leqslant n\}$$

En el caso de dos conjuntos A y B, tendremos

$$A \times B = \{(a, b) : a \in A \text{ y } b \in B\}$$

y este producto se llama *binario* si $A = B$, o sea,

$$A \times A = \{(a, b) : a \in A \text{ y } b \in A\}$$

y suele notarse por A^2.

Su extensión a n conjuntos se define como

$$A \times A \times \overset{(n}{\cdots} \times A = \{(a_1, a_2, \ldots, a_n) : a_i \in A,\ 1 \leqslant i \leqslant n\}$$

y lo notaremos por A^n.

■

Ejemplo 4.9

Sean $A_1 = \{1, 2\}$, $A_2 = \{a, b\}$ *y* $A_3 = \{x, y\}$. *Calcular* $A_1 \times A_2 \times A_3$, $A_2 \times A_1 \times A_3$ *y* A_3^2.

Solución

$$\begin{aligned} A_1 \times A_2 \times A_3 &= \{(1,a,x),(1,a,y),(1,b,x),(1,b,y),(2,a,x),(2,a,y),(2,b,x),(2,b,y)\} \\ A_2 \times A_1 \times A_3 &= \{(a,1,x),(a,1,y),(a,2,x),(a,2,y),(b,1,x),(b,1,y),(b,2,x),(b,2,y)\} \\ A_3^2 = A_3 \times A_3 &= \{(x,x),(x,y),(y,x),(y,y)\} \end{aligned}$$

■

Nota 4.1 Considerando el conjunto $\mathbb{R}$ de los números reales, el producto cartesiano $\mathbb{R}^2 = \mathbb{R} \times \mathbb{R}$ es el conjunto de todos los pares ordenados de números reales.

$$\mathbb{R} \times \mathbb{R} = \mathbb{R}^2 = \{(x, y) : x, y \in \mathbb{R}\}$$

Cada punto P del plano representa un par ordenado (x, y) de números reales y viceversa. A $\mathbb{R}^2$ se le llama normalmente *plano cartesiano.*

■

Ejemplo 4.10

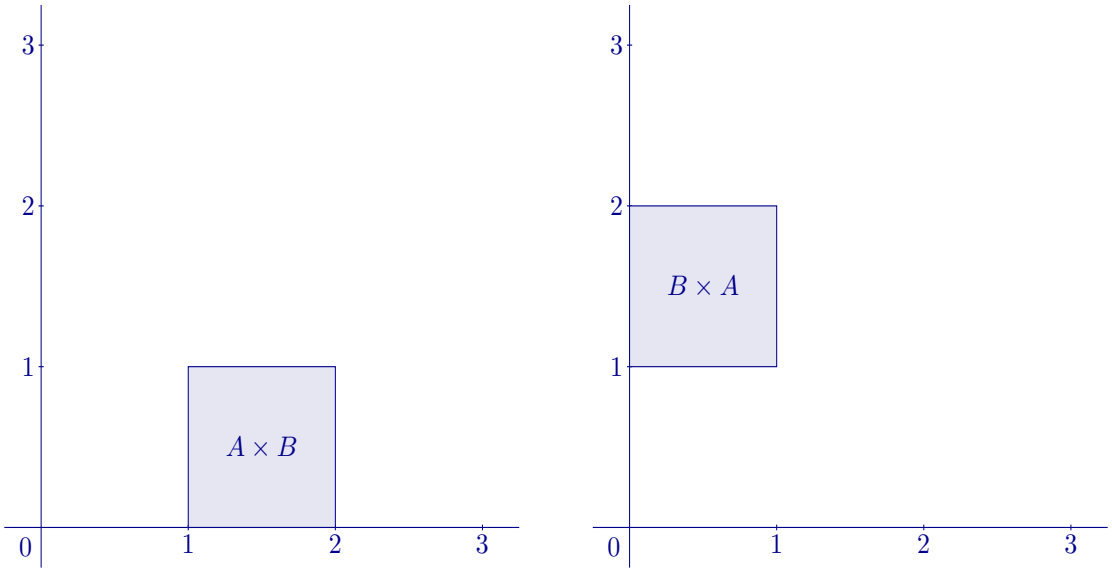
Sean $A = \{x \in \mathbb{R} : 1 \leqslant x \leqslant 2\}$ *y* $B = \{y \in \mathbb{R} : 0 \leqslant y \leqslant 1\}$. *Representar gráficamente* $A \times B$ *y* $B \times A$.

Solución

Cuando A y B son, como en este caso, conjuntos de números reales, su producto cartesiano puede representarse como un conjunto de puntos en el plano cartesiano.

$$A \times B = \{(x, y) : 1 \leqslant x \leqslant 2 \text{ y } 0 \leqslant y \leqslant 1\}$$

$$B \times A = \{(y, x) : 0 \leqslant y \leqslant 1 \text{ y } 1 \leqslant x \leqslant 2\}$$



■

Ejemplo 4.11

Sea $A = \{1, 2\}$ *y* $B = \{a, b, c\}$. *Calcular* $A \times B$, $B \times A$, $A \times A$ *y* $B \times B$.

Solución

$$\begin{aligned} B \times A &= \{(a,1),(a,2),(b,1),(b,2),(c,1),(c,2)\} \\ A \times B &= \{(1,a),(1,b),(1,c),(2,a),(2,b),(2,c)\} \\ A \times A &= \{(1,1),(1,2),(2,1),(2,2)\} \\ B \times B &= \{(a,a),(a,b),(a,c),(b,a),(b,b),(b,c),(c,a),(c,b),(c,c)\} \end{aligned}$$

■

Nota 4.2 En los ejemplos anteriores se observa que el producto cartesiano de dos conjuntos no es conmutativo. Es decir, en general, $A \times B \neq B \times A$

■

Ejemplo 4.12

Demostrar que una condición necesaria y suficiente para que el producto cartesiano de dos conjuntos sea el conjunto vacío es que uno de los dos, al menos, sea el vacío.

Solución

Sean A y B dos conjuntos cualesquiera. La condición es, por tanto, $A = \emptyset$ ó $B = \emptyset$.

⁎ La condición es *necesaria*. Utilizaremos el método de demostración por la contrarrecíproca, (1.5.4), para probar,

$$A \times B = \emptyset \Longrightarrow A = \emptyset \text{ ó } B = \emptyset$$

es decir, probaremos que

$$A \neq \emptyset \text{ y } B \neq \emptyset \Longrightarrow A \times B \neq \emptyset$$

En efecto,

$$\left.\begin{array}{ccc} A \neq \emptyset & \Longrightarrow & \exists a \in A \\ \text{y} & & \text{y} \\ B \neq \emptyset & \Longrightarrow & \exists b \in B \end{array}\right\} \Longrightarrow \exists (a,b) \in A \times B \Longrightarrow A \times B \neq \emptyset$$

⁎ La condición es *suficiente*. Probaremos, también por la contrarrecíproca, (1.5.4),

$$A = \emptyset \text{ ó } B = \emptyset \Longrightarrow A \times B = \emptyset$$

o sea, probaremos que

$$A \times B \neq \emptyset \Longrightarrow A \neq \emptyset \text{ y } B \neq \emptyset$$

En efecto,

$$A \times B \neq \emptyset \Longrightarrow \exists (a,b) \in A \times B \Longrightarrow \left\{\begin{array}{ccc} \exists a \in A & \Longrightarrow & A \neq \emptyset \\ \text{y} & & \text{y} \\ \exists b \in B & \Longrightarrow & B \neq \emptyset \end{array}\right.$$

Obsérvese que podríamos haber utilizado la doble implicación y hacer una sola demostración. En efecto,

$$A \times B \neq \emptyset \Longleftrightarrow \exists (a,b) \in A \times B \Longleftrightarrow \left\{\begin{array}{ccc} \exists a \in A & \Longleftrightarrow & A \neq \emptyset \\ \text{y} & & \text{y} \\ \exists b \in B & \Longleftrightarrow & B \neq \emptyset \end{array}\right.$$

es decir, hemos probado por la contrarrecíproca, (1.5.4), que

$$A \times B = \emptyset \Longleftrightarrow A = \emptyset \text{ ó } B = \emptyset$$

■

4.4.4 Propiedades

El producto cartesiano es distributivo respecto de la unión y la intersección de conjuntos, es decir, si A, B y C son tres conjuntos cualesquiera, se verifica:

(a) $A \times (B \cup C) = (A \times B) \cup (A \times C)$

(b) $A \times (B \cap C) = (A \times B) \cap (A \times C)$

(c) $(A \cup B) \times C = (A \times C) \cup (B \times C)$

(d) $(A \cap B) \times C = (A \times C) \cap (B \times C)$

Demostración

(a) $A \times (B \cup C) = (A \times B) \cup (A \times C)$

En efecto, sea (a, b) un elemento arbitrario de $A \times (B \cup C)$, entonces,

$$\begin{aligned}
(a,b) \in A \times (B \cup C) &\iff a \in A \ \wedge \ b \in (B \cup C) && \{\text{Def. producto cartesiano}\}\\
&\iff a \in A \ \wedge \ (b \in B \ \vee \ b \in C) && \{\text{Def. de unión}\}\\
&\iff (a \in A \ \wedge \ b \in B) \ \vee \ (a \in A \ \wedge \ b \in C) && \{\text{Dist. de } \wedge \text{ respecto de } \vee\}\\
&\iff (a,b) \in (A \times B) \ \vee \ (a,b) \in (A \times C) && \{\text{Def. producto cartesiano}\}\\
&\iff (a,b) \in (A \times B) \cup (A \times C) && \{\text{Definición de unión}\}
\end{aligned}$$

luego,

$$\forall (x,y), ((x,y) \in A \times (B \cup C) \longleftrightarrow (x,y) \in (A \times B) \cup (A \times C))$$

es decir,

$$A \times (B \cup C) = (A \times B) \cup (A \times C)$$

Los apartados (b), (c) y (d) se demuestran de una forma similar.

■

Ejemplo 4.13

Si $\mathscr{U} = \mathbb{Z}^+$, $A = \{1, 2, 3, 4\}$, $B = \{2, 5\}$ *y* $C = \{3, 4, 7\}$, *determínense los conjuntos siguientes:*

(a) $A \times B$

(b) $B \times A$

(c) $A \cup (B \times C)$

(d) $(A \cup B) \times C$

(e) $(A \times C) \cup (B \times C)$

Solución

(a) $A \times B = \{(x, y) : x \in A \wedge y \in B\}$
luego,
$$A \times B = \{(1,2), (1,5), (2,2), (2,5), (3,2), (3,5), (4,2), (4,5)\}$$

(b) $B \times A = \{(y, x) : y \in B \wedge x \in A\}$
luego,
$$B \times A = \{(2,1), (2,2), (2,3), (2,4), (5,1), (5,2), (5,3), (5,4)\}$$

(c)
$$A \cup (B \times C) = \{1, 2, 3, 4, (2,3), (2,4), (2,7), (5,3), (5,4), (5,7)\}$$

(d)
$$\begin{aligned}
(A \cup B) \times C \ = \ &\{(1,3), (1,4), (1,7), (2,3), (2,4), (2,7), (3,3),\\
&(3,4), (3,7), (4,3), (4,4), (4,7), (5,3), (5,4), (5,7)\}
\end{aligned}$$

(e)
$$\begin{aligned}
(A \times C) \cup (B \times C) \ = \ &\{(1,3), (1,4), (1,7), (2,3), (2,4), (2,7), (3,3),\\
&(3,4), (3,7), (4,3), (4,4), (4,7), (5,3), (5,4), (5,7)\}
\end{aligned}$$

■

Ejemplo 4.14

Dados tres conjuntos arbitrarios $A, B, C \subset \mathscr{U}$*, probar* $A \times (B \cap C) = (A \times B) \cap (A \times C)$

Solución

$A \times (B \cap C) = (A \times B) \cap (A \times C)$ En efecto, sea (a, b) cualquiera de $A \times (B \cap C)$. Entonces,

$$\begin{aligned}
(a,b) \in A \times (B \cap C) &\iff a \in A \ \wedge \ b \in (B \cap C) \\
&\iff a \in A \ \wedge \ (b \in B \ \wedge \ b \in C) \\
&\iff (a \in A \ \wedge \ b \in B) \ \wedge \ (a \in A \ \wedge \ b \in C) \\
&\iff (a,b) \in A \times B \ \wedge \ (a,b) \in A \times C \\
&\iff (a,b) \in (A \times B) \cap (A \times C)
\end{aligned}$$

luego,

$$\forall (x,y), ((x,y) \in A \times (B \cap C) \longleftrightarrow (x,y) \in (A \times B) \cap (A \times C))$$

es decir,

$$A \times (B \cap C) = (A \times B) \cap (A \times C)$$

■

Ejemplo 4.15

Se consideran los conjuntos $A = \{x \in \mathbb{Z} : 3 \leqslant x \leqslant 8\}$ *y* $B = \{x \in \mathbb{Z} : -6 < x \leqslant -4\}$*. Hallar* $A \times B$

Solución

$$A = \{x \in \mathbb{Z} : 3 \leqslant x \leqslant 8\} = \{3, 4, 5, 6, 7, 8\}$$

$$B = \{x \in \mathbb{Z} : -6 < x \leqslant -4\} = \{-5, -4\}$$

luego,

$$A \times B =$$
$$\{(3,-5), (4,-5), (5,-5), (6,-5), (7,-5), (8,-5), (3,-4), (4,-4), (5,-4), (6,-4), (7,-4), (8,-4)\}$$

■

Ejemplo 4.16

Demostrar que

$$(A_1 \times B_1) \cap (A_2 \times B_2) = (A_1 \cap A_2) \times (B_1 \cap B_2)$$

Solución

En efecto, sea (a, b) un elemento arbitrario de $(A_1 \times B_1) \cap (A_2 \times B_2)$. Entonces,

$$\begin{aligned}
(a,b) \in (A_1 \times B_1) \cap (A_2 \times B_2) &\iff (a,b) \in (A_1 \times B_1)) \ \wedge \ (a,b) \in (A_2 \times B_2) && \{\text{Def. de } \cap\} \\
&\iff (a \in A_1 \ \wedge \ b \in B_1) \ \wedge \ (a \in A_2 \ \wedge \ b \in B_2) && \{\text{Def. de } \times\} \\
&\iff (a \in A_1 \ \wedge \ a \in A_2) \ \wedge \ (b \in B_1 \ \wedge \ b \in B_2) && \{\text{Asoc. y conm.}\} \\
&\iff a \in (A_1 \cap A_2) \ \wedge \ b \in (B_1 \cap B_2) \\
&\iff (a,b) \in (A_1 \cap A_2) \times (B_1 \cap B_2)
\end{aligned}$$

luego,

$$\forall (x,y)\,((x,y) \in (A_1 \times B_1) \cap (A_2 \times B_2) \longleftrightarrow (x,y) \in (A_1 \cap A_2) \times (B_1 \cap B_2))$$

es decir,

$$(A_1 \times B_1) \cap (A_2 \times B_2) = (A_1 \cap A_2) \times (B_1 \cap B_2)$$

■

Ejemplo 4.17

Dados los conjuntos $A = \{a, b, c, d\}$, $B = \{1, 2, 3\}$ *y* $C = \{\alpha, \beta, \gamma\}$, *hallar*

(a) $A \times B \times C$

(b) $A \times (B \cap C)$

(c) $A \times (B \cup C)$

Solución

(a)

$$\begin{aligned}
A \times B \times C \ = \ \{&(a,1,\alpha),(a,1,\beta),(a,1,\gamma),(a,2,\alpha),(a,2,\beta),(a,2,\gamma),(a,3,\alpha),(a,3,\beta), \\
&(a,3,\gamma),(b,1,\alpha),(b,1,\beta),(b,1,\gamma),(b,2,\alpha),(b,2,\beta),(b,2,\gamma),(b,3,\alpha), \\
&(b,3,\beta),(b,3,\gamma),(c,1,\alpha),(c,1,\beta),(c,1,\gamma),(c,2,\alpha),(c,2,\beta),(c,2,\gamma), \\
&(c,3,\alpha),(c,3,\beta),(c,3,\gamma),(d,1,\alpha),(d,1,\beta),(d,1,\gamma),(d,2,\alpha),(d,2,\beta), \\
&(d,2,\gamma),(d,3,\alpha),(d,3,\beta),(d,3,\gamma)\}
\end{aligned}$$

(b) $A \times (B \cap C) = A \times \emptyset = \emptyset$

(c) $A \times (B \cup C)$

Según hemos visto en la lección,

$$A \times (B \cup C) = (A \times B) \cup (A \times C)$$

luego,

$$\begin{aligned}
A \times (B \cup C) \ = \ \{&(a,1),(a,2),(a,3),(b,1),(b,2),(b,3),(c,1),(c,2),(c,3),(d,1),(d,2),(d,3) \\
&(a,\alpha),(a,\beta),(a,\gamma),(b,\alpha),(b,\beta),(b,\gamma),(c,\alpha),(c,\beta),(c,\gamma),(d,\alpha),(d,\beta),(d,\gamma)\}
\end{aligned}$$

■

Ejemplo 4.18

Para $A, B, C \subseteq \mathscr{U}$, probar que $A \times (B \setminus C) = (A \times B) \setminus (A \times C)$.

Solución

En efecto, sea (a, b) cualquiera de $A \times (B \setminus C)$. Entonces,

$$\begin{aligned}
(a,b) \in A \times (B \setminus C) &\iff a \in A \ \wedge \ b \in B \setminus C \\
&\iff a \in A \ \wedge \ (b \in B \ \wedge \ b \notin C) \\
&\iff (a \in A \ \wedge \ b \in B) \ \wedge \ (a \in A \ \wedge \ b \notin C) \\
&\iff (a,b) \in A \times B \ \wedge \ (a,b) \notin (A \times C) \\
&\iff (a,b) \in (A \times B) \setminus (A \times C)
\end{aligned}$$

luego,

$$\forall (x,y), ((x,y) \in A \times (B \setminus C) \longleftrightarrow (x,y) \in (A \times B) \setminus (A \times C))$$

es decir,

$$A \times (B \setminus C) = (A \times B) \setminus (A \times C)$$

■

Unidad Temática III

Relaciones y Funciones

Lección 5

Relaciones

Las matemáticas aparecen como la ciencia que estudia las relaciones entre ciertos objetos abstractos.

Emile Borel

En esta lección estudiaremos algunas estructuras básicas que pueden representarse a través de la relación entre elementos de conjuntos. Las relaciones tienen una importancia fundamental tanto en la teoría como en las aplicaciones a la informática.

Una estructura de datos tales como una lista, una matriz o un árbol, se usan para representar conjuntos de elementos junto con una relación entre los mismos.

Las relaciones que son parte de un modelo matemático están a menudo implícitamente representadas por relaciones en una estructura de datos.

Aplicaciones numéricas, recuperación de información y problemas de redes son algunos ejemplos donde las relaciones ocurren como parte de la descripción del problema, y la manipulación de relaciones es importante en la resolución de procedimientos.

Las relaciones también juegan un importante papel en la teoría de computación, incluyendo estructuras de programas y análisis de algoritmos.

En esta lección desarrollaremos algunas de las herramientas fundamentales y los conceptos asociados a las relaciones.

5.1 Generalidades

Hemos estudiado la relación de subconjunto para conjuntos. En álgebra y cálculo son importantes las relaciones entre variables; en geometría lo son las relaciones entre figuras. Hasta el momento no hemos necesitado una definición precisa de la palabra *relación*. Sin embargo, sin una definición formal es difícil responder preguntas sobre relaciones. ¿Qué se quiere dar a entender, por ejemplo, cuando se dice que dos relaciones aparentemente diferentes son iguales?

En la realidad que nos circunda existen relaciones entre elementos, entre conjuntos y entre elementos y conjuntos. Existen relaciones de parentesco, de amistad, de paisanaje, etc., entre personas; relaciones diplomáticas, económicas, etc., entre países; relaciones de paralelismo o de perpendicularidad entre rectas de un plano; relaciones de inclusión entre conjuntos; relaciones como "mayor que" o "menor o igual que" entre números, etc. La matemática intenta, como ahora veremos, hacerse eco de tales sucesos y, mediante un proceso de abstracción, expresarlas y estudiarlas científicamente.

5.1.1 Relación

Sean los conjuntos $A_1, A_2, \ldots, A_n$. Una relación $\mathscr{R}$ sobre $A_1 \times A_2 \times \cdots \times A_n$ es cualquier subconjunto de este producto cartesiano, es decir,

$$\mathscr{R} \subseteq A_1 \times A_2 \times \cdots \times A_n$$

Si $\mathscr{R} = \emptyset$, llamaremos a $\mathscr{R}$, la relación vacía.

Si $\mathscr{R} = A_1 \times A_2 \times \cdots \times A_n$, llamaremos a $\mathscr{R}$ la relación universal.

Si $A_i = A,\ \forall i = 1, 2, \ldots, n$, entonces $\mathscr{R}$ es una relación n-aria sobre A.

Si $n = 2$, diremos que $\mathscr{R}$ es una relación binaria y si $n = 3$, una relación ternaria.

Ejemplo 5.1

Sean $A_1 = \{a, b\}$, $A_2 = \{1, 2, 3\}$ y $A_3 = \{p, q, r\}$. Escribir tres relaciones definidas en $A_1 \times A_2 \times A_3$.

Solución

El producto cartesiano de estos tres conjuntos es

$$\begin{aligned} A_1 \times A_2 \times A_3 \quad = \quad & \{(a,1,p),(a,1,q),(a,1,r),(a,2,p),(a,2,q),(a,2,r),\\ & (a,3,p),(a,3,q),(a,3,r),(b,1,p),(b,1,q),(b,1,r),\\ & (b,2,p),(b,2,q),(b,2,r),(b,3,p),(b,3,q),(b,3,r)\} \end{aligned}$$

y cualquier subconjunto de este producto cartesiano sería una relación definida sobre ellos. Por ejemplo,

$$\begin{aligned} \mathscr{R}_1 &= \{(a,1,p)\} \\ \mathscr{R}_2 &= \{(a,1,p),(a,2,p)\} \\ \mathscr{R}_3 &= \{(b,1,p),(b,1,q),(b,1,r),(b,2,p),(b,2,q),(b,2,r),(b,3,p),(b,3,q),(b,3,r)\} \end{aligned}$$

son tres relaciones definidas en $A_1 \times A_2 \times A_3$.

■

Ejemplo 5.2

Sea $A = \{$huevos, leche, maíz$\}$ y $B = \{$vacas, cabras, gallinas$\}$. Escribir la relación $\mathscr{R}$ de A a B definida por:

$$(a, b) \in \mathscr{R} \Longleftrightarrow a \text{ es producido por } b$$

Solución

La relación sería:

$$\mathscr{R} = \{\text{(huevos,gallinas),(leche,vacas),(leche,cabras)}\}$$

■

5.1.2 Igualdad de Relaciones

Sean $\mathscr{R}_1$ una relación sobre $A_1 \times A_2 \times \cdots \times A_n$ y $\mathscr{R}_2$ una relación sobre $B_1 \times B_2 \times \cdots \times B_m$. Entonces $\mathscr{R}_1 = \mathscr{R}_2$ si, y sólo si $n = m$ y $A_i = B_i$, $\forall i = 1, 2, \ldots, n$ y $\mathscr{R}_1$ y $\mathscr{R}_2$ son conjuntos de n-tuplas ordenadas iguales.

5.1.3 Dominio e Imagen

Llamaremos dominio de una relación $\mathscr{R}$ al conjunto formado por todos los primeros elementos de los pares ordenados que pertenecen a $\mathscr{R}$, e imagen o rango al conjunto formado por los segundos elementos. Es decir, si $\mathscr{R}$ es una relación de A a B, entonces

$$\begin{aligned} Dom(\mathscr{R}) &= \{a \in A, \exists b : b \in B \ \wedge \ (a,b) \in \mathscr{R}\} \\ Img(\mathscr{R}) &= \{b \in B, \exists a : a \in A \ \wedge \ (a,b) \in \mathscr{R}\} \end{aligned}$$

Así en el ejemplo anterior,

$$\begin{aligned} \mathrm{Dom}(\mathscr{R}) &= \{1,3\} \\ \text{e} & \\ \mathrm{Img}(\mathscr{R}) &= \{2,3\} \end{aligned}$$

■

Ejemplo 5.3

Para $\mathscr{U} = \mathbb{Z}^+$, $A = \{2,3,4,5,6,7\}$, $B = \{10,11,12,13,14\}$, escribir los elementos de la relación $\mathscr{R} \subset A \times B$, donde

$$a \mathscr{R} b \text{ si y sólo si } a \text{ divide a } b.$$

Solución

$$\mathscr{R} = \{(2,10),(2,12),(2,14),(3,12),(4,12),(5,10),(6,12),(7,14)\}$$

■

5.2 Relaciones Binarias

La clase más importante de relaciones es la de las relaciones binarias. Debido a que este tipo de relaciones son las más frecuentes, el término "*relación*" denota generalmente una relación binaria; adoptaremos este criterio cuando no haya confusión y especificaremos las que no sean binarias con términos tales como "ternaria" o "n-aria".

Si $(a,b) \in \mathscr{R}$ diremos que a está relacionado con b y lo notaremos por $a \mathscr{R} b$.

Si $(a,b) \notin \mathscr{R}$, escribiremos $a \not\mathscr{R} b$ y diremos que a no está relacionado con b.

Ejemplo 5.4

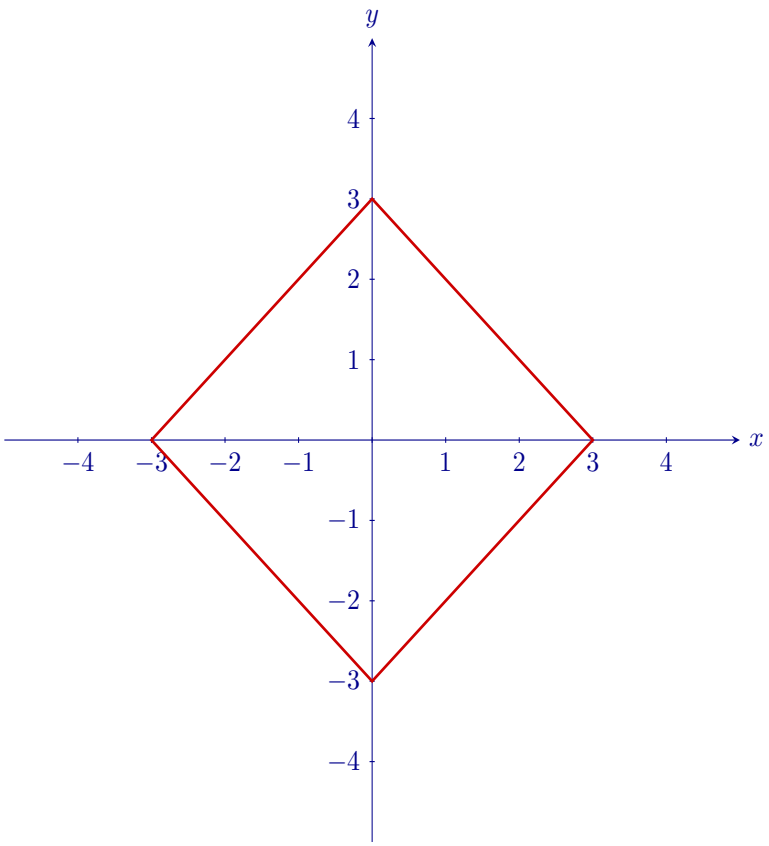
(a) *Sea $\mathscr{R}$ la relación "menor que" definida en el conjunto $\mathbb{Z}$ de los números enteros.*
Escribiremos $3 < 5$ para indicar que $(3,5) \in \mathscr{R}$ y $5 \not< 3$ para indicar que $(3,5) \notin \mathscr{R}$

(b) *Sea $\mathscr{R}$ la relación "es un múltiplo de" en el conjunto de los enteros positivos.*
Entonces,

$4\mathscr{R}2$ *pero* $2\not\mathscr{R}4$, *es decir 4 es múltiplo de 2, pero 2 no es múltiplo de 4.*
En general, $a\mathscr{R}b$ *si, y sólo si* $a = kb$ *para algún* $k \in \mathbb{Z}^+$, *así para todo* x, $x\mathscr{R}1$.
Un número x es impar si $x\not\mathscr{R}2$.

(c) *Como dijimos anteriormente, una relación binaria sobre el conjunto de los números reales puede representarse gráficamente en el plano cartesiano. La figura siguiente es la gráfica de la relación*

$$\mathscr{R} = \{(x,y) \in \mathbb{R} \times \mathbb{R} : |x| + |y| = 3\}$$



■

Ejemplo 5.5

Sea $A = \{1,2,3\}$ y $\mathscr{R} = \{(1,2),(1,3),(3,2)\}$. $\mathscr{R}$ es una relación en A ya que es un subconjunto de $A \times A$. Con respecto a esta relación, tendremos que

$$1\mathscr{R}2,\ 1\mathscr{R}3,\ 3\mathscr{R}2,\ \textit{pero}\ 1\not\mathscr{R}1,\ 2\not\mathscr{R}1,\ 2\not\mathscr{R}2,\ 2\not\mathscr{R}3,\ 3\not\mathscr{R}1,\ 3\not\mathscr{R}3$$

■

5.3 Matriz de una Relación

En este apartado veremos una de las formas de representar una relación entre dos conjuntos finitos, como es su matriz booleana o matriz de ceros y unos.

5.3.1 Definición

Dados dos conjuntos finitos, no vacíos,

$$A = \{a_1, a_2, \ldots, a_m\} \text{ y } B = \{b_1, b_2, \ldots, b_n\}$$

y una relación $\mathscr{R}$ cualquiera de A a B, llamaremos matriz de $\mathscr{R}$ a la matriz booleana siguiente:

$$M_{\mathscr{R}} = \left(r_{ij}\right) : r_{ij} = \begin{cases} 1, & si\ (a_i, b_j) \in \mathscr{R} \\ 0, & si\ (a_i, b_j) \notin \mathscr{R} \end{cases}$$

donde $i = 1, 2, \ldots\ldots, m;\ j = 1, 2, \ldots\ldots, n$.

Directamente de la definición dada se deduce que la matriz de una relación binaria es cuadrada.

Ejemplo 5.6

Sea $A = \{1, 2, 3, 4\}$ y definimos la relación

$$a \mathscr{R} b \Longleftrightarrow b \text{ es múltiplo de } a,\ \forall a, b \in A$$

Calcularemos la matriz de la relación $\mathscr{R}$.

Solución

La relación vendrá dada por el conjunto

$$\mathscr{R} = \{(1,1), (1,2), (1,3), (1,4), (2,2), (2,4), (3,3), (4,4)\}$$

y la matriz será, por tanto,

$$M_{\mathscr{R}} = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

■

Nota 5.1

- Obsérvese que la matriz de una relación caracteriza a la misma, o sea, si se conoce la relación se conoce la matriz y si se conoce la matriz sabremos de que relación trata.
- Obsérvese también lo siguiente: si $M_{\mathscr{R}}$ es la matriz de una relación $\mathscr{R}$ de A a B, cada fila se corresponde con un elemento de A y cada columna con un elemento de B. Para calcular el dominio de $\mathscr{R}$ bastará ver en que filas hay, al menos, un uno y para calcular la imagen bastará con ver en que columnas hay, al menos, un uno.

En el ejemplo anterior,

$$\text{Dom}\,(\mathscr{R}) = \{1, 2, 3, 4\} \text{ e } \text{Img}\,(\mathscr{R}) = \{1, 2, 3, 4\}$$

Existe otra forma de representar una relación cuando es de un conjunto en si mismo, es decir, cuando la relación es binaria.

5.4 Grafo Dirigido de una Relación

Los grafos nos ofrecen una forma bastante conveniente de visualizar cuestiones relativas a una relación binaria. Por esta razón desarrollaremos algunos conceptos de grafos dirigidos paralelamente a nuestro tratamiento de las relaciones binarias.

5.4.1 Definición

Un grafo dirigido o digrafo es un par ordenado $D = (A, \mathscr{R})$ donde A es un conjunto finito y $\mathscr{R}$ es una relación binaria definida sobre A. Al conjunto A lo llamaremos conjunto de nodos o vértices de D. A los elementos de $\mathscr{R}$ los llamaremos arcos o aristas del digrafo D.

- Un grafo dirigido caracteriza a una relación, es decir, conociendo la relación se conoce el digrafo y conociendo el digrafo, puede establecerse la relación.
- Si $G_{\mathscr{R}}$ es el grafo dirigido de una relación en un conjunto finito A, entonces el dominio y la imagen de $\mathscr{R}$ están formados por los puntos que son, respectivamente, extremo inicial y final de algún arco.

■

5.4.2 Representación Gráfica de un Grafo Dirigido

Tomaremos los elementos de A como puntos del plano y cuando dos elementos x e y de A estén relacionados, es decir, $x\mathscr{R}y$, trazaremos un arco dirigido desde x hasta y.

A x lo llamaremos vértice inicial y al y, vértice final de la arista (x, y).

A una arista que una un punto consigo mismo, la llamaremos bucle.

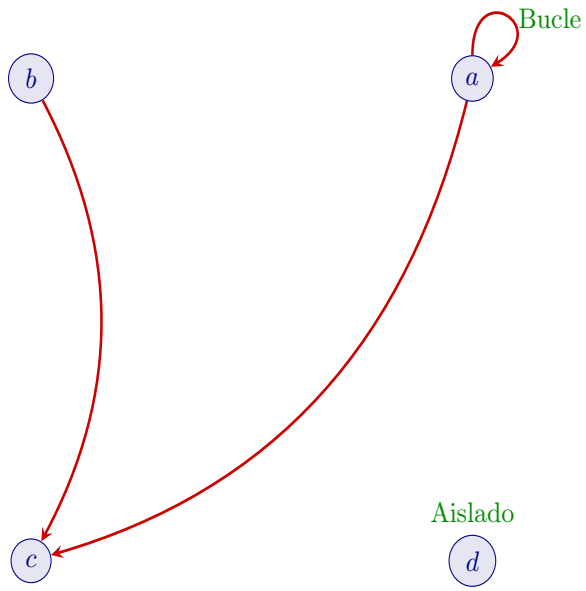
A un vértice que no sea inicial ni final de ninguna arista, lo llamaremos aislado.

Grado de entrada de un vértice es el número de aristas que llegan hasta él. Representaremos por $gr_e(a)$ al del vértice a.

Grado de salida de un vértice es el número de aristas que salen de él. Representaremos por $gr_s(a)$ al del vértice a.

Ejemplo 5.7

En la figura siguiente mostramos una representación gráfica del digrafo $D = (A, \mathscr{R})$, siendo A el conjunto $\{a, b, c, d\}$ y $\mathscr{R} = \{(a, a), (a, c), (b, c)\}$.



Las aristas son $(a,a),(a,c)$ y (b,c).

d es un vértice aislado.

Los grados de entrada son:

$$\mathrm{gr}_e\,(a)=1,\ \mathrm{gr}_e\,(b)=0,\ \mathrm{gr}_e\,(c)=2,\ \mathrm{gr}_e\,(d)=0$$

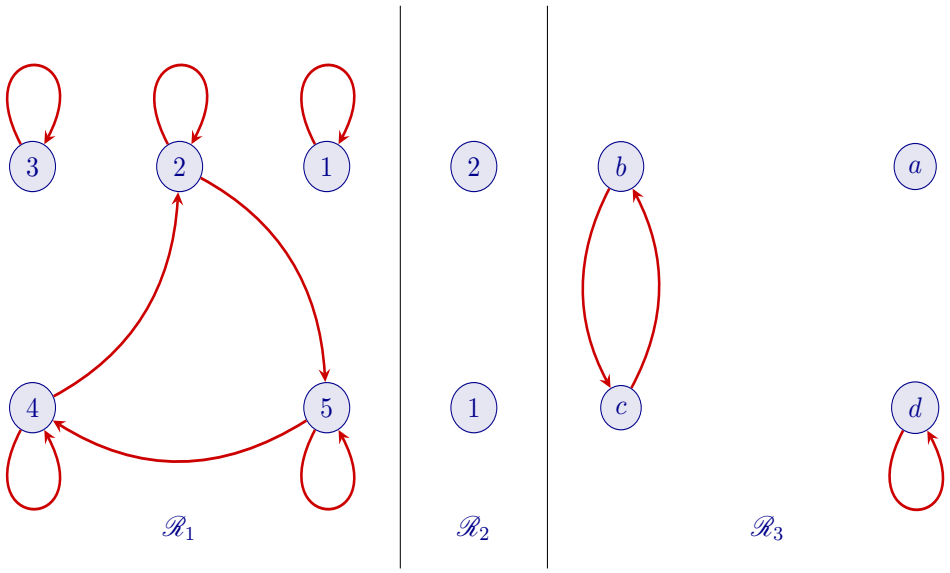
y los de salida,

$$\mathrm{gr}_s\,(a)=2,\ \mathrm{gr}_s\,(b)=1,\ \mathrm{gr}_s\,(c)=0,\ \mathrm{gr}_s\,(d)=0$$

■

Ejemplo 5.8

Escribir como conjuntos de pares ordenados las relaciones cuyos grafos dirigidos son los de la figura siguiente:



Solución

$$\mathscr{R}_1 = \{(1,1),(2,2),(2,5),(3,3),(4,2),(4,4),(5,4),(5,5)\}$$
$$\mathscr{R}_2 = \emptyset$$
$$\mathscr{R}_3 = \{(b,c),(c,b),(d,d)\}$$

■

Ejemplo 5.9

Representar gráficamente el digrafo $D = (\mathbb{Z}^+, \mathscr{R})$, donde $\mathscr{R}$ es la relación definida sobre el conjunto de los números enteros positivos consistente en todos los pares de números de la forma $(a, a+2)$.

Solución

$$\mathscr{R} = \left\{(a, a+2) : a \in \mathbb{Z}^+\right\}$$

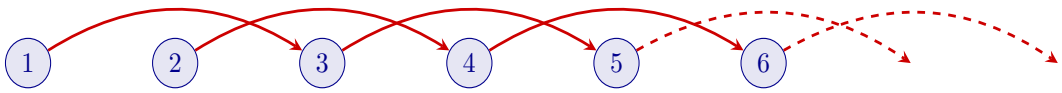
Observemos que la relación puede escribirse también, en la forma,

$$a\mathscr{R}b \Longleftrightarrow b = a+2$$

es decir,

$$\mathscr{R} = \{(1,3),(2,4),(3,5),(4,6),\ldots\ldots\}$$

La representación gráfica de su grafo dirigido sería:



Como $\mathbb{Z}^+$ es un conjunto infinito, en la figura hemos hecho un diagrama que es, necesariamente, incompleto.

■

5.5 Propiedades de las Relaciones

Las relaciones binarias, es decir definidas sobre un único conjunto A, pueden tener ciertas propiedades que expondremos en este apartado.

5.5.1 Reflexividad

Una relación binaria $\mathscr{R}$ definida sobre un conjunto A se dice que es reflexiva, cuando todos y cada uno de los elementos de A están relacionados consigo mismo, es decir,

$$\mathscr{R} \text{ es reflexiva} \Longleftrightarrow \forall x, (x \in A \longrightarrow x\mathscr{R}x)$$

Ejemplo 5.10

Obtener una condición necesaria y suficiente para que una relación binaria no sea reflexiva.

Solución

Según hemos visto en la definición anterior,

$$\mathscr{R} \text{ es reflexiva} \Longleftrightarrow \forall x, (x \in A \longrightarrow x \mathscr{R} x)$$

luego negando ambos miembros

$$\mathscr{R} \text{ no es reflexiva} \Longleftrightarrow \neg \forall x, (x \in A \longrightarrow x \mathscr{R} x)$$

y la proposición $\neg \forall x, (x \in A \longrightarrow x \mathscr{R} x)$ es verdadera si $\forall x, (x \in A \longrightarrow x \mathscr{R} x)$ es falsa, luego por el valor de verdad del cuantificador universal tiene que haber, al menos, un valor de x en A que haga que la propiedad $x \in A \longrightarrow x \mathscr{R} x$ no se cumpla, o lo que es igual que verifique la propiedad $x \in A$ y no verifique $x \mathscr{R} x$, o sea $x \not\mathscr{R} x$. Por lo tanto,

$$\mathscr{R} \text{ no es reflexiva} \Longleftrightarrow \exists x : (x \in A \ \wedge \ x \not\mathscr{R} x)$$

Consecuentemente, una condición necesaria y suficiente para que una relación definida en un conjunto A no sea reflexiva es que podamos encontrar, al menos, un elemento en A que no esté relacionado consigo mismo.

■

Ejemplo 5.11

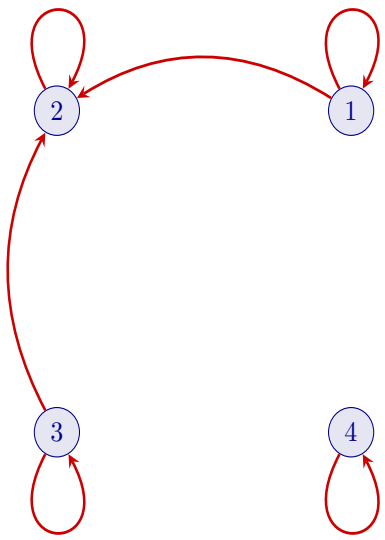
Sea $A = \{1, 2, 3, 4\}$ *y* $\mathscr{R} = \{(1, 1), (1, 2), (2, 2), (3, 3), (3, 2), (4, 4)\}$ *una relación definida en* A.

¿Es reflexiva? Dibujar el digrafo y escribir la matriz de la relación

Solución

La relación es, en efecto, reflexiva ya que $1 \mathscr{R} 1$, $2 \mathscr{R} 2$, $3 \mathscr{R} 3$ y $4 \mathscr{R} 4$, o sea, todos y cada uno de los elementos del conjunto A sobre el que está definida la relación están relacionados consigo mismo.

Una representación gráfica del grafo dirigido de la relación sería:



y la matriz booleana es:

$$M_{\mathscr{R}} = \begin{pmatrix} 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

■

Nota 5.2 Obsérvese lo siguiente:

- El digrafo de una relación reflexiva se caracteriza por tener un bucle en cada uno de los vértices.
- La matriz de una relación reflexiva se caracteriza por tener todos los elementos de su diagonal principal iguales a 1 por lo tanto, si hay, al menos, un elemento en la diagonal principal que sea 0, entonces la relación no será reflexiva, es decir, si $M_{\mathscr{R}} = (r_{ij})$,

$$\mathscr{R} \text{ es reflexiva} \iff r_{ii} = 1, \forall i$$

y

$$\mathscr{R} \text{ no es reflexiva} \iff \exists i : r_{ii} = 0$$

Ejemplo 5.12

Estudiar la reflexividad de la relación "menor o igual que" definida en el conjunto de los números enteros.

Solución

Sean a y b dos enteros cualesquiera y sea $\mathscr{R}$ la relación propuesta. Entonces,

$$\mathscr{R} = \{(a, b) \in \mathbb{Z} \times \mathbb{Z} : a \leqslant b\}$$

o lo que es igual,

$$a\mathscr{R}b \iff a \leqslant b$$

Veamos que significa exactamente $a \leqslant b$. En efecto,

$$\begin{aligned} a \leqslant b &\iff b - a \geqslant 0 \\ &\iff b - a \in \mathbb{Z}_0^+ \\ &\iff \exists k \in \mathbb{Z}_0^+ : b - a = k \\ &\iff b = a + k, \text{ siendo } k \in \mathbb{Z}_0^+. \end{aligned}$$

Podremos decir por tanto,

$$a\mathscr{R}b \iff b = a + k, \text{ siendo } k \in \mathbb{Z}_0^+.$$

Estudiemos, ahora, la reflexividad. Tenemos que comprobar que todos y cada uno de los números enteros está relacionado consigo mismo. Pues bien, sea a un entero cualquiera. Entonces, obviamente,

$$a = a$$

o lo que es igual,

$$a = a + 0, \text{ siendo } 0 \in \mathbb{Z}_0^+.$$

Consecuentemente, y según acabamos de ver,

$$a\mathscr{R}a$$

y la relación "menor o igual" definida en el conjunto de los números enteros es reflexiva.

■

Ejemplo 5.13

Estudiar la reflexividad de la relación de "divisibilidad" definida en el conjunto de los números enteros positivos.

Solución

Sean a y b dos enteros positivos cualesquiera y sea $\mathscr{R}$ la relación propuesta. Entonces,

$$a\mathscr{R}b \Longleftrightarrow b \text{ es divisible por } a.$$

Analicemos el significado exacto de b "es divisible por" a. En efecto,

$$\begin{aligned} b \text{ es divisible por } a &\iff \frac{b}{a} \in \mathbb{Z}^+ \\ &\iff \exists k \in \mathbb{Z}^+ : \frac{b}{a} = k \\ &\iff b = a \cdot k, \text{ siendo } k \in \mathbb{Z}^+. \end{aligned}$$

La definición de $\mathscr{R}$ será, por tanto,

$$a\mathscr{R}b \Longleftrightarrow b = a \cdot k, \text{ siendo } k \in \mathbb{Z}^+$$

Veamos, ahora, si es reflexiva. Como siempre, habrá que comprobar que todos y cada uno de los enteros positivos está relacionado consigo mismo. Sea, pues, a un entero positivo cualquiera. Obviamente,

$$a = a$$

o lo que es igual,

$$a = a \cdot 1, \text{ siendo } 1 \in \mathbb{Z}^+.$$

Consecuentemente, y según la definición de $\mathscr{R}$,

$$a\mathscr{R}a$$

y la relación propuesta es reflexiva.

■

5.5.2 Simetría

Una relación binaria $\mathscr{R}$ sobre un conjunto A es simétrica si cada vez que x está relacionado con y se sigue que y está relacionado con x. Es decir,

$$\mathscr{R} \text{ es simétrica} \Longleftrightarrow \forall x, y \in A\,(x\mathscr{R}y \longrightarrow y\mathscr{R}x)$$

Ejemplo 5.14

Sea $A = \{1, 2, 3, 4\}$ *y* $\mathscr{R} = \{(1,1), (1,2), (2,1), (2,3), (3,2), (3,3)\}$ *una relación definida en* A.

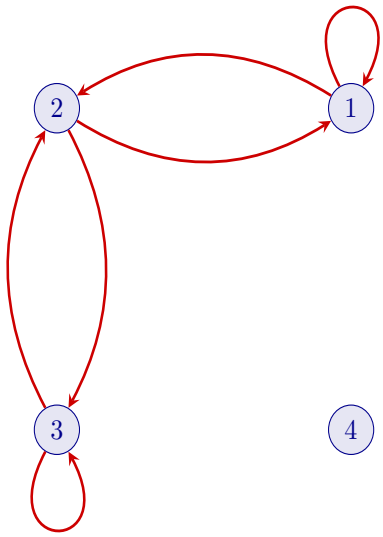
¿Es simétrica? Dibujar el digrafo y escribir la matriz de la relación.

Solución

$\mathscr{R}$ es simétrica ya que para cada par $(a, b) \in \mathscr{R}$, el par (b, a) también pertenece a $\mathscr{R}$. En efecto,

$$\begin{array}{lll} (1,1) \in \mathscr{R} & \text{y} & (1,1) \in \mathscr{R} \\ (1,2) \in \mathscr{R} & \text{y} & (2,1) \in \mathscr{R} \\ (2,3) \in \mathscr{R} & \text{y} & (3,2) \in \mathscr{R} \\ (3,3) \in \mathscr{R} & \text{y} & (3,3) \in \mathscr{R} \end{array}$$

Veamos una representación gráfica del grafo dirigido de la relación.



La matriz booleana de la relación es:

$$M_{\mathscr{R}} = \begin{pmatrix} 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}$$

■

Nota 5.3 Obsérvese lo siguiente:

– Si D es el digrafo de una relación simétrica, entonces entre cada dos vértices distintos de D existen dos aristas o no existe ninguna.

– La matriz de una relación simétrica, satisface la propiedad de que todo par de elementos colocados simétricamente respecto de la diagonal principal son iguales. Luego si $M_{\mathscr{R}} = (r_{ij})$ es la matriz de $\mathscr{R}$, entonces

$$\mathscr{R} \text{ es simétrica} \Longleftrightarrow r_{ij} = r_{ji}, \forall i, j$$

y

$$\mathscr{R} \text{ es no simétrica} \Longleftrightarrow \exists i, j : r_{ij} \neq r_{ji}$$

■

5.5.3 Antisimetría

Una relación binaria $\mathscr{R}$ sobre un conjunto A se dice antisimétrica si de $(x, y) \in \mathscr{R}$ e $(y, x) \in \mathscr{R}$, se sigue que $a = b$. Es decir,

$$\mathscr{R} \textit{ es antisimétrica} \Longleftrightarrow \forall x, y, (x \mathscr{R} y \ \wedge \ y \mathscr{R} x \longrightarrow x = y)$$

Nota 5.4 Obsérvese que en virtud de la equivalencia lógica entre una proposición condicional y su contrarrecíproca, otra forma de expresar esta definición es

$$\mathscr{R} \text{ es antisimétrica} \iff \forall x, y, (x \neq y \longrightarrow x \not\mathscr{R} y \ \vee \ y \not\mathscr{R} x)$$

o lo que es igual,

$$\mathscr{R} \text{ antisimétrica} \Longleftrightarrow \forall x, y, [x \neq y \longrightarrow (x \not\mathscr{R} y \wedge y \mathscr{R} x) \vee (x \mathscr{R} y \wedge y \not\mathscr{R} x) \vee (x \not\mathscr{R} y \wedge y \not\mathscr{R} x)]$$

es decir, elegidos dos elementos cualesquiera en A, si son distintos, entonces no pueden estar relacionados, al mismo tiempo, entre sí.

■

Nota 5.5 La equivalencia

$$\mathscr{R} \text{ es antisimétrica} \Longleftrightarrow \forall x, y (x \mathscr{R} y \ \wedge \ y \mathscr{R} x \longrightarrow x = y)$$

la podemos escribir en la forma

$$\mathscr{R} \text{ es antisimétrica} \Longleftrightarrow \forall x, y \, [\neg \, (x \mathscr{R} y \ \wedge \ y \mathscr{R} x) \ \vee \ (x = y)]$$

de donde, negando ambos miembros, resulta

$$\mathscr{R} \text{ es no antisimétrica} \Longleftrightarrow \exists x, y : (x \mathscr{R} y \ \wedge \ y \mathscr{R} x \ \wedge \ x \neq y) \, .$$

O sea, si podemos encontrar dos elementos x y y en A tales que x esté relacionado con y e y relacionado con x, siendo ambos distintos, entonces la relación es *no antisimétrica.*

■

Ejemplo 5.15

Sea $A = \{1, 2, 3, 4\}$ *y sea* $\mathscr{R} = \{(1, 2), (2, 2), (3, 4), (4, 1)\}$ *una relación definida en* A. *¿Es antisimétrica? Dibujar el digrafo y escribir la matriz de* $\mathscr{R}$.

Solución

Observemos lo siguiente:

$1 \neq 2$ y $(1, 2) \in \mathscr{R}$, pero $(2, 1) \notin \mathscr{R}$, es decir $1 \mathscr{R} 2 \ \wedge \ 2 \not\mathscr{R} 1$.

$1 \neq 3$ y $(1, 3) \notin \mathscr{R}$ y $(3, 1) \notin \mathscr{R}$, es decir $1 \not\mathscr{R} 3 \ \wedge 3 \not\mathscr{R} 1$.

$1 \neq 4$ y $(4, 1) \in \mathscr{R}$, pero $(1, 4) \notin \mathscr{R}$, es decir $4 \mathscr{R} 1 \ \wedge \ 1 \not\mathscr{R} 4$.

$2 \neq 3$ y $(2, 3) \notin \mathscr{R}$, $(3, 2) \notin \mathscr{R}$, es decir $2 \not\mathscr{R} 3 \ \wedge 3 \not\mathscr{R} 2$.

$2 \neq 4$ y $(2, 4) \notin \mathscr{R}$, $(4, 2) \notin \mathscr{R}$, es decir $2 \not\mathscr{R} 4 \ \wedge 4 \not\mathscr{R} 2$.

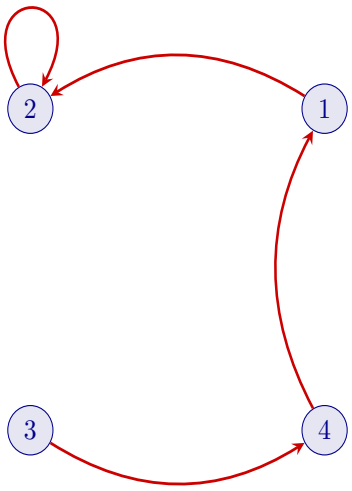
$3 \neq 4$ y $(3, 4) \in \mathscr{R}$, pero $(4, 3) \notin \mathscr{R}$, es decir $3 \mathscr{R} 4 \ \wedge \ 4 \not\mathscr{R} 3$.

luego,

$$\text{si } a \neq b, \text{ entonces } (a, b) \notin \mathscr{R} \text{ ó } (b, a) \notin \mathscr{R}$$

de aquí que $\mathscr{R}$ sea antisimétrica.

Veamos una representación gráfica del grafo dirigido de la relación.



La matriz booleana de la relación es:

$$M_{\mathscr{R}} = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \end{pmatrix}$$

■

Nota 5.6 Obsérvese lo siguiente:

- Si D es el digrafo de una relación antisimétrica, entonces entre cada dos vértices distintos de A, existe un arco o no existe ninguno.
- La matriz $M_{\mathscr{R}} = (r_{ij})$ de una relación antisimétrica, satisface la propiedad de que si $i \neq j$, entonces $r_{ij} = 0$ ó $r_{ji} = 0$. Es decir,

$$\mathscr{R} \text{ es antisimétrica} \Longleftrightarrow \forall i \neq j, r_{ij} = 0 \ \vee r_{ji} = 0$$

y

$$\mathscr{R} \text{ es no antisimétrica} \Longleftrightarrow \exists i, j : r_{ij} = 1 \ \wedge \ r_{ji} = 1 \ \wedge \ i \neq j$$

■

Ejemplo 5.16

Estudiar la antisimetría de la relación "menor o igual que" definida en el conjunto de los números enteros.

Solución

Sean a y b dos enteros cualesquiera y sea $\mathscr{R}$ la relación propuesta. Según hemos visto en 5.12 , la relación puede definirse en la forma:

$$a\mathscr{R}b \Longleftrightarrow b - a = k, \text{ siendo } k \in \mathbb{Z}_0^+$$

Pues bien, supongamos que $a\mathscr{R}b$ y $b\mathscr{R}a$, entonces

$$\left.\begin{array}{lll} a\mathscr{R}b & \Longleftrightarrow & b - a = k_1, \text{ siendo } k_1 \in \mathbb{Z}_0^+ \\ \text{y} & & \\ b\mathscr{R}a & \Longleftrightarrow & a - b = k_2, \text{ siendo } k_2 \in \mathbb{Z}_0^+ \end{array}\right\} \Longrightarrow k_1 + k_2 = 0, \text{ siendo } k_1, k_2 \in \mathbb{Z}_0^+$$

luego,

$$k_1 = 0 \text{ y } k_2 = 0$$

de aquí que

$$b - a = 0 \text{ y } a - b = 0$$

es decir,

$$a = b$$

y, consecuentemente, la relación "menor o igual" definida en el conjunto de los números enteros es antisimétrica.

Probemos lo mismo, es decir la antisimetría de la relación, de otra forma. En efecto, sean a y b dos números enteros cualesquiera, entonces

$$a\mathscr{R}b \Longleftrightarrow b - a \in \mathbb{Z}_0^+$$

y si $a \neq b$,

$$a\mathscr{R}b \Longleftrightarrow b - a \in \mathbb{Z}^+$$

y si negamos ambos miembros,

$$a\not\mathscr{R}\, b \iff b - a \notin \mathbb{Z}^+ \iff b - a \in \mathbb{Z}^-$$

Pues bien,

$$\begin{aligned} a \neq b &\iff b - a \neq 0 \\ &\iff b - a \in \mathbb{Z} \setminus \{0\} \\ &\iff b - a \in \mathbb{Z}^+ \cup \mathbb{Z}^- \\ &\iff \begin{cases} b - a \in \mathbb{Z}^+ \quad \text{y} \quad a - b \in \mathbb{Z}^- \\ \text{ó} \\ b - a \in \mathbb{Z}^- \quad \text{y} \quad a - b \in \mathbb{Z}^+ \end{cases} \\ &\iff \begin{cases} a \mathscr{R} b \quad \text{y} \quad b \not\mathscr{R} a \\ \text{ó} \\ a \not\mathscr{R} b \quad \text{y} \quad b \mathscr{R} a \end{cases} \end{aligned}$$

Por lo tanto, la relación "menor o igual que" definida en el conjunto de los enteros es antisimétrica.

■

Ejemplo 5.17

Estudiar la antisimetría de la relación de divisibilidad definida en el conjunto de los números enteros positivos.

Solución

Según vimos en el ejemplo 5.13 la relación de divisibilidad en el conjunto de los enteros positivos se definía de la siguiente forma:

$$a \mathscr{R} b \iff b = a \cdot k, \text{ siendo } k \in \mathbb{Z}^+, \ \forall a, b \in \mathbb{Z}^+$$

Pues bien, sean a y b dos enteros positivos cualesquiera y supongamos que $a \mathscr{R} b$ y $b \mathscr{R} a$. Entonces,

$$\left.\begin{array}{lll} a \mathscr{R} b & \iff & b = a \cdot k_1, \text{ siendo } k_1 \in \mathbb{Z}^+ \\ y & & \\ b \mathscr{R} a & \iff & a = b \cdot k_2, \text{ siendo } k_2 \in \mathbb{Z}^+ \end{array}\right\} \Longrightarrow b = b \cdot k_1 \cdot k_2 \Longrightarrow k_1 k_2 = 1 \Longrightarrow k_1 = k_2 = 1$$

luego,

$$a = b$$

y, consecuentemente, la relación propuesta es antisimétrica.

■

5.5.4 Transitividad

Se dice que una relación $\mathscr{R}$ definida en un conjunto A es transitiva si de $(a, b) \in \mathscr{R}$ y $(b, c) \in \mathscr{R}$, se deduce $(a, c) \in \mathscr{R}$. Es decir,

$$\mathscr{R} \text{ es transitiva} \iff \forall x, y, z \, (x \mathscr{R} y \ \wedge \ y \mathscr{R} z \longrightarrow x \mathscr{R} z)$$

Nota 5.7 Negando los dos miembros de la equivalencia anterior, tendremos

$$\mathscr{R} \text{ es no transitiva} \Longleftrightarrow \exists x, y, z : x\mathscr{R}y \ \wedge \ y\mathscr{R}z \ \wedge \ x\not\mathscr{R}z$$

es decir, la relación $\mathscr{R}$ no es transitiva, si podemos encontrar elementos x, y, z en A tales que $x\mathscr{R}y$ y $y\mathscr{R}z$, pero $x\not\mathscr{R}z$.

■

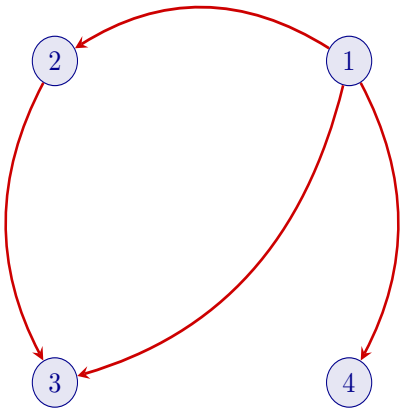
Ejemplo 5.18

Sea $A = \{1, 2, 3, 4\}$ *y* $\mathscr{R} = \{(1, 2), (1, 3), (1, 4), (2, 3)\}$ *una relación definida sobre* A. *¿Es transitiva? Dibujar el digrafo y escribir la matriz de la relación.*

Solución

En efecto, $\mathscr{R}$ es transitiva porque $(1, 2) \in \mathscr{R}$ y $(2, 3) \in \mathscr{R}$ y, también está en $\mathscr{R}$, el par $(1, 3)$.

Veamos una representación gráfica del grafo dirigido de la relación.



La matriz booleana de la relación es:

$$M_{\mathscr{R}} \ = \ \begin{pmatrix} 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}$$

■

Nota 5.8 Obsérvese lo siguiente:

- Si D es el digrafo de una relación transitiva y existen arcos desde a hasta b y desde b hasta c, entonces existirá un arco desde a hasta c.
- Es posible caracterizar la relación transitiva por su matriz booleana $M_{\mathscr{R}} = (r_{ij})$,

$$\mathscr{R} \text{ es transitiva} \ \Longleftrightarrow (r_{ij} = 1 \ \wedge \ r_{jk} = 1 \Longrightarrow r_{ik} = 1)$$

y

$$\mathscr{R} \text{ es no transitiva} \ \Longleftrightarrow r_{ij} = 1 \ \wedge \ r_{jk} = 1 \ \wedge r_{ik} = 0$$

■

Ejemplo 5.19

Estudiar la transitividad de la relación "menor o igual que" definida en el conjunto de los números enteros.

Solución

Sean a, b y c tres enteros cualesquiera y sea $\mathscr{R}$ la relación propuesta. Según hemos visto en 5.12 , la relación puede definirse en la forma:

$$a\mathscr{R}b \Longleftrightarrow b-a=k, \text{ siendo } k\in\mathbb{Z}_0^+$$

Pues bien, supongamos que $a\mathscr{R}b$ y $b\mathscr{R}c$, entonces

$$\left.\begin{array}{lll} a\mathscr{R}b & \Longleftrightarrow & b-a=k_1, \text{ siendo } k_1\in\mathbb{Z}_0^+ \\ \text{y} & & \\ b\mathscr{R}c & \Longleftrightarrow & c-b=k_2, \text{ siendo } k_2\in\mathbb{Z}_0^+ \end{array}\right\} \Longrightarrow c-a=k_1+k_2, \text{ siendo } k_1+k_2\in\mathbb{Z}_0^+$$

luego,

$$a\mathscr{R}c$$

y, consecuentemente, la relación "menor o igual" definida en el conjunto de los números enteros es transitiva.

■

Ejemplo 5.20

Estudiar la transitividad de la relación de divisibilidad definida en el conjunto de los números enteros positivos.

Solución

Según vimos en el ejemplo 5.13 la relación de divisibilidad en el conjunto de los enteros positivos se definía de la siguiente forma:

$$a\mathscr{R}b \Longleftrightarrow b=a\cdot k, \text{ siendo } k\in\mathbb{Z}^+, \ \forall a,b\in\mathbb{Z}^+$$

Pues bien, sean a, b y c tres enteros positivos cualesquiera y supongamos que $a\mathscr{R}b$ y $b\mathscr{R}c$. Entonces,

$$\left.\begin{array}{lll} a\mathscr{R}b & \Longleftrightarrow & b=a\cdot k_1, \text{ siendo } k_1\in\mathbb{Z}^+ \\ y & & \\ b\mathscr{R}c & \Longleftrightarrow & c=b\cdot k_2, \text{ siendo } k_2\in\mathbb{Z}^+ \end{array}\right\} \Longrightarrow c=a\cdot k_1k_2, \text{ siendo } k_1k_2\in\mathbb{Z}^+ \Longrightarrow a\mathscr{R}c$$

luego,

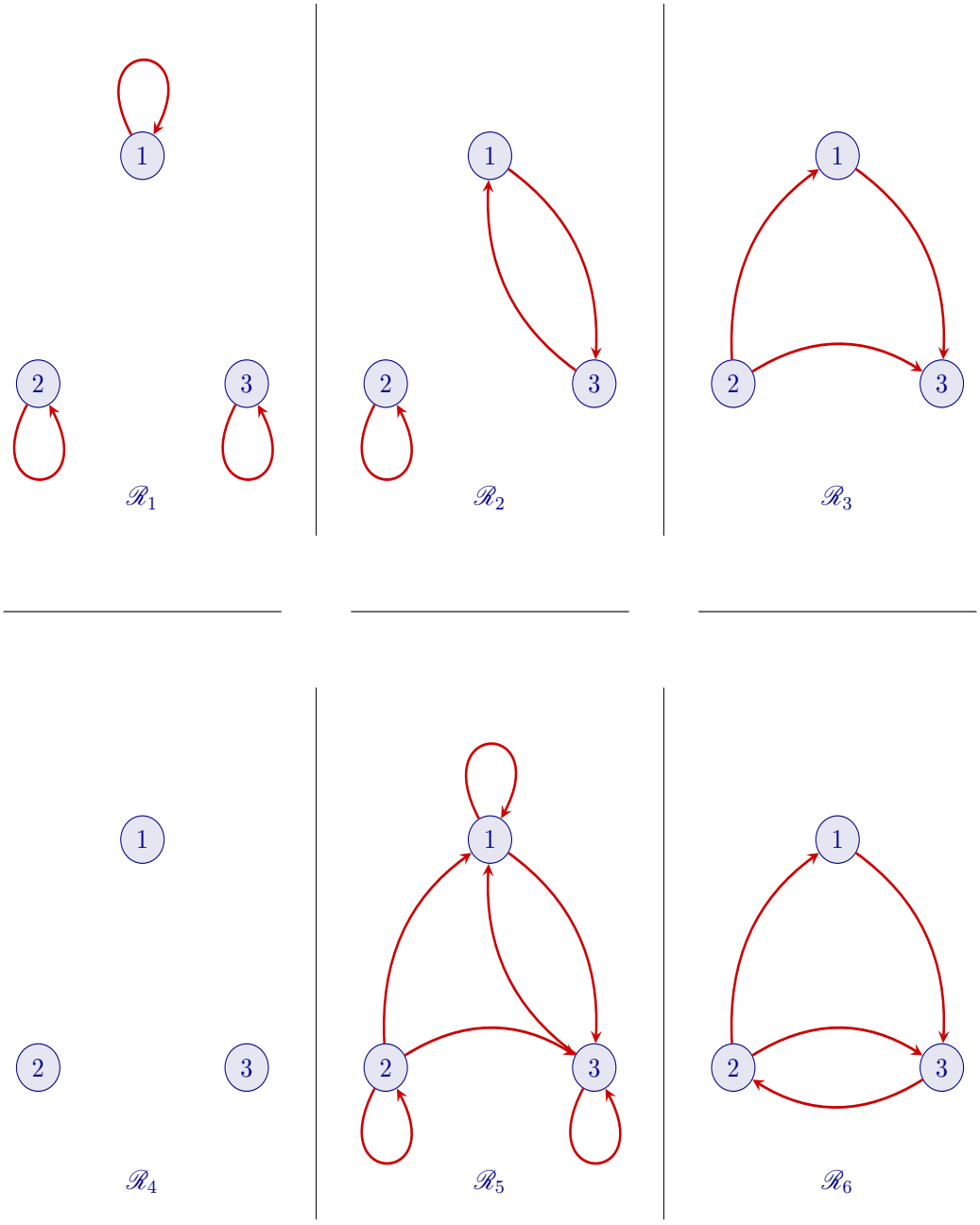
$$a\mathscr{R}c$$

y, consecuentemente, la relación de divisibilidad es transitiva.

■

Ejemplo 5.21

Estudiar las propiedades de las relaciones definidas en el conjunto $A = \{1, 2, 3\}$ *cuyos grafos dirigidos son los de la figura siguiente.*



Solución

$\mathscr{R}_1$. Es la relación de igualdad sobre A.

- Reflexividad. Es reflexiva ya que todos y cada uno de los elementos de A está relacionado consigo mismo.
- Simetría. En efecto lo es, ya que cada vez que a está relacionado con b, ($1\mathscr{R}_1 1$, $2\mathscr{R}_1 2$ y $3\mathscr{R}_1 3$), se verifica que b está relacionado con a ($1\mathscr{R}_1 1$, $2\mathscr{R}_1 2$ y $3\mathscr{R}_1 3$).

- Antisimetría. La relación $\mathscr{R}_1$ es antisimétrica ya que,

  $1 \neq 2$ y $1 \not\mathscr{R}_1 2$ y $2 \not\mathscr{R}_1 1$.
  $1 \neq 3$ y $1 \not\mathscr{R}_1 3$ y $3 \not\mathscr{R}_1 1$.
  $2 \neq 3$ y $2 \not\mathscr{R}_1 3$ y $3 \not\mathscr{R}_1 2$.

- Transitividad. También lo es ya que cada vez que a está relacionado con b y b lo está con c, se verifica que a está relacionado con c, siendo a, b y c cualesquiera de A.

$\mathscr{R}_2$.

- Reflexividad. La relación no es reflexiva ya que hay, al menos, un elemento (el 1 y el 3) que no está relacionado consigo mismo.
- Simetría. En efecto lo es, ya que cada vez que a está relacionado con b, ($1\mathscr{R}_2 3$ y $2\mathscr{R}_2 2$, se verifica que b está relacionado con a ($3\mathscr{R}_2 1$ y $2\mathscr{R}_2 2$).
- Antisimetría. La relación no es antisimétrica ya que, $1\mathscr{R}_2 3$, $3\mathscr{R}_2 1$ y, sin embargo, $1 \neq 3$.
- Transitividad. No lo es, ya que, $1\mathscr{R}_2 3$, $3\mathscr{R}_2 1$ y, sin embargo, $1 \not\mathscr{R}_1 1$.

$\mathscr{R}_3$.

- Reflexividad. La relación no es reflexiva ya que ninguno de los elementos de A está relacionado consigo mismo.
- Simetría. No lo es, ya que, por ejemplo, $2\mathscr{R}_3 1$ y, sin embargo, $1 \not\mathscr{R}_3 2$.
- Antisimetría. En efecto lo es, ya que

  $2 \neq 1$ y $2\mathscr{R}_3 1$ y $1 \not\mathscr{R}_3 2$.
  $2 \neq 3$ y $2\mathscr{R}_3 3$ y $3 \not\mathscr{R}_3 2$.
  $1 \neq 3$ y $1\mathscr{R}_3 3$ y $3 \not\mathscr{R}_3 1$.

- Transitividad. $\mathscr{R}_3$ es transitiva ya que

$$\left.\begin{array}{l} 2\mathscr{R}_3 1 \\ \text{y} \\ 1\mathscr{R}_3 3 \end{array}\right\} \implies 2\mathscr{R}_3 3$$

$\mathscr{R}_4$. Es la relación vacía ya que no tiene ningún elemento.

- Reflexividad. No es reflexiva, ya que ningún elemento del conjunto A sobre el que está definida la relación está relacionado consigo mismo.
- Simetría. La relación propuesta es simétrica ya que si a y b son cualesquiera de A, se verifica que si $b \not\mathscr{R}_4 a$, entonces $a \not\mathscr{R}_3 b$.
- Antisimetría. La relación $\mathscr{R}_4$ es antisimétrica ya que,

  $1 \neq 2$ y $1 \not\mathscr{R}_4 2$ y $2 \not\mathscr{R}_4 1$.
  $1 \neq 3$ y $1 \not\mathscr{R}_4 3$ y $3 \not\mathscr{R}_4 1$.
  $2 \neq 3$ y $2 \not\mathscr{R}_4 3$ y $3 \not\mathscr{R}_4 2$.

- Transitividad. La relación es, en efecto, transitiva ya que si a, b y c son tres elementos cualesquiera de A, se verifica que

$$a \not\mathscr{R}_4 c \implies \left\{\begin{array}{l} a \not\mathscr{R}_4 b \\ \text{ó} \\ b \not\mathscr{R}_4 c \end{array}\right.$$

$\mathscr{R}_5$.

- Reflexividad. La relación propuesta es reflexiva ya que todos y cada uno de los elementos del conjunto A sobre el que está definida están relacionados consigo mismos.
- Simetría. Esta relación no es simétrica ya que, por ejemplo, 2 está relacionado con 3 y, sin embargo, 3 no lo está con 2.
- Antisimetría. La relación no es antisimétrica ya que, por ejemplo, 1 está relacionado con 3, 3 está relacionado con 1 y, sin embargo, 1 es distinto de 3.

⁕ Transitividad. La relación es transitiva ya que

$$\left.\begin{array}{l} 1\mathscr{R}_5 3 \\ \text{y} \\ 3\mathscr{R}_5 1 \end{array}\right\} \Longrightarrow 1\mathscr{R}_5 1 \qquad \left.\begin{array}{l} 1\mathscr{R}_5 1 \\ \text{y} \\ 1\mathscr{R}_5 3 \end{array}\right\} \Longrightarrow 1\mathscr{R}_5 3$$

$$\left.\begin{array}{l} 2\mathscr{R}_5 3 \\ \text{y} \\ 3\mathscr{R}_5 3 \end{array}\right\} \Longrightarrow 2\mathscr{R}_5 3 \qquad \left.\begin{array}{l} 2\mathscr{R}_5 1 \\ \text{y} \\ 1\mathscr{R}_5 1 \end{array}\right\} \Longrightarrow 2\mathscr{R}_5 1 \qquad \left.\begin{array}{l} 2\mathscr{R}_5 2 \\ \text{y} \\ 2\mathscr{R}_5 3 \end{array}\right\} \Longrightarrow 2\mathscr{R}_5 3$$

$$\left.\begin{array}{l} 3\mathscr{R}_5 1 \\ \text{y} \\ 1\mathscr{R}_5 3 \end{array}\right\} \Longrightarrow 3\mathscr{R}_5 3 \qquad \left.\begin{array}{l} 3\mathscr{R}_5 3 \\ \text{y} \\ 3\mathscr{R}_5 1 \end{array}\right\} \Longrightarrow 3\mathscr{R}_5 1$$

$\mathscr{R}_6$. ⁕ Reflexividad. La relación no es reflexiva ya que hay, al menos, un elemento en A (por ejemplo el 1) que no está relacionado consigo mismo.

⁕ Simetría. No hay simetría en esta relación ya que, por ejemplo, 1 está relacionado con 3 y, sin embargo, 3 no está relacionado con 1.

⁕ Antisimetría. La relación propuesta no es antisimétrica ya que, por ejemplo, 2 está relacionado con 3, 3 está relacionado con 2 y, sin embargo, 2 y 3 son distintos.

⁕ Transitividad. La relación no es transitiva ya que, por ejemplo, 1 está relacionado con 3, 3 lo está con 2 y, sin embargo, 1 no está relacionado con 2.

■

Ejemplo 5.22

Dibujar el grafo dirigido de las relaciones siguientes:

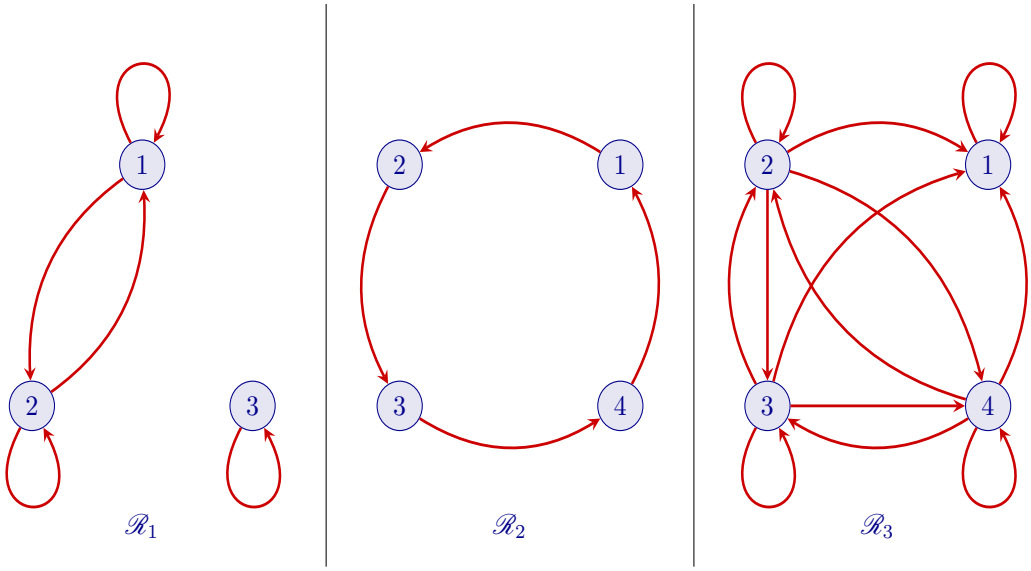
(a) La relación $\mathscr{R}_1 = \{(1,2),(2,1),(3,3),(1,1),(2,2)\}$ *definida en* $A = \{1,2,3\}$.

(b) La relación $\mathscr{R}_2 = \{(1,2),(2,3),(3,4),(4,1)\}$ *definida en* $A = \{1,2,3,4\}$.

(c) La relación $\mathscr{R}_3$ *definida sobre el conjunto* $A = \{1,2,3,4\}$ *por*

$$a\mathscr{R}_3 b \Longleftrightarrow a^2 \geqslant b,\ \forall a, b \in A$$

Solución



■

Ejemplo 5.23

Estudiar la relación en $\mathbb{Q}$ *dada por*

$$a\mathscr{R}b \text{ si y sólo si } |a-b|<1$$

Solución

Veamos que propiedades tiene la relación dada.

- ⊛ Reflexividad. Dado cualquier número racional a, se verifica que $|a-a|=0<1$, luego $a\mathscr{R}a$.
- ⊛ Simetría. Dados dos racionales cualesquiera a y b,

  $$a\mathscr{R}b \Longleftrightarrow |a-b|<1 \Longrightarrow |b-a|<1 \Longrightarrow b\mathscr{R}a$$

  luego la relación es simétrica.
- ⊛ Antisimetría. Observemos lo siguiente: sean a y b dos racionales cualesquiera cuya diferencia sea menor que 1, por ejemplo $a=1$ y $b=1/2$. Entonces,

  $$|a-b|=\left|1-\frac{1}{2}\right|=\frac{1}{2}<1 \quad \text{y} \quad |b-a|=\left|\frac{1}{2}-1\right|=\frac{1}{2}<1 \quad \text{y} \quad 1\neq\frac{1}{2}.$$

  Hemos encontrado, al menos, dos racionales a y b tales que

  $$a\mathscr{R}b \text{ y } b\mathscr{R}a \text{ y, sin embargo, } a\neq b$$

  luego la relación no es antisimétrica.
- ⊛ Transitividad. Sean a, b y c tres números racionales tales que $a\mathscr{R}b$ y $b\mathscr{R}c$. Entonces

  $$a\mathscr{R}b \Longleftrightarrow |a-b|<1$$

  y

  $$b\mathscr{R}c \Longleftrightarrow |b-c|<1$$

sin embargo,

$$|a-c| = |a-b+b-c| \leqslant |a-b| + |b-c| < 2$$

por tanto,

$$\exists a, b, c \in \mathbb{Q} : a \mathscr{R} b \ \wedge \ b \mathscr{R} c \ \wedge \ a \not\mathscr{R} c$$

por tanto, $\mathscr{R}$ no es transitiva.

■

Lección 6

Relaciones de Orden

Estudiamos en esta lección una de las relaciones binarias más importantes que pueden definirse en un conjunto, las relaciones de orden.

6.1 Generalidades

Definiremos el concepto principal de la lección y resolveremos algunos ejemplos.

6.1.1 Relación de Orden

Una relación binaria $\mathscr{R}$ sobre un conjunto A se dice que es de orden, si es reflexiva, antisimétrica y transitiva.

Nota 6.1 Los órdenes más comunes son las relaciones $\leqslant$ y $\geqslant$ en $\mathbb{Z}$ y en $\mathbb{R}$. Por esta razón cuando nos refiramos, en general, a una relación de orden, $\mathscr{R}$, definida sobre un conjunto A, usaremos los símbolos $\preccurlyeq$ y $\succcurlyeq$ en vez de $\mathscr{R}$. Estos son similares a los $\leqslant$ y $\geqslant$ que seguiremos utilizando cuando el conjunto sea $\mathbb{Z}$ o $\mathbb{R}$.

Si $\preccurlyeq$ es una relación de orden sobre un conjunto A, entonces

$a \preccurlyeq b$ se lee "a es anterior a b".

Si $a \preccurlyeq b$ y $a \neq b$, emplearemos $a \prec b$ y diremos que "a es estrictamente anterior a b".

$a \succcurlyeq b$ se lee "a es posterior a b"

$a \succ b$ se lee "a es estrictamente posterior a b".

■

Ejemplo 6.1

Probar que la relación "menor o igual" definida en el conjunto $\mathbb{Z}$ de los números enteros es de orden.

Solución

Según vimos en 5.12 , 5.16 y 5.19 , la relación "menor o igual" definida en el conjunto de los enteros es reflexiva, antisimétrica y transitiva, por lo tanto es una relación de orden.

■

6.2 Conjuntos Ordenados

6.2.1 Elementos Comparables

Dados dos elementos a y b de un conjunto A sobre el que se ha definido una relación de orden $\preccurlyeq$, diremos que son comparables si uno de ellos es anterior al otro. En caso contrario se dice que a y b "no son comparables".

$$a \text{ y } b \text{ son comparables} \iff a \preccurlyeq b \text{ ó } b \preccurlyeq a$$

luego,

$$a \text{ y } b \text{ no son comparables} \iff a \not\preccurlyeq b \text{ y } b \not\preccurlyeq a$$

■

6.2.2 Orden Parcial y Total

Una relación de orden se dice que es total cuando todos los elementos del conjunto sobre el que está definida son comparables por dicha relación. En caso contrario, es decir, si existen elementos no comparables, diremos que la relación definida es de orden parcial. Así pues, dada la relación de orden $\preccurlyeq$ definida en un conjunto A, diremos

$$\preccurlyeq \text{ es de orden total} \iff \forall a, b, (a \preccurlyeq b \text{ ó } b \preccurlyeq a)$$

$$\preccurlyeq \text{ es de orden parcial} \iff \exists a, b : (a \not\preccurlyeq b \text{ y } b \not\preccurlyeq a)$$

■

Ejemplo 6.2

Probar que la relación de orden "menor o igual" definida en el conjunto $\mathbb{Z}$ de los números enteros es total.

Solución

En efecto, sean a y b dos enteros cualesquiera, veamos que $a \leqslant b$ o $b \leqslant a$, es decir, todos los enteros son comparables por la relación.

Como a y b están arbitrariamente elegidos, puede ocurrir que sean iguales ($a = b$) o distintos ($a \neq b$). Pues bien,

$$\begin{aligned}
a = b \text{ ó } a \neq b &\iff a = b \text{ ó } b - a \neq 0 \\
&\iff a = b \text{ ó } b - a \in \mathbb{Z} \setminus \{0\} \\
&\iff a = b \text{ ó } b - a \in \mathbb{Z}^- \cup \mathbb{Z}^+ \\
&\iff a = b \text{ ó } \begin{cases} b - a \in \mathbb{Z}^- \\ \text{ó} \\ b - a \in \mathbb{Z}^+ \end{cases} \\
&\iff a = b \text{ ó } \begin{cases} a - b \in \mathbb{Z}^+ \\ \text{ó} \\ b - a \in \mathbb{Z}^+ \end{cases} \\
&\iff a = b \text{ ó } \begin{cases} \exists q \in \mathbb{Z}^+ : a - b = q \\ \text{ó} \\ \exists q \in \mathbb{Z}^+ : b - a = q \end{cases} \\
&\iff a = b \text{ ó } \begin{cases} \exists q \in \mathbb{Z}^+ : a = b + q \\ \text{ó} \\ \exists q \in \mathbb{Z}^+ : b = a + q \end{cases} \\
&\iff \begin{cases} a = b \text{ ó } b < a \\ \text{ó} \\ a = b \text{ ó } a < b \end{cases} \\
&\iff \begin{cases} b \leqslant a \\ \text{ó} \\ a \leqslant b \end{cases}
\end{aligned}$$

Por tanto, la relación de orden "menor o igual" definida en el conjunto de los números enteros es total.

■

Ejemplo 6.3

En el conjunto $\mathbb{Z}^+$ de los números enteros positivos, se considera la relación de divisibilidad.

(a) Probar que es una relación de orden.

(b) ¿Es total o parcial?

Solución

Recordemos (5.13) que el significado de la relación de divisibilidad era:

$$a \preccurlyeq b \iff b \text{ es divisible por } a$$

o lo que es igual,

$$a \preccurlyeq b \iff a \text{ es divisor de } b.$$

(a) Según vimos en 5.13 , 5.17 y 5.20 , esta relación es reflexiva, antisimétrica y transitiva y, por lo tanto, es de orden.

(b) Veamos, ahora, si este orden es total o parcial. En efecto, sean a y b dos enteros positivos cualesquiera distintos y distintos, ambos, de 1 y supongamos que son primos entre sí. Entonces,

$$a \text{ no es divisor de } b \text{ y } b \text{ no es divisor de } a$$

es decir,

$$a \not\preccurlyeq b \text{ y } b \not\preccurlyeq a$$

luego, según hemos visto en 6.2.2, la relación de divisibilidad es de orden parcial.

■

Ejemplo 6.4

Sea A un conjunto y sea $\mathscr{P}(A)$ el conjunto de las partes de A, es decir, el conjunto cuyos elementos son todos los posibles subconjuntos de A.

En $\mathscr{P}(A)$ se define la siguiente relación:

$$\forall X, Y, (X \preccurlyeq Y \iff X \subseteq Y)$$

Probar que es una relación de orden.

Solución

Veamos que la relación propuesta es de orden.

$$\forall X, Y, (X \preccurlyeq Y \iff X \subseteq Y)$$

⁕ Reflexividad.

En efecto, sea B cualquier subconjunto de A. Entonces, según vimos en 3.3.6,

$$B \subseteq B$$

luego,

$$B \preccurlyeq B$$

de aquí que

$$\forall X, (X \in \mathscr{P}(A) \Longrightarrow X \preccurlyeq X)$$

y, consecuentemente, la relación sea reflexiva.

⁕ Antisimetría.

En efecto, sean B y C cualesquiera de $\mathscr{P}(A)$. Entonces,

$$\left.\begin{array}{ccc} B \preccurlyeq C & \iff & B \subseteq C \\ \wedge & & \wedge \\ C \preccurlyeq B & \iff & C \subseteq B \end{array}\right\} \overset{3.3.5}{\Longrightarrow} B = C$$

luego,

$$\forall X, Y, (X \preccurlyeq Y \wedge Y \preccurlyeq X \Longrightarrow X = Y)$$

y, consecuentemente, la relación es antisimétrica.

⁕ Transitividad.

En efecto, sean B, C y D tres subconjuntos cualesquiera de A. Entonces,

$$\left.\begin{array}{ccc} B \preccurlyeq C & \Longleftrightarrow & B \subseteq C \\ \wedge & & \wedge \\ C \preccurlyeq D & \Longleftrightarrow & C \subseteq D \end{array}\right\} \overset{3.3.7}{\Longrightarrow} \quad B \subseteq D \iff B \preccurlyeq D$$

luego,

$$\forall X, Y, Z, (X \preccurlyeq Y \wedge Y \preccurlyeq Z \Longrightarrow X \preccurlyeq Z)$$

y, consecuentemente, la relación es transitiva.

Por ser reflexiva, antisimétrica y transitiva la relación propuesta es de orden. De ahora en adelante la llamaremos relación de orden de inclusión.

■

Ejemplo 6.5

En el conjunto de los enteros positivos, $\mathbb{Z}^+$, se consideran dos relaciones:

1 *La relación de orden de divisibilidad,*

$$\forall n_1, n_2, (n_1 \preccurlyeq_1 n_2 \longleftrightarrow n_1 \text{ es divisor de } n_2)$$

2 *La relación de orden de inclusión entre los conjuntos de divisores de un número,*

$$\forall n_1, n_2, (n_1 \preccurlyeq_2 n_2 \longleftrightarrow D_{n_1} \subseteq D_{n_2})$$

siendo, naturalmente, $D_a = \{n : n \text{ es divisor de } a\}$.

Comprobar que ambas relaciones son equivalentes.

Solución

Comprobaremos que

$$\forall n_1, n_2, (n_1 \preccurlyeq_1 n_2 \longleftrightarrow n_1 \preccurlyeq_2 n_2)$$

o lo que es igual,

$$\forall n_1, n_2, (n_1 \text{ es divisor de } n_2 \longleftrightarrow D_{n_1} \subseteq D_{n_2})$$

En efecto, sean a y b dos enteros positivos cualesquiera.

⁕ a es divisor de $b \Longrightarrow D_a \subseteq D_b$.

En efecto, sea d cualquier entero positivo. Entonces,

$$\begin{array}{rcll} d \in D_a & \Longleftrightarrow & d \text{ es divisor de } a & \\ & \Longleftrightarrow & (d \text{ es divisor de } a) \wedge (a \text{ es divisor de } b) & \{\text{Hipótesis}\} \\ & \Longrightarrow & d \text{ es divisor de } b & \{\text{Transitividad}\} \\ & \Longleftrightarrow & d \in D_b & \end{array}$$

Como d es cualquiera, hemos probado que la proposición,

$$\forall n, (n \in D_a \longrightarrow n \in D_b)$$

es verdadera, luego por la definición de inclusión, (3.3.1),

$$D_a \subseteq D_b$$

⋇ $D_a \subseteq D_b \Longrightarrow a$ es divisor de b.

En efecto, por la reflexividad de la relación de orden de divisibilidad,

$$\begin{aligned} a \text{ es divisor de } a &\iff a \in D_a \\ &\Longrightarrow a \in D_b && \{\text{Hipótesis}\} \\ &\iff a \text{ es divisor de } b \end{aligned}$$

Como a y b eran cualesquiera de $\mathbb{Z}^+$, hemos probado que

$$\forall n_1, n_2, (n_1 \text{ es divisor de } n_2 \longleftrightarrow D_{n_1} \subseteq D_{n_2})$$

es decir las relaciones de orden $\preccurlyeq_1$ y $\preccurlyeq_2$ son equivalentes.

■

Ejemplo 6.6

En el conjunto de los enteros positivos, $\mathbb{Z}^+$, se consideran dos relaciones:

1 *La relación de orden de divisibilidad,*

$$\forall n_1, n_2, (n_1 \succcurlyeq_1 n_2 \longleftrightarrow n_1 \textit{ es múltiplo de } n_2)$$

2 *La relación de orden de inclusión entre los conjuntos de divisores de un número,*

$$\forall n_1, n_2, (n_1 \succcurlyeq_2 n_2 \longleftrightarrow M_{n_1} \subseteq M_{n_2})$$

siendo, naturalmente, $M_a = \{n : n \textit{ es múltiplo de } a\} = \{n : n = aq, q \in \mathbb{Z}^+\}$.

Comprobar que ambas relaciones son equivalentes.

Solución

Comprobaremos que

$$\forall n_1, n_2, (n_1 \succcurlyeq_1 n_2 \longleftrightarrow n_1 \succcurlyeq_2 n_2)$$

o lo que es igual,

$$\forall n_1, n_2, (n_1 \text{ es múltiplo de } n_2 \longleftrightarrow M_{n_1} \subseteq M_{n_2})$$

En efecto, sean a y b dos enteros positivos cualesquiera.

⋇ a es múltiplo de $b \Longrightarrow M_a \subseteq M_b$.

En efecto, sea m cualquier entero positivo. Entonces,

$$\begin{aligned} m \in M_a &\iff m \text{ es múltiplo de } a \\ &\iff (m \text{ es múltiplo de } a) \wedge (a \text{ es múltiplo de } b) && \{\text{Hipótesis}\} \\ &\Longrightarrow m \text{ es múltiplo de } b && \{\text{Transitividad}\} \\ &\iff m \in M_b \end{aligned}$$

Como m es cualquiera, hemos probado la veracidad de la proposición,

$$\forall n, (n \in M_a \longrightarrow n \in M_b)$$

luego, por la definición de inclusión, (3.3.1),

$$M_a \subseteq M_b$$

⋇ $M_a \subseteq M_b \Longrightarrow a$ es múltiplo de b.

En efecto, por la reflexividad de la relación de orden de divisibilidad,

$$\begin{array}{rcll} a \text{ es múltiplo de } a & \Longleftrightarrow & a \in M_a & \\ & \Longrightarrow & a \in M_b & \{\text{Hipótesis}\} \\ & \Longleftrightarrow & a \text{ es múltiplo de } b & \end{array}$$

Como a y b eran cualesquiera de $\mathbb{Z}^+$, hemos probado que

$$\forall n_1, n_2, (n_1 \text{ es múltiplo de } n_2 \longleftrightarrow M_{n_1} \subseteq M_{n_2})$$

es decir las relaciones de orden $\succcurlyeq_1$ y $\succcurlyeq_2$ son equivalentes.

■

Ejemplo 6.7

En el conjunto $\mathbb{Z}$ de los números enteros se considera la siguiente relación:

$$\forall n_1, n_2 \left(n_1 \preccurlyeq n_2 \longleftrightarrow \exists q \in \mathbb{Z}^+ : n_2 = n_1^q\right)$$

Probar que es una relación de orden.

Solución

Veamos si la relación cumple las condiciones para ser de orden.

◎ Reflexividad. En efecto, sea a un número entero cualquiera. Entonces,

$$a = a^1, \text{ siendo } 1 \in \mathbb{Z}^+$$

y como a es cualquiera, la proposición,

$$\forall n, n \preccurlyeq n$$

será verdadera y, consecuentemente, la relación propuesta es reflexiva.

◎ Antisimetría. En efecto, sean a y b dos enteros cualesquiera tales que $a \preccurlyeq b$ y $b \preccurlyeq a$. Entonces,

$$\left.\begin{array}{l} a \preccurlyeq b \iff b = a^{q_1}, q_1 \in \mathbb{Z}^+ \\ \text{y} \\ b \preccurlyeq a \iff a = b^{q_2}, q_2 \in \mathbb{Z}^+ \end{array}\right\} \Longrightarrow b = (b^{q_2})^{q_1}$$

$$\Longleftrightarrow b = b^{q_1 q_2}$$

$$\Longrightarrow \left\{\begin{array}{l} q_1 q_2 = 1 \\ \text{ó} \\ b = 1 \\ \text{ó} \\ b = -1, \ q_1 \text{ impar y } q_2 \text{ impar} \end{array}\right.$$

Analicemos los tres casos.

– Si $q_1 q_2 = 1$, entonces $q_1 = 1$ y $q_2 = 1$ ya que ambos son enteros positivos. En tal caso,

$$\left.\begin{array}{l} b = a^{q_1} \\ \text{y} \\ q_1 = 1 \end{array}\right\} \implies b = a$$

$$\left.\begin{array}{l} a = b^{q_2} \\ \text{y} \\ q_2 = 1 \end{array}\right\} \implies a = b$$

– Si $b = 1$, entonces

$$\left.\begin{array}{rcl} b & = & a^{q_1} \\ \text{y} & & \\ b & = & 1 \end{array}\right\} \implies 1 = a^{q_1},\ q_1 \in \mathbb{Z}^+ \implies a = 1$$

$$\left.\begin{array}{rcl} a & = & b^{q_2} \\ \text{y} & & \\ b & = & 1 \end{array}\right\} \implies a = 1^{q_2},\ q_2 \in \mathbb{Z}^+ \implies a = 1$$

$$\Big\} \implies a = b$$

– Si $b = -1$ y $q_1, q_2 \in \mathbb{Z}^+$, impares,

$$\left.\begin{array}{rcl} b & = & a^{q_1} \\ \text{y} & & \\ b & = & -1 \end{array}\right\} \implies -1 = a^{q_1},\ q_1 \text{ impar} \implies a = -1$$

$$\left.\begin{array}{rcl} a & = & b^{q_2} \\ \text{y} & & \\ b & = & -1 \end{array}\right\} \implies a = (-1)^{q_2},\ q_2 \text{ impar} \implies a = -1$$

$$\Big\} \implies a = b$$

Así pues, la proposición,

$$\forall n_1, n_2, [(n_1 \preccurlyeq n_2 \text{ y } n_2 \preccurlyeq n_1) \longrightarrow n_1 = n_2]$$

es, en cualquier caso, verdadera y, consecuentemente, la relación propuesta es antisimétrica.

◎ Transitividad. Sean a, b y c tres enteros cualesquiera tales que a sea anterior a b y b anterior a c. Entonces,

$$\left.\begin{array}{l} a \preccurlyeq b \iff b = a^{q_1},\ q_1 \in \mathbb{Z}^+ \\ \text{y} \\ b \preccurlyeq c \iff c = b^{q_2},\ q_2 \in \mathbb{Z}^+ \end{array}\right\} \implies c = (a^{q_1})^{q_2}$$

$$\iff c = a^{q_1 q_2},\ q_1 q_2 \in \mathbb{Z}^+$$

$$\iff a \preccurlyeq c$$

Hemos probado, pues, la veracidad de la proposición,

$$\forall n_1, n_2, n_3, [(n_1 \preccurlyeq n_2 \text{ y } n_2 \preccurlyeq n_1) \longrightarrow n_1 \preccurlyeq n_3]$$

y, consecuentemente, la relación es transitiva.

Por ser reflexiva, antisimétrica y transitiva, la relación propuesta es de orden.

■

6.2.3 Conjuntos Ordenados

Dado un conjunto A diremos que está ordenado si en él hay definida una relación de orden. Dicho conjunto estará parcial o totalmente ordenado según que la relación definida sea parcial o total.

Notaremos $(A, \preccurlyeq)$ al conjunto A ordenado con la relación $\preccurlyeq$.

■

6.3 Representación Gráfica

6.3.1 Diagrama de Hasse

Dada una relación de orden, $\preccurlyeq$, sobre un conjunto A, un diagrama de Hasse es un grafo dirigido de la misma simplificado según los criterios siguientes:

1. *Dado que toda relación de orden es reflexiva, en cada punto de su digrafo habrá un bucle. Simplificaremos el dibujo eliminándolos todos.*

2. *Como toda relación de orden es transitiva, suprimimos todos los arcos del digrafo que se obtenga al hallar el cierre transitivo de los restantes.*

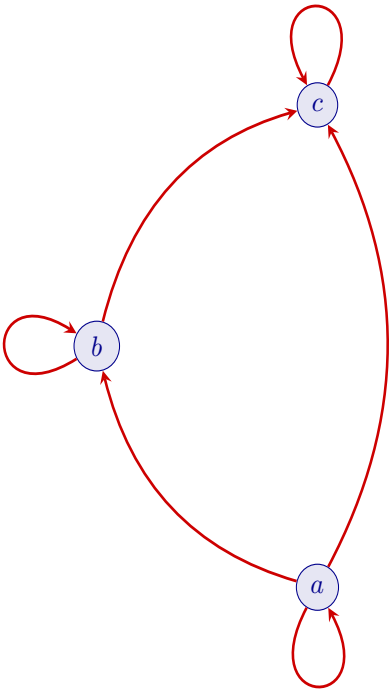
3. *Al igual que en un digrafo, cada punto de A lo representamos por un punto del plano, aunque conviniendo en que si "a es anterior a b", dibujaremos el punto a por debajo del b. Todas las líneas que unan puntos serán, por tanto, ascendentes, de aquí que se supriman las direcciones utilizadas en los digrafos.*

Ejemplo 6.8

Consideremos definida en el conjunto $A = \{a, b, c\}$ la siguiente relación de orden

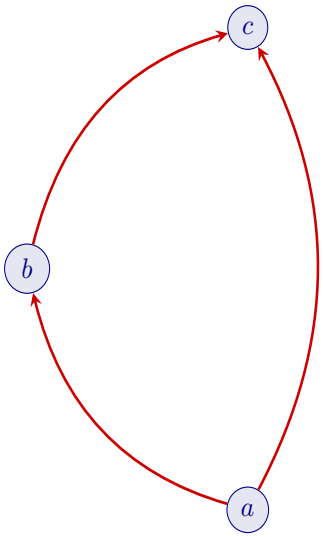
$$\preccurlyeq = \{(a,a), (a,b), (a,c), (b,b), (b,c), (c,c)\}.$$

Su grafo dirigido sería:

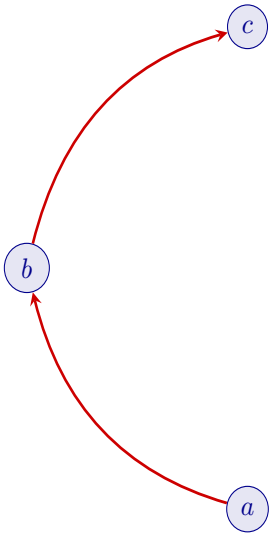


Veamos como se obtiene el diagrama de Hasse de la relación mediante la aplicación de los criterios anteriores.

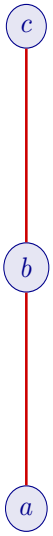
1. Eliminamos todos los bucles.



2. Como de $a \preccurlyeq b$ y $b \preccurlyeq c$, se sigue que $a \preccurlyeq c$, omitiremos la arista que va desde a hasta c y mantendremos las que van desde a hasta b y desde b a c.



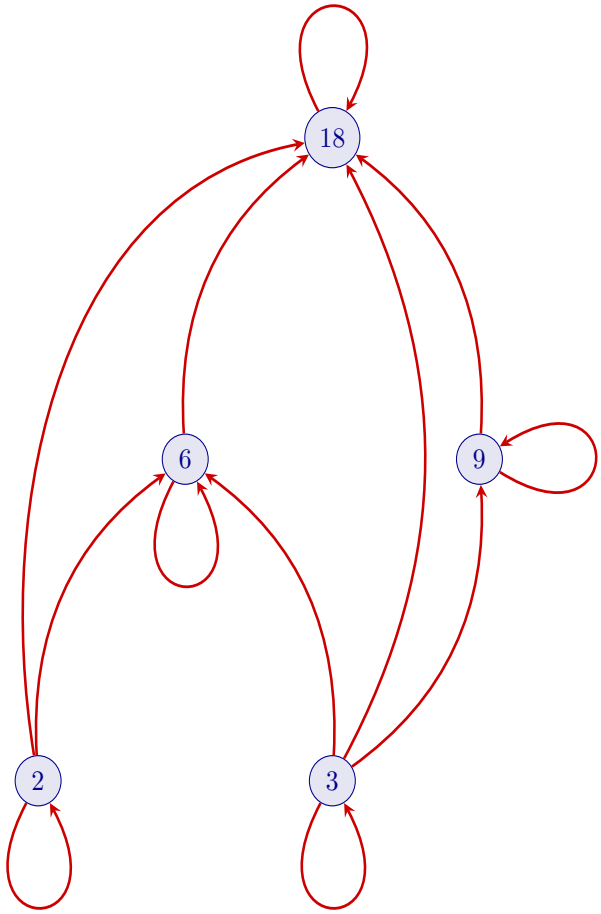
3. Eliminamos las direcciones y ya tenemos el diagrama de Hasse.



■

Ejemplo 6.9

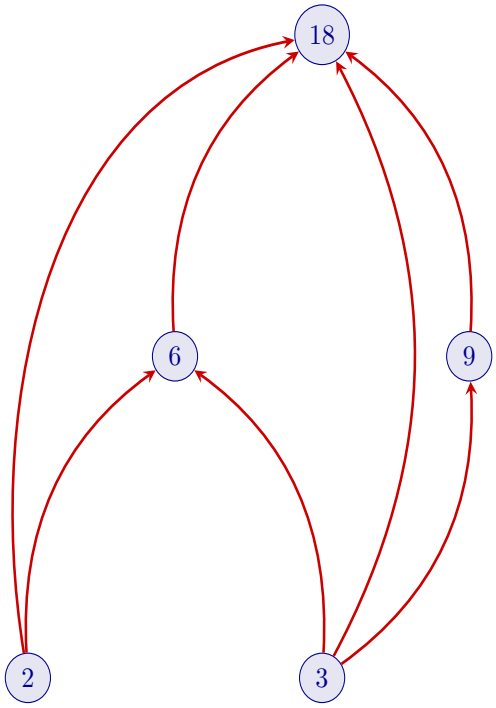
El siguiente grafo dirigido representa el conjunto $A = \{2, 3, 6, 9, 18\}$ *ordenado por la relación de divisibilidad.*



Obtener, paso a paso, el diagrama de Hasse de esta relación.

Solución

1. Los bucles significan que cada uno de los números de A se divide a sí mismo. Los eliminamos todos.

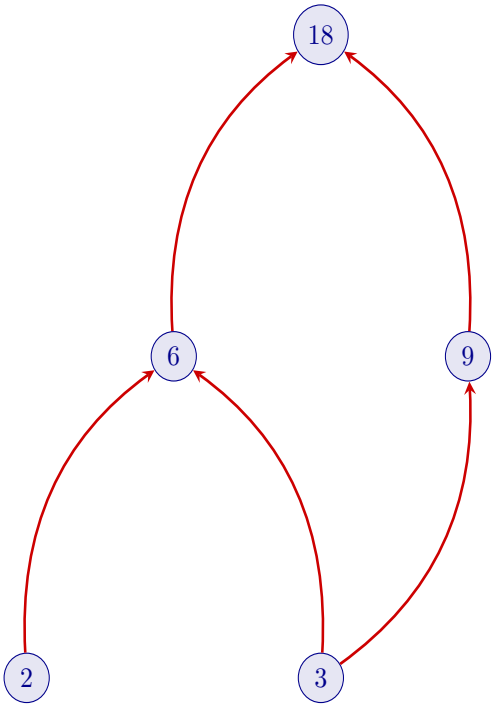


2. Eliminamos los cierres transitivos.

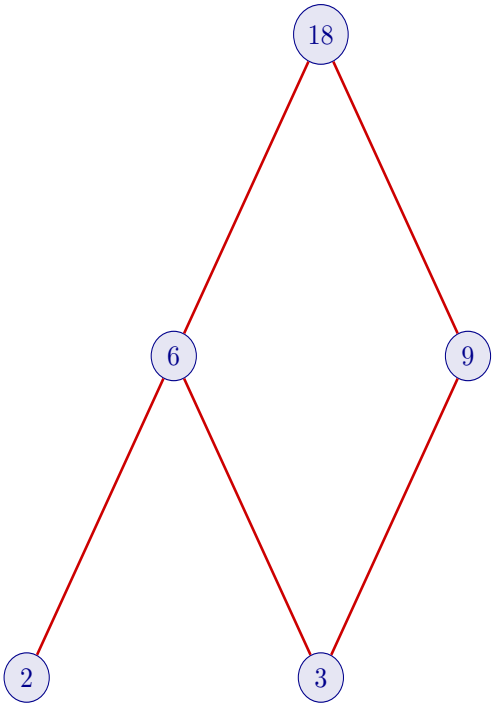
$$\left.\begin{array}{l}\text{2 divide a 6}\\ \text{y}\\ \text{6 divide a 18}\end{array}\right\} \Longrightarrow \text{2 divide a 18. Eliminamos el arco que une 2 con 18.}$$

$$\left.\begin{array}{l}\text{3 divide a 6}\\ \text{y}\\ \text{6 divide a 18}\end{array}\right\} \Longrightarrow \text{3 divide a 18. Eliminamos el arco que une 3 con 18.}$$

$$\left.\begin{array}{l}\text{3 divide a 9}\\ \text{y}\\ \text{9 divide a 18}\end{array}\right\} \Longrightarrow \text{3 divide a 18. Eliminamos el arco que une 3 con 18.}$$



3. Eliminamos las direcciones y tendremos el diagrama de Hasse.



Como puede apreciarse este diagrama nos da una idea más clara de la ordenación que el grafo dirigido. En efecto, el 2 y el 3 están al mismo nivel ya que 2 no divide a 3, ni 3 divide a 2, es decir no son comparables y lo mismo ocurre con 6 y 9. El 6 es posterior a 2 y 3 ya que es múltiplo de ambos, al igual que 18 que es múltiplo de 6 y 9. Finalmente, el 9 es posterior a 3 ya que es múltiplo suyo.

■

Ejemplo 6.10

Hacer el diagrama de Hasse de las siguientes relaciones de orden.

(a) $\preccurlyeq = \{(1,1),(1,2),(2,2),(2,4),(1,3),(3,3),(3,4),(1,4),(4,4)\}$ *definida en el conjunto* $A = \{1,2,3,4\}$.

(b)

$$\begin{aligned}\preccurlyeq \quad = \quad & \{(a,a),(b,b),(c,c),(a,c),(c,d),(c,e),(a,d)\\ & (d,d),(a,e),(b,c),(b,d),(b,e),(e,e)\}\end{aligned}$$

definida en $A = \{a,b,c,d,e\}$.

Solución

(a) $\preccurlyeq = \{(1,1),(1,2),(2,2),(2,4),(1,3),(3,3),(3,4),(1,4),(4,4)\}$.

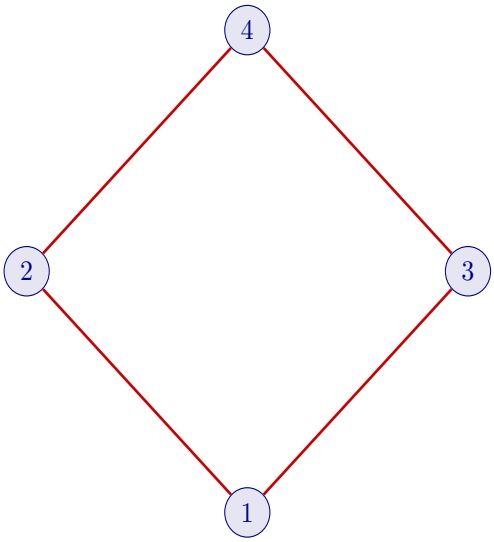
Observemos que

$$1 \preccurlyeq 2 \preccurlyeq 4$$

y

$$1 \preccurlyeq 3 \preccurlyeq 4$$

pero $2 \not\preccurlyeq 3$ y $3 \not\preccurlyeq 2$, es decir 2 y 3 no está relacionados. El diagrama de Hasse será, por tanto,



(b)

$$\begin{aligned}\preccurlyeq \quad = \quad & \{(a,a),(b,b),(c,c),(a,c),(c,d),(c,e),(a,d)\\ & (d,d),(a,e),(b,c),(b,d),(b,e),(e,e)\}\end{aligned}$$

Como puede observarse,

$$a \preccurlyeq c \preccurlyeq d$$

$$a \preccurlyeq c \preccurlyeq e$$

$$b \preccurlyeq c \preccurlyeq e$$

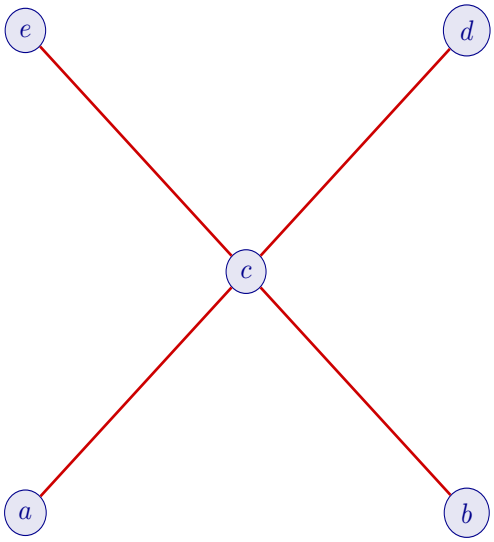
$$b \preccurlyeq c \preccurlyeq d$$

pero,

$$a \not\preccurlyeq b \quad \text{y} \quad b \not\preccurlyeq a$$

$$d \not\preccurlyeq e \quad \text{y} \quad e \not\preccurlyeq d$$

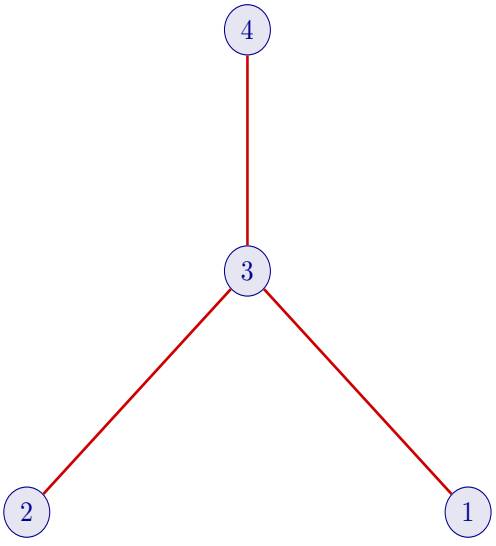
es decir, a y b no están relacionados y tampoco d y e. De todo esto se sigue que el diagrama de Hasse es:



■

Ejemplo 6.11

Escribir las parejas ordenadas de la relación determinada por los siguientes diagramas de Hasse en el conjunto $A = \{1, 2, 3, 4\}$.



(a)

(b)

Solución

(a) $\preccurlyeq = \{(1,1),(1,3),(1,4),(2,2),(2,3),(2,4),(3,3),(3,4),(4,4)\}$

(b) $\preccurlyeq = \{(1,1),(1,2),(1,3),(1,4),(2,2),(2,3),(2,4),(3,3),(3,4),(4,4)\}$

■

6.4 Elementos Característicos de un Conjunto Ordenado

Ciertos elementos en un conjunto ordenado son de especial importancia para muchas de las aplicaciones de esos conjuntos. Explicaremos quienes son estos elementos y posteriormente veremos el importante papel que juegan.

A lo largo de este apartado $(A, \preccurlyeq)$ será un conjunto ordenado y B un subconjunto suyo ($B \subseteq A$).

6.4.1 Elemento Minimal

Un elemento b de B se dice que es minimal de B, respecto de la relación $\preccurlyeq$, si ningún elemento de B es estrictamente anterior a él. Es decir,

$$b \text{ es minimal de } B \iff \forall x, (x \in B \longrightarrow x \not\prec b)$$

■

Ejemplo 6.12

En el conjunto $\mathbb{Z}^+$ de los enteros positivos se considera la relación de divisibilidad, es decir, dados dos enteros positivos cualesquiera n_1 y n_2,

$$n_1 \preccurlyeq n_2 \longleftrightarrow n_1 \text{ es divisor de } n_2$$

Obtener, de forma razonada, los elementos minimales del conjunto

$$A = \{4, 6, 8, 9, 12, 18, 24, 27, 36, 54\}$$

ordenado por la relación anterior.

Solución

La relación está definida en el conjunto de los enteros positivos, $\mathbb{Z}^+$, en la forma siguiente:

$$\forall n_1, n_2, (n_1 \preccurlyeq n_2 \longleftrightarrow n_1 \text{ es divisor de } n_2)\,.$$

Si llamamos D_{n_2} al conjunto formado por todos los divisores de n_2, sería lo mismo que escribir,

$$\forall n_1, n_2, (n_1 \preccurlyeq n_2 \longleftrightarrow n_1 \in D_{n_2})\,.$$

Por ejemplo, los divisores de 12 son 1, 2, 3, 4, 6 y 12, luego,

$$D_{12} = \{1, 2, 3, 4, 6, 12\}\,.$$

Entonces,

$$4 \in D_{12}, \text{ por lo tanto, } 4 \preccurlyeq 12$$

$$6 \in D_{12}, \text{ por lo tanto, } 6 \preccurlyeq 12$$

$$12 \in D_{12}, \text{ por lo tanto, } 12 \preccurlyeq 12$$

Lo primero que haremos es "adecuar" la definición de minimal a nuestra relación, es decir a la relación de divisibilidad. Sea b cualquiera de los números que integran el conjunto A. Entonces, según la definición (6.4.1),

b es minimal de A respecto de la relación $\preccurlyeq$, si ningún elemento de A es estrictamente anterior a b.

es decir,

$$b \text{ es minimal de } A \Longleftrightarrow \forall n, (n \in A \longrightarrow n \not\prec b)$$

Sea a cualquier entero positivo, entonces,

$$\begin{aligned} a \in A \longrightarrow a \not\prec b \quad &\Longleftrightarrow \quad a \in A \longrightarrow \neg (a \prec b) \\ &\Longleftrightarrow \quad a \in A \longrightarrow \neg (a \preccurlyeq b \wedge a \neq b) \\ &\Longleftrightarrow \quad a \in A \longrightarrow (\neg (a \preccurlyeq b) \vee a = b) \\ &\Longleftrightarrow \quad a \in A \longrightarrow (a \preccurlyeq b \longrightarrow a = b) \\ &\Longleftrightarrow \quad (a \in A \wedge a \preccurlyeq b) \longrightarrow a = b \\ &\Longleftrightarrow \quad (a \in A \wedge a \in D_b) \longrightarrow a \in \{b\} \\ &\Longleftrightarrow \quad a \in (A \cap D_b) \longrightarrow a \in \{b\} \end{aligned}$$

y como a era cualquiera, tendremos que

$$\forall n, (n \in A \longrightarrow n \not\prec b) \Longleftrightarrow \forall n, (n \in (A \cap D_b) \longrightarrow n \in \{b\})$$

y, por definición de inclusión de conjuntos,

$$\forall n, (n \in (A \cap D_b) \longrightarrow n \in \{b\}) \Longleftrightarrow A \cap D_b \subseteq \{b\}$$

luego,

$$\forall n, (n \in A \longrightarrow n \not\prec b) \Longleftrightarrow A \cap D_b \subseteq \{b\}$$

Por otra parte,

$$\left.\begin{array}{l} b \in A \\ \text{y} \\ b \in D_b \end{array}\right\} \implies b \in A \cap D_b \implies \{b\} \subseteq A \cap D_b$$

de aquí que

$$A \cap D_b \subseteq \{b\} \Longleftrightarrow A \cap D_b \subseteq \{b\} \text{ y } \{b\} \subseteq A \cap D_b \Longleftrightarrow A \cap D_b = \{b\}$$

y, por lo tanto,

$$\forall n, (n \in A \longrightarrow n \not\prec b) \Longleftrightarrow A \cap D_b = \{b\}$$

es decir,

$$b \text{ es minimal de } A \text{ respecto de la relación de divisibilidad} \Longleftrightarrow A \cap D_b = \{b\}$$

siendo D_b el conjunto integrado por todos los divisores de b.

Pues bien,

$$D_4 = \{1, 2, 4\}$$

luego,

$$A \cap D_4 = \{4, 6, 8, 9, 12, 18, 24, 27, 36, 54\} \cap \{1, 2, 4\} = \{4\}$$

y, por lo tanto, el 4 es minimal del conjunto A. Además, ninguno de sus múltiplos, salvo el propio 4, puede ser minimal ya que todos ellos tendrían al 4 como divisor, es decir el 4 sería estrictamente anterior a ellos. Así que 8, 12, 24 y 36 no son minimales.

También,

$$A \cap D_6 = \{4, 6, 8, 9, 12, 18, 24, 27, 36, 54\} \cap \{1, 2, 3, 6\} = \{6\}$$

luego el 6 es minimal y, por la misma razón que antes, ninguno de los múltiplos de 6 que quedan pueden ser minimales, es decir, el 18 y el 54 no son minimales.

Finalmente,

$$A \cap D_9 = \{4, 6, 8, 9, 12, 18, 24, 27, 36, 54\} \cap \{1, 3, 9\} = \{9\}$$

por lo tanto el 9 es minimal y, por la misma razón que antes, el 27 no lo es.

Como ya no quedan más números en A que puedan ser minimales, los elementos minimales del conjunto A ordenado por la relación de divisibilidad serán el 4, el 6 y el 9.

■

6.4.2 Elemento Maximal

Un elemento b de B se dice que es maximal de B, respecto de la relación $\preccurlyeq$, si ningún elemento de B es estrictamente posterior a él. Es decir,

$$b \text{ es maximal de } B \iff \forall x, (x \in B \longrightarrow x \not\succ b)$$

■

Ejemplo 6.13

En el conjunto $\mathbb{Z}^+$ de los enteros positivos se considera la relación de divisibilidad, es decir, dados dos enteros positivos cualesquiera n_1 y n_2,

$$n_1 \preccurlyeq n_2 \longleftrightarrow n_1 \text{ es divisor de } n_2$$

Obtener, de forma razonada, los elementos maximales del conjunto

$$A = \{4, 6, 8, 9, 12, 18, 24, 27, 36, 54\}$$

ordenado por la relación anterior.

Solución

La relación está definida en el conjunto de los enteros positivos, $\mathbb{Z}^+$, en la forma siguiente:

$$\forall n_1, n_2, (n_1 \preccurlyeq n_2 \longleftrightarrow n_1 \text{ es divisor de } n_2)$$

y si tenemos en cuenta que

$$n_1 \text{ es divisor de } n_2 \longleftrightarrow n_2 \text{ es múltiplo de } n_1$$

podemos escribir,

$$\forall n_1, n_2, (n_1 \preccurlyeq n_2 \longleftrightarrow n_2 \text{ es múltiplo de } n_1)$$

lo cual equivale a decir,

$$\forall n_1, n_2, (n_2 \succcurlyeq n_1 \longleftrightarrow n_2 \text{ es múltiplo de } n_1)$$

es decir, n_2 es posterior a n_1 es equivalente a decir que n_2 es múltiplo de n_1.

Si llamamos M_{n_1} al conjunto formado por todos los múltiplos de n_1, sería lo mismo que escribir,

$$\forall n_1, n_2, (n_2 \succcurlyeq n_1 \longleftrightarrow n_2 \in M_{n_1})$$

siendo, naturalmente, $M_{n_1} = \{n : n = n_1 q; q \in \mathbb{Z}^+\}$.

Calcularemos, ahora, los elementos maximales de nuestro conjunto.

Lo primero que haremos es "adecuar" la definición de maximal a nuestra relación, es decir a la relación de divisibilidad. Sea b cualquiera de los números que integran el conjunto A. Entonces, según la definición (6.4.2),

b es maximal de A respecto de la relación $\preccurlyeq$, si ningún elemento de A es estrictamente posterior a b.

es decir,

$$b \text{ es maximal de } A \Longleftrightarrow \forall n, (n \in A \longrightarrow n \not\succ b)$$

Sea a cualquier entero positivo, entonces,

$$\begin{aligned} a \in A \longrightarrow a \not\succ b &\iff a \in A \longrightarrow \neg (a \succ b) \\ &\iff a \in A \longrightarrow \neg (a \succcurlyeq b \wedge a \neq b) \\ &\iff a \in A \longrightarrow (\neg (a \succcurlyeq b) \vee a = b) \\ &\iff a \in A \longrightarrow (a \succcurlyeq b \longrightarrow a = b) \\ &\iff (a \in A \wedge a \succcurlyeq b) \longrightarrow a = b \\ &\iff (a \in A \wedge a \in M_b) \longrightarrow a \in \{b\} \\ &\iff a \in (A \cap M_b) \longrightarrow a \in \{b\} \end{aligned}$$

y como a era cualquiera, tendremos que

$$\forall n, (n \in A \longrightarrow n \not\succ b) \Longleftrightarrow \forall n, (n \in (A \cap M_b) \longrightarrow n \in \{b\})$$

y, por definición de inclusión de conjuntos,

$$\forall n, (n \in (A \cap M_b) \longrightarrow n \in \{b\}) \Longleftrightarrow A \cap M_b \subseteq \{b\}$$

luego,

$$\forall n, (n \in A \longrightarrow n \not\succ b) \Longleftrightarrow A \cap M_b \subseteq \{b\}$$

Por otra parte,

$$\left.\begin{array}{l} b \in A \\ \text{y} \\ b \in M_b \end{array}\right\} \implies b \in A \cap M_b \implies \{b\} \subseteq A \cap M_b$$

de aquí que

$$A \cap M_b \subseteq \{b\} \Longleftrightarrow A \cap M_b \subseteq \{b\} \text{ y } \{b\} \subseteq A \cap M_b \Longleftrightarrow A \cap M_b = \{b\}$$

y, por lo tanto,

$$\forall n, (n \in A \longrightarrow n \not\succ b) \Longleftrightarrow A \cap M_b = \{b\}$$

es decir,

$$b \text{ es maximal de } A \text{ respecto de la relación de divisibilidad} \Longleftrightarrow A \cap M_b = \{b\}$$

siendo M_b el conjunto formado por todos los múltiplos de b.

Pues bien,

$$M_{54} = \left\{n : n = 54q,\ q \in \mathbb{Z}^+\right\}$$

luego,

$$A \cap M_{54} = \{4, 6, 8, 9, 12, 18, 24, 27, 36, 54\} \cap \left\{n : n = 54q,\ q \in \mathbb{Z}^+\right\} = \{54\}$$

y, por tanto, el 54 es maximal del conjunto A. Además, ninguno de sus divisores, salvo el propio 54, puede ser maximal ya que todos ellos tendrían al 54 como múltiplo, es decir el 54 sería estrictamente posterior a ellos. Así que 6, 9, 18 y 27 no son maximales.

También,

$$A \cap M_{36} = \{4, 6, 8, 9, 12, 18, 24, 27, 36, 54\} \cap \left\{n : n = 36q,\ q \in \mathbb{Z}^+\right\} = \{36\}$$

luego el 36 es maximal y, por la misma razón que antes, ninguno de los divisores de 36 que quedan pueden ser maximales, es decir, el 4 y el 12 no son maximales.

Finalmente,

$$A \cap M_{24} = \{4, 6, 8, 9, 12, 18, 24, 27, 36, 54\} \cap \left\{n : n = 24q,\ q \in \mathbb{Z}^+\right\} = \{24\}$$

por lo tanto el 24 es maximal y, por la misma razón que antes, el 8, único divisor de 24 que queda, no lo es.

Como ya no quedan más números en A que puedan serlo, los elementos maximales del conjunto A ordenado por la relación de divisibilidad serán el 54, el 36 y el 24.

■

6.4.3 Existencia del Maximal y Minimal

Todo conjunto ordenado finito posee, al menos, un elemento maximal y un elemento minimal.

Demostración

Sea $(A, \preccurlyeq)$ un conjunto ordenado con n elementos, y sea a cualquier elemento de A.

- Si a es minimal, hemos terminado.
- Si a no es minimal, entonces existirá, al menos, a_1 en A que sea estrictamente anterior a él, es decir,

  $$\exists a_1 : (a_1 \in A \text{ y } a_1 \prec a)$$

  y habrá dos opciones:

  - a_1 es minimal y habríamos terminado.
  - a_1 no es minimal, en cuyo caso,

    $$\exists a_2 : (a_2 \in A \text{ y } a_2 \prec a_1)$$

    es decir, existen a_1 y a_2 en A tales que

    $$a_2 \prec a_1 \prec a$$

Este razonamiento no puede continuar más allá del número de elementos que tenga A y, como éste es finito, obtendríamos una cadena

$$a_p \prec a_{p-1} \prec \cdots \prec a_2 \prec a_1 \prec a$$

que ya no puede extenderse. A partir de ese momento no sería posible encontrar un elemento en A que fuese estrictamente anterior a a_p es decir,

$$\forall n, (n \in A \longrightarrow n \not\prec a_p)$$

y, consecuentemente, a_p sería minimal.

La existencia de elemento maximal se demuestra de una forma similar.

■

6.4.4 Elemento Mínimo

Un elemento b de A se dice que es mínimo de B, respecto de la relación $\preccurlyeq$, si está en B y es anterior a todos los elementos de B. Es decir,

$$b \text{ es mínimo de } B \Longleftrightarrow (b \in B) \wedge \forall x, (x \in B \longrightarrow b \preccurlyeq x)$$

■

Ejemplo 6.14

En el conjunto $\mathbb{Z}^+$ de los enteros positivos se considera la relación de divisibilidad, es decir, dados dos enteros positivos cualesquiera n_1 y n_2,

$$n_1 \preccurlyeq n_2 \Longleftrightarrow n_1 \text{ es divisor de } n_2$$

Obtener, de forma razonada, el elemento mínimo, si lo tiene, del conjunto

$$A = \{6, 12, 18, 24, 36, 54, 72, 108, 216\}$$

ordenado por la relación anterior.

Solución

La relación está definida en el conjunto de los enteros positivos, $\mathbb{Z}^+$, en la forma siguiente:

$$\forall n_1, n_2, (n_1 \preccurlyeq n_2 \Longleftrightarrow n_1 \text{ es divisor de } n_2)\,.$$

Si llamamos D_{n_2} al conjunto formado por todos los divisores de n_2, sería lo mismo que escribir,

$$\forall n_1, n_2, (n_1 \preccurlyeq n_2 \Longleftrightarrow n_1 \in D_{n_2})\,.$$

Por ejemplo, los divisores de 12 son 1, 2, 3, 4, 6 y 12, luego,

$$D_{12} = \{1, 2, 3, 4, 6, 12\}\,.$$

Entonces,

$$4 \in D_{12}, \text{ por lo tanto, } 4 \preccurlyeq 12$$

$$6 \in D_{12}, \text{ por lo tanto, } 6 \preccurlyeq 12$$

$$12 \in D_{12}, \text{ por lo tanto, } 12 \preccurlyeq 12$$

Lo primero que haremos es "adecuar" la definición de mínimo a nuestra relación, es decir a la relación de divisibilidad.

Pues bien, sea b cualquier entero positivo. Entonces, según la definición de mínimo, (6.4.4),

> *b es mínimo de A respecto de la relación $\preccurlyeq$, si pertenece a A y es anterior a todos los elementos de A.*

lo cual "traducido" a nuestra relación querrá decir,

> *b es mínimo de A respecto a relación de divisibilidad, si b pertenece a A y es divisor de todos los elementos de A.*

Por lo tanto,

$$\begin{aligned}
b \text{ es mínimo de } A &\iff (b \in A) \wedge (b \in D_a, \text{ para todos y cada uno de los } a \text{ de } A) \\
&\iff (b \in A) \wedge \left(b \in \bigcap_{a \in A} D_a \right) \\
&\iff (b \in A) \wedge (b \in D_6 \cap D_{12} \cap D_{18} \cap D_{24} \cap D_{36} \cap D_{54} \cap D_{72} \cap D_{108} \cap D_{216}) \\
&\quad \left\{ \begin{array}{l} \text{Por (6.5), } D_6 \subseteq D_{12} \subseteq D_{36} \subseteq D_{72} \subseteq D_{216}, \text{ luego} \\ D_6 \cap D_{12} \cap D_{36} \cap D_{72} \cap D_{216} = D_6 \end{array} \right\} \\
&\implies (b \in A) \wedge (b \in D_6 \cap D_{18} \cap D_{24} \cap D_{54} \cap D_{108}) \\
&\quad \left\{ \begin{array}{l} \text{Por (6.5), } D_6 \subseteq D_{18} \subseteq D_{54} \subseteq D_{108}, \text{ luego} \\ D_6 \cap D_{18} \cap D_{54} \cap D_{108} = D_6 \end{array} \right\} \\
&\implies (b \in A) \wedge (b \in D_6 \cap D_{24}) \\
&\quad \left\{ \begin{array}{l} \text{Por (6.5), } D_6 \subseteq D_{24}, \text{ luego} \\ D_6 \cap D_{24} = D_6 \end{array} \right\} \\
&\iff (b \in A \cap D_6) \\
&\iff b \in (\{6, 12, 18, 24, 36, 54, 72, 108, 216\} \cap \{1, 2, 3, 6\}) \\
&\iff b \in \{6\} \\
&\iff b = 6
\end{aligned}$$

Concluyendo, el mínimo del conjunto A ordenado por la relación de divisibilidad es el 6. Lo notaremos,

$$\text{Min}\,(A) = 6$$

■

6.4.5 Elemento Máximo

Un elemento b de A se dice que es máximo de B, respecto de la relación $\preccurlyeq$, si está en B y es posterior a todos los elementos de B. Es decir,

$$b \text{ es máximo de } B \iff (b \in B) \wedge \forall x, (x \in B \longrightarrow b \succcurlyeq x)$$

■

Ejemplo 6.15

En el conjunto $\mathbb{Z}^+$ de los enteros positivos se considera la relación de divisibilidad, es decir, dados dos enteros positivos cualesquiera n_1 y n_2,

$$n_1 \preccurlyeq n_2 \iff n_1 \text{ es divisor de } n_2$$

Obtener, de forma razonada, el elemento máximo, si lo tiene, del conjunto

$$A = \{6, 12, 18, 24, 36, 54, 72, 108, 216\}$$

ordenado por la relación anterior.

Solución

La relación está definida en el conjunto de los enteros positivos, $\mathbb{Z}^+$, en la forma siguiente:

$$\forall n_1, n_2, (n_1 \preccurlyeq n_2 \iff n_1 \text{ es divisor de } n_2)$$

y si tenemos en cuenta que

$$n_1 \text{ es divisor de } n_2 \iff n_2 \text{ es múltiplo de } n_1$$

podemos escribir,

$$\forall n_1, n_2, (n_1 \preccurlyeq n_2 \iff n_2 \text{ es múltiplo de } n_1)$$

lo cual equivale a decir,

$$\forall n_1, n_2, (n_2 \succcurlyeq n_1 \iff n_2 \text{ es múltiplo de } n_1)$$

es decir, n_2 es posterior a n_1 es equivalente a decir que n_2 es múltiplo de n_1.

Lo primero que haremos es "adecuar" la definición de máximo a nuestra relación, es decir a la relación de divisibilidad.

Pues bien, sea b cualquier entero positivo. Entonces, según la definición de mínimo, (6.4.4),

> *b es máximo de A respecto de la relación $\preccurlyeq$, si b pertenece a A y es posterior a todos los elementos de A.*

lo cual "traducido" a nuestra relación querrá decir,

> *b es máximo de A respecto a relación de divisibilidad, si b pertenece a A y es múltiplo de todos los elementos de A.*

Por lo tanto,

$$\begin{aligned}
b \text{ es máximo de } A &\iff (b \in A) \wedge (b \in M_a, \text{ para todos y cada uno de los } a \text{ de } A) \\
&\iff (b \in A) \wedge \left(b \in \bigcap_{a \in A} M_a \right) \\
&\iff (b \in A) \wedge (b \in (M_{216} \cap M_{108} \cap M_{72} \cap M_{54} \cap M_{36} \cap M_{24} \cap M_{18} \cap M_{12} \cap M_6)) \\
&\qquad \left\{ \begin{array}{l} \text{Por (6.6), } M_{216} \subseteq M_{108} \subseteq M_{54} \subseteq M_{18} \subseteq M_6, \text{ luego} \\ M_{216} \cap M_{108} \cap M_{54} \cap M_{18} \cap M_6 = M_{216} \end{array} \right\} \\
&\iff (b \in A) \wedge (b \in (M_{216} \cap M_{72} \cap M_{36} \cap M_{24} \cap M_{18} \cap M_{12})) \\
&\qquad \left\{ \begin{array}{l} \text{Por (6.6), } M_{216} \subseteq M_{72} \subseteq M_{36} \subseteq M_{18}, \text{ luego} \\ M_{216} \cap M_{72} \cap M_{36} \cap M_{18} = M_{216} \end{array} \right\} \\
&\iff (b \in A) \wedge (M_{216} \cap M_{24} \cap M_{12}) \\
&\qquad \left\{ \begin{array}{l} \text{Por (6.6), } M_{216} \subseteq M_{24} \subseteq M_{12}, \text{ luego} \\ M_{216} \cap M_{24} \cap M_{12} = M_{216} \end{array} \right\} \\
&\iff (b \in A) \wedge (M_{216}) \\
&\iff b \in (A \cap M_{216}) \\
&\iff b \in (\{6, 12, 18, 24, 36, 54, 72, 108, 216\} \cap \{216q; q \in \mathbb{Z}^+\}) \\
&\iff b \in \{216\} \\
&\iff b = 216
\end{aligned}$$

Concluyendo, el máximo del conjunto A ordenado por la relación de divisibilidad es el 216. Lo notaremos,

$$\text{Máx}\,(A) = 216$$

■

6.4.6 Unicidad del Máximo y el Mínimo

Todo conjunto ordenado finito posee, a lo sumo, un elemento máximo y uno mínimo.

Demostración

En efecto, supongamos que un conjunto ordenado $\{A, \preccurlyeq\}$ tiene dos elementos m_1 y m_2 que son máximos, entonces

$$\left.\begin{array}{l} m_1,\ \text{máximo} \\ m_2 \in A \end{array}\right\} \Longrightarrow m_2 \preccurlyeq m_1$$

Por otra parte,

$$\left.\begin{array}{l} m_2,\ \text{máximo} \\ m_1 \in A \end{array}\right\} \Longrightarrow m_1 \preccurlyeq m_2$$

luego por la antisimetría,

$$m_1 = m_2$$

y el máximo, si existe, es único.

De una forma similar se prueba que el mínimo de un conjunto ordenado, si existe, es único.

■

6.4.7 Cota Inferior

El elemento a de A se dice que es cota inferior de B, subconjunto de A, si es anterior a todos los elementos de B; es decir,

$$a \text{ es cota inferior de } B \subseteq A \Longleftrightarrow \forall x, (x \in B \longrightarrow a \preccurlyeq x)$$

■

Ejemplo 6.16

En el conjunto $\mathbb{Z}^+$ de los enteros positivos se considera la relación de divisibilidad, es decir, dados dos enteros positivos cualesquiera n_1 y n_2,

$$n_1 \preccurlyeq n_2 \longleftrightarrow n_1 \text{ es divisor de } n_2$$

Obtener, de forma razonada, las cotas inferiores del conjunto

$$A = \{12, 18, 24, 36, 54, 72, 108\}$$

ordenado por la relación anterior.

Solución

La relación está definida en el conjunto de los enteros positivos, $\mathbb{Z}^+$, en la forma siguiente:

$$\forall n_1, n_2, (n_1 \preccurlyeq n_2 \longleftrightarrow n_1 \text{ es divisor de } n_2)$$

Si llamamos D_{n_2} al conjunto formado por todos los divisores de n_2, sería lo mismo que escribir,

$$\forall n_1, n_2, (n_1 \preccurlyeq n_2 \longleftrightarrow n_1 \in D_{n_2}) .$$

Por ejemplo, los divisores de 12 son 1, 2, 3, 4, 6 y 12, luego,

$$D_{12} = \{1, 2, 3, 4, 6, 12\} .$$

Entonces,

$$4 \in D_{12}, \text{ por lo tanto, } 4 \preccurlyeq 12$$

$$6 \in D_{12}, \text{ por lo tanto, } 6 \preccurlyeq 12$$

$$12 \in D_{12}, \text{ por lo tanto, } 12 \preccurlyeq 12$$

Calcularemos, ahora, las cotas inferiores de A.

Lo primero que haremos es "adecuar" la definición de cota inferior a nuestra relación, es decir a la relación de divisibilidad.

Pues bien, sea b cualquier entero positivo. Entonces, según la definición de cota inferior, (6.4.7),

> *b es cota inferior de A en $\mathbb{Z}^+$ respecto de la relación $\preccurlyeq$, si b es anterior a todos los elementos de A.*

y bastaría con que b fuera anterior a los elementos minimales de A ya que, por definición de minimal, todos los demás elementos de A serán posteriores a algún minimal, o sea,

> *b es cota inferior de A en $\mathbb{Z}^+$ respecto de la relación $\preccurlyeq$, si b es anterior a los elementos minimales de A.*

lo cual "traducido" a nuestra relación querrá decir,

> *b es cota inferior de A en $\mathbb{Z}^+$ respecto de la relación de divisibilidad, si b es divisor de los elementos minimales de A.*

Como los minimales del conjunto A son el 12 y el 18,

> *b es cota inferior de A en $\mathbb{Z}^+$ respecto de la relación de divisibilidad, si b es divisor de 12 y 18.*

Sea, pues, $C_{\inf}(A)$ el conjunto formado por todas las cotas inferiores de A y sea b cualquier entero positivo. Entonces,

$$
\begin{aligned}
b \in C_{\inf}(A) &\iff \begin{cases} b \text{ es divisor de } 12 \\ \text{y} \\ b \text{ es divisor de } 18 \end{cases} \\
&\iff \begin{cases} b \text{ es divisor de } 2^2 \cdot 3 \\ \text{y} \\ b \text{ es divisor de } 2 \cdot 3^2 \end{cases} \\
&\iff b = 2^{\alpha_1} \cdot 3^{\alpha_2} : \begin{cases} 0 \leqslant \alpha_1 \leqslant \min\{1,2\} \\ \text{y} \\ 0 \leqslant \alpha_2 \leqslant \min\{1,2\} \end{cases} \\
&\iff b = 2^{\alpha_1} \cdot 3^{\alpha_2} : \begin{cases} 0 \leqslant \alpha_1 \leqslant 1 \\ \text{y} \\ 0 \leqslant \alpha_2 \leqslant 1 \end{cases} \\
&\iff b = 2^{\alpha_1} \cdot 3^{\alpha_2} : \begin{cases} \alpha_1 = 0 \text{ y } \alpha_2 = 0 \\ \text{o} \\ \alpha_1 = 1 \text{ y } \alpha_2 = 0 \\ \text{o} \\ \alpha_1 = 0 \text{ y } \alpha_2 = 1 \\ \text{o} \\ \alpha_1 = 1 \text{ y } \alpha_2 = 1 \end{cases} \\
&\iff \begin{cases} b = 2^0 \cdot 3^0 \\ \text{o} \\ b = 2^1 \cdot 3^0 \\ \text{o} \\ b = 2^0 \cdot 3^1 \\ \text{o} \\ b = 2^1 \cdot 3^1 \end{cases} \\
&\iff \begin{cases} b = 1 \\ \text{o} \\ b = 2 \\ \text{o} \\ b = 3 \\ \text{o} \\ b = 6 \end{cases} \\
&\iff b \in \{1,2,3,6\}
\end{aligned}
$$

Como b es cualquiera, tendremos que el conjunto de las cotas inferiores del conjunto A ordenado por la

relación de divisibilidad es

$$C_{\inf}(A) = \{1, 2, 3, 6\}$$

■

6.4.8 Cota Superior

El elemento a de A se dice que es cota superior de B, subconjunto de A, si es posterior a todos los elementos de B; es decir,

$$a \text{ es cota superior de } B \subseteq A \Longleftrightarrow \forall x, (x \in B \longrightarrow a \succcurlyeq x)$$

■

Ejemplo 6.17

En el conjunto $\mathbb{Z}^+$ de los enteros positivos se considera la relación de divisibilidad, es decir, dados dos enteros positivos cualesquiera n_1 y n_2,

$$n_1 \preccurlyeq n_2 \longleftrightarrow n_1 \text{ es divisor de } n_2$$

Obtener, de forma razonada, las cotas superiores del conjunto

$$A = \{12, 18, 24, 36, 54, 72, 108\}$$

ordenado por la relación anterior.

Solución

La relación está definida en el conjunto de los enteros positivos, $\mathbb{Z}^+$, en la forma siguiente:

$$\forall n_1, n_2, (n_1 \preccurlyeq n_2 \longleftrightarrow n_1 \text{ es divisor de } n_2)$$

y si tenemos en cuenta que

$$n_1 \text{ es divisor de } n_2 \longleftrightarrow n_2 \text{ es múltiplo de } n_1$$

podemos escribir,

$$\forall n_1, n_2, (n_1 \preccurlyeq n_2 \longleftrightarrow n_2 \text{ es múltiplo de } n_1)$$

lo cual equivale a decir,

$$\forall n_1, n_2, (n_2 \succcurlyeq n_1 \longleftrightarrow n_2 \text{ es múltiplo de } n_1)$$

es decir, n_2 es posterior a n_1 es equivalente a decir que n_2 es múltiplo de n_1.

Si llamamos M_{n_1} al conjunto formado por todos los múltiplos de n_1, sería lo mismo que escribir,

$$\forall n_1, n_2, (n_2 \succcurlyeq n_1 \longleftrightarrow n_2 \in M_{n_1})$$

siendo, naturalmente, $M_{n_1} = \{n : n = n_1 q; q \in \mathbb{Z}^+\}$.

Calcularemos, ahora, las cotas superiores de A.

Lo primero que haremos es "adecuar" la definición de cota superior a nuestra relación, es decir a la relación de divisibilidad.

Pues bien, sea b cualquier entero positivo. Entonces, según la definición de cota inferior, (6.4.8),

> *b es cota superior de A en $\mathbb{Z}^+$ respecto de la relación $\preccurlyeq$, si b es posterior a todos los elementos de A.*

y bastaría con que b fuera posterior a los elementos maximales de A ya que, por definición de maximal, todos los demás elementos de A serán anteriores, o sea,

> *b es cota superior de A en $\mathbb{Z}^+$ respecto de la relación $\preccurlyeq$, si b es posterior a los elementos maximales de A.*

lo cual "traducido" a nuestra relación querrá decir,

> *b es cota superior de A en $\mathbb{Z}^+$ respecto de la relación de divisibilidad, si b es múltiplo de todos los elementos de A.*

como lo maximales de nuestro conjunto son el 72 y el 108,

> *b es cota superior de A en $\mathbb{Z}^+$ respecto de la relación de divisibilidad, si b es múltiplo de* 72 *y* 108.

Sea, pues, $C_{\sup}(A)$ el conjunto formado por las cotas superiores de A en $\mathbb{Z}^+$ y sea b cualquier entero positivo. Entonces,

$$
\begin{aligned}
b \in C_{\sup}(A) &\iff \begin{cases} b \text{ es múltiplo de } 72 \\ \text{y} \\ b \text{ es múltiplo de } 108 \end{cases} \\
&\iff \begin{cases} b \text{ es múltiplo de } 2^3 \cdot 3^2 \\ \text{y} \\ b \text{ es múltiplo de } 2^2 \cdot 3^3 \end{cases} \\
&\iff \exists q_1 \in \mathbb{Z}^+ : b = 2^{\alpha_1} \cdot 3^{\alpha_2} \cdot q_1 \begin{cases} \alpha_1 \geqslant \max\{2,3\} \\ \text{y} \\ \alpha_2 \geqslant \max\{2,3\} \end{cases} \\
&\iff \exists q_1 \in \mathbb{Z}^+ : b = 2^{\alpha_1} \cdot 3^{\alpha_2} \cdot q_1,\ \alpha_1 \geqslant 3,\ \alpha_2 \geqslant 3 \\
&\iff \exists q_1 \in \mathbb{Z}^+ : b = 2^3 \cdot 2^{\alpha_1 - 3} \cdot 3^3 \cdot 3^{\alpha_2 - 3} \cdot q_1,\ \alpha_1 \geqslant 3,\ \alpha_2 \geqslant 3 \\
&\quad \left\{\text{Tomando } q = 2^{\alpha_1 - 3} \cdot 3^{\alpha_2 - 3} \cdot q_1\right\} \\
&\iff \exists q \in \mathbb{Z}^+ : b = 216 \cdot q \\
&\iff b \in \{n : n = 216q,\ q \in \mathbb{Z}^+\}
\end{aligned}
$$

Consecuentemente, y al ser b cualquier entero positivo, las cotas superiores del conjunto A ordenado por la relación de divisibilidad serán todos los múltiplos de 216. Lo notaremos,

$$C_{\sup}(A) = \left\{n : n = 216q, q \in \mathbb{Z}^+\right\}$$

o simplemente,

$$C_{\sup}(A) = M_{216}$$

■

6.4.9 Conjunto Acotado

Cuando un conjunto tiene cota inferior se dice que está acotado inferiormente y acotado superiormente cuando tiene cota superior. Cuando un conjunto posee ambas cotas se dice que está acotado.

■

6.4.10 Ínfimo

Sea B un subconjunto de A. Llamaremos ínfimo de B a la cota inferior máxima de B en A.

Si llamamos $C_{\inf}(B)$ al conjunto de las cotas inferiores de B en A, tendremos:

$$\begin{aligned} a \text{ es el ínfimo de } B \text{ en } A &\iff a \text{ es el máximo del conjunto de las cotas inferiores de } B \text{ en } A \\ &\iff (a \in C_{\inf}(B)) \wedge (\forall x, (x \in C_{\inf}(B) \longrightarrow a \succcurlyeq x)) \end{aligned}$$

■

6.4.11 Supremo

Sea B un subconjunto de A. Llamaremos supremo de B a la cota superior mínima de B en A.

Si llamamos $C_{\sup}(B)$ al conjunto de las cotas superiores de B en A, tendremos:

$$\begin{aligned} a \text{ es el supremo de } B \text{ en } A &\iff a \text{ es el mínimo del conjunto de las cotas superiores de } B \text{ en } A \\ &\iff (a \in C_{\sup}(B)) \wedge (\forall x, (x \in C_{\sup}(B) \longrightarrow a \preccurlyeq x)) \end{aligned}$$

■

Ejemplo 6.18

En el conjunto $\mathbb{Z}^+$ de los enteros positivos se considera la relación de divisibilidad, es decir, dados dos enteros positivos cualesquiera n_1 y n_2,

$$n_1 \preccurlyeq n_2 \longleftrightarrow n_1 \text{ es divisor de } n_2$$

Obtener, de forma razonada, el ínfimo y el supremo del conjunto

$$A = \{12, 18, 24, 36, 54, 72, 108\}$$

ordenado por la relación anterior.

Solución

⁎ Ínfimo. Particularizamos, primero, la definición de ínfimo, (6.4.10), a nuestra relación.

En efecto, sea b cualquier entero positivo.

$$\begin{aligned} b \text{ es el ínfimo de } A \text{ en } \mathbb{Z}^+ &\iff b \text{ es el máximo del conjunto de las cotas inferiores de } A \text{ en } \mathbb{Z}^+ \\ &\iff (b \in C_{\inf}(A)) \wedge (\forall n, (n \in C_{\inf}(A) \longrightarrow b \succcurlyeq n)) \\ &\iff (b \in C_{\inf}(A)) \wedge (b \text{ es múltiplo de todos los elementos de } C_{\inf}(A)) \\ &\iff (b \in C_{\inf}(A)) \wedge \left(b \in \bigcap_{a \in C_{\inf}(A)} M_a \right) \end{aligned}$$

Pues bien, como en el ejemplo 6.16 hemos obtenido que las cotas inferiores de A son los divisores de 6, es decir,

$$C_{\inf}(A) = D_6$$

tendremos que

$$\begin{aligned} b \text{ es el ínfimo de } A \text{ en } \mathbb{Z}^+ &\iff (b \in C_{\inf}(A)) \wedge \left(b \in \bigcap_{a \in C_{\inf}(A)} M_a \right) \\ &\iff (b \in D_6) \wedge \left(b \in \bigcap_{a \in D_6} M_a \right) \\ &\iff b \in (D_6 \cap (M_1 \cap M_2 \cap M_3 \cap M_6)) \\ &\quad \{M_6 \subseteq M_3 \subseteq M_1 \Longrightarrow M_1 \cap M_3 \cap M_6 = M_6\} \\ &\iff b \in (D_6 \cap (M_2 \cap M_6)) \\ &\quad \{M_6 \subseteq M_2 \Longrightarrow M_2 \cap M_6 = M_6\} \\ &\iff b \in (D_6 \cap M_6) \\ &\iff b \in \{6\} \\ &\iff b = 6 \end{aligned}$$

Por lo tanto, el ínfimo del conjunto A ordenado por la relación de divisibilidad, será el 6. Lo notaremos,

$$\text{Ínf}(A) = 6$$

⁎ Supremo. Particularizamos, primero, la definición de supremo, (6.4.11), a nuestra relación.

En efecto, sea b cualquier entero positivo.

$$\begin{aligned} b \text{ es el supremo de } A \text{ en } \mathbb{Z}^+ &\iff b \text{ es el mínimo del conjunto de las cotas superiores de } A \text{ en } \mathbb{Z}^+ \\ &\iff (b \in C_{\sup}(A)) \wedge (\forall n, (n \in C_{\sup}(A) \Longrightarrow b \preccurlyeq n)) \\ &\iff (b \in C_{\sup}(A)) \wedge (b \text{ es divisor de todos los elementos de } C_{\sup}(A)) \\ &\iff (b \in C_{\sup}(A)) \wedge \left(b \in \bigcap_{a \in C_{\sup}(A)} D_a \right) \end{aligned}$$

Pues bien, como en el ejemplo 6.17 hemos obtenido que las cotas superiores de A son los múltiplos de 216, es decir,

$$C_{\sup}(A) = M_{216}$$

tendremos que

$$\begin{aligned}
b \text{ es el supremo de } B \text{ en } A &\iff (b \in C_{\sup}(A)) \wedge \left(b \in \bigcap_{a \in C_{\sup}(A)} D_a \right) \\
&\iff (b \in M_{216}) \wedge \left(b \in \bigcap_{a \in M_{216}} D_a \right) \\
&\iff (b \in M_{216}) \wedge \left(b \in \bigcap_{q \in \mathbb{Z}^+} D_{216q} \right) \\
&\iff (b \in M_{216}) \wedge (b \in D_{216}) \\
&\iff b \in (M_{216} \cap D_{216}) \\
&\iff b \in \{216\} \\
&\iff b = 216
\end{aligned}$$

Por lo tanto, el supremo del conjunto A ordenado por la relación de divisibilidad, será el 216. Lo notaremos,

$$\operatorname{Sup}(A) = 216$$

■

6.4.12 Unicidad del Ínfimo y el Supremo

Todo conjunto ordenado finito posee, a lo sumo, un ínfimo y un supremo.

Demostración

En efecto, supongamos que un conjunto ordenado $(A, \preccurlyeq)$ tiene dos elementos s_1 y s_2 que son supremos, entonces

$$\left.\begin{array}{l} s_1, \text{ supremo} \\ \text{y} \\ s_2 \in A \end{array}\right\} \Longrightarrow s_2 \preccurlyeq s_1$$

Por otra parte,

$$\left.\begin{array}{l} s_2, \text{ supremo} \\ \text{y} \\ s_1 \in A \end{array}\right\} \Longrightarrow s_1 \preccurlyeq s_2$$

luego por la antisimetría,

$$s_1 = s_2$$

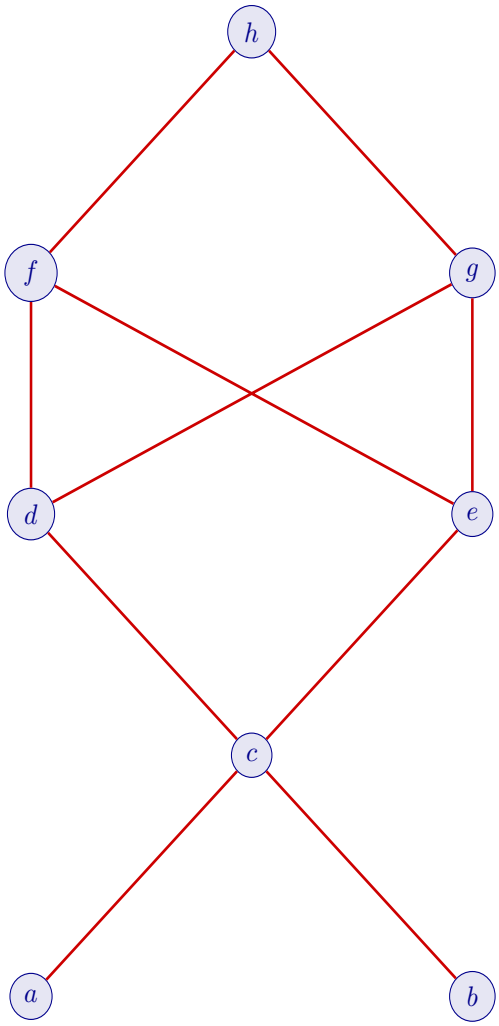
y el supremo, si existe, es único.

De una forma similar se prueba que el ínfimo de un conjunto ordenado, si existe, es único.

■

Ejemplo 6.19

Sea $A = \{a, b, c, d, e, f, g, h\}$ y la figura, el diagrama de Hasse del conjunto ordenado $(A, \preccurlyeq)$. Se pide:



(a) Encontrar maximales, minimales, máximo y mínimo del conjunto A.

(b) Encontrar cotas superiores, inferiores, supremo e ínfimo del subconjunto $B_1 = \{a, b\}$ de A.

(c) Idem al apartado anterior para el subconjunto de A, $B_2 = \{c, d, e\}$.

Solución

(a) $A = \{a, b, c, d, e, f, g, h\}$

- Hay un único maximal que es h ya que no hay en A ningún elemento que sea posterior a él.
- Los elementos a y b son, ambos, minimales porque no hay en A elemento alguno que sea anterior a ellos.
- El máximo es h ya que es posterior a todos los elementos de A.
- No hay elemento mínimo ya que no hay en A ningún elemento que sea anterior a todos los demás.

(b) $B_1 = \{a, b\}$

- ◎ Las cotas superiores son c, d, e, f, g y h ya que todos ellos son posteriores a todos los elementos de B_1.
- ◎ El supremo de B_1 es c ya que
  1. c es cota superior de B_1 en A.
  2. c es el mínimo del conjunto de las cotas superiores.
- ◎ No tiene cotas inferiores ya que no hay en A ningún elemento que sea anterior a todos los elementos de B_1. Al no haber cotas inferiores no hay ínfimo.

(c) $B_2 = \{c, d, e\}$

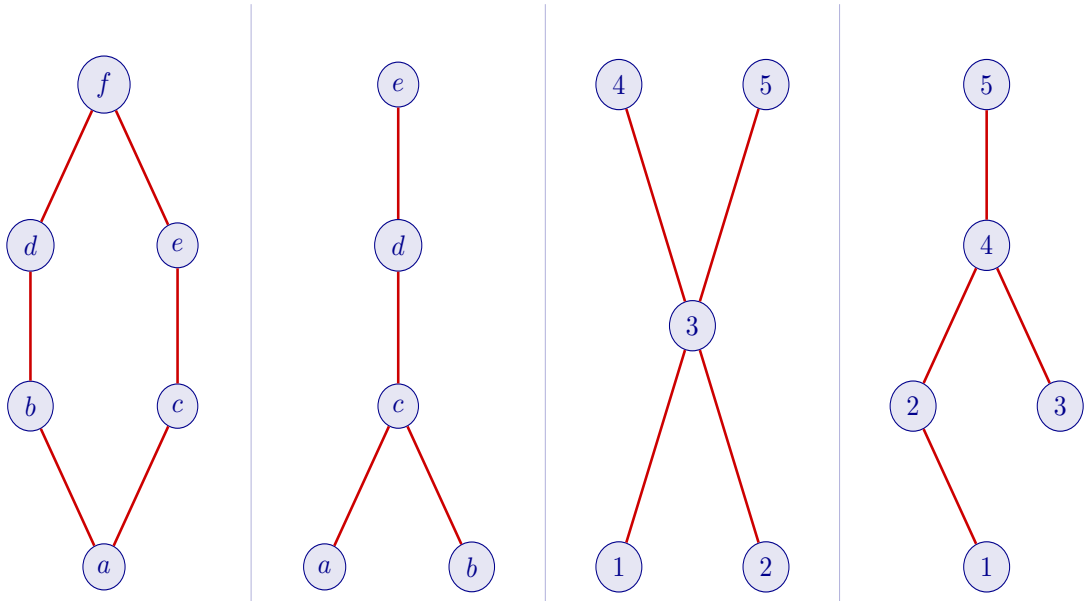
- ⊛ Las cotas superiores son f, g y h porque los tres son posteriores a todos los elementos de B_2.
- ⊛ B_2 no tiene supremo ya que el conjunto de las cotas superiores $\{f, g, h\}$ no tiene mínimo.
- ⊛ Las cotas inferiores son a, b y c ya que estos tres elementos son anteriores a todos los elementos de de B_2.
- ⊛ El ínfimo de B_1 es c ya que
  1. c es cota superior de B_2 en A.
  2. c es el máximo del conjunto de las cotas inferiores.

Obsérvese que un subconjunto B de un conjunto ordenado A puede tener o no cotas superiores o inferiores en A. Además una cota superior o inferior de B podrá o no pertenecer a B.

■

Ejemplo 6.20

Determinar maximales, minimales, máximo y mínimo de los conjuntos ordenados cuyo diagrama de Hasse es el siguiente:



(a) *(b)* *(c)* *(d)*

Solución

(a)
- ◊ El maximal es f ya que no hay ningún elemento que sea estrictamente posterior a él.
- ◊ El minimal es a ya que no hay ningún elemento que sea estrictamente anterior a él.
- ◊ El máximo es f ya que es posterior a todos los demás elementos.
- ◊ El mínimo es a ya que es anterior a todos los demás elementos.

(b)
- ⊛ El maximal es e.
- ⊛ Los minimales son a y b.
- ⊛ El máximo es e ya que es posterior a todos los demás elementos.
- ⊛ No existe elemento mínimo ya que no hay en el conjunto ningún elemento que sea anterior a todos los demás.

(c)
- ⋇ Los maximales son 4 y 5 ya que no hay elemento alguno que sea estrictamente posterior a ellos.
- ⋇ Los minimales son 1 y 2 ya que no hay elemento alguno que sea estrictamente anterior a ellos.
- ⋇ No existe elemento máximo ya que no hay en el conjunto ningún elemento que sea posterior a todos los demás.
- ⋇ No existe elemento mínimo ya que no hay en el conjunto ningún elemento que sea anterior a todos los demás.

(d)
- ⊠ El maximal es 5.
- ⊠ Los minimales son 1 y 3 ya que no hay elemento alguno que sea estrictamente anterior a ellos.
- ⊠ El elemento máximo es el 5.
- ⊠ No existe elemento mínimo ya que no hay en el conjunto ningún elemento que sea anterior a todos los demás.

■

Ejemplo 6.21

Encontrar los elementos característicos de los siguientes conjuntos ordenados con la relación "menor o igual".

(a) $A = \{x \in \mathbb{R} : 0 < x < 1\}$.

(b) $A = \{x \in \mathbb{R} : 0 \leqslant x \leqslant 1\}$.

Solución

(a) $A = \{x \in \mathbb{R} : 0 < x < 1\}$.

- ⋇ No hay elemento maximales ya que cualquier número real que elijamos en A siempre está seguido por otro estrictamente mayor que él.
- ⋇ No hay elemento máximo ya que no hay en A ningún número que sea mayor que todos los demás.
- ⋇ No hay elemento minimales ya que cualquier número real que elijamos en A siempre está precedido por otro estrictamente menor que él.
- ⋇ No hay elemento mínimo ya que no hay en A ningún número que sea menor que todos los demás.

⋇ Cotas superiores.
Sea s cualquier número real. Entonces,

$$\begin{aligned} s \text{ es cota superior de } A \text{ en } \mathbb{R} &\iff s \text{ es posterior a todo elemento de } A \\ &\iff x \leqslant s,\ \forall x \in A \\ &\iff 1 \leqslant s \end{aligned}$$

por lo tanto, cotas superiores son todos los números reales del conjunto

$$C_s = \{x \in \mathbb{R} : 1 \leqslant s < +\infty\}$$

⋇ Supremo.
Sea s cualquier número real. Entonces,

$$\begin{aligned} s \text{ es supremo de } A &\iff \begin{cases} 1.\ s \text{ es cota superior de } A \text{ en } \mathbb{R} \\ 2.\ s' \text{ es otra cota superior de } A \Longrightarrow s \leqslant s' \end{cases} \\ &\iff s \text{ es la mínima de las cotas superiores de } A \text{ en } \mathbb{R} \\ &\iff s \text{ es el mínimo del conjunto } C_s \\ &\iff s = 1 \end{aligned}$$

luego el supremo de A es el 1.

⋇ Cotas inferiores.
Sea i cualquier número real. Entonces,

$$\begin{aligned} i \text{ es cota inferior de } A \text{ en } \mathbb{R} &\iff i \text{ es anterior a todo elemento de } A \\ &\iff i \leqslant x,\ \forall x \in A \\ &\iff i \leqslant 0 \end{aligned}$$

por lo tanto, cotas inferiores son todos los números reales del conjunto

$$C_i = \{x \in \mathbb{R} : -\infty < i \leqslant 0\}$$

⋇ Ínfimo.
Sea i cualquier número real. Entonces,

$$\begin{aligned} i \text{ es ínfimo de } A &\iff \begin{cases} 1.\ i \text{ es cota inferior de } A \text{ en } \mathbb{R} \\ 2.\ i' \text{ es otra cota inferior de } A \Longrightarrow i' \leqslant i \end{cases} \\ &\iff i \text{ es la máxima de las cotas inferiores de } A \text{ en } \mathbb{R} \\ &\iff i \text{ es el máximo del conjunto } C_i \\ &\iff i = 0 \end{aligned}$$

luego el ínfimo de A es el 0.

(b) $A = \{x \in \mathbb{R} : 0 \leqslant x \leqslant 1\}$.

⊛ El elemento maximal es el 1 ya que no hay, en A, elemento alguno que sea estrictamente mayor que él.

⊛ El máximo es el 1 ya que es posterior, o sea mayor, a todos los elementos de A.

⊛ El elemento minimal es el 0 ya que no hay, en A, elemento alguno que sea estrictamente menor que él.

⊛ El mínimo es el 0 ya que es anterior, o sea menor, a todos los elementos de A.

⊛ Cotas superiores.

Sea s cualquier número real. Entonces,

$$\begin{aligned} s \text{ es cota superior de } A \text{ en } \mathbb{R} &\iff s \text{ es posterior a todo elemento de } A \\ &\iff x \leqslant s,\ \forall x \in A \\ &\iff 1 \leqslant s \end{aligned}$$

por lo tanto, cotas superiores son todos los números reales del conjunto

$$C_s = \{x \in \mathbb{R} : 1 \leqslant s < +\infty\}$$

⊛ Supremo.

Sea s cualquier número real. Entonces,

$$\begin{aligned} s \text{ es supremo de } A &\iff \begin{cases} 1.\ s \text{ es cota superior de } A \text{ en } \mathbb{R} \\ 2.\ s' \text{ es otra cota superior de } A \Longrightarrow s \leqslant s' \end{cases} \\ &\iff s \text{ es la mínima de las cotas superiores de } A \text{ en } \mathbb{R} \\ &\iff s \text{ es el mínimo del conjunto } C_s \\ &\iff s = 1 \end{aligned}$$

luego el supremo de A es el 1.

⊛ Cotas inferiores.

Sea i cualquier número real. Entonces,

$$\begin{aligned} i \text{ es cota inferior de } A \text{ en } \mathbb{R} &\iff i \text{ es anterior a todo elemento de } A \\ &\iff i \leqslant x,\ \forall x \in A \\ &\iff i \leqslant 0 \end{aligned}$$

por lo tanto, cotas inferiores son todos los números reales del conjunto

$$C_i = \{x \in \mathbb{R} : -\infty < i \leqslant 0\}$$

⊛ Ínfimo.

Sea i cualquier número real. Entonces,

$$\begin{aligned} i \text{ es ínfimo de } A &\iff \begin{cases} 1.\ i \text{ es cota inferior de } A \text{ en } \mathbb{R} \\ 2.\ i' \text{ es otra cota inferior de } A \Longrightarrow i' \leqslant i \end{cases} \\ &\iff i \text{ es la máxima de las cotas inferiores de } A \text{ en } \mathbb{R} \\ &\iff i \text{ es el máximo del conjunto } C_i \\ &\iff i = 0 \end{aligned}$$

luego el ínfimo de A es el 0.

■

Ejemplo 6.22

En el conjunto $\mathbb{Z}^+$ de los enteros positivos se considera la relación de divisibilidad, es decir, dados dos enteros positivos cualesquiera n_1 y n_2,

$$n_1 \preccurlyeq n_2 \Longleftrightarrow n_1 \text{ sea divisor de } n_2.$$

Los elementos característicos del conjunto

$$A = \{12, 18, 24, 36, 54, 72, 108\}$$

ordenado por la relación anterior son:

- *Minimales.* $Min\,(A) = \{12, 18\}$.
- *Maximales.* $Max\,(A) = \{72, 108\}$.
- *Cotas inferiores.* $C_{\text{inf}}\,(A) = \{1, 2, 3, 6\}$.
- *Cotas superiores.* $C_{\text{sup}}\,(A) = \{216q, q \in \mathbb{Z}^+\}$.
- *Ínfimo.* $Ínf(A) = 6$.
- *Supremo.* $Sup\,(A) = 216$.

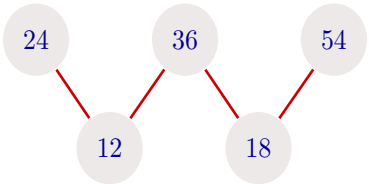
Hacer, de forma razonada, un diagrama de Hasse que represente la ordenación del conjunto anterior.

Solución

Comenzaremos el diagrama situando en un primer nivel a los minimales del conjunto, 12 y 18.

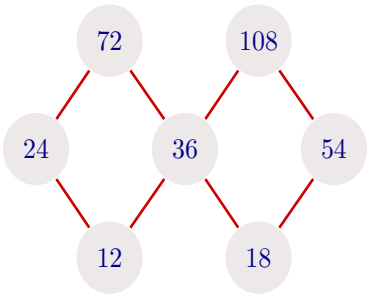
Situaremos ahora los elementos posteriores a los minimales.

- Inmediatamente posteriores al 12. Serán los primeros múltiplos de 12, es decir, $24 = 12 \cdot 2$ y $36 = 12 \cdot 3$.
- Inmediatamente posteriores al 18. Serán los primeros múltiplos de 18, es decir, $36 = 18 \cdot 2$ y $54 = 18 \cdot 3$.

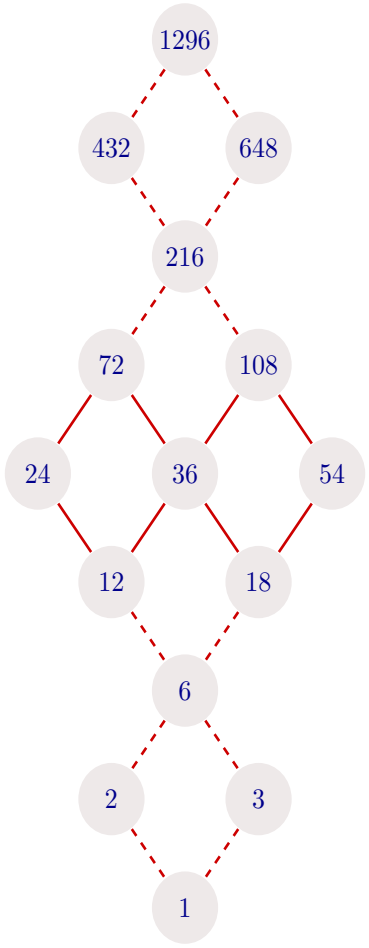


Ahora sólo quedan por situar los maximales.

- Inmediatamente posterior al 24. Será el único múltiplo de 24, es decir, $72 = 24 \cdot 3$.
- Inmediatamente posteriores al 36. Serán los múltiplos de 36, es decir, $72 = 36 \cdot 2$ y $108 = 36 \cdot 3$.
- Inmediatamente posterior al 54. Será el único múltiplo de 54, es decir, $108 = 54 \cdot 2$.



Finalmente, si queremos completar el diagrama podemos añadir las cotas inferiores, algunas cotas superiores, el ínfimo y el supremo.



■

Lección 7

Relaciones de Equivalencia

La verdad no es un objeto que se encuentre al cabo de una cadena lógica rígida; tampoco está indeterminada en todas las direcciones del discurso. En una región limitada por contornos excepcionales: descubrir estos contornos es iluminar esa región, es explorar lo posible y precisar lo probable, es aplicar a las cosas la potencia de la claridad y de orden del espíritu; en una palabra es comprender

Jean Ullmo

7.1 Generalidades

Este tipo de relaciones binarias juegan un papel importante en todas las ciencias porque permiten *clasificar* los elementos del conjunto en el que están definidas.

Muchas veces trataremos a los elementos de un conjunto más por sus propiedades que como objetos individuales. En tales situaciones, podremos ignorar todas las propiedades que no sean de interés y tratar elementos diferentes como "equivalentes" o indistinguibles, a menos que puedan diferenciarse utilizando únicamente las propiedades que nos interesen.

La noción de "equivalencia" tiene tres características principales:

(i) Todo elemento es equivalente a sí mismo. (*Reflexividad*).

(ii) Si a es equivalente a b, entonces b es equivalente a a. (*Simetría*).

(iii) Si a es equivalente a b y b es equivalente a c, entonces a es equivalente a c. (*Transitividad*).

Estas propiedades son la base para una clase importante de relaciones binarias sobre un conjunto.

7.1.1 Definición

Una relación binaria $\mathscr{R}$ definida sobre un conjunto A se dice que es de equivalencia cuando es reflexiva, simétrica y transitiva.

Ejemplo 7.1

Sea $A = \{1, 2, 3, 4\}$ *y*

$$\mathscr{R} = \{(1,1), (1,2), (2,1), (2,2), (3,4), (4,3), (3,3), (4,4)\}.$$

Ver si $\mathscr{R}$ *es de equivalencia.*

Solución

Reflexividad. En efecto,

$$(1,1) \in \mathscr{R},\ (2,2) \in \mathscr{R},\ (3,3) \in \mathscr{R} \text{ y } (4,4) \in \mathscr{R}$$

luego,

$$\forall x\,(x \in A \longrightarrow x\mathscr{R}x)$$

es decir, $\mathscr{R}$ es reflexiva.

Simetría. En efecto,

$$(1,2) \in \mathscr{R} \text{ y } (2,1) \in \mathscr{R}$$

$$(3,4) \in \mathscr{R} \text{ y } (4,3) \in \mathscr{R}$$

luego,

$$\forall x, y\,[(x,y) \in \mathscr{R} \longrightarrow (y,x) \in \mathscr{R}]$$

es decir, la relación propuesta es simétrica.

Transitividad. En efecto,

$$\begin{aligned}
(1,1) \in \mathscr{R} \text{ y } (1,2) \in \mathscr{R} &\implies (1,2) \in \mathscr{R}\\
(1,2) \in \mathscr{R} \text{ y } (2,1) \in \mathscr{R} &\implies (1,1) \in \mathscr{R}\\
(1,2) \in \mathscr{R} \text{ y } (2,2) \in \mathscr{R} &\implies (1,2) \in \mathscr{R}\\
(2,1) \in \mathscr{R} \text{ y } (1,1) \in \mathscr{R} &\implies (2,1) \in \mathscr{R}\\
(2,1) \in \mathscr{R} \text{ y } (1,2) \in \mathscr{R} &\implies (2,2) \in \mathscr{R}\\
(2,2) \in \mathscr{R} \text{ y } (2,1) \in \mathscr{R} &\implies (2,1) \in \mathscr{R}\\
(3,4) \in \mathscr{R} \text{ y } (4,4) \in \mathscr{R} &\implies (3,4) \in \mathscr{R}\\
(3,3) \in \mathscr{R} \text{ y } (3,4) \in \mathscr{R} &\implies (3,4) \in \mathscr{R}\\
(4,3) \in \mathscr{R} \text{ y } (3,3) \in \mathscr{R} &\implies (4,3) \in \mathscr{R}\\
(4,4) \in \mathscr{R} \text{ y } (4,3) \in \mathscr{R} &\implies (4,3) \in \mathscr{R}
\end{aligned}$$

luego,

$$\forall x, y, z, [(x,y) \in \mathscr{R} \text{ y } (y,z) \in \mathscr{R} \longrightarrow (x,z) \in \mathscr{R}]$$

y la relación es, por tanto, transitiva.

■

Ejemplo 7.2

(a) La relación universal sobre cualquier conjunto A es una relación de equivalencia.

(b) La relación vacía $\emptyset$ *es una relación de equivalencia sobre el conjunto vacío* $\emptyset$*. No es, sin embargo, una relación de equivalencia sobre cualquier conjunto no vacío ya que no es reflexiva.*

(c) La relación de igualdad sobre cualquier conjunto es una relación de equivalencia.

7.1.2 Digrafo asociado a una Relación de Equivalencia

El digrafo asociado a una relación de equivalencia, $\mathscr{R}$, definida sobre un conjunto A tiene algunas características especiales.

- *Al ser $\mathscr{R}$ una relación reflexiva, todos y cada uno de los elementos del conjunto A está relacionado consigo mismo, es decir,*

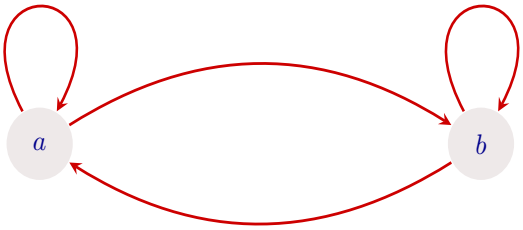
$$\forall a, (a \in A \longrightarrow a \mathscr{R} a)$$

y esto significa que en cada vértice del grafo hay un bucle, o sea, si a es cualquiera de A,

- *La simetría de $\mathscr{R}$ implica que dados dos elementos cualesquiera de A, a y b, si a está relacionado con b, entonces b lo está con a, es decir,*

$$\mathscr{R} \text{ es simétrica} \Longleftrightarrow \forall a, b, (a \mathscr{R} b \longrightarrow b \mathscr{R} a)$$

lo cual significa que si existe un arco desde a hasta b, también ha de existir un arco desde b hasta a.



Utilizando el contrarrecíproco también podemos definir la simetría de la forma siguiente:

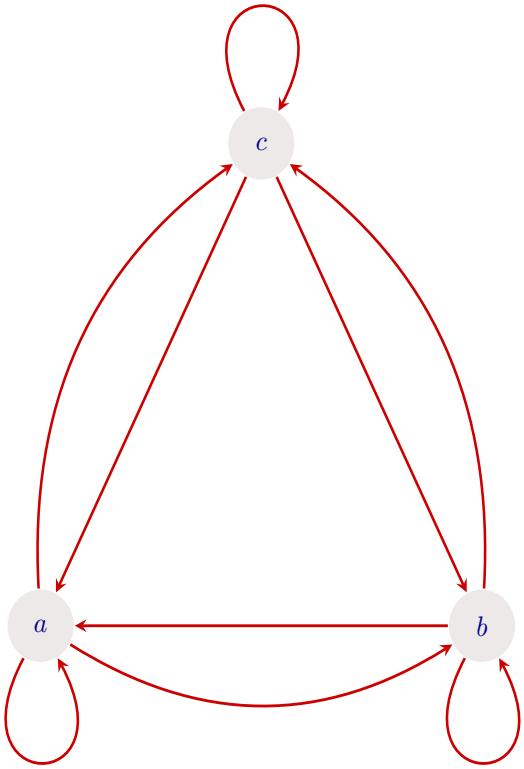
$$\mathscr{R} \text{ es simétrica} \Longleftrightarrow \forall a, b, (b \not\mathscr{R} a \longrightarrow a \not\mathscr{R} b)$$

y esto quiere decir que si no hay un arco entre b y a, tampoco debe haberlo entre a y b.

- *La transitividad de $\mathscr{R}$ significa que dados a, b y c cualesquiera de A si a está relacionado con b y b, a su vez, lo está con c, entonces a ha de estar relacionado con c, es decir,*

$$\mathscr{R} \text{ es transitiva} \Longleftrightarrow \forall a, b, c, (a \mathscr{R} b \text{ y } b \mathscr{R} c \longrightarrow a \mathscr{R} c)$$

lo cual quiere decir si existe un arco desde a hasta b y otro desde b hasta c, entonces tiene que haber un arco desde a hasta c.



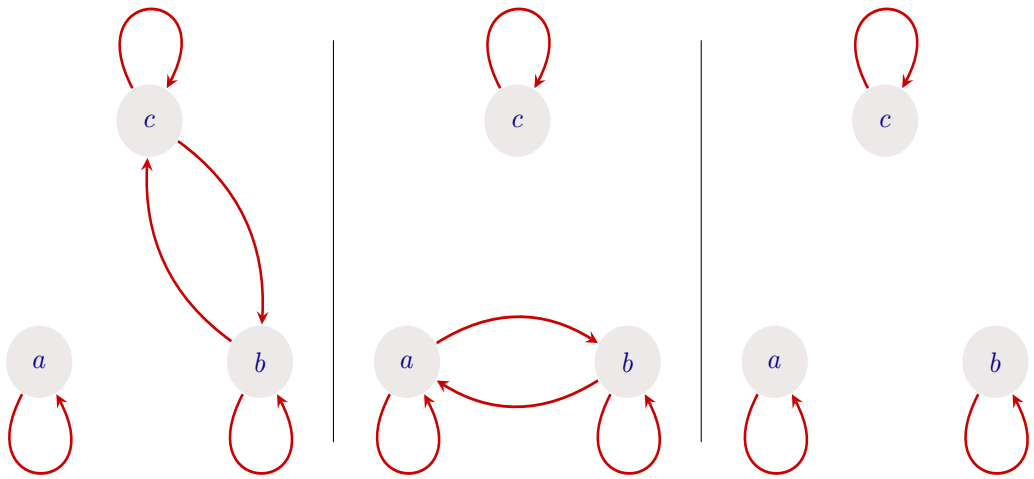
Utilizando el contrarrecíproco podemos definir, también, la transitividad en la siguiente forma:

$$\mathscr{R} \text{ es transitiva} \iff \forall a,b,c,(a\not\mathscr{R}\, c \Longrightarrow a\not\mathscr{R}\, b \text{ ó } b\not\mathscr{R}\, c)$$

$$\iff \forall a,b,c, a\not\mathscr{R}\, c \Longrightarrow \begin{cases} a\not\mathscr{R}\, b \text{ y } b\mathscr{R} c \\ \text{ó} \\ a\mathscr{R} b \text{ y } b\not\mathscr{R}\, c \\ \text{ó} \\ a\not\mathscr{R}\, b \text{ y } b\not\mathscr{R}\, c \end{cases}$$

lo cual significa que si no hay un arco entre a y c, entonces puede ocurrir una de las siguientes opciones:

- *no hay arco entre a y b y si lo hay entre b y c.*
- *Hay un arco entre a y b, pero no lo hay entre b y c.*
- *No hay arco entre a y b y tampoco lo hay entre b y c.*



7.1.3 Matriz asociada a una Relación de Equivalencia

La matriz de incidencia o matriz de ceros y unos asociada a una relación de equivalencia, $\mathscr{R}$, definida sobre un conjunto A, también tiene, al igual que el digrafo, algunas características especiales que la distinguen. Para que sea más fácil de entender supondremos que $A = \{a_1, a_2, \ldots, a_n\}$ y la matriz de la relación es:

$$\mathscr{R} = \begin{pmatrix} r_{11} & r_{12} & r_{13} & \cdots & r_{1n} \\ r_{21} & r_{22} & r_{23} & \cdots & r_{2n} \\ r_{31} & r_{32} & r_{33} & \cdots & r_{3n} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ r_{n1} & r_{n2} & r_{n3} & \cdots & r_{nn} \end{pmatrix}$$

es decir el elemento r_{ij} representa el cruce del elemento a_i de A que está en la fila i y el a_j que está en la columna j. De esta forma,

$$r_{ij} = 1 \Longleftrightarrow a_i \mathscr{R} a_j$$

y

$$r_{ij} = 0 \Longleftrightarrow a_i \not\mathscr{R}\, a_j$$

Pues bien,

- *Reflexividad.*

$$\begin{aligned} \mathscr{R} \text{ es reflexiva} &\iff \forall a_i, (a_i \in A \Longrightarrow a_i \mathscr{R} a_i) \\ &\iff r_{ii} = 1,\ \forall i = 1, 2, \ldots, n \end{aligned}$$

  es decir, todos los elementos de la diagonal principal de la matriz son unos.

- *Simetría.*

$$\begin{aligned} \mathscr{R} \text{ es simétrica} &\iff \forall a_i, a_j, (a_i \mathscr{R} a_j \Longrightarrow a_j \mathscr{R} a_i) \\ &\iff \forall i, j, (r_{ij} = 1 \Longrightarrow r_{ji} = 1) \end{aligned}$$

  o bien, utilizando el contrarrecíproco,

$$\begin{aligned} \mathscr{R} \text{ es simétrica} &\iff \forall a_i, a_j, (a_j \not\mathscr{R}\, a_i \Longrightarrow a_i \not\mathscr{R}\, a_j) \\ &\iff \forall i, j, (r_{ji} = 0 \Longrightarrow r_{ji} = 0) \end{aligned}$$

  o sea, los elementos simétricos respecto a la diagonal principal de la matriz son, ambos, ceros o unos.

⊛ *Transitividad.*

$$\begin{aligned} \mathscr{R} \text{ es transitiva} &\iff \forall a_i, a_j, a_k, (a_i \mathscr{R} a_j \ y \ a_j \mathscr{R} a_k \Longrightarrow a_i \mathscr{R} a_k) \\ &\iff \forall i, j, k, (r_{ij} = 1 \ y \ r_{jk} = 1 \Longrightarrow r_{ik} = 1) \end{aligned}$$

y si utilizamos el contrarrecíproco en la definición de transitividad,

$$\begin{aligned} \mathscr{R} \text{ es transitiva} &\iff \forall a_i, a_j, a_k, (a_i \not\mathscr{R} a_k \Longrightarrow a_i \not\mathscr{R} a_j \ ó \ a_j \not\mathscr{R} a_k) \\ &\iff \forall a_i, a_j, a_k, \ a_i \not\mathscr{R} a_k \Longrightarrow \begin{cases} a_i \not\mathscr{R} a_j \ y \ a_j \mathscr{R} a_k \\ ó \\ a_i \mathscr{R} a_j \ y \ a_j \not\mathscr{R} a_k \\ ó \\ a_i \not\mathscr{R} a_j \ y \ a_j \not\mathscr{R} a_k \end{cases} \\ &\iff \forall i, j, k, \ r_{ik} = 0 \Longrightarrow \begin{cases} r_{ij} = 0 \ y \ r_{jk} = 1 \\ ó \\ r_{ij} = 1 \ y \ r_{jk} = 0 \\ ó \\ r_{ij} = 0 \ y \ r_{jk} = 0 \end{cases} \end{aligned}$$

Ejemplo 7.3

Determinar si la relaciones cuyas matrices se dan son de equivalencia sobre el conjunto $A = \{a, b, c\}$.

(a) $M_{\mathscr{R}_1} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 1 & 1 \end{pmatrix}$

(b) $M_{\mathscr{R}_2} = \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$

Solución

Supongamos que r_{ij} es un elemento cualquiera de la matriz, donde i indica la fila a la que pertenece y j la columna.

(a) Veamos si $\mathscr{R}_1$ cumple las condiciones necesarias para ser de equivalencia.

Reflexividad. Todos los elementos de la diagonal principal son unos, es decir,

$$r_{ii} = 1, \ \forall i = 1, 2, 3$$

por lo tanto, la relación es reflexiva.

Simetría. En efecto,

$$\begin{aligned} r_{12} = 0 \quad \text{y} \quad r_{21} = 0 \\ r_{13} = 0 \quad \text{y} \quad r_{31} = 0 \\ r_{23} = 1 \quad \text{y} \quad r_{32} = 1 \end{aligned}$$

es decir, los elementos de la matriz simétricos respecto de la diagonal principal son iguales, por lo tanto, la relación es simétrica.

Transitividad. En efecto,

$$\begin{aligned} r_{22}=1 \quad \text{y} \quad r_{23}=1 &\implies r_{23}=1 \\ r_{23}=1 \quad \text{y} \quad r_{33}=1 &\implies r_{23}=1 \\ r_{32}=1 \quad \text{y} \quad r_{22}=1 &\implies r_{32}=1 \\ r_{33}=1 \quad \text{y} \quad r_{32}=1 &\implies r_{32}=1 \end{aligned}$$

luego,

$$\text{si } r_{ij}=1 \text{ y } r_{jk}=1, \text{ entonces } r_{ik}=1$$

y

$$r_{12}=0 \implies \begin{cases} r_{11}=1 \quad \text{y} \quad r_{12}=0 \\ r_{12}=0 \quad \text{y} \quad r_{22}=1 \\ r_{13}=0 \quad \text{y} \quad r_{32}=1 \end{cases}$$

$$r_{13}=0 \implies \begin{cases} r_{11}=1 \quad \text{y} \quad r_{13}=0 \\ r_{12}=0 \quad \text{y} \quad r_{23}=1 \\ r_{13}=0 \quad \text{y} \quad r_{33}=1 \end{cases}$$

es decir,

$$\text{si } r_{ik}=0, \text{ entonces } r_{ij}=0 \text{ ó } r_{jk}=0$$

y, consecuentemente, la relación es transitiva.

(b) La relación no es de equivalencia ya que $r_{13}=1$ y $r_{31}=0$, lo cual significa que

$$a\mathscr{R}c \text{ y, sin embargo, } c\not\mathscr{R}\,_2 a$$

es decir, la relación propuesta no es simétrica.

■

7.2 Clases de Equivalencia

7.2.1 Definición

Sea $\mathscr{R}$ una relación de equivalencia definida sobre un conjunto A. Para cada $a \in A$, llamaremos clase de equivalencia de a, al conjunto formado por todos los elementos de A que estén relacionados con él. La notaremos $[a]$, es decir,

$$[a]=\{x \in A : x\mathscr{R}a\}$$

Obsérvese que la clase de equivalencia de un elemento a nunca es vacía, ya que la reflexividad de $\mathscr{R}$ implica que $a \in [a]$.

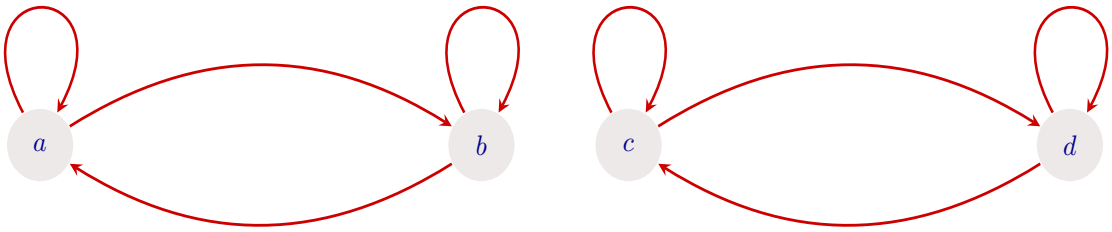
Ejemplo 7.4

Sea $A = \{a, b, c, d\}$ *y* $\mathscr{R}$ *el conjunto*

$$\mathscr{R} = \{(a,a), (a,b), (b,a), (b,b), (c,c), (c,d), (d,c), (d,d)\}$$

Representar el digrafo de $\mathscr{R}$ *y calcular las clases de equivalencia.*

Solución



Las clases de equivalencia son:

$[a] = \{a, b\}$

$[b] = \{a, b\}$

$[c] = \{c, d\}$

$[d] = \{c, d\}$

Obsérvese que $[a] = [b]$ y $[c] = [d]$, es decir, existen sólo dos clases de equivalencia.

■

7.2.2 Lema

Sea $\mathscr{R}$ *una relación de equivalencia sobre el conjunto* A*. Entonces, para cualquier par de elementos* a *y* b *de* A*, se verifica:*

(i) $[a] = [b]$ *si, y sólo si* $a\mathscr{R}b$*.*

(ii) Si $[a] \neq [b]$*, entonces* $[a] \cap [b] = \emptyset$

Demostración

(i) $[a] = [b]$ si, y sólo si $a\mathscr{R}b$.

"Sólo si". En efecto, supongamos que $[a] = [b]$. Como $a \in [a]$ y $[a] = [b]$, entonces $a \in [b]$ de aquí que $a\mathscr{R}b$.

"Si". Supongamos que $a\mathscr{R}b$ y sea x cualquiera de A, entonces

$$\begin{aligned} x \in [a] &\iff x\mathscr{R}a \\ &\implies x\mathscr{R}a \text{ y } a\mathscr{R}b && \{\text{Hipótesis}\} \\ &\implies x\mathscr{R}b && \{\text{Transitividad de } \mathscr{R}\} \\ &\iff x \in [b] \end{aligned}$$

tenemos, pues, que

$$\forall x, (x \in [a] \longrightarrow x \in [b])$$

es decir, $[a] \subseteq [b]$.

Por otra parte,

$$\begin{aligned} x \in [b] &\iff x\mathscr{R}b \\ &\implies x\mathscr{R}a \text{ y } b\mathscr{R}a && \{\text{Hipótesis y Simetría de } \mathscr{R}\} \\ &\implies x\mathscr{R}a && \{\text{Transitividad de } \mathscr{R}\} \\ &\iff x \in [a] \end{aligned}$$

tenemos, pues, que

$$\forall x, (x \in [b] \longrightarrow x \in [a])$$

es decir, $[b] \subseteq [a]$.

De la doble inclusión hallada se sigue el resultado.

(ii) Si $[a] \neq [b]$, entonces $[a] \cap [b] = \emptyset$

Probaremos la contrarrecíproca. Es decir,

$$[a] \cap [b] \neq \emptyset \implies [a] = [b]$$

En efecto,

$$\begin{aligned} [a] \cap [b] \neq \emptyset &\implies \exists x \in A : x \in [a] \text{ y } x \in [b] \\ &\iff \exists x \in A : x\mathscr{R}a \text{ y } x\mathscr{R}b \\ &\implies \exists x \in A : a\mathscr{R}x \text{ y } x\mathscr{R}b && \{\text{Simetría}\} \\ &\implies a\mathscr{R}b && \{\text{Transitividad}\} \\ &\iff [a] = [b] && \{\text{Apartado (i)}\} \end{aligned}$$

Obsérvese que de todo lo anterior se sigue que cualquiera de los elementos que componen una clase de equivalencia puede elegirse como representante de la misma.

■

7.3 Conjunto Cociente

7.3.1 Teorema

Si $\mathscr{R}$ es una relación de equivalencia en un conjunto A, entonces la familia de todas las clases de equivalencia de los elementos de A produce una partición de A.

Demostración

Dado que cada clase de equivalencia es un subconjunto de A, el conjunto de todas ellas será una familia de subconjuntos de A.

Veamos que, en efecto, es una partición de A.

1. $[a] \neq \emptyset,\ \forall a \in A$
   En efecto, como ya dijimos antes, al menos a pertenece a su clase de equivalencia, luego son no vacías.
2. Si $[a] \neq [b]$, entonces $[a] \cap [b] = \emptyset$
   Directamente de (ii) en el lema anterior.
3. $\bigcup_{a \in A} [a] = A$
   Veamos que la unión de todas las clases de equivalencia es el conjunto A. En efecto,
   $$x \in \bigcup_{a \in A} [a] \Longrightarrow \exists a \in A : x \in [a] \overset{[a] \subseteq A}{\Longrightarrow} x \in A$$
   luego,
   $$\forall x, \left(x \in \bigcup_{a \in A} [a] \Longrightarrow x \in A \right)$$
   es decir,
   $$\bigcup_{a \in A} [a] \subseteq A$$
   Por otra parte,
   $$x \in A \Longrightarrow x \in [x] \Longrightarrow x \in \bigcup_{a \in A} [a]$$
   luego,
   $$\forall x, \left(x \in A \Longrightarrow x \in \bigcup_{a \in A} [a] \right)$$
   es decir,
   $$A \subseteq \bigcup_{a \in A} [a]$$
   de la doble inclusión se sigue el resultado,
   $$A = \bigcup_{a \in A} [a]$$

■

7.3.2 Definición

Dada una relación de equivalencia sobre un conjunto A, llamaremos conjunto cociente al formado por todas las clases de equivalencia, lo notaremos por $A/\mathscr{R}$, indicando así que es el conjunto A partido por la relación de equivalencia $\mathscr{R}$.

$$A/\mathscr{R} = \{[a] : a \in A\}$$

■

Ejemplo 7.5

Sea $A = \{a, b, c, d, e, f\}$ *y la relación de equivalencia definida en él,*

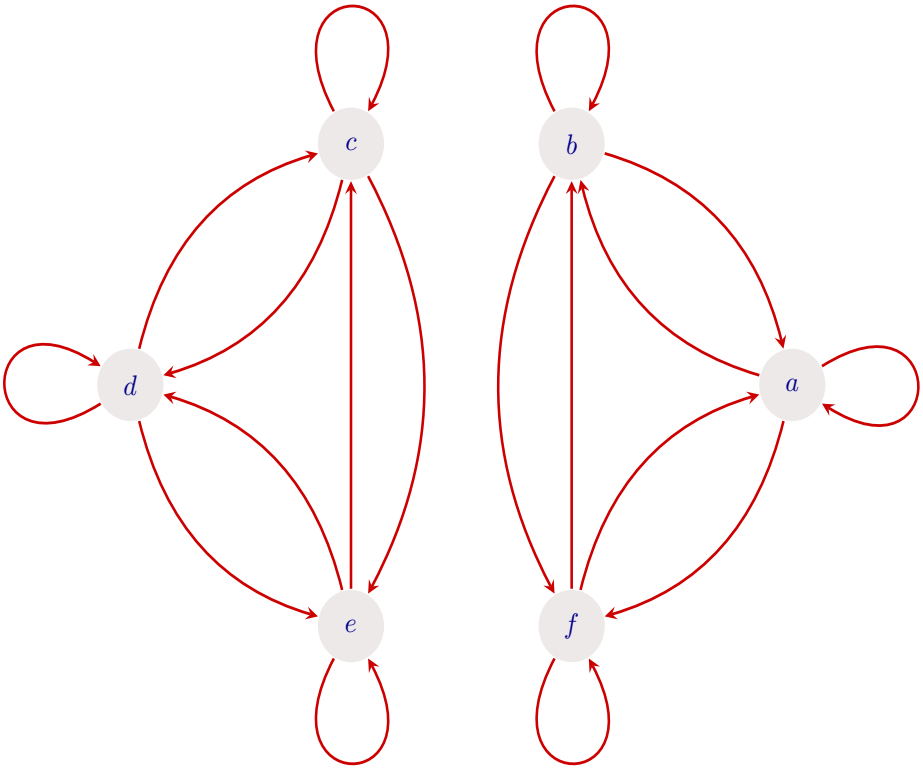
$$\begin{aligned}\mathscr{R} \quad = \quad & \{(a,a),(a,b),(a,f),(b,b),(b,a),(b,f),(c,c),(c,d),(c,e),\\ & (d,c),(d,e),(d,d),(e,c),(e,d),(e,e),(f,a),(f,b),(f,f)\}\end{aligned}$$

(a) Dibujar el grafo dirigido de la relación.

(b) Determinar el conjunto cociente $A/_{\mathscr{R}}$.

Solución

(a) Veamos el grafo dirigido.



(b) Determinemos el conjunto cociente.

Veamos, primero, las clases de equivalencia.

$[a] = \{a, b, f\}$
$[b] = \{a, b, f\}$
$[f] = \{a, b, f\}$
$[c] = \{c, d, e\}$
$[d] = \{c, d, e\}$
$[e] = \{c, d, e\}$

Hay, pues, dos clases de equivalencia. El conjunto cociente será:

$$A/_{\mathscr{R}} = \{[a], [c]\} = \{\{a, b, f\}, \{c, d, e\}\}$$

■

Ejemplo 7.6

En el conjunto universal de los números enteros se define la relación

$$\forall n_1, n_2, (n_1 \mathscr{R} n_2 \text{ si, y sólo si } n_1 - n_2 \text{ es múltiplo de } 3)$$

Se pide:

a) Probar que $\mathscr{R}$ es una relación de equivalencia.

b) Hallar las clases de equivalencia de los elementos del conjunto $A = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$.

c) Obtener el conjunto cociente que la relación $\mathscr{R}$ determina en A.

Solución

Obsérvese que

$$\forall n_1, n_2, (n_1 - n_2 \text{ es múltiplo de } 3 \iff \exists q \in \mathbb{Z} : n_1 - n_2 = 3q)$$

por lo tanto, la relación $\mathscr{R}$ puede escribirse en la forma:

$$\forall n_1, n_2, (n_1 \mathscr{R} n_2 \iff \exists q \in \mathbb{Z} : n_1 - n_2 = 3q)$$

a) Veamos si $\mathscr{R}$ es reflexiva, simétrica y transitiva.

Reflexiva. Sea a cualquier entero. Entonces,

$$a = a \iff a - a = 0 \implies a - a = 3 \cdot 0, 0 \in \mathbb{Z} \iff a \mathscr{R} a$$

luego, $n \mathscr{R} n$, $\forall n$, es decir todos y cada uno de los enteros está relacionado consigo mismo y, consecuentemente, la relación es reflexiva.

Simétrica. Sean a y b dos enteros cualesquiera. Entonces,

$$\begin{aligned} a \mathscr{R} b &\iff \exists q_1 \in \mathbb{Z} : a - b = 3q_1 \\ &\iff \exists q_1 \in \mathbb{Z} : b - a = 3(-q_1) \\ &\iff \exists q \in \mathbb{Z} : b - a = 3q \ \ \{q = -q_1\} \\ &\iff b \mathscr{R} a \end{aligned}$$

De la arbitrariedad en la elección de a y b se sigue que la proposición,

$$\forall n_1, n_2, (n_1 \mathscr{R} n_2 \longrightarrow n_2 \mathscr{R} n_1)$$

es verdadera y, consecuentemente, $\mathscr{R}$ es simétrica.

Transitiva. Sean a, b y c tres enteros cualesquiera. Entonces,

$$\left.\begin{array}{l} a \mathscr{R} b \\ \text{y} \\ b \mathscr{R} c \end{array}\right\} \iff \left\{\begin{array}{l} \exists q_1 \in \mathbb{Z} : a - b = 3q_1 \\ \text{y} \\ \exists q_2 \in \mathbb{Z} : b - c = 3q_2 \end{array}\right.$$

$$\begin{aligned} &\iff \exists q_1, q_2 \in \mathbb{Z} : a - b + b - c = 3q_1 + 3q_2 \\ &\iff \exists q_1, q_2 \in \mathbb{Z} : a - c = 3(q_1 + q_2) \\ &\implies \exists q \in \mathbb{Z} : a - c = 3q \ \ \{q = q_1 + q_2\} \\ &\iff a \mathscr{R} c \end{aligned}$$

Como a, b y c están elegidos arbitrariamente, tendremos que

$$\forall n_1, n_2, n_3, (n_1 \mathscr{R} n_2 \ \wedge \ n_2 \mathscr{R} n_3 \longrightarrow n_1 \mathscr{R} n_3)$$

es verdad y la relación, por tanto, es transitiva.

b) Hallar las clases de equivalencia de los elementos del conjunto $A = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$.

Sea a cualquier número entero. Entonces,

$$\begin{aligned}
a \in [0] &\iff \begin{cases} a \in A \\ \text{y} \\ a \mathscr{R} 0 \end{cases} \\
&\iff \begin{cases} 0 \leqslant a \leqslant 9 \\ \text{y} \\ a - 0 = 3q \end{cases} \\
&\iff \begin{cases} a = 3q \\ \text{y} \\ 0 \leqslant 3q \leqslant 9 \end{cases} \\
&\iff \begin{cases} a = 3q \\ \text{y} \\ 0 \leqslant q \leqslant 3 \end{cases} \\
&\iff a \in \{0, 3, 6, 9\}
\end{aligned}$$

Como a era la cualquiera, hemos probado la veracidad de la proposición

$$\forall n, (n \in [0] \longleftrightarrow n \in \{0, 3, 6, 9\})$$

y, por lo tanto,

$$[0] = \{0, 3, 6, 9\}$$

Por otra parte, por el Lema 7.2.2,

$$\begin{aligned}
3 \in [0] &\iff 3 \mathscr{R} 0 \iff [3] = [0] \\
6 \in [0] &\iff 6 \mathscr{R} 0 \iff [6] = [0] \\
9 \in [0] &\iff 9 \mathscr{R} 0 \iff [9] = [0]
\end{aligned}$$

Calculemos ahora la clase de equivalencia del 1.

$$
\begin{aligned}
a \in [1] &\iff \begin{cases} a \in A \\ \text{y} \\ a \mathscr{R} 1 \end{cases} \\
&\iff \begin{cases} 0 \leqslant a \leqslant 9 \\ \text{y} \\ a - 1 = 3q \end{cases} \\
&\iff \begin{cases} a = 3q + 1 \\ \text{y} \\ 0 \leqslant 3q + 1 \leqslant 9 \end{cases} \\
&\quad \left\{ \begin{aligned} 0 \leqslant 3q + 1 \leqslant 9 &\iff 0 < 3q + 1 < 9 \ \{3q + 1 \neq 0 \text{ y } 3q + 1 \neq 9\} \\ &\iff -1 < 3q < 8 \\ &\iff \frac{-1}{3} < q < \frac{8}{3} \\ &\iff -0,33 < q < 2,66 \\ &\iff 0 \leqslant q \leqslant 2 \ \{q \in \mathbb{Z}\} \end{aligned} \right\} \\
&\iff \begin{cases} a = 3q + 1 \\ \text{y} \\ 0 \leqslant q \leqslant 2, \ q \in \mathbb{Z} \end{cases} \\
&\iff a \in \{1, 4, 7\}
\end{aligned}
$$

Como a era la cualquiera, hemos probado la veracidad de la proposición

$$\forall n, (n \in [1] \longleftrightarrow n \in \{1, 4, 7\})$$

y, por lo tanto,

$$[1] = \{1, 4, 7\}$$

De nuevo, por el Lema 7.2.2,

$$
\begin{aligned}
4 \in [1] &\iff 4 \mathscr{R} 1 \iff [4] = [1] \\
7 \in [1] &\iff 7 \mathscr{R} 1 \iff [7] = [1]
\end{aligned}
$$

Veamos ahora la clase de equivalencia del 2.

$$
\begin{aligned}
a \in [2] &\iff \begin{cases} a \in A \\ \text{y} \\ a \mathscr{R} 2 \end{cases} \\
&\iff \begin{cases} 0 \leqslant a \leqslant 9 \\ \text{y} \\ a - 2 = 3q \end{cases} \\
&\iff \begin{cases} a = 3q + 2 \\ \text{y} \\ 0 \leqslant 3q + 2 \leqslant 9 \end{cases} \\
&\qquad \left\{ \begin{aligned} 0 \leqslant 3q + 2 \leqslant 9 &\iff 0 < 3q + 2 < 9 \ \{3q + 2 \neq 0 \text{ y } 3q + 2 \neq 9\} \\ &\iff -2 < 3q < 7 \\ &\iff \frac{-2}{3} < q < \frac{7}{3} \\ &\iff -0,66 < q < 2,33 \\ &\iff 0 \leqslant q \leqslant 2 \ \{q \in \mathbb{Z}\} \end{aligned} \right\} \\
&\iff \begin{cases} a = 3q + 2 \\ \text{y} \\ 0 \leqslant q \leqslant 2, \ q \in \mathbb{Z} \end{cases} \\
&\iff a \in \{2, 5, 8\}
\end{aligned}
$$

Como a era la cualquiera, hemos probado la veracidad de la proposición

$$\forall n, (n \in [2] \longleftrightarrow n \in \{2, 5, 8\})$$

y, por lo tanto,

$$[2] = \{2, 5, 8\}$$

De nuevo, por el Lema 7.2.2,

$$
\begin{aligned}
5 \in [2] &\iff 5 \mathscr{R} 2 \iff [5] = [2] \\
8 \in [2] &\iff 8 \mathscr{R} 2 \iff [8] = [2]
\end{aligned}
$$

c) Obtengamos ahora el conjunto cociente, $A/_{\mathscr{R}}$, que determina $\mathscr{R}$ en el conjunto A.

Según la definición de conjunto cociente, 7.3.2,

$$A/_{\mathscr{R}} = \{[a] : a \in A\}$$

Pues bien, sea N cualquier subconjunto de números enteros. Entonces,

$$
\begin{aligned}
N \in A/_{\mathscr{R}} &\iff \exists a \in A : N = [a] \\
&\iff N = [0] \ \vee \ N = [1] \ \vee N = [2] \\
&\iff N \in \{[0], [1], [2]\}
\end{aligned}
$$

luego,

$$\begin{aligned} A/_{\mathscr{R}} &= \{[0],[1],[2]\} \\ &= \{\{0,3,6,9\},\{1,4,7\}\{2,5,8\}\} \end{aligned}$$

■

Ejemplo 7.7

En el conjunto, $\mathbb{Z}$, de los números enteros se define la relación,

$$\forall n_1, n_2, (n_1 \mathscr{R} n_2 \text{ si, y solo si } n_1 - n_2 \text{ es múltiplo de } m)$$

a) Probar que $\mathscr{R}$ es una relación de equivalencia.

b) Obtener el conjunto cociente que la relación $\mathscr{R}$ determina en $\mathbb{Z}$.

Solución

a) Probar que $\mathscr{R}$ es una relación de equivalencia.
Basta sustituir en el ejemplo anterior, 3 por m.

b) Obtener el conjunto cociente que la relación $\mathscr{R}$ determina en $\mathbb{Z}$.
Según la definición de conjunto cociente, 7.3.2,

$$\mathbb{Z}/_{\mathscr{R}} = \{[a] : a \in \mathbb{Z}\}$$

Tendremos que hallar, pues, las clases de equivalencia.

Sea a cualquier número entero. Por el teorema de existencia y unicidad de cociente y resto, (13.2.1), existirán q_2 y r, enteros y únicos tales que

$$a = mq_2 + r,\ 0 \leqslant r < m$$

Pues bien, sea b, arbitrariamente elegido en $\mathbb{Z}$. Entonces,

$$\begin{aligned} b \in [a] &\iff b \mathscr{R} a \\ &\iff \exists q_1 \in \mathbb{Z} : b - a = mq_1 \\ &\iff \exists q_1 \in \mathbb{Z} : b = mq_1 + a \\ &\implies \exists q_1, q_2, r \in \mathbb{Z} : b = mq_1 + mq_2 + r, \text{ siendo } 0 \leqslant r < m \\ &\iff \exists q_1, q_2, r \in \mathbb{Z} : b = m(q_1 + q_2) + r, \text{ siendo } 0 \leqslant r < m \\ &\implies \exists q, r \in \mathbb{Z} : b = mq + r, \text{ siendo } 0 \leqslant r < m \ \{\text{Tomando } q = q_1 + q_2\} \\ &\iff b \in \{n : n = mq + r, q \in \mathbb{Z}\ 0 \leqslant r < m\} \end{aligned}$$

Por lo tanto, y al ser b cualquier entero, hemos probado que la proposición,

$$\forall x, (x \in [a] \longrightarrow x \in \{n : n = mq + r, q \in \mathbb{Z} \text{ y } 0 \leqslant r < m\})$$

es verdadera y, consecuentemente,

$$[a] \subseteq \{n : n = mq + r, q \in \mathbb{Z} \text{ y } 0 \leqslant r < m\}$$

Recíprocamente,

$$\begin{aligned}
b \in \{n : n = mq + r, q \in \mathbb{Z}\ 0 \leqslant r < m\} &\iff \exists q_1 \in \mathbb{Z} : b = mq_1 + r, \text{ siendo } 0 \leqslant r < m \\
&\implies \exists q_1, q_2 \in \mathbb{Z} : b = mq_1 + a - mq_2 \\
&\iff \exists q_1, q_2 \in \mathbb{Z} : b = m(q_1 - q_2) + a \\
&\implies \exists q \in \mathbb{Z} : b = mq + a \ \{\text{Tomando } q = q_1 - q_2\} \\
&\iff \exists q \in \mathbb{Z} : b - a = mq \\
&\iff b \mathscr{R} a \\
&\iff b \in [a]
\end{aligned}$$

Nuevamente, por la arbitrariedad de b, la proposición,

$$\forall x, (x \in \{n : n = mq + r, q \in \mathbb{Z} \text{ y } 0 \leqslant r < m\} \longrightarrow x \in [a])$$

es verdadera y, consecuentemente,

$$\{n : n = mq + r, q \in \mathbb{Z} \text{ y } 0 \leqslant r < m\} \subseteq [a]$$

De la doble inclusión obtenida, se sigue que

$$[a] = \{n : n = mq + r, q \in \mathbb{Z} \text{ y } 0 \leqslant r < m\}$$

es decir, la clase de equivalencia de un entero cualquiera, a, viene dada por el conjunto formado por todos los números enteros que dan el mismo resto, r, que a al dividirlos por m.

Ahora bien, si r es cualquier entero entre 0 y $m - 1$, entonces,

$$r = mq + r, \text{siendo } 0 \leqslant r < m \text{ y } q = 0$$

es decir, el resto al dividirlos por m es r, por lo tanto,

$$[r] = \{n : n = mq + r, q \in \mathbb{Z} \text{ y } 0 \leqslant r < m\}$$

o sea,

$$\begin{aligned}
[0] &= \{n : n = mq, q \in \mathbb{Z}\} \\
[1] &= \{n : n = mq + 1, q \in \mathbb{Z}\} \\
[2] &= \{n : n = mq + 2, q \in \mathbb{Z}\} \\
&\vdots \qquad\qquad \vdots \\
[m-1] &= \{n : n = mq + m - 1, q \in \mathbb{Z}\}
\end{aligned}$$

Volviendo al principio, teníamos que si a era cualquier entero,

$$a = mq_2 + r,\ 0 \leqslant r < m$$

es decir, el resto de dividir a entre m es 0 o 1 o 2 o $\ldots$ o $m-1$, luego,

$$\left.\begin{array}{c} a \in \{n : n = mq, q \in \mathbb{Z}\} \\ \text{o} \\ a \in \{n : n = mq+1, q \in \mathbb{Z}\} \\ \text{o} \\ a \in \{n : n = mq+2, q \in \mathbb{Z}\} \\ \text{o} \\ \vdots \\ \text{o} \\ a \in \{n : n = mq+m-1, q \in \mathbb{Z}\} \end{array}\right\} \iff \left\{\begin{array}{l} a \in [0] \\ \text{o} \\ a \in [1] \\ \text{o} \\ a \in [2] \\ \text{o} \\ \vdots \\ \text{o} \\ a \in [m-1] \end{array}\right.$$

$$\iff \left\{\begin{array}{l} [a] = [0] \\ \text{o} \\ [a] = [1] \\ \text{o} \\ [a] = [2] \\ \text{o} \\ \vdots \\ \text{o} \\ [a] = [m-1] \end{array}\right.$$

Ahora podemos escribir el conjunto cociente. En efecto, según la definición de conjunto cociente, 7.3.2,

$$\mathbb{Z}/_{\mathscr{R}} = \{[a] : a \in \mathbb{Z}\}$$

Pues bien, sea N cualquier subconjunto de números enteros. Entonces,

$$\begin{aligned} N \in \mathbb{Z}/_{\mathscr{R}} &\iff \exists a \in \mathbb{Z} : N = [a] \\ &\iff N = [r]\,, \text{ siendo } 0 \leqslant r < m-1 \\ &\iff N = [0] \ \vee\ N = [1] \ \vee\ N = [2] \ \vee\ \ldots \ \vee\ N = [m-1] \\ &\iff N \in \{[0]\,, [1]\,, [2]\,, \ldots, [m-1]\} \end{aligned}$$

luego,

$$\mathbb{Z}/_{\mathscr{R}} = \{[0]\,, [1]\,, [2]\,, \ldots, [m-1]\}$$

■

Ejemplo 7.8

En el conjunto $\mathbb{Z}$ de los números enteros se considera la siguiente relación:

$$\forall n_1, n_2,\ n_1 \mathscr{R} n_2 \iff \left\{\begin{array}{lcl} n_1 - n_2 = 0 \\ \acute{o} \\ n_1 + n_2 = 3 \end{array}\right.$$

(a) Probar que $\mathscr{R}$ es una relación de equivalencia.

(b) Calcular la clase de equivalencia del -1.

(c) Escribir el conjunto cociente en el caso de que el conjunto sobre el que está definida la relación sea $A = \{-5, -4, -3, -2, -1, 0, 1, 2, 3, 4, 5, 6, 7, 8\}$.

Solución

(a) Veamos si es de equivalencia.

Reflexividad. Sea a un número entero cualquiera. Entonces,

$$a = a \Longrightarrow a - a = 0 \Longrightarrow a \mathscr{R} a$$

luego todos los elementos del conjunto sobre el que está definida la relación están relacionados consigo mismos y, consecuentemente, ésta es reflexiva.

Simetría. Sean a y b enteros cualesquiera. Entonces,

$$a \mathscr{R} b \Longleftrightarrow \left\{ \begin{array}{rcrcl} a & - & b & = & 0 \\ \text{y} & & & & \\ a & + & b & = & 3 \end{array} \right\} \Longleftrightarrow \left\{ \begin{array}{rcrcl} b & - & a & = & 0 \\ \text{y} & & & & \\ b & + & a & = & 3 \end{array} \right\} \Longleftrightarrow b \mathscr{R} a$$

y, por lo tanto, la relación es simétrica.

Transitividad. Sean a, b y c tres números enteros. Entonces,

$$\left.\begin{array}{rcl} a\mathscr{R}b & \Longleftrightarrow & a-b=0 \quad \text{ó} \quad a+b=3 \\ \text{y} & & \text{y} \\ b\mathscr{R}c & \Longleftrightarrow & b-c=0 \quad \text{ó} \quad b+c=3 \end{array}\right\} \Longrightarrow \left\{\begin{array}{l} \left.\begin{array}{l} a-b=0 \quad \text{ó} \quad a+b=3 \\ \text{y} \\ b-c=0 \end{array}\right\} \\ \text{ó} \\ \left.\begin{array}{l} a-b=0 \quad \text{ó} \quad a+b=3 \\ \text{y} \\ b+c=3 \end{array}\right\} \end{array}\right.$$

$$\Longrightarrow \left\{\begin{array}{l} \left.\begin{array}{rcl} a-b & = & 0 \\ \text{y} & & \\ b-c & = & 0 \end{array}\right\} \\ \text{ó} \\ \left.\begin{array}{rcl} a+b & = & 3 \\ \text{y} & & \\ b-c & = & 0 \end{array}\right\} \\ \text{ó} \\ \left.\begin{array}{rcl} a-b & = & 0 \\ \text{y} & & \\ b+c & = & 3 \end{array}\right\} \\ \text{ó} \\ \left.\begin{array}{rcl} a+b & = & 3 \\ \text{y} & & \\ b+c & = & 3 \end{array}\right\} \end{array}\right.$$

$$\Longrightarrow \left\{\begin{array}{l} a-c = 0 \\ \text{ó} \\ a+c = 3 \\ \text{ó} \\ a+c = 3 \\ \text{ó} \\ a-c = 0 \end{array}\right.$$

$$\Longrightarrow \quad a\mathscr{R}c$$

y, consecuentemente, la relación es transitiva.

(b) Calculamos la clase de equivalencia de cualquier número entero, a.

En efecto, si b es un entero elegido arbitrariamente,

$$\begin{aligned} b \in [a] &\iff b \mathscr{R} a \\ &\iff \begin{cases} b - a = 0 \\ \text{o} \\ b + a = 3 \end{cases} \\ &\iff \begin{cases} b = a \\ \text{o} \\ b = 3 - a \end{cases} \\ &\iff b \in \{a, 3 - a\} \end{aligned}$$

y de la arbitrariedad de b, se sigue que la proposición,

$$\forall n, (n \in [a] \longleftrightarrow n \in \{a, 3 - a\})$$

es verdadera y, consecuentemente,

$$[a] = \{a, 3 - a\}$$

En particular,

$$[-1] = \{-1, 4\}$$

(c) Veamos como sería el conjunto cociente en el caso de que la relación estuviera definida sobre el conjunto $A = \{-5, -4, -3, -2, -1, 0, 1, 2, 3, 4, 5, 6, 7, 8\}$. Según el apartado (b),

$$\begin{aligned} [0] &= \{0, 3\} \\ [1] &= \{1, 2\} \\ [4] &= \{4, -1\} \\ [5] &= \{5, -2\} \\ [6] &= \{6, -3\} \\ [7] &= \{7, -4\} \\ [8] &= \{8, -5\} \end{aligned}$$

de aquí que

$$\begin{aligned} A\Big/_{\mathscr{R}} &= \{[0], [1], [2], [3], [4], [5], [6], [7], [8]\} \\ &= \{\{0, 3\}, \{1, 2\}, \{4, -1\}, \{5, -2\}, \{6, -3\}, \{7, -4\}, \{8, -5\}\} \end{aligned}$$

■

Ejemplo 7.9

En el conjunto $\mathbb{Z}^+$ de los enteros positivos se define la siguiente relación $\mathscr{R}$

$$\forall n_1, n_2, (n_1 \mathscr{R} n_2 \iff E(\sqrt{n_1}) = E(\sqrt{n_2}))$$

donde $E(n)$ significa "parte entera de n".

Demostrar que se trata de una relación de equivalencia, hallar las clases de equivalencia y el conjunto cociente.

Solución

$\mathscr{R}$ es de equivalencia.

En efecto, para cada entero positivo a se verifica que $E\left(\sqrt{a}\right) = E\left(\sqrt{a}\right)$, luego,

$$\forall n, \left(n \in \mathbb{Z}^+ \Longrightarrow n\mathscr{R}n\right)$$

es decir, $\mathscr{R}$ es *reflexiva.*

También es *simétrica* puesto que si a y b son dos enteros positivos cualesquiera,

$$a\mathscr{R}b \Longrightarrow E(\sqrt{a}) = E(\sqrt{b}) \Longleftrightarrow E(\sqrt{b}) = E(\sqrt{a}) \Longrightarrow b\mathscr{R}a$$

y *transitiva*, ya que si a, b y c son tres números enteros positivos cualesquiera, se verifica que

$$a\mathscr{R}b \text{ y } b\mathscr{R}c \Longrightarrow \left(E(\sqrt{a}) = E(\sqrt{b})\right) \text{y } \left(E(\sqrt{b}) = E(\sqrt{c})\right) \Longrightarrow E(\sqrt{a}) = E(\sqrt{c}) \Longrightarrow a\mathscr{R}c$$

Clases de equivalencia.

Sea a cualquiera de $\mathbb{Z}^+$. Entonces,

$$\begin{aligned}
[a] &= \{x \in \mathbb{Z}^+ : x\mathscr{R}a\} \\
&= \{x \in \mathbb{Z}^+ : E\left(\sqrt{x}\right) = E\left(\sqrt{a}\right)\} \\
&= \{x \in \mathbb{Z}^+ : E\left(\sqrt{a}\right) \leqslant \sqrt{x} < E\left(\sqrt{a}\right) + 1\} \\
&= \left\{x \in \mathbb{Z}^+ : \left(E\left(\sqrt{a}\right)\right)^2 \leqslant x < \left(E\left(\sqrt{a}\right) + 1\right)^2\right\}
\end{aligned}$$

Por ejemplo,

$$\begin{aligned}
[1] &= \left\{x \in \mathbb{Z}^+ : \left(E\left(\sqrt{1}\right)\right)^2 \leqslant x < \left(E\left(\sqrt{1}\right) + 1\right)^2\right\} \\
&= \{x \in \mathbb{Z}^+ : 1 \leqslant x < 4\} \\
&= \{1, 2, 3\} \\
[4] &= \left\{x \in \mathbb{Z}^+ : \left(E\left(\sqrt{4}\right)\right)^2 \leqslant x < \left(E\left(\sqrt{4}\right) + 1\right)^2\right\} \\
&= \{x \in \mathbb{Z}^+ : 4 \leqslant x < 9\} \\
&= \{4, 5, 6, 7, 8\}
\end{aligned}$$

Conjunto cociente.

Observemos lo siguiente:

- $E\left(\sqrt{1}\right) = E\left(\sqrt{2}\right) = E\left(\sqrt{3}\right) = 1$ y $E\left(\sqrt{4}\right) = 2$, luego la raíz de todos los enteros positivos entre 1 y 3 tienen la misma parte entera, es decir,

$$[1] = [2] = [3] = \{1, 2, 3\}$$

- $E\left(\sqrt{4}\right) = E\left(\sqrt{5}\right) = E\left(\sqrt{6}\right) = E\left(\sqrt{7}\right) = E\left(\sqrt{8}\right) = 2$ y $E\left(\sqrt{9}\right) = 3$, luego la raíz de todos los enteros positivos entre 4 y 8 tienen la misma parte entera, es decir,

$$[4] = [5] = [6] = [7] = [8] = \{4, 5, 6, 7, 8\}$$

- $E\left(\sqrt{9}\right) = E\left(\sqrt{10}\right) = E\left(\sqrt{11}\right) = E\left(\sqrt{12}\right) = E\left(\sqrt{13}\right) = E\left(\sqrt{14}\right) = E\left(\sqrt{15}\right) = 3$ y $E\left(\sqrt{16}\right) = 4$, luego la raíz de todos los enteros positivos entre 9 y 15 tienen la misma parte entera, es decir,

$$[9] = [10] = [11] = [12] = [13] = [14] = [15] = \{9, 10, 11, 12, 13, 14, 15\}$$

y así sucesivamente. Las únicas clases distintas que existen son, por tanto, las de los cuadrados de los enteros positivos, o sea,

$$[1^2], [2^2], [3^2], [4^2], [5^2], \ldots\ldots$$

siendo,

$$\begin{aligned}[a^2] &= \left\{x \in \mathbb{Z}^+ : \left(E\left(\sqrt{a^2}\right)\right)^2 \leqslant x < \left(E\left(\sqrt{a^2}\right)+1\right)^2\right\} \\ &= \left\{x \in \mathbb{Z}^+ : a^2 \leqslant x < (a+1)^2\right\}.\end{aligned}$$

El conjunto cociente será, por tanto,

$$\begin{aligned}\mathbb{Z}^+/_{\mathscr{R}} &= \left\{\left[a^2\right] : a \in \mathbb{Z}^+\right\} \\ &= \{\{1,2,3\}, \{4,5,6,7,8\}, \{9,10,11,12,13,14,15\}, \ldots\}\end{aligned}$$

■

7.3.3 Teorema

Dada una partición de un conjunto A, puede definirse en él una relación de equivalencia $\mathscr{R}$ tal que el conjunto cociente $A/_{\mathscr{R}}$ coincida con la partición dada.

Demostración

Sea $\mathscr{P} = \{A_1, A_2, \ldots, A_n\}$ una partición del conjunto A. Definimos la siguiente relación:

> *Dos elementos de A están relacionados si, y sólo si pertenecen al mismo subconjunto de la partición.*

es decir, si a y b son cualesquiera de A, entonces

$$a \mathscr{R} b \Longleftrightarrow \exists A_i \in \mathscr{P} : a \text{ y } b \in A_i$$

Veamos que $\mathscr{R}$ es de equivalencia.

En efecto,

> *Reflexividad.* Si a es cualquiera de A, como $\mathscr{P} = \{A_1, A_2, \ldots, A_n\}$ es una partición de A, será
>
> $$A = \bigcup_{i=1}^{n} A_i$$
>
> luego,
>
> $$a \in \bigcup_{i=1}^{n} A_i \Longrightarrow \exists A_i : a \in A_i \Longrightarrow a \text{ y } a \in A_i \Longrightarrow a \mathscr{R} a$$
>
> por lo tanto,
>
> $$\forall a, (a \in A \Longrightarrow a \mathscr{R} a)$$
>
> es decir, la relación es reflexiva.

Simetría. Sean a y b dos elementos cualesquiera de A, entonces

$$a\mathscr{R}b \Longleftrightarrow \exists A_i \in \mathscr{P} : a \text{ y } b \in A_i \Longrightarrow \exists A_i \in \mathscr{P} : b \text{ y } a \in A_i \Longleftrightarrow b\mathscr{R}a$$

o sea,

$$\forall a, b, (a\mathscr{R}b \Longrightarrow b\mathscr{R}a)$$

y la relación es, por tanto, simétrica.

Transitividad. En efecto, si a, b y c son tres elementos arbitrariamente elegidos en A, entonces

$$a\mathscr{R}b \Longleftrightarrow \exists A_i \in \mathscr{P} : a \text{ y } b \in A_i$$

y

$$b\mathscr{R}c \Longleftrightarrow \exists A_j \in \mathscr{P} : b \text{ y } c \in A_j$$

de donde se sigue que $b \in A_i \cap A_j$, consecuentemente $A_i \cap A_j \neq \emptyset$ y por la definición de partición tendremos que $A_i = A_j$.

Resulta, pues, que a y c pertenecen al mismo subconjunto de la partición y, por lo tanto, $a\mathscr{R}c$.

Así pues,

$$\forall a, b, c, (a\mathscr{R}b \text{ y } b\mathscr{R}c \Longrightarrow a\mathscr{R}c)$$

es decir, $\mathscr{R}$ es transitiva.

Veamos las *clases de equivalencia.*

Calculamos $[a]$, siendo a cualquier elemento de A. En efecto,

$$a \in A \Longleftrightarrow a \in \bigcup_{i=1}^{n} A_i \Longleftrightarrow \exists A_i : a \in A_i$$

Pues bien, si b es un elemento elegido arbitrariamente en A, entonces como $a \in A_i$,

$$b \in [a] \Longleftrightarrow b\mathscr{R}a \Longleftrightarrow b \in A_i$$

luego,

$$\forall x, (x \in [a] \longleftrightarrow x \in A_i)$$

es verdadera y, consecuentemente,

$$[a] = A_i, \text{ siendo } A_i \text{ el conjunto de la partición al que pertenece } a$$

Obtengamos el *conjunto cociente.*

Sea X cualquier subconjunto de A. Entonces, por la definición de conjunto cociente, 7.3.2,

$$\begin{aligned}
X \in A\Big/_{\mathscr{R}} &\Longleftrightarrow \exists a \in A : X = [a] \\
&\Longleftrightarrow \exists A_i \in \mathscr{P} : a \in A_i \text{ y } X = [a] \\
&\Longleftrightarrow \exists A_i \in \mathscr{P} : [a] = A_i \text{ y } X = [a] \\
&\Longleftrightarrow \exists A_i \in \mathscr{P} : X = A_i \\
&\Longleftrightarrow X \in \mathscr{P} \\
&\Longleftrightarrow X \in \{A_1, A_2, \ldots, A_n\}
\end{aligned}$$

luego,

$$A\Big/_{\mathscr{R}} = \{A_1, A_2, \ldots, A_n\}$$

■

Ejemplo 7.10

Sea $A = \{1, 2, 3, 4\}$ *y* $\mathscr{P} = \{\{1, 2, 3\}, \{4\}\}$ *una partición de* A. *Determínese la relación de equivalencia correspondiente en* A.

Solución

Si tenemos en cuenta que las clases de equivalencia son los subconjuntos de la partición, tendremos

$$[1] = \{1, 2, 3\} \text{ y } [4] = \{4\}$$

A partir de la definición de clases de equivalencia y de que $\mathscr{R}$ ha de ser de equivalencia, tendremos:

$$[1] = \{1, 2, 3\}, \text{ luego } (1,1), (1,2), (1,3), (2,1), (2,2), (2,3), (3,1), (3,2), (3,3) \in \mathscr{R}$$
$$[4] = \{4\}, \text{luego } (4,4) \in \mathscr{R}$$

de aquí que

$$\mathscr{R} = \{(1,1), (1,2), (1,3), (2,1), (2,2), (2,3), (3,1), (3,2), (3,3), (4,4)\}$$

■

Ejemplo 7.11

Si $\{\{a, c, e\}, \{b, d, f\}\}$ *es una partición del conjunto* $A = \{a, b, c, d, e, f\}$, *determinar la relación de equivalencia correspondiente.*

Solución

Si $\mathscr{R}$ es la relación de equivalencia buscada, entonces el conjunto cociente es

$$A/_{\mathscr{R}} = \{\{a, c, e\}, \{b, d, f\}\}$$

luego las clases de equivalencia son

$$[a] = \{a, c, e\} \text{ y } [b] = \{b, d, f\}$$

Pues bien,

$$[a] = \{a, c, e\}, \text{ luego } (a,a), (a,c), (a,e), (c,a), (c,c), (c,e), (e,a), (e,c) \text{ y } (e,e) \text{ están en } \mathscr{R}$$

también,

$$[b] = \{b, d, f\}, \text{ luego } (b,b), (b,d), (b,f), (d,b), (d,d), (d,f), (f,b), (f,d) \text{ y } (f,f) \text{ están en } \mathscr{R}$$

Consecuentemente, la relación es

$$\begin{aligned} \mathscr{R} = \{&(a,a), (a,c), (a,e), (c,a), (c,c), (c,e), (e,a), (e,c), (e,e), \\ &(b,b), (b,d), (b,f), (d,b), (d,d), (d,f), (f,b), (f,d), (f,f)\} \end{aligned}$$

■

Lección 8

Funciones

Hija orgullosa del Número y del Espacio, he aquí a la función.

François Le lionnais

Las funciones son un tipo especial de relaciones binarias. Una función puede tomarse como una relación de entrada-salida; es decir, para cada entrada o argumento, una función produce una salida o valor. Las funciones son la base de muchas de las más poderosas herramientas matemáticas, y muchos de nuestros conocimientos en informática pueden ser codificados convenientemente describiendo las propiedades de cierto tipo de funciones. En esta lección definiremos las funciones en general y varios casos particulares. La notación y terminología que utilizamos se usa ampliamente en matemáticas e informática.

8.1 Definiciones y Generalidades

Una función de un conjunto A en otro conjunto B es una regla que asigna un elemento de B a cada elemento de A. Notaremos las funciones con las letras $f, g, h, \ldots$.

8.1.1 Función

Sean A y B dos conjuntos no vacíos. Una función de A en B, y que notaremos $f : A \longrightarrow B$, es una relación de A a B en la que para cada $a \in A$, existe un único elemento $b \in B$ tal que $(a, b) \in f$. Si $(a, b) \in f$, escribiremos $f(a) = b$ y diremos que b es la imagen de a mediante f. Es decir, una función f de A en B es una relación de A a B con las características especiales siguientes:

1. Cada elemento de A se presenta como la primera componente de un par ordenado de la relación f. Obsérvese que esto significa que $\text{Dom}\,(f) = A$, luego

   $$\forall a \in A,\ \exists b \in B : f(a) = b$$

   o sea, para cada elemento a de A ha de encontrarse un elemento b en B tal que $f(a) = b$.

2. Si $f(a) = b_1$ y $f(a) = b_2$, entonces $b_1 = b_2$.

Las dos condiciones anteriores nos ofrecen la siguiente caracterización de una función.

$$f : A \longrightarrow B \text{ es función } \iff \begin{cases} 1.\ \forall a \in A,\ \exists b \in B : f(a) = b \\ \text{y} \\ 2.\ \forall a \in A, [f(a) = b_1\ \wedge\ f(a) = b_2 \longrightarrow b_1 = b_2] \end{cases}$$

■

Nota 8.1 Si en la caracterización anterior negamos ambos miembros, la contrarrecíproca nos ofrece una forma sencilla de comprobar que f no es una función.

$$f : A \longrightarrow B \text{ no es función } \iff \begin{cases} 1.\ \exists a \in A : f(a) \neq b,\ \forall b \in B \\ \text{ó} \\ 2.\ \exists a \in A : (f(a) = b_1\ \wedge\ f(a) = b_2\ \wedge\ b_1 \neq b_2) \end{cases}$$

Es decir, una relación f de A a B puede dejar de ser función porque exista algún elemento en A que no sea imagen, mediante f, de ninguno de B, o bien porque exista algún elemento en A que tenga dos imágenes.

Las funciones reciben también el nombre de aplicaciones o transformaciones, ya que desde un punto de vista geométrico, podemos considerarlas como reglas que asignan a cada elemento $a \in A$, el único elemento $f(a) \in B$.

8.1.2 Dominio e Imagen

Si f es una función de A en B, entonces A es el dominio de f y su imagen es el subconjunto de B,

$$Img\,(f) = \{b \in B, \exists a : a \in A\ \wedge\ f(a) = b\}$$

Ejemplo 8.1

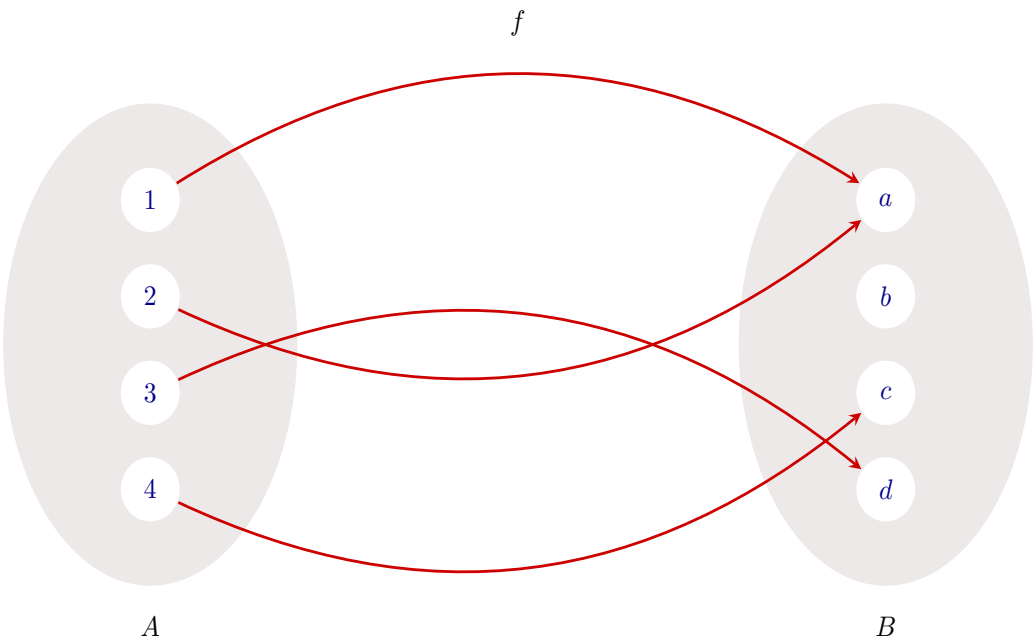
Sean $A = \{1, 2, 3, 4\}$, $B = \{a, b, c, d\}$ y $f = \{(1, a), (2, a), (3, d), (4, c)\}$. Comprobar que f es una función.

Solución

En efecto, todos los elementos de A aparecen como primer elemento de un par ordenado en la relación, y ninguno como primero de dos pares diferentes. En la función propuesta,

$$f(1) = a,\ f(2) = a,\ f(3) = d,\ f(4) = c$$

La figura siguiente muestra un esquema de la situación.



Obsérvese que el elemento $a \in B$ aparece como segundo elemento de dos pares diferentes de f, es decir, es imagen de dos elementos distintos de A y además existen elementos en B que no son imagen de ningún elemento de A. Ninguna de las dos cosas causa conflicto con la definición de función.

■

Ejemplo 8.2

Sean $A = \{1, 2, 3\}$ y $B = \{x, y, z\}$. Determinar si las relaciones siguientes son funciones de A en B.

(a) $\mathscr{R}_1 = \{(1, x), (2, x)\}$

(b) $\mathscr{R}_2 = \{(1, x), (1, y), (2, z), (3, y)\}$

Solución

(a) $\mathscr{R}_1$ no es una función ya que existen elementos de A que no son primer elemento de ningún par de la relación, es decir, que no tienen imagen en el conjunto B.

(b) $\mathscr{R}_2$ tampoco es función ya que contiene los pares ordenados $(1, x)$ y $(1, y)$, es decir, el 1 tiene dos imágenes distintas, x e y, lo cual viola la segunda condición de la definición de relación.

La dificultad que encontramos en $\mathscr{R}_1$ para que no sea función, no es tan seria como la que presenta la relación $\mathscr{R}_2$. Obsérvese que $\mathscr{R}_1$ es una función del conjunto $\{1, 2\}$ en B. Esto ilustra la idea general de que, si una relación f de A en B satisface la segunda condición de la definición anterior, entonces f será una función del $\mathrm{Dom}\,(f)$ en B.

■

Ejemplo 8.3

Sean $A = B = \mathbb{Z}$ y f definida en la forma:

$$f : A \longrightarrow B : f(a) = a + 1,\ \forall a \in A$$

Determinar si f es una función.

Solución

La relación definida está formada por todos los pares ordenados $(a, a + 1)$, siendo $a \in \mathbb{Z}$, es decir, f hace corresponder a cada número entero el siguiente. Veamos si f es función.

1. Sea a cualquier número entero.

   La ecuación $b = a + 1$ siempre tiene solución en $\mathbb{Z}$, es decir siempre podemos encontrar el siguiente al número a. Por lo tanto,

   $$\forall a \in A,\ \exists b \in B : f(a) = b$$

2. Veamos ahora que la imagen de cada entero es única. En efecto, supongamos que un entero cualquiera a tiene dos imágenes, b_1 y b_2. Entonces,

   $$\left.\begin{array}{l} f(a) = b_1 \\ \text{y} \\ f(a) = b_2 \end{array}\right\} \Longrightarrow \left\{\begin{array}{l} a + 1 = b_1 \\ \text{y} \\ a + 1 = b_2 \end{array}\right\} \Longrightarrow b_1 - b_2 = 0 \Longrightarrow b_1 = b_2$$

f cumple, pues, las dos condiciones exigidas para ser función.

■

Ejemplo 8.4

Sean $A = \{a, b, c, d\}$ y $B = \{1, 2, 3\}$. Determinar si las siguientes relaciones de A en B son funciones. En caso de que lo sean dar su imagen.

(a) $\mathscr{R} = \{(a, 1), (b, 2), (c, 1), (d, 2)\}$

(b) $\mathscr{R} = \{(a, 1), (b, 2), (a, 2), (c, 1), (d, 2)\}$

(c) $\mathscr{R} = \{(a, 3), (b, 2), (c, 1)\}$

(d) $\mathscr{R} = \{(a, 1), (b, 1), (c, 1), (d, 1)\}$

Solución

Llamaremos f a las relaciones que sean funciones.

(a) $\mathscr{R} = \{(a, 1), (b, 2), (c, 1), (d, 2)\}$
Si es función.
$$f : A \longrightarrow B \text{ tal que } f(a) = 1,\ f(b) = 2,\ f(c) = 1,\ f(d) = 2$$
$$\text{Img}\,(f) = \{y \in B,\ \exists x \in A \text{ tal que } f(x) = y\} = \{1, 2\}$$

(b) $\mathscr{R} = \{(a, 1), (b, 2), (a, 2), (c, 1), (d, 2)\}$
No es función, ya que $f(a) = 1$ y $f(a) = 2$, siendo $1 \neq 2$.

(c) $\mathscr{R} = \{(a, 3), (b, 2), (c, 1)\}$
No es función, ya que $\text{Dom}\,(\mathscr{R}) \neq A$

(d) $\mathscr{R} = \{(a, 1), (b, 1), (c, 1), (d, 1)\}$
Si es función.
$$f : A \longrightarrow B \text{ tal que } f(x) = 1,\ \forall x \in A$$
$$\text{Img}\,(f) = \{1\}$$

■

Ejemplo 8.5

Verificar que las fórmulas siguientes producen una función de A en B.

(a) $A = B = \mathbb{Z};\ f(a) = a^2$

(b) $A = \mathbb{R},\ B = \{0, 1\};\ f(a) = \begin{cases} 0, & \text{si } a \notin \mathbb{Z} \\ 1, & \text{si } a \in \mathbb{Z} \end{cases}$

(c) $A = \mathbb{R},\ B = \mathbb{Z}$ *y* $f(a)$ *es igual al mayor número entero que sea menor o igual que* a.

Solución

Veamos si se cumplen las condiciones de función.

(a) $A = B = \mathbb{Z};\ f(a) = a^2$

$$f : A \longrightarrow B \text{ tal que } f(a) = a^2,\ \forall a \in A$$

1. Sea a cualquiera de A. Tomando b tal que $\sqrt{b} = a$ (bastaría que b fuera cuadrado perfecto), tendríamos que $b \in \mathbb{Z}$ y

$$f(a) = a^2 \Longrightarrow f(a) = \left(\sqrt{b}\right)^2 \Longrightarrow f(a) = b$$

luego,

$$\forall a \in A,\ \exists b \in B : f(a) = b$$

2. Veamos ahora que la imagen mediante f de un entero cualquiera a es única.
En efecto, supongamos que no lo es. Entonces, existirían b_1 y b_2 en B tales que

$$\left.\begin{array}{l} f(a) = b_1 \\ \text{y} \\ f(a) = b_2 \end{array}\right\} \Longrightarrow \left\{\begin{array}{l} a^2 = b_1 \\ \text{y} \\ a^2 = b_2 \end{array}\right.$$

$$\Longleftrightarrow \left\{\begin{array}{l} a = \pm\sqrt{b_1} \\ \text{y} \\ a = \pm\sqrt{b_2} \end{array}\right.$$

$$\Longrightarrow \pm\sqrt{b_1} = \pm\sqrt{b_2}$$

$$\Longleftrightarrow \left(\pm\sqrt{b_1}\right)^2 = \left(\pm\sqrt{b_2}\right)^2$$

$$\Longleftrightarrow b_1 = b_2$$

Es decir, la imagen es única.

f cumple las dos condiciones, luego es una función de $\mathbb{Z}$ en $\mathbb{Z}$.

(b) $A = \mathbb{R},\ B = \{0, 1\}$ y

$$f : A \longrightarrow \{0,1\} \text{ tal que } f(a) = \left\{\begin{array}{l} 0,\ \text{si } a \notin \mathbb{Z} \\ 1,\ \text{si } a \in \mathbb{Z} \end{array}\right.,\ \forall a \in A$$

Observemos lo siguiente:

$$A = \mathbb{R} \Longleftrightarrow A = (\mathbb{R} \setminus \mathbb{Z}) \cup \mathbb{Z}$$

siendo,

$$(\mathbb{R} \setminus \mathbb{Z}) \cap \mathbb{Z} = \mathbb{R} \cap \mathbb{Z}^c \cap \mathbb{Z} = \emptyset$$

luego,

$$a \in A \Longleftrightarrow \left\{\begin{array}{l} a \in \mathbb{Z} \\ \text{o} \\ a \notin \mathbb{Z} \end{array}\right. \Longrightarrow\ a \in \mathbb{R} \setminus \mathbb{Z}$$

Podemos escribir, por tanto, la función como,

$$f : (\mathbb{R} \setminus \mathbb{Z}) \cup \mathbb{Z} \longrightarrow \{0,1\} : f(a) = \left\{\begin{array}{l} 0,\ \text{si } a \in \mathbb{R} \setminus \mathbb{Z} \\ \text{y} \\ 1,\ \text{si } a \in \mathbb{Z} \end{array}\right.$$

Veamos si f es una función.

1. Sea a cualquiera de A. Habrá, por tanto, dos opciones:
   ⁕ $a \in \mathbb{R} \setminus \mathbb{Z}$. Entonces, $a \notin \mathbb{Z}$ y tomando $b = 0$, tendremos que
   $$f(a) = 0 \Longrightarrow f(a) = b$$
   ⁕ $a \in \mathbb{Z}$. En tal caso, tomando $b = 1$,
   $$f(a) = 1 \Longrightarrow f(a) = b$$
   Por lo tanto,
   $$\forall a \in A, \exists b \in B : f(a) = b$$
2. Veamos que la imagen de cualquier a de $\mathbb{R}$, mediante f, es única.
   En efecto, si no fuera única, existirían b_1 y b_2 en B tales que $f(a) = b_1$ y $f(a) = b_2$ y habrá, al igual que antes, dos opciones:
   ⁕ $a \in \mathbb{R} \setminus \mathbb{Z}$. Entonces, $a \notin \mathbb{Z}$, luego
   $$\left.\begin{array}{l} f(a) = b_1 \\ \text{y} \\ f(a) = b_2 \end{array}\right\} \Longleftrightarrow \left.\begin{array}{l} 0 = b_1 \\ \text{y} \\ 0 = b_2 \end{array}\right\} \Longrightarrow b_1 = b_2$$
   ⁕ $a \notin \mathbb{Z}$. En tal caso,
   $$\left.\begin{array}{l} f(a) = b_1 \\ \text{y} \\ f(a) = b_2 \end{array}\right\} \Longleftrightarrow \left.\begin{array}{l} 1 = b_1 \\ \text{y} \\ 1 = b_2 \end{array}\right\} \Longrightarrow b_1 - b_2 = 0 \Longleftrightarrow b_1 = b_2$$

Por tanto, f es una función de $\mathbb{R}$ en $\{0, 1\}$.

(c) $A = \mathbb{R}$, $B = \mathbb{Z}$ y $f(a)$ es igual al mayor número entero que sea menor o igual que a.

$$f : \mathbb{R} \longrightarrow \mathbb{Z} \text{ tal que } f(a) = \text{Máx}\,\{n \in \mathbb{Z} : n \leqslant a\}\,,\ \forall a \in \mathbb{R}$$

Sea $E(a)$ la parte entera de a. Entonces, habrá dos opciones:

⁕ a no es entero.
En este caso, $E(a) < a < E(a) + 1$, luego,

$$\begin{aligned} \{n \in \mathbb{Z} : n \leqslant a\} &= \mathbb{Z} \cap (-\infty, a] \\ &= \mathbb{Z} \cap [(-\infty, E(a)] \cup (E(a), a]] \\ &= [\mathbb{Z} \cap (-\infty, E(a)]] \cup [\mathbb{Z} \cap (E(a), a]] \\ &= [\mathbb{Z} \cap (-\infty, E(a)]] \cup \emptyset \\ &= [\mathbb{Z} \cap (-\infty, E(a)]] \\ &= \{n \in \mathbb{Z} : n \leqslant E(a)\} \end{aligned}$$

Por lo tanto,
$$\text{Máx}\,\{n \in \mathbb{Z} : n \leqslant a\} = \text{Máx}\,\{n \in \mathbb{Z} : n \leqslant E(a)\} = E(a)$$

⁕ a es entero. En tal caso, $E(a) = a$, luego,

$$\text{Máx}\,\{n \in \mathbb{Z} : n \leqslant a\} = \text{Máx}\,\{n \in \mathbb{Z} : n \leqslant E(a)\} = E(a)$$

Veamos ahora que se cumplen las dos condiciones de función.

1. Sea a cualquier número real. Tomando $b = E(a)$, tendremos que $b \in \mathbb{Z}$ y,

$$f(a) = \text{Máx}\{n \in \mathbb{Z} : n \leqslant a\} = E(a) = b$$

2. Veamos que la imagen, mediante f, de cualquier número real a es única.
En efecto, supongamos que existieran b_1 y b_2 en $\mathbb{Z}$ tales que $f(a) = b_1$ y $f(a) = b_2$. Entonces,

$$\left.\begin{array}{l} b_1 = \text{Máx}\{n \in \mathbb{Z} : n \leqslant a\} \\ \text{y} \\ b_1 = \text{Máx}\{n \in \mathbb{Z} : n \leqslant a\} \end{array}\right\} \Longrightarrow b_1 = b_2$$

Ya que el máximo de un conjunto es único.

Consecuentemente, f es una función.

■

8.1.3 Igualdad de Funciones

Dadas dos funciones f y g definidas entre los mismos conjuntos A y B, diremos que son iguales cuando toman idénticos valores sobre los mismos elementos de dominio. Es decir,

$$f = g \Longleftrightarrow f(a) = g(a),\ \forall a \in A$$

■

8.1.4 Función Identidad

Dado un conjunto A, se define la identidad i_A como la función

$$i_A : A \longrightarrow A : i_A(a) = a,\ \forall a \in A$$

■

8.2 Composición de Funciones

Estudiamos en este apartado una nueva función que se obtiene componiendo dos funciones conocidas. Introduciremos el concepto con un ejemplo.

Sean los conjuntos

$$A = \{a, b, c\},\ B = \{1, 2\}\ C = \{\alpha, \beta\}$$

y consideremos las funciones

$$f : A \longrightarrow B : f(a) = 1,\ f(b) = 2,\ f(c) = 1$$

y

$$g : B \longrightarrow C : g(1) = \beta,\ g(2) = \alpha$$

Observemos lo siguiente:

$$\left.\begin{array}{l} g(1)=\beta \\ f(a)=1 \end{array}\right\} \implies g\left[f(a)\right]=\beta$$

$$\left.\begin{array}{l} g(1)=\beta \\ f(c)=1 \end{array}\right\} \implies g\left[f(c)\right]=\beta$$

$$\left.\begin{array}{l} g(2)=\alpha \\ f(b)=2 \end{array}\right\} \implies g\left[f(b)\right]=\alpha$$

Si ahora llamamos h a la función

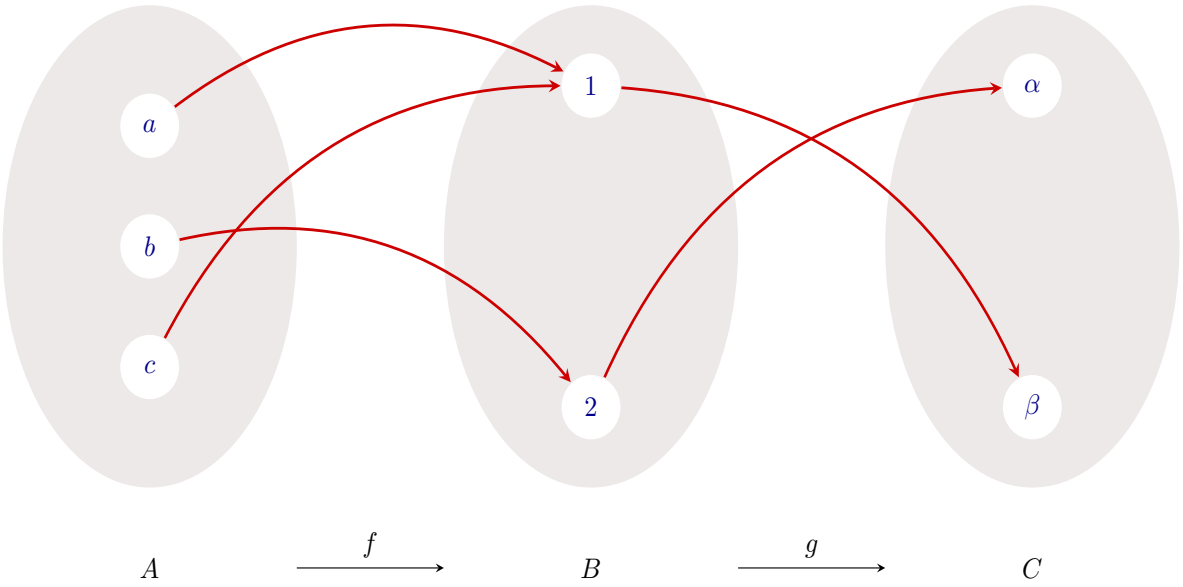
$$h: A \longrightarrow C : h(a)=\beta,\ h(b)=\alpha,\ \text{y}\ h(c)=\beta$$

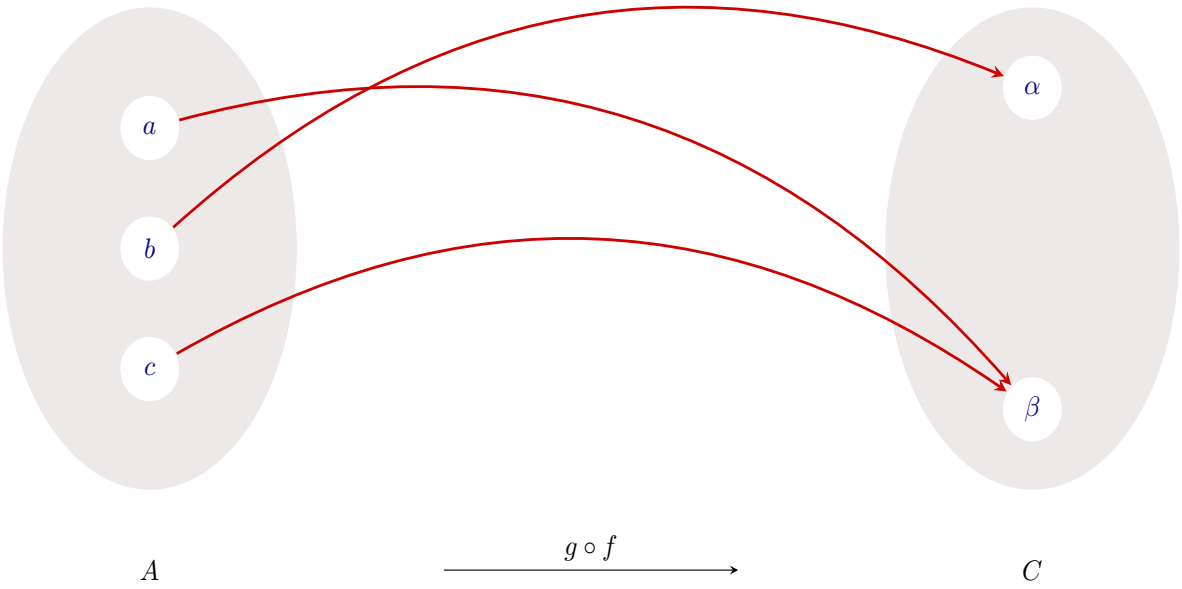
y comparamos con la anterior, tendremos

$$\begin{array}{rcl} h(a) & = & g\left[f(a)\right] \\ h(b) & = & g\left[f(b)\right] \\ h(c) & = & g\left[f(c)\right] \end{array}$$

es decir, h hace el mismo efecto que la f y la g juntas.

A esta nueva función la llamaremos *composición o producto* de f y g. La figura siguiente ilustra el ejemplo.





8.2.1 Definición

Dadas dos funciones $f : A \longrightarrow B$ *y* $g : B \longrightarrow C$*, llamaremos composición de* f *y* g*, y la notaremos* $g \circ f$ *a una nueva relación*

$$g \circ f : A \longrightarrow C : (g \circ f)(a) = g\left[f(a)\right],\ \forall a \in A$$

■

Veamos ahora que esta nueva relación también es una función, es decir, probaremos que la composición de dos funciones es una función.

8.2.2 Proposición

Dadas dos funciones $f : A \longrightarrow B$ *y* $g : B \longrightarrow C$*, la composición de ambas,* $g \circ f$ *es una función de* A *en* C*.*

Demostración

Según hemos definido:

$$g \circ f : A \longrightarrow C : (g \circ f)(a) = g\left[f(a)\right];\ \forall a \in A$$

Veamos que cumple las dos condiciones de función.

1. Sea a cualquiera de A. Entonces, al ser $f : A \longrightarrow B$ una función, existirá $b \in B$ tal que $f(a) = b$.
   Dado que $g : B \longrightarrow C$ también es una función, para el $b \in B$ recién encontrado, existirá un $c \in C$ tal que $g(b) = c$.
   Tenemos, pues,
   $$\left.\begin{array}{l} f(a) = b \\ \text{y} \\ g(b) = c \end{array}\right\} \Longrightarrow g\left[f(a)\right] = c \Longrightarrow (g \circ f)(a) = c$$
   luego,
   $$\forall a \in A,\ \exists c \in C : (g \circ f)(a) = c$$
   es decir, todos los elementos de A tienen imagen mediante $g \circ f$.

2. Sea a cualquiera de A y sean $c_1, c_2 \in C$ tales que $(g \circ f)(a) = c_1$ y $(g \circ f)(a) = c_2$. Entonces,

$$\left.\begin{array}{l}(g \circ f)(a) = c_1 \\ \text{y} \\ (g \circ f)(a) = c_2\end{array}\right\} \implies \left\{\begin{array}{l} g\,[f(a)] = c_1 \\ \text{y} \\ g\,[f(a)] = c_2\end{array}\right.$$

$$\implies \left\{\begin{array}{ll} g(b) = c_1 & \\ \text{y} & \{f \text{ función } \implies \exists b \in B : f(a) = b\} \\ g(b) = c_2 & \end{array}\right.$$

$$\implies c_1 = c_2 \qquad \{g \text{ es funcion}\}$$

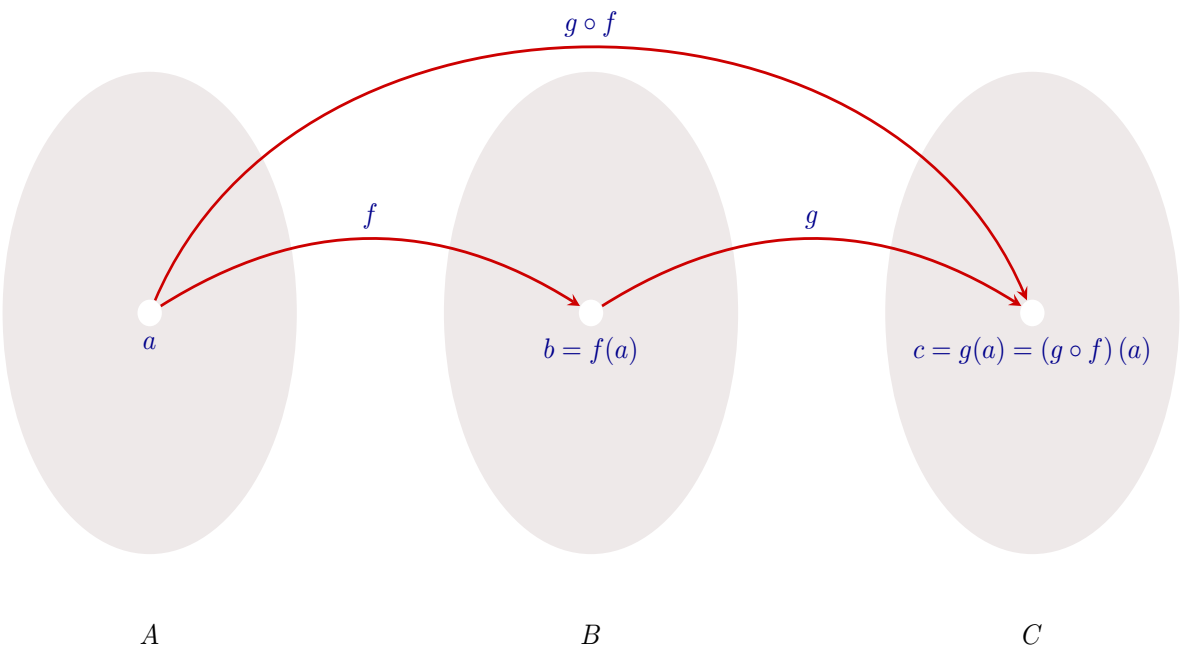
es decir,

$$\forall a \in A\,[(g \circ f)(a) = c_1 \ \wedge \ (g \circ f)(a) = c_2 \implies c_1 = c_2]$$

Consecuentemente, la composición de dos funciones es una función.

■

La figura siguiente ilustra como se calcula el valor de $g \circ f$ en un punto $a \in A$.



Ejemplo 8.6

Sean $A = \mathbb{Z}$, $B = \mathbb{Z}$ y C el conjunto de todos los números enteros pares y

$$f : A \longrightarrow B : f(a) = a + 1, \ \ g : B \longrightarrow C : g(b) = 2b$$

Encontrar $g \circ f$.

Solución

Sea a cualquiera de A. Entonces,

$$(g \circ f)(a) = g\,[f(a)] = g(a + 1) = 2(a + 1)$$

es decir,

$$g \circ f : A \longrightarrow C : (g \circ f)(a) = 2(a+1),\ \forall a \in A$$

■

Ejemplo 8.7

Dadas las funciones

$$f : \mathbb{R} \longrightarrow \mathbb{R} : f(x) = x^2$$

$$g : \mathbb{R} \longrightarrow \mathbb{R} : g(x) = x + 5$$

Calcular $g \circ f$ *y* $f \circ g$.

Solución

Para cada x de $\mathbb{R}$, se verifica que

$$(g \circ f)(x) = g\left[f(x)\right] = g(x^2) = x^2 + 5$$
$$(f \circ g)(x) = f\left[g(x)\right] = (x+5)^2 = x^2 + 10x + 25$$

luego

$$g \circ f : \mathbb{R} \longrightarrow \mathbb{R} : (g \circ f)(x) = x^2 + 5$$

y

$$f \circ g : \mathbb{R} \longrightarrow \mathbb{R} : (f \circ g)(x) = x^2 + 10x + 25$$

■

Obsérvese que $g \circ f \neq f \circ g$, es decir, la composición de aplicaciones no es, en general, conmutativa.

Puede ocurrir incluso que una de las dos no exista.

Ejemplo 8.8

Sean

$$f : \mathbb{Z}^+ \longrightarrow \mathbb{Z}^+ \textit{ tal que } f(x) = x,\ \forall x \in \mathbb{Z}^+ \textit{ y } g : \{0,1,2\} \longrightarrow \mathbb{Z}^+ \textit{ tal que } g(x) = x,\ \forall x \in \{0,1,2\}$$

Calcular $g \circ f$ *y* $f \circ g$.

Solución

$g \circ f$ no existe ya que el dominio de g no es igual a la imagen de f.

$f \circ g$ está definida en la forma siguiente:

$$f \circ g : \{0,1,2\} \longrightarrow \mathbb{Z}^+ \text{ tal que } (f \circ g)(x) = f\left[g(x)\right] = f(x) = x$$

En este caso, $f \circ g = g$.

■

Ejemplo 8.9

Sean f y g las funciones,

$$f:\mathbb{Z}_0^+ \longrightarrow \mathbb{Z}_0^+ \text{ tal que } f(x)=\begin{cases} \dfrac{x}{2}, & \text{si } x \text{ es par.} \\ 0, & \text{en cualquier otro caso.} \end{cases}$$

$$g:\mathbb{Z}_0^+ \longrightarrow \mathbb{Z}_0^+ \text{ tal que } g(x)=2x$$

Calcular $g\circ f$ y $f\circ g$.

Solución

Sea x cualquiera de $\mathbb{Z}_0^+$. Entonces,

$$(g\circ f)(x)=g\left[f(x)\right]=\left\{\begin{array}{l} g\left(\dfrac{x}{2}\right), \text{ si } x \text{ es par.} \\ g(0), \text{ en cualquier otro caso.} \end{array}\right\}=\left\{\begin{array}{l} 2\dfrac{x}{2}=x, \text{ si } x \text{ es par.} \\ 2\cdot 0=0, \text{ en cualquier otro caso.} \end{array}\right.$$

es decir,

$$g\circ f:\mathbb{Z}_0^+ \longrightarrow \mathbb{Z}_0^+ \text{ tal que } (g\circ f)(x)=\begin{cases} x, \text{ si } x \text{ es par.} \\ 0, \text{ en cualquier otro caso.} \end{cases}$$

Por otra parte,

$$(f\circ g)(x)=f\left[g(x)\right]=f(2x)=\frac{2x}{2}, \text{ ya que } 2x \text{ siempre es par.}$$

luego,

$$f\circ g:\mathbb{Z}_0^+ \longrightarrow \mathbb{Z}_0^+ \text{ tal que } (f\circ g)(x)=x$$

es decir $f\circ g=i_{\mathbb{Z}_0^+}$

■

8.2.3 Asociatividad

Dadas tres aplicaciones

$$f:A\longrightarrow B \; g:B\longrightarrow C \text{ y } h:C\longrightarrow D$$

se verifica que

$$(h\circ g)\circ f=h\circ(g\circ f)$$

Demostración

$$\left.\begin{array}{l} g:B\longrightarrow C \\ h:C\longrightarrow D \end{array}\right\}\Longrightarrow \left.\begin{array}{r} h\circ g:B\longrightarrow D \\ f:A\longrightarrow B \end{array}\right\}\Longrightarrow (h\circ g)\circ f:A\longrightarrow D$$

Por otra parte,

$$\left.\begin{array}{l} f:A\longrightarrow B \\ g:B\longrightarrow C \end{array}\right\} \implies \begin{array}{l} g\circ f:A\longrightarrow C \\ \\ h:C\longrightarrow D \end{array} \Bigg\} \implies h\circ(g\circ f):A\longrightarrow D$$

es decir, $(h\circ g)\circ f$ y $h\circ(g\circ f)$ tienen el mismo dominio y el mismo conjunto final.

Además, para cada a de A, tenemos:

$$[(h\circ g)\circ f](a) = (h\circ g)(f(a)) = h[g(f(a))]$$

$$[h\circ(g\circ f)](a) = h[(g\circ f)(a)] = h[g(f(a))]$$

por tanto,

$$(h\circ g)\circ f = h\circ(g\circ f)$$

■

Ejemplo 8.10

Sean $A=B=C=\mathbb{R}$ y sean $f:A\longrightarrow B,\ g:B\longrightarrow C$ definidas por $f(a)=a-1$ y $g(b)=b^2$. Encontrar

(a) $(g\circ f)(2)$

(b) $(f\circ g)(2)$

(c) $(f\circ g)(x)$

(d) $(g\circ f)(x)$

(e) $(f\circ f)(y)$

(f) $(g\circ g)(y)$

Solución

(a) $(g\circ f)(2) = g[f(2)] = g(2-1) = g(1) = 1^2 = 1$

(b) $(f\circ g)(2) = f[g(2)] = f(2^2) = 2^2 - 1 = 3$

(c) $(f\circ g)(x) = f[g(x)] = f(x^2) = x^2 - 1$

(d) $(g\circ f)(x) = g[f(x)] = g(x-1) = (x-1)^2 = x^2 - 2x + 1$

(e) $(f\circ f)(y) = f[f(y)] = f(y-1) = y - 1 - 1 = y - 2$

(f) $(g\circ g)(y) = g[g(y)] = g(y^2) = y^4$

■

Ejemplo 8.11

Sean $A = B = C = \mathbb{R}$ y sean $f : A \longrightarrow B,\ g : B \longrightarrow C$ definidas por $f(a) = a+1$ y $g(b) = b^2+2$. Encontrar:

(a) $(f \circ g)(-2)$

(b) $(g \circ f)(-2)$

(c) $(f \circ g)(x)$

(d) $(g \circ f)(x)$

(e) $(f \circ f)(y)$

(f) $(g \circ g)(y)$

Solución

(a) $(f \circ g)(-2) = f\left[g(-2)\right] = f\left((-2)^2+2\right) = (-2)^2+2+1 = 7$

(b) $(g \circ f)(-2) = g\left[f(-2)\right] = g(-2+1) = g(-1) = (-1)^2+2 = 3$

(c) $(f \circ g)(x) = f\left[g(x)\right] = f(x^2+2) = x^2+2+1 = x^2+3$

(d) $(g \circ f)(x) = g\left[f(x)\right] = g(x+1) = (x+1)^2+2 = x^2+2x+3$

(e) $(f \circ f)(y) = f\left[f(y)\right] = f(y+1) = y+1+1 = y+2$

(f) $(g \circ g)(y) = g\left[g(y)\right] = g(y^2+2) = (y^2+2)^2+2 = y^4+4y^2+6$

■

Ejemplo 8.12

Sean $A = B = \{x : x \in \mathbb{R} \setminus \{0,1\}\}$. Examine las siguientes funciones de A en B, cada una definida por su fórmula.

$$f_1(x) = x \qquad f_2(x) = 1-x \qquad f_3(x) = \frac{1}{x}$$

$$f_4(x) = \frac{1}{1-x} \quad f_5(x) = \frac{x}{x-1} \quad f_6(x) = \frac{x-1}{x}$$

Demuestre, sustituyendo una fórmula en otra, que la composición de cualquier par de estas seis funciones es alguna otra de ellas.

Solución

Antes que nada, observemos que si i_A es la función identidad sobre el conjunto A, entonces

$$(i_A \circ f_i)(a) = i_A\left[f_i(a)\right] = f_i(a),\ \forall a \in A \Longrightarrow i_A \circ f_i = f_i,\ \forall i = 1,2,3,4,5,6$$

$$(f_i \circ i_A)(a) = f_i\left[i_A(a)\right] = f_i(a),\ \forall a \in A \Longrightarrow f_i \circ i_A = f_i,\ \forall i = 1,2,3,4,5,6$$

Pues bien, dado que f_1 es la función identidad sobre A, tendremos que

$$f_1 \circ f_i = f_i \text{ y } f_i \circ f_1 = f_i,\ i = 1,2,3,4,5,6$$

Por otra parte, para cada $x \in A$ se verifica:

$$(f_2 \circ f_2)(x) = f_2\left[f_2(x)\right] = f_2(1-x) = 1-(1-x) = x = f_1(x) \Longrightarrow f_2 \circ f_2 = f_1$$

$$(f_2 \circ f_3)(x) = f_2\left[f_3(x)\right] = f_2\left(\frac{1}{x}\right) = 1 - \frac{1}{x} = \frac{x-1}{x} = f_6(x) \Longrightarrow f_2 \circ f_3 = f_6$$

$$(f_2 \circ f_4)(x) = f_2\left[f_4(x)\right] = f_2\left(\frac{1}{1-x}\right) = 1 - \frac{1}{1-x} = \frac{x}{x-1} = f_5(x) \Longrightarrow f_2 \circ f_4 = f_5$$

$$f_2 \circ f_5 = f_2 \circ (f_2 \circ f_4) = (f_2 \circ f_2) \circ f_4 = f_1 \circ f_4 = f_4$$

$$f_2 \circ f_6 = f_2 \circ (f_2 \circ f_3) = (f_2 \circ f_2) \circ f_3 = f_1 \circ f_3 = f_3$$

$$(f_3 \circ f_2)(x) = f_3\left[f_2(x)\right] = f_3(1-x) = \tfrac{1}{1-x} \Longrightarrow f_3 \circ f_2 = f_4$$

$$(f_3 \circ f_3)(x) = f_3\left[f_3(x)\right] = f_3\left(\tfrac{1}{x}\right) = x = i(x) \Longrightarrow f_3 \circ f_3 = f_1$$

$$f_3 \circ f_4 = f_3 \circ (f_3 \circ f_2) = (f_3 \circ f_3) \circ f_2 = f_1 \circ f_2 = f_2$$

$$(f_3 \circ f_5(x) = f_3\left[f_5(x)\right] = f_3\left(\tfrac{x}{x-1}\right) = \frac{1}{\frac{x}{x-1}} = \frac{x-1}{x} = f_6(x) \Longrightarrow f_3 \circ f_5 = f_6$$

$$f_3 \circ f_6 = f_3 \circ (f_3 \circ f_5) = (f_3 \circ f_3) \circ f_5 = f_1 \circ f_5 = f_5$$

$$f_4 \circ f_2 = (f_3 \circ f_2) \circ f_2 = f_3 \circ (f_2 \circ f_2) = f_3 \circ f_1 = f_3$$

$$f_4 \circ f_3 = (f_3 \circ f_2) \circ f_3 = f_3 \circ (f_2 \circ f_3) = f_3 \circ f_6 = f_5$$

$$f_4 \circ f_4 = (f_3 \circ f_2) \circ f_4 = f_3 \circ (f_2 \circ f_4) = f_3 \circ f_5 = f_6$$

$$f_4 \circ f_5 = (f_3 \circ f_2) \circ f_5 = f_3 \circ (f_2 \circ f_5) = f_3 \circ f_4 = f_2$$

$$f_4 \circ f_6 = (f_3 \circ f_2) \circ f_6 = f_3 \circ (f_2 \circ f_6) = f_3 \circ f_3 = f_1$$

$$f_5 \circ f_2 = (f_2 \circ f_4) \circ f_2 = f_2 \circ (f_4 \circ f_2) = f_2 \circ f_3 = f_6$$

$$f_5 \circ f_3 = (f_2 \circ f_4) \circ f_3 = f_2 \circ (f_4 \circ f_3) = f_2 \circ f_5 = f_4$$

$$f_5 \circ f_4 = (f_2 \circ f_4) \circ f_4 = f_2 \circ (f_4 \circ f_4) = f_2 \circ f_6 = f_3$$

$$f_5 \circ f_5 = (f_2 \circ f_4) \circ f_5 = f_2 \circ (f_4 \circ f_5) = f_2 \circ f_2 = f_1$$

$$f_5 \circ f_6 = (f_2 \circ f_4) \circ f_6 = f_2 \circ (f_4 \circ f_6) = f_2 \circ f_1 = f_2$$

$$f_6 \circ f_2 = (f_2 \circ f_3) \circ f_2 = f_2 \circ (f_3 \circ f_2) = f_2 \circ f_4 = f_5$$

$$f_6 \circ f_3 = (f_2 \circ f_3) \circ f_3 = f_2 \circ (f_3 \circ f_3) = f_2 \circ f_1 = f_2$$

$$f_6 \circ f_4 = (f_2 \circ f_3) \circ f_4 = f_2 \circ (f_3 \circ f_4) = f_2 \circ f_2 = f_1$$

$$f_6 \circ f_5 = (f_2 \circ f_3) \circ f_5 = f_2 \circ (f_3 \circ f_5) = f_2 \circ f_6 = f_3$$

$$f_6 \circ f_6 = (f_2 \circ f_3) \circ f_6 = f_2 \circ (f_3 \circ f_6) = f_2 \circ f_5 = f_4$$

■

Ejemplo 8.13

Dadas las funciones $f : A \longrightarrow B$ y $g : B \longrightarrow C$, probar que $(g \circ f)(A) \subseteq g(B)$. ¿Es cierto el recíproco?. Justificar la respuesta.

Solución

Probaremos que todos los elementos de $(g \circ f)(A)$ están en $g(B)$.

Por definición de composición de funciones,

$$\left.\begin{array}{l} f:A\longrightarrow B \\ g:B\longrightarrow C \end{array}\right\}\Longrightarrow g\circ f:A\longrightarrow C$$

luego,

$$(g\circ f)(A)=\{c\in C,\ \exists a:a\in A,\ \wedge\ (g\circ f)(a)=c\}$$

y

$$g(B)=\{c\in C,\ \exists b:b\in B\ \wedge\ g(b)=c\}$$

por tanto,

$$\begin{array}{rcll} \forall c\in(g\circ f)(A) & \Longleftrightarrow & \exists a:a\in A\ \wedge\ (g\circ f)(a)=c & \\ & \Longleftrightarrow & \exists a:a\in A\ \wedge\ g\left[f(a)\right]=c & \{f \text{ es función, luego } \exists b:b\in B\ \wedge\ f(a)=b\} \\ & \Longrightarrow & \exists b:b\in B\ \wedge\ g(b)=c & \\ & \Longleftrightarrow & c\in g(B) & \end{array}$$

de aquí que

$$(g\circ f)(A)\subset g(B)$$

El recíproco, en general, no es cierto. El siguiente contraejemplo lo prueba.

Sean $A=\{x,y\}$, $B=\{1,2,3\}$ y $C=\{\alpha,\beta\}$ y sean f y g las funciones

$$\begin{array}{l} f:A\longrightarrow B:f(x)=1,\ f(y)=2 \\ g:B\longrightarrow C:g(1)=\alpha,\ g(2)=\alpha,\ g(3)=\beta \end{array}$$

entonces,

$$\left.\begin{array}{l} (g\circ f)(x)=g\left[f(x)\right]=g(1)=\alpha \\ (g\circ f)(y)=g\left[f(y)\right]=g(2)=\alpha \end{array}\right\}\Longrightarrow(g\circ f)(A)=\{\alpha\}$$

por otro lado,

$$\left.\begin{array}{l} g(1)=\alpha \\ g(2)=\alpha \\ g(3)=\beta \end{array}\right\}\Longrightarrow g(B)=\{\alpha,\beta\}$$

y es obvio que

$$\{\alpha,\beta\}\nsubseteq\{\alpha\}$$

luego,

$$g(B)\nsubseteq(g\circ f)(A)$$

■

Ejemplo 8.14

Si $\mathscr{U}$ es el conjunto universal, $S,T\subseteq\mathscr{U}$, $g:\mathscr{P}(\mathscr{U})\longrightarrow\mathscr{P}(\mathscr{U})$ y $g(A)=T\cap(S\cup A)$.

Probar que $g^2=g$, siendo $g^2=g\circ g$.

Solución

Sea A cualquiera de $\mathscr{P}(\mathscr{U})$,entonces

$$\begin{aligned} g^2(A) &= (g \circ g)(A) \\ &= g\,[g(A)] \\ &= g\,[T \cap (S \cup A)] \\ &= T \cap [S \cup (T \cap (S \cup A))] \\ &= (T \cap S) \cup [T \cap (S \cup A)] \\ &= (T \cap S) \cup [(T \cap S) \cup (T \cap A)] \\ &= (T \cap S) \cup (T \cap A) \\ &= T \cap (S \cup A) \\ &= g(A) \end{aligned}$$

luego,

$$g^2 = g \circ g$$

■

Ejemplo 8.15

Se considera un conjunto no vacío $\mathscr{U}$ y un subconjunto suyo X. Se define la función característica f_X del conjunto X como la función

$$f_X : \mathscr{U} \longrightarrow \{0,1\} \ \textit{tal que}\ f_X(x) = \left\{ \begin{array}{l} 1, \ \textit{si}\ x \in X \\ 0, \ \textit{si}\ x \notin X \end{array} \right\}$$

Si A y B son dos subconjuntos de $\mathscr{U}$, demostrar:

(a) $f_A = f_B \Longleftrightarrow A = B$

(b) $f_{A \cup B} = f_A + f_B - f_{A \cap B}$

(c) $f_{A \setminus B} = f_A(1 - f_B)$

Solución

(a) $f_A = f_B \Longleftrightarrow A = B$

$\Longrightarrow$) Supongamos que $f_A = f_B$ y sea a cualquiera de A. Entonces,

$$a \in A \Longleftrightarrow f_A(a) = 1 \Longleftrightarrow f_B(a) = 1 \Longleftrightarrow a \in B$$

luego,

$$\forall a\,(a \in A \Longleftrightarrow a \in B)$$

es decir, $A = B$.

$\Longleftarrow$) Recíprocamente, supongamos que $A = B$ y sea x cualquiera de $\mathscr{U}$.
Si $x \in A$, entonces al ser $A = B$, será $x \in B$, luego

$$f_A(x) = 1 = f_B(x)$$

y si $x \notin A$, por la misma razón, $x \notin B$, luego

$$f_A(x) = 0 = f_B(x)$$

Consecuentemente,

$$f_A(x) = f_B(x),\ \forall x \in \mathscr{U}$$

es decir,

$$f_A = f_B$$

(b) $f_{A\cup B} = f_A + f_B - f_{A\cap B}$
En efecto, sea $x \in \mathscr{U}$, cualquiera.
Si $x \in (A \cup B)$, entonces $f_{A\cup B}(x) = 1$, pero

$$x \in (A \cup B) \Longleftrightarrow \begin{cases} x \notin A \text{ y } x \in B \Longrightarrow f_A(x) + f_B(x) - f_{A\cap B}(x) = 0 + 1 - 0 = 1 \\ \vee \\ x \in A \text{ y } x \in B \Longrightarrow f_A(x) + f_B(x) - f_{A\cap B}(x) = 1 + 1 - 1 = 1 \\ \vee \\ x \in A \text{ y } x \notin B \Longrightarrow f_A(x) + f_B(x) - f_{A\cap B}(x) = 1 + 0 - 0 = 1 \end{cases}$$

y si $x \notin (A \cup B)$, entonces $f_{A\cup B}(x) = 0$, pero

$$x \notin (A \cup B) \Longleftrightarrow x \notin A \text{ y } x \notin B \Longleftrightarrow f_A(x) + f_B(x) - f_{A\cap B}(x) = 0 + 0 - 0 = 0$$

Así pues,

$$f_{A\cup B}(x) = (f_A + f_B - f_{A\cap B})(x),\ \forall x \in \mathscr{U}$$

de aquí que

$$f_{A\cup B} = f_A + f_B - f_{A\cap B}$$

(c) $f_{A\setminus B} = f_A(1 - f_B)$. En efecto, sea x cualquiera de $\mathscr{U}$. Entonces,

$$\begin{aligned} &x \in A \text{ y } x \in B,\ \text{luego},\ f_{A\setminus B} = 0 \text{ y } f_A(x)\,(1 - f_B(x)) = 1(1-1) = 0 \\ &x \in A \text{ y } x \notin B,\ \text{luego},\ f_{A\setminus B} = 1 \text{ y } f_A(x)\,(1 - f_B(x)) = 1(1-0) = 1 \\ &x \notin A \text{ y } x \in B,\ \text{luego},\ f_{A\setminus B} = 0 \text{ y } f_A(x)\,(1 - f_B(x)) = 0(1-1) = 0 \\ &x \notin A \text{ y } x \notin B,\ \text{luego},\ f_{A\setminus B} = 0 \text{ y } f_A(x)\,(1 - f_B(x)) = 0(1-0) = 0 \end{aligned}$$

Consecuentemente,

$$f_{A\setminus B}(x) = (f_A(1 - f_B))\,(x),\ \forall x \in \mathscr{U}$$

y

$$f_{A\setminus B} = f_A(1 - f_B)$$

■

8.3 Tipos de Funciones

Examinaremos en este apartado distintas clases especiales de funciones.

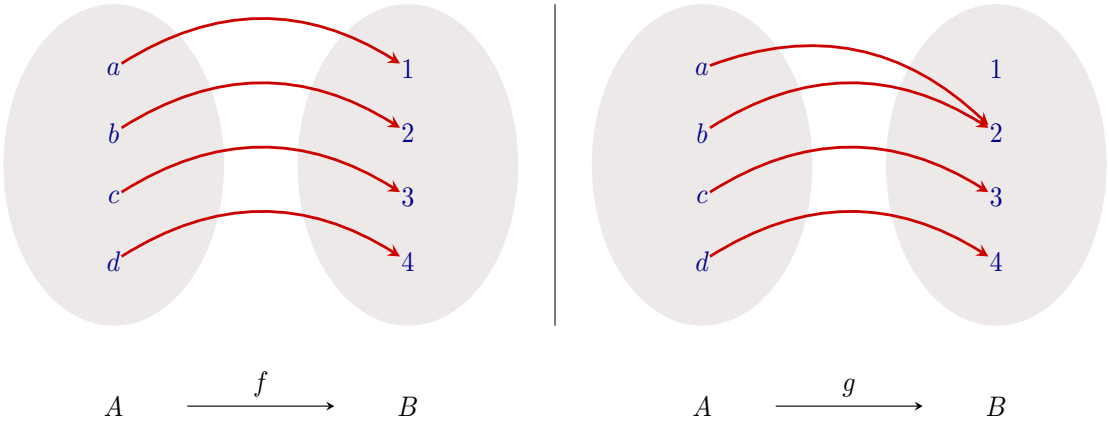
8.3.1 Función Inyectiva

Una función f entre los conjuntos A y B se dice que es inyectiva, cuando cada elemento de la imagen de f lo es, a lo sumo, de un elemento de A. Suele decirse también que la función es uno-a-uno. Dicho de otra forma:

$$f : A \longrightarrow B \text{ es inyectiva} \Longleftrightarrow \forall a_1, a_2 \in A, [a_1 \neq a_2 \Longrightarrow f(a_1) \neq f(a_2)]$$

La "mejor forma" de probar en la práctica la inyectividad de una función es utilizar la contrarrecíproca, es decir,

$$f : A \longrightarrow B \text{ es inyectiva} \Longleftrightarrow \forall a_1, a_2 \in A, [f(a_1) = f(a_2) \Longrightarrow a_1 = a_2]$$



f es inyectiva g no es inyectiva

Ejemplo 8.16

Determinar si cada una de las aplicaciones siguientes es inyectiva.

(a) A cada alumno de Matemática Discreta se le asigna el número que se corresponde con su edad.

(b) A cada país en el mundo se le asigna la longitud y la latitud de su capital.

(c) A cada libro escrito por un determinado autor, se le designa con el nombre del mismo.

(d) A cada país en el mundo que tenga un primer ministro se le asigna su primer ministro.

Solución

(a) No, ya que hay muchos alumnos de Matemática Discreta que tienen la misma edad.

(b) Si, porque a dos países distintos le corresponderán diferentes longitudes y latitudes.

(c) No, ya que hay diferentes libros que están escritos por el mismo autor.

(d) Si, porque a países diferentes les corresponderán distintos primeros ministros.

■

Ejemplo 8.17

Determinar si la función $f : \mathbb{R} \longrightarrow \mathbb{R}$ tal que $f(x) = x + 2$ es inyectiva.

Solución

En efecto, sean x_1 y x_2 dos números reales cualesquiera, entonces

$$f(x_1) = f(x_2) \Longrightarrow x_1 + 2 = x_2 + 2 \Longrightarrow x_1 = x_2$$

luego f es inyectiva.

■

Nota 8.2 Observemos lo siguiente:

$$f : A \longrightarrow B \text{ es inyectiva} \Longleftrightarrow \forall a_1, a_2 \in A\,(a_1 \neq a_2 \longrightarrow f(a_1) \neq f(a_2))$$

y negando ambos miembros, tendremos

$$f : A \longrightarrow B \text{ no es inyectiva} \Longleftrightarrow \exists a_1, a_2 \in A \text{ tal que } a_1 \neq a_2 \ \wedge \ f(a_1) = f(a_2)$$

es decir, la función f no es inyectiva si podemos encontrar dos elementos a_1 y a_2 en A, tales que siendo distintos sus imágenes sean iguales.

■

Ejemplo 8.18

Sea $f : \mathbb{R} \longrightarrow \mathbb{R}$ tal que $f(x) = 2$. ¿Es inyectiva?

Solución

La función propuesta no lo es. En efecto, si tomamos dos números reales x_1 y x_2, distintos, tendríamos

$$x_1 \neq x_2 \text{ y } f(x_1) = 2 = f(x_2)$$

luego según lo dicho en la nota anterior, la función no es inyectiva.

■

Ejemplo 8.19

Sea $f : \mathbb{R} \longrightarrow \mathbb{R}$ tal que $f(x) = x^2$. ¿Es inyectiva?

Solución

Sea x_1 cualquiera de $\mathbb{R}$. Si tomamos $x_2 = -x_1$, entonces $x_2 \in \mathbb{R}$ y

$$f(x_1) = x_1^2 \text{ y } f(x_2) = f(-x_1) = (-x_1)^2 = x_1^2$$

luego

$$\exists x_1, x_2 \in \mathbb{R} : x_1 \neq x_2 \ \wedge \ f(x_1) = f(x_2)$$

es decir, f no es inyectiva.

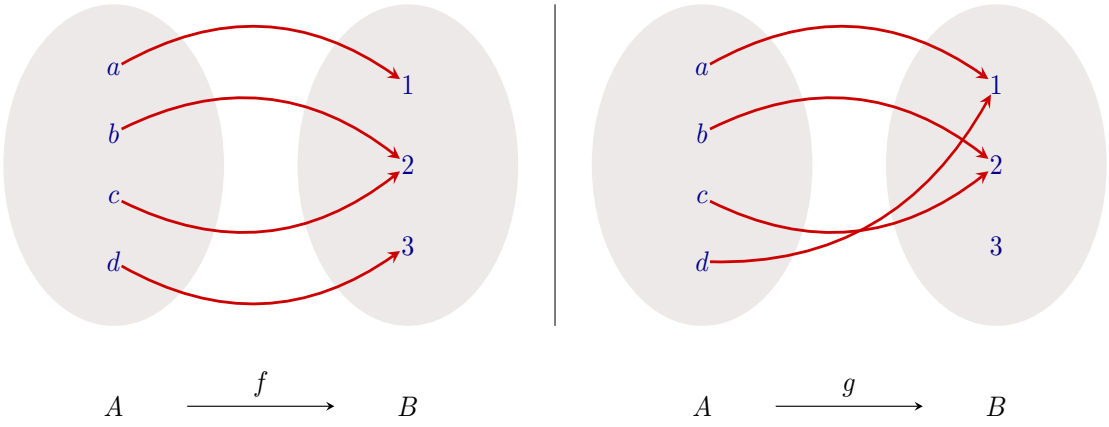
■

8.3.2 Función Suprayectiva

Una función f entre los conjuntos A y B se dice que es suprayectiva, sobreyectiva o exhaustiva, cuando cada elemento de B es imagen de, al menos, un elemento de A. Es decir,

$$f : A \longrightarrow B \text{ es suprayectiva} \Longleftrightarrow \forall b \in B,\ \exists a \in A \text{ tal que } f(a) = b$$

En otras palabras, f es sobreyectiva si la imagen de f es todo el conjunto B, es decir si $Img(f) = B$.



f es sobreyectiva

g no es sobreyectiva

Ejemplo 8.20

Sea $f : A \longrightarrow B$ donde $A = B = \mathbb{R}$ y $f(x) = x + 1,\ \forall x \in A$. ¿Es suprayectiva?

Solución

Sea y cualquiera de B. Hemos de encontrar un x en A tal que $f(x) = y$. Dicho de otra forma se trata de ver si la ecuación

$$x + 1 = y$$

tiene solución, lo cual, en este caso, es evidente. En efecto,

$$x + 1 = y \Longleftrightarrow x = y - 1$$

luego dado $y \in \mathbb{R}$, tomando $x = y - 1$, se verifica que

$$f(x) = f(y - 1) = y - 1 + 1 = y$$

es decir,

$$\forall y \in B,\ \exists x \in A : f(x) = y$$

luego f es suprayectiva.

■

Nota 8.3 Obsérvese lo siguiente:

$$f \text{ es suprayectiva} \Longleftrightarrow \forall b \in B,\ \exists a \in A : f(a) = b$$

si negamos ambos miembros, tendremos

$$f \text{ no es suprayectiva} \Longleftrightarrow \exists b \in B : f(a) \neq b, \forall a \in A$$

es decir, f no es suprayectiva si podemos encontrar un elemento en B tal que no es imagen de ningún elemento de A.

■

Ejemplo 8.21

Sea $f : A \longrightarrow B$, siendo $A = B = \mathbb{R}$ y $f(x) = x^2,\ \forall x \in A$

Solución

Esta función no es suprayectiva. En efecto, dado un y cualquiera negativo en B, no existe ningún x en A tal que su cuadrado sea y, ya que el cuadrado de cualquier número siempre es positivo. Es decir,

$$\text{si } y < 0, \text{ entonces } x^2 \neq y,\ \forall x \in A$$

luego,

$$\exists y \in B : f(x) \neq y \forall x \in A$$

de aquí que según la nota anterior, la función propuesta no sea suprayectiva.

■

8.3.3 Función Biyectiva

Una función f entre los conjuntos A y B se dice que es biyectiva, cuando es, al mismo tiempo, inyectiva y suprayectiva.

Ejemplo 8.22

Sea $f : A \longrightarrow B$ tal que $A = B = \mathbb{R}$ y $f(x) = 2x - 3,\ \forall x \in A$. ¿Es biyectiva?

Solución

Veamos si es inyectiva y suprayectiva.

(a) *Inyectiva.* Sean x_1 y x_2 dos números reales arbitrarios. Entonces,

$$f(x_1) = f(x_2) \Longrightarrow 2x_1 - 3 = 2x_2 - 3 \Longrightarrow 2x_1 = 2x_2 \Longrightarrow x_1 = x_2$$

luego f es inyectiva.

(b) *Suprayectiva.* Sea y cualquiera de B. Entonces,

$$y = 2x - 3 \Longleftrightarrow 2x = y + 3 \Longleftrightarrow x = \frac{y+3}{2}$$

luego tomando $x = \dfrac{y+3}{2}$, se verifica que $x \in A$ y

$$f(x) = f\left(\frac{y+3}{2}\right) = 2\frac{y+3}{2} - 3 = y$$

Consecuentemente,

$$\forall y \in B,\ \exists x \in A : f(x) = y$$

o sea, f es suprayectiva.

Por ser inyectiva y suprayectiva, f es biyectiva.

■

Ejemplo 8.23

Estudiar la función

$$f : \mathbb{R} \longrightarrow \mathbb{R} : f(x) = \frac{x}{x^2+1}$$

Solución

Veamos si f es inyectiva.

En efecto, sean x_1 y x_2 dos números reales cualesquiera. Entonces,

$$\begin{aligned} f(x_1) = f(x_2) &\implies \frac{x_1}{x_1^2+1} = \frac{x_2}{x_2^2+1} \\ &\implies x_1x_2^2 + x_1 = x_1^2x_2 + x_2 \\ &\implies x_1x_2^2 - x_1^2x_2 + x_1 - x_2 = 0 \\ &\implies x_1x_2(x_2 - x_1) + x_1 - x_2 = 0 \\ &\implies (x_1 - x_2)(1 - x_1x_2) = 0 \\ &\implies x_1 = x_2 \text{ ó } x_1 = \frac{1}{x_2} \end{aligned}$$

Así pues, tomando $x_1 \in \mathbb{R}$ y $x_2 = \dfrac{1}{x_1}$, tendremos que $x_1 \neq x_2$ y, sin embargo, $f(x_1) = f(x_2)$, por lo tanto f no es inyectiva.

Veamos si f es suprayectiva.

Tendremos que ver que dado cualquier número real, y, podemos encontrar un número x, también real, tal que $f(x) = y$, o sea, la ecuación $y = \dfrac{x}{x^2+1}$ ha de tener solución en $\mathbb{R}$. Pues bien,

$$\begin{aligned} y = \frac{x}{x^2+1} &\Longleftrightarrow x = x^2y + y \\ &\Longleftrightarrow x^2y - x + y = 0 \\ &\Longleftrightarrow x = \frac{1 \pm \sqrt{1-4y^2}}{2y} \end{aligned}$$

Ahora bien, si $1-4y^2<0$, entonces $x\notin\mathbb{R}$, y como

$$1-4y^2<0\Longleftrightarrow 4y^2>1\Longleftrightarrow y^2>\frac{1}{4}\Longleftrightarrow y>\pm\frac{1}{2}\Longleftrightarrow |y|>\frac{1}{2}$$

tomando cualquier $y\in\mathbb{R}$ tal que $|y|>\dfrac{1}{2}$, ningún $x\in\mathbb{R}$ hace que $f(x)=y$, es decir,

$$\exists y\in\mathbb{R}: f(x)\neq y, \forall x\in\mathbb{R}$$

y, consecuentemente, f no es suprayectiva.

■

Ejemplo 8.24

Sea $f:[0,1]\longrightarrow[a,b]: f(x)=(b-a)x+a$. *Determinar qué tipo de función es.*

Solución

(a) Veamos si f es inyectiva.
Sean x_1 y x_2 cualesquiera de $[0,1]$. Entonces,

$$\begin{aligned} f(x_1)=f(x_2) &\Longleftrightarrow (b-a)x_1+a=(b-a)x_2+a\\ &\Longrightarrow (b-a)x_1=(b-a)x_2 \qquad \{a\neq b\}\\ &\Longrightarrow x_1=x_2\end{aligned}$$

luego,

$$\forall x_1,x_2,\in[0,1]\ (f(x_1)=f(x_2)\Longrightarrow x_1=x_2)$$

es decir, f es inyectiva.

(b) Veamos si f es suprayectiva.
Sea y cualquiera de $[a,b]$. Tenemos que encontrar, al menos, un x en $[0,1]$ tal que $f(x)=y$. En efecto,

$$y=(b-a)x+a\Longleftrightarrow x=\frac{y-a}{b-a}$$

y al ser $a\neq b$, será $b-a\neq 0$, luego existe x, siendo

$$\begin{aligned} y\in[a,b] &\Longleftrightarrow a\leqslant y\leqslant b\\ &\Longleftrightarrow -b\leqslant -y\leqslant -a\\ &\Longleftrightarrow a-b\leqslant a-y\leqslant a-a\\ &\Longleftrightarrow 0\leqslant y-a\leqslant b-a\\ &\Longleftrightarrow 0\leqslant \frac{y-a}{b-a}\leqslant 1\\ &\Longleftrightarrow 0\leqslant x\leqslant 1\\ &\Longleftrightarrow x\in[0,1]\end{aligned}$$

y además,

$$f(x)=f\left(\frac{y-a}{b-a}\right)=(b-a)\frac{y-a}{b-a}+a=y$$

luego,

$$\forall y\in[a,b],\ \exists x\in[0,1]: f(x)=y$$

es decir, f es suprayectiva.

Al ser inyectiva y suprayectiva, la función propuesta es biyectiva.

■

Ejemplo 8.25

Determinar el carácter de las funciones siguientes:

(a) $A = \{1,2,3,4\} = B$ *y* $f = \{(1,1),(2,3),(3,4),(4,2)\}$

(b) $A = \{1,2,3\}$, $B = \{a,b,c,d\}$ *y* $f = \{(1,a),(2,a),(3,c)\}$

(c) $A = \left\{\frac{1}{2},\frac{1}{3},\frac{1}{4}\right\}$, $B = \{x,y,z,w\}$ *y* $f = \left\{\left(\frac{1}{2},x\right),\left(\frac{1}{4},y\right),\left(\frac{1}{3},w\right)\right\}$

(d) $A = \{1.1,7,0.06\}$ $B = \{p,q\}$ *y* $f = \{(1.1,p),(7,q),(0.06,p)\}$

Solución

(a) Según los datos del enunciado,

$$f : A \longrightarrow B : f(1) = 1, f(2) = 3, f(3) = 4, f(4) = 2$$

y se observa que

$$\forall a_1, a_2 \in A,\ a_1 \neq a_2 \Longrightarrow f(a_1) \neq f(a_2)$$

y

$$\forall b \in B, \exists a \text{ tal que } a \in A \ \wedge\ f(a) = b$$

Consecuentemente f es inyectiva y sobreyectiva y, por tanto, biyectiva.

(b) Según el enunciado,

$$f : A \longrightarrow B \text{ tal que } f(1) = a, f(2) = a, f(3) = c$$

Pues bien, se observa que existen dos elementos distintos en A, el 1 y el 2, con la misma imagen, es decir,

$$\exists a_1, a_2 \in A : a_1 \neq a_2 \ \wedge f(a_1) = f(a_2)$$

luego f no es inyectiva.

También se observa que existen dos elementos en B, el b y el d que no son imagen de ninguno de A, es decir,

$$\exists b_1 \in B : (f(a_1) \neq b_1,\ \forall a_1 \in A$$

por tanto, f no es sobreyectiva.

(c) Razonando igual que en los casos anteriores, se observa que la función propuesta es inyectiva, pero no sobreyectiva.

(d) De una forma similar se prueba que f es sobreyectiva y no inyectiva.

■

Ejemplo 8.26

Determinar el carácter de cada una de las siguientes funciones.

(a) $A = B = \mathbb{Z},\ f : A \longrightarrow B$ *tal que* $f(a) = a - 1$

(b) $A = B = \mathbb{R},\ f : A \longrightarrow B$ *tal que* $f(a) = |a|$

(c) $A = \mathbb{R},\ B = \mathbb{R}_0^+,\ f : A \longrightarrow B$ *tal que* $f(a) = |a|$

(d) $A = \mathbb{R},\ B = \mathbb{R}_0^+,\ f : A \longrightarrow B$ *tal que* $f(a) = a^2$

Solución

Determinar el carácter de cada una de las siguientes funciones.

(a) $A = B = \mathbb{Z},\ f : A \longrightarrow B$ tal que $f(a) = a - 1$

Inyectividad. Sean a_1 y a_2 cualesquiera de A. Entonces,

$$f(a_1) = f(a_2) \Longrightarrow a_1 - 1 = a_2 - 1 \Longrightarrow a_1 = a_2$$

luego,

$$\forall a_1, a_2 \in A,\ (f(a_1) = f(a_2) \Longrightarrow a_1 = a_2)$$

es decir, f es inyectiva.

Sobreyectividad. Sea b cualquiera de B. Tomando $a = b + 1$, tendremos que $a \in A$, y

$$f(a) = f(b + 1) \Longrightarrow f(a) = b + 1 - 1 = b$$

luego,

$$\forall b \in B, \exists a \in A : f(a) = b$$

o sea, f es sobreyectiva.

Biyectividad. Por ser inyectiva y sobreyectiva, la función propuesta es biyectiva.

(b) $A = B = \mathbb{R},\ f : A \longrightarrow B$ tal que $f(a) = |a|$

Recordemos que si a es un número real arbitrario,

$$|a| = \begin{cases} a, & \text{si } a \geqslant 0 \\ -a, & \text{si } a < 0 \end{cases}$$

luego $|a| \geqslant 0$.

Inyectividad. Sea a cualquiera de A. Si tomamos $a_1 = a$ y $a_2 = -a$, tendremos

$$f(a_1) = f(a) = |a|$$
$$f(a_2) = f(-a) = |-a| = |-1||a| = |a|$$

luego,

$$\exists a_1, a_2 \in A : a_1 \neq a_2 \ \wedge \ f(a_1) = f(a_2)$$

es decir, f no es inyectiva.

Sobreyectividad. Sea b un elemento arbitrario de B. Si $b < 0$ entonces, ningún a en A hace que $f(a) = b$ luego la función no es sobreyectiva.

Biyectividad. Al no ser inyectiva ni sobreyectiva, la función propuesta no es biyectiva.

(c) $A = \mathbb{R},\ B = \mathbb{R}_0^+,\ f : A \longrightarrow B$ tal que $f(a) = |a|$

Inyectividad. Por un razonamiento idéntico al del apartado anterior, la función no es inyectiva.

Sobreyectividad. Dado cualquier $b \in B$, bastaría tomar $a = b$ o $a = -b$, y $a \in A$, siendo

$$a = b \Longrightarrow f(a) = f(b) \Longrightarrow f(a) = |b| \Longrightarrow f(a) = b$$

o

$$a = -b \Longrightarrow f(a) = f(-b) \Longrightarrow f(a) = |-b| \Longrightarrow f(a) = b$$

luego f es sobreyectiva.

Biyectividad. Por no ser inyectiva, tampoco será biyectiva.

(d) $A = \mathbb{R},\ B = \mathbb{R}_0^+,\ f : A \longrightarrow B$ tal que $f(a) = a^2$

Inyectividad. Sea a cualquiera de A. Si tomamos $a_1 = a$ y $a_2 = -a$, entonces

$$f(a_1) = f(a) = a^2 \text{ y } f(a_2) = f(-a) = (-a)^2 = a^2$$

luego,

$$\exists a_1, a_2 \in A : a_1 \neq a_2 \text{ y } f(a_1) = f(a_2)$$

es decir, f no es inyectiva.

Sobreyectividad. Sea b cualquiera de B. Tomando $a = \sqrt{b}$, entonces, como $b \geqslant 0$, $a \in A$, y

$$f(a) = f\left(\sqrt{b}\right) \Longrightarrow f(a) = \left(\sqrt{b}\right)^2 \Longrightarrow f(a) = b$$

luego,

$$\forall b \in B,\ \exists a \in A : f(a) = b$$

y f es sobreyectiva.

Biyectividad. f no es biyectiva ya que no es inyectiva.

■

%beginEjemplo

Ejemplo 8.27

Sean a y b dos números enteros y

$$f : \mathbb{Z} \longrightarrow \mathbb{Z} \text{ tal que } f(x) = ax + b$$

Discutir para que valores de a y b,

(a) f es inyectiva.

(b) f es sobreyectiva.

(c) f es biyectiva.

Solución

(a) Sean x_1 y x_2 dos números enteros arbitrarios, entonces

$$\begin{aligned} f(x_1) = f(x_2) &\iff ax_1 + b = ax_2 + b \\ &\implies ax_1 = ax_2,\ \forall b \in \mathbb{Z} \\ &\implies x_1 = \frac{a}{a}x_2,\ \forall b \in \mathbb{Z} \\ &\implies x_1 = x_2,\ \forall b \in \mathbb{Z},\ \text{y } \forall a \in \mathbb{Z} \setminus \{0\} \end{aligned}$$

luego f es inyectiva para cada entero a distinto de cero y para cualquier entero b.

(b) Sea y cualquier número entero, tomando

$$x = \frac{y-b}{a}$$

entonces

$$x \in \mathbb{Z} \iff \frac{y-b}{a} \in \mathbb{Z} \iff \exists q \in \mathbb{Z} : y - b = aq \iff \exists q \in \mathbb{Z} : b = a(-q) + y$$

además,

$$f(x) = f\left(\frac{y-b}{a}\right) = f\left(\frac{y-a(-q)-y}{a}\right) = f(q) = aq + b = y,\ \forall a \in \mathbb{Z} \setminus \{0\}$$

luego f es sobreyectiva para cada a, b tales que a sea distinto de cero y b sea un múltiplo de a más y, para cualquier y, entero.

(c) De (a) y (b) se sigue que f es biyectiva

$$\forall a \in \mathbb{Z} \setminus \{0\}\ \text{ y } \forall b : \frac{y-b}{a} \in \mathbb{Z}$$

■

8.3.4 Composición y Tipos de Funciones

Dadas las funciones $f : A \longrightarrow B$ y $g : B \longrightarrow C$, se verifica:

(i) Si f y g son inyectivas, entonces la composición de ambas es inyectiva.

(ii) Si f y g son sobreyectivas, entonces la composición de ambas es sobreyectiva.

(iii) Si f y g son biyectivas, entonces la composición de ambas es biyectiva.

(iv) Si la composición de dos funciones es inyectiva, entonces la primera de ellas es inyectiva.

(v) Si la composición de dos funciones es sobreyectiva, entonces la segunda de ellas es sobreyectiva.

(vi) Si la composición de dos funciones es inyectiva y la primera de ellas es sobreyectiva, entonces la segunda es inyectiva.

(vii) Si la composición de dos funciones es sobreyectiva y la segunda de ellas es inyectiva, entonces la primera es sobreyectiva.

Demostración

(i) Si f y g son inyectivas, entonces $g \circ f$ es inyectiva.

En efecto, sean a_1 y a_2 dos elementos cualesquiera de A, entonces,

$$\begin{aligned}(g \circ f)(a_1) = (g \circ g)(a_2) &\implies g\,[f(a_1)] = g\,[f(a_2)] && \{g \text{ es inyectiva}\}\\ &\implies f(a_1) = f(a_2) && \{f \text{ es inyectiva}\}\\ &\implies a_1 = a_2\end{aligned}$$

(ii) Si f y g son sobreyectivas, entonces $g \circ f$ es sobreyectiva.

En efecto, dado c cualquiera de C, como g es sobreyectiva, existe $b \in B$ tal que $g(b) = c$ y al ser f también sobreyectiva, dado $b \in B$, existirá $a \in A$ tal que $f(a) = b$, luego

$$(g \circ f)(a) = g\,[f(a)] = g(b) = c$$

y $g \circ f$ es, por tanto, sobreyectiva.

(iii) Si f y g son biyectivas, entonces $g \circ f$ es biyectiva.

Se sigue directamente de (i) e (ii).

(iv) Si $g \circ f$ es inyectiva, entonces f es inyectiva.

En efecto, sean a_1 y a_2 cualesquiera de A, entonces por ser g función

$$\begin{aligned}f(a_1) = f(a_2) &\implies g\,[f(a_1)] = g\,[f(a_2)]\\ &\implies (g \circ f)(a_1) = (g \circ f)(a_2) && \{g \circ f \text{ es inyectiva}\}\\ &\implies a_1 = a_2\end{aligned}$$

luego f es inyectiva.

(v) Si $g \circ f$ es sobreyectiva, entonces g es sobreyectiva.

En efecto, sea $c \in C$, cualquiera, entonces al ser $g \circ f$ sobreyectiva, existirá $a \in A$ tal que $(g \circ f)(a) = c$, es decir,

$$g\,[f(a)] = c$$

pero si $a \in A$, como f es función $f(a)$ pertenece a B, tomando $b = f(a)$, tendremos que

$$\exists b \in B : g(b) = c$$

luego g es sobreyectiva.

(vi) Si $g \circ f$ es inyectiva y f es sobreyectiva, entonces g es inyectiva.

En efecto, sean $b_1, b_2 \in B$ cualesquiera, entonces al ser f sobreyectiva, existirán $a_1, a_2 \in A$ tales que $f(a_1) = b_1$, $f(a_2) = b_2$. Pues bien,

$$\begin{aligned}g(b_1) = g(b_2) &\iff g\,[f(a_1)] = g\,[f(a_2)]\\ &\iff (g \circ f)(a_1) = (g \circ f)(a_2) && \{g \circ f \text{ es inyectiva}\}\\ &\iff a_1 = a_2 && \{f \text{ es función}\}\\ &\iff f(a_1) = f(a_2)\\ &\iff b_1 = b_2\end{aligned}$$

(vii) Si $g \circ f$ es sobreyectiva y g es inyectiva, entonces f es sobreyectiva.

En efecto, sea $b \in B$, cualquiera. Al ser g función $g(b) \in C$ y como $g \circ f : A \longrightarrow C$ es sobreyectiva, existirá $a \in A$ tal que

$$(g \circ f)(a) = g(b)$$

es decir,

$$g\left[f(a)\right] = g(b)$$

de donde teniendo en cuenta que g es, por hipótesis, inyectiva, se sigue que

$$f(a) = b.$$

Resumiendo,

$$\forall b \in B,\ \exists a \in A : f(a) = b$$

luego f es sobreyectiva.

■

8.4 Función Inversa

Dada una función f entre los conjuntos A y B, consideremos su relación inversa, es decir aquella que se obtiene intercambiando cada uno de los pares que componen la relación.

Pues bien, según hemos visto en el apartado anterior, la relación inversa de una función no es, en general, otra función.

Dedicamos este apartado al estudio de las relaciones inversas que son funciones.

8.4.1 Función Invertible

Dada una función f entre los conjuntos A y B, diremos que es invertible si su relación inversa también es función. En tal caso, a la relación inversa de f, la notaremos f^{-1} y la llamaremos función inversa de f, estando definida en la forma:

$$f^{-1} : B \longrightarrow A : f^{-1}(b) = a \Longleftrightarrow b = f(a),\ \forall b \in B$$

8.4.2 Caracterización de una Función Invertible

La condición necesaria y suficiente para que una función f sea invertible es que sea biyectiva.

Demostración

Sea $f : A \longrightarrow B$ una función entre los conjuntos A y B.

"*La condición es necesaria*"

En efecto, supongamos que f es invertible, es decir, que su relación inversa f^{-1} es una función,

$$f^{-1} : B \longrightarrow A \text{ tal que } f^{-1}(b) = a \Longleftrightarrow b = f(a),\ \forall b \in B$$

Pues bien,

f es *inyectiva*. En efecto, sean a_1, a_2 cualesquiera de A.

Como f es función, existirán b_1 y b_2 en B tales que

$$f(a_1) = b_1 \text{ y } f(a_2) = b_2$$

y también

$$f^{-1}(b_1) = a_1 \text{ y } f^{-1}(b_2) = a_2$$

Pues bien,

$$\begin{aligned} f(a_1) = f(a_2) &\implies b_1 = b_2 \\ &\implies f^{-1}(b_1) = f^{-1}(b_2) \quad \{\text{Por ser } f^{-1} \text{ función}\} \\ &\iff a_1 = a_2 \end{aligned}$$

f es *suprayectiva*. En efecto, como f^{-1} es función, tendremos que

$$\forall b \in B,\ \exists a \in A : f^{-1}(b) = a$$

y al ser,

$$f^{-1}(b) = a \iff f(a) = b$$

tendremos que

$$\forall b \in B,\ \exists a \in A : f(a) = b$$

luego f es sobreyectiva.

Como $f$es inyectiva y sobreyectiva, será biyectiva.

"*La condición es suficiente*"

En efecto, si f es biyectiva, entonces será sobreyectiva, luego,

$$\forall b \in B, \exists a \in A : f(a) = b$$

y al ser,

$$f(a) = b \iff f^{-1}(b) = a$$

tendremos que

$$\forall b \in B,\ \exists a \in A : f^{-1}(b) = a$$

luego todos los elementos de B tienen imagen mediante f^{-1}, además por ser f inyectiva, tendremos que si $b \in B$ es tal que

$$\left.\begin{array}{l} f^{-1}(b) = a_1 \iff f(a_1) = b \\ \wedge \\ f^{-1}(b) = a_2 \iff f(a_2) = b \end{array}\right\} \implies f(a_1) = f(a_2) \implies a_1 = a_2$$

luego f^{-1} es una función y, por definición, f será invertible.

■

Ejemplo 8.28

Sean $A = B = \mathbb{R}$ *y* $f : A \longrightarrow B$ *tal que* $f(x) = 2x,\ \forall x \in A$. *Calcularemos* f^{-1}.

Solución

Según la definición de función inversa,

$$f^{-1} : B \longrightarrow A \text{ tal que } f^{-1}(y) = x \Longleftrightarrow y = f(x),\ \forall y \in B$$

Sea y cualquiera de B. Como f es sobreyectiva, existirá $x \in A$ tal que $f(x) = y$. Pues bien,

$$f(x) = y \Longleftrightarrow 2x = y \Longleftrightarrow x = \frac{y}{2} \Longleftrightarrow f^{-1}(y) = \frac{y}{2}$$

Es decir, f^{-1} es la función de B en A que hace corresponder a cada número real su mitad.

$$f^{-1} : B \longrightarrow A \text{ tal que } f^{-1}(y) = \frac{y}{2},\ \forall y \in B$$

■

Ejemplo 8.29

Sean $A = B = \mathbb{R}$ *y* $f : A \longrightarrow B$ *tal que* $f(x) = 2x - 3$

(a) ¿Es f *invertible?*

(b) Si (a) es afirmativo, hallar f^{-1}

Solución

(a) Veamos si f es invertible.

Inyectiva. Sean x_1 y x_2 dos números reales cualesquiera, entonces

$$f(x_1) = f(x_2) \Longrightarrow 2x_1 - 3 = 2x_2 - 3 \Longrightarrow 2x_1 = 2x_2 \Longrightarrow x_1 = x_2$$

Sobreyectiva. Sea $y \in B$, cualquiera. Tomando

$$x = \frac{y+3}{2}$$

tendremos que

$$x \in \mathbb{R} \text{ y } f(x) = f\left(\frac{y+3}{2}\right) = 2\frac{y+3}{2} - 3 = y$$

luego f es sobreyectiva.

Por ser inyectiva y sobreyectiva, f es biyectiva, luego por 8.4.2, f es invertible.

(b) Calculamos f^{-1}.

Sea y un elemento arbitrario de B. Entonces, al ser f sobreyectiva, existirá x en A tal que $f(x) = y$. Pues bien, apoyándonos en la definición de f^{-1},

$$f(x) = y \Longleftrightarrow 2x - 3 = y \Longleftrightarrow x = \frac{y+3}{2} \Longleftrightarrow f^{-1}(y) = \frac{y+3}{2}$$

luego,

$$f^{-1} : B \longrightarrow A \text{ tal que } f^{-1}(y) = \frac{y+3}{2},\ \forall y \in B$$

■

Ejemplo 8.30

Sean $A = B = \mathbb{R}$ y $f : A \longrightarrow B$ definida por $f(x) = x^3 + 2$. Encontrar una fórmula para la función inversa de f.

Solución

(a) Veamos si f es invertible.

Inyectiva. Sean x_1 y x_2 cualesquiera de A.

$$f(x_1) = f(x_2) \Longrightarrow x_1^3 + 2 = x_2^3 + 2 \Longrightarrow x_1^3 = x_2^3 \Longrightarrow x_1 = x_2$$

Sobreyectiva. Para cada $y \in B$, tomando $x = \sqrt[3]{y-2}$, tenemos que $x \in A$ y

$$f(x) = f\left(\sqrt[3]{y-2}\right) = \left(\sqrt[3]{y-2}\right)^3 + 2 = y - 2 + 2 = y$$

Por ser inyectiva y sobreyectiva es biyectiva y, por tanto, invertible.

(b) Calculamos su inversa.

Sea f^{-1} la inversa de f e y cualquiera de B. Dado que f es sobreyectiva, existe x en A tal que $f(x) = y$. Pues bien,

$$f(x) = y \Longleftrightarrow x^3 + 2 = y \Longleftrightarrow x = \sqrt[3]{y-2} \Longleftrightarrow f^{-1}(y) = \sqrt[3]{y-2}$$

luego,

$$f^{-1} : B \longrightarrow A \text{ tal que } f^{-1}(y) = \sqrt[3]{y-2},\ \forall y \in B$$

■

8.5 Composición de Funciones e Inversa de una Función

Veremos ahora como la composición de funciones nos permite definir y caracterizar de otra forma la inversa de una función.

A lo largo de todo el apartado, f será una función entre dos conjuntos A y B.

8.5.1 Proposición

La función f es invertible si, y sólo si existe una función f^{-1} de B en A tal que $f^{-1} \circ f = i_A$ y $f \circ f^{-1} = i_B$, donde i_A y i_B son las identidades en A y B, respectivamente.

Demostración

$$f \text{ es invertible } \Longleftrightarrow \exists f^{-1} : B \longrightarrow A \text{ tal que } f^{-1} \circ f = i_A \text{ y } f \circ f^{-1} = i_B$$

$\Longrightarrow$) Supongamos que f es una función invertible y sea f^{-1} su función inversa. Teniendo en cuenta la definición de inversa, tendremos

$$f^{-1} : B \longrightarrow A \text{ tal que } f^{-1}(b) = a \Longleftrightarrow b = f(a),\ \forall b \in B$$

Pues bien,

$$\left.\begin{array}{l} f : A \longrightarrow B \\ f^{-1} : B \longrightarrow A \end{array}\right\} \Longrightarrow f^{-1} \circ f : A \longrightarrow A$$

y si a es cualquiera de A, tenemos

$$(f^{-1} \circ f)(a) = f^{-1}\left[f(a)\right] = f^{-1}(b) = a = i_A(a)$$

es decir,

$$f^{-1} \circ f = i_A$$

donde

$$i_A : A \longrightarrow A \text{ tal que } i_A(a) = a,\ \forall a \in A$$

es decir, i_A es la identidad en A.

Análogamente,

$$\left.\begin{array}{l} f^{-1} : B \longrightarrow A \\ f : A \longrightarrow B \end{array}\right\} \Longrightarrow f \circ f^{-1} : B \longrightarrow B$$

y si b es cualquiera de B, tendremos que

$$(f \circ f^{-1})(b) = f\left[f^{-1}(b)\right] = f(a) = b = i_B(b)$$

por tanto,

$$f^{-1} \circ f = i_B$$

donde,

$$i_B : B \longrightarrow B \text{ tal que } i_B(b) = b,\ \forall b \in B$$

o sea, i_B es la identidad en B.

$\Longleftarrow$) Recíprocamente, supongamos que existe una función f^{-1} de B en A tal que $f^{-1} \circ f = i_A$ y $f \circ f^{-1} = i_B$, entonces,

(a) f es *inyectiva*. En efecto, si a_1, a_2 son dos elementos cualesquiera de A, entonces

$$\begin{array}{rcl} f(a_1) = f(a_2) & \Longrightarrow & f^{-1}\left[f(a_1)\right] = f^{-1}\left[f(a_2)\right] \\ & \Longrightarrow & (f^{-1} \circ f)(a_1) = (f^{-1} \circ f)(a_2) \quad \{\text{Por hipótesis } f^{-1} \circ f = i_A\} \\ & \Longrightarrow & i_A(a_1) = i_A(a_2) \\ & \Longrightarrow & a_1 = a_2 \end{array}$$

(b) f es *sobreyectiva*. En efecto, sea $b \in B$, cualquiera. Entonces,

$$f^{-1}(b) \in A$$

tomando $f^{-1}(b) = a$, tendremos que $a \in A$ y

$$f(a) = f\left[f^{-1}(b)\right] = (f \circ f^{-1})(b) = I_B(b) = b$$

luego f es sobreyectiva.

De (a) y (b) se sigue que f es biyectiva luego por 8.4.2 tendremos que f es invertible.

■

Obsérvese que además de caracterizar las funciones invertibles, con la proposición anterior, hemos construido f^{-1}, inversa de la función f.

Ejemplo 8.31

Sea f una función de A en B. Encontrar f^{-1} en los siguientes casos:

(a) $A = \{x : x \in \mathbb{R} \text{ y } x \geqslant -1\}$, $B = \{x : x \in \mathbb{R} \text{ y } x \geqslant 0\}$ y $f(a) = \sqrt{a+1}$.

(b) $A = B = \mathbb{R}$ y $f(a) = a^3 + 1$

(c) $A = B = \mathbb{R}$ y $f(a) = \dfrac{2a-1}{3}$

(d) $A = B = \{1, 2, 3, 4, 5\}$ y $f = \{(1, 3), (2, 2), (3, 4), (4, 5), (5, 1)\}$

Solución

(a) $A = \{x : x \in \mathbb{R} \text{ y } x \geqslant -1\}$, $B = \{x : x \in \mathbb{R} \text{ y } x \geqslant 0\}$ y $f(a) = \sqrt{a+1}$.
Sea f^{-1} la inversa de f. Según hemos visto en 8.5.1, $f \circ f^{-1} = i_B$. Pues bien,

$$\begin{aligned} f \circ f^{-1} = i_B &\iff (f \circ f^{-1})(b) = i_B(b),\ \forall b \in B \\ &\iff f\left[f^{-1}(b)\right] = b,\ \forall b \in B \\ &\iff \sqrt{f^{-1}(b)+1} = b,\ \forall b \in B \\ &\iff f^{-1}(b) = b^2 - 1,\ \forall b \in B \end{aligned}$$

luego,

$$f^{-1} : B \longrightarrow A \text{ tal que } f^{-1}(b) = b^2 - 1,\ \forall b \in B$$

es la inversa de f.

(b) $A = B = \mathbb{R}$ y $f(a) = a^3 + 1$
Procediendo igual que en el apartado anterior,

$$\begin{aligned} f \circ f^{-1} = i_B &\iff (f \circ f^{-1})(b) = i_B(b),\ \forall b \in B \\ &\iff f\left[f^{-1}(b)\right] = b,\ \forall b \in B \\ &\iff (f^{-1}(b))^3 + 1 = b,\ \forall b \in B \\ &\iff f^{-1}(b) = \sqrt[3]{b-1},\ \forall b \in B \end{aligned}$$

luego,

$$f^{-1} : B \longrightarrow A \text{ tal que } f^{-1}(b) = \sqrt[3]{b-1},\ \forall b \in B$$

es la inversa de f.

(c) $A = B = \mathbb{R}$ y $f(a) = \dfrac{2a-1}{3}$
De un modo similar a los apartados anteriores,

$$\begin{aligned} f \circ f^{-1} = i_B &\iff (f \circ f^{-1})(b) = i_B(b),\ \forall b \in B \\ &\iff f\left[f^{-1}(b)\right] = b,\ \forall b \in B \\ &\iff \frac{2f^{-1}(b)-1}{3},\ \forall b \in B \\ &\iff f^{-1}(b) = \frac{3b+1}{2},\ \forall b \in B \end{aligned}$$

luego,

$$f^{-1} : B \longrightarrow A \text{ tal que } f^{-1}(b) = \frac{3b+1}{2},\ \forall b \in B$$

es la inversa de f.

(d) $A = B = \{1, 2, 3, 4, 5\}$ y $f = \{(1, 3), (2, 2), (3, 4), (4, 5), (5, 1)\}$
Es inmediato que

$$f^{-1} = \{(3, 1), (2, 2), (4, 3), (5, 4), (1, 5)\}$$

es la inversa de f.

■

8.5.2 Unicidad de la Inversa

Si f es invertible, entonces su inversa es única.

Demostración

Supongamos que f es invertible y sea f^{-1} su inversa, es decir,

$$f^{-1} : B \longrightarrow A \text{ tal que } f^{-1}(b) = a \Longleftrightarrow b = f(a),\ \forall b \in B$$

con $f^{-1} \circ f = i_A$ y $f \circ f^{-1} = i_B$.

Supongamos que existe otra función h que es también inversa de f,

$$h : B \longrightarrow A \text{ tal que } h \circ f = i_A \text{ y } f \circ h = i_B$$

entonces,

$$h = h \circ i_B = h \circ (f \circ f^{-1}) = (h \circ f) \circ f^{-1} = i_A \circ f^{-1} = f^{-1}$$
$$h = i_A \circ h = (f^{-1} \circ f) \circ h = f^{-1} \circ (f \circ h) = f^{-1} \circ i_B = f^{-1}$$

es decir,

$$h = f^{-1}$$

Consecuentemente la inversa de f, si existe, es única.

■

8.5.3 Inversa de la Composición de Funciones

Si f y g son invertibles, entonces $g \circ f$ es invertible y

$$(g \circ f)^{-1} = f^{-1} \circ g^{-1}$$

Demostración

Sea g una función entre los conjuntos B y C.

(a) $g \circ f$ es invertible. En efecto,

$$\left.\begin{array}{l} f \text{ es invertible, luego es biyectiva} \\ g \text{ es invertible, luego es biyectiva} \end{array}\right\} \overset{(8.3.4)}{\Longrightarrow} g \circ f \text{ es biyectiva} \Longleftrightarrow g \circ f \text{ es invertible}$$

(b) Veamos ahora quien es la inversa de la composición.

Por definición,

$$f^{-1} : B \longrightarrow A \text{ tal que } f^{-1}(b) = a \Longleftrightarrow b = f(a),\ \forall b \in B$$

$$g^{-1} : C \longrightarrow B \text{ tal que } g^{-1}(c) = b \Longleftrightarrow c = g(b),\ \forall c \in C$$

Pues bien, para cada $c \in C$ se verifica

$$\begin{aligned}
(g \circ f) \circ (f^{-1} \circ g^{-1})(c) &= (g \circ f)\left[\left(f^{-1} \circ g^{-1}\right)(c)\right] \\
&= (g \circ f)\left[f^{-1}\left(g^{-1}(c)\right)\right] \\
&= (g \circ f)\left[f^{-1}(b)\right] \\
&= (g \circ f)(a) \\
&= g\left[f(a)\right] \\
&= g(b) \\
&= c \\
&= i_C(c)
\end{aligned}$$

luego,

$$(g \circ f) \circ (f^{-1} \circ g^{-1}) = i_C \tag{8.1}$$

Por otro lado, para cada $a \in A$, tenemos

$$\begin{aligned}
(f^{-1} \circ g^{-1}) \circ (g \circ f)(a) &= (f^{-1} \circ g^{-1})\left[(g \circ f)(a)\right] \\
&= (f^{-1} \circ g^{-1})\left[g\left(f(a)\right)\right] \\
&= (f^{-1} \circ g^{-1})\left[g(b)\right] \\
&= (f^{-1} \circ g^{-1})(c) \\
&= f^{-1}\left[g^{-1}(c)\right] \\
&= f^{-1}(b) \\
&= a \\
&= i_A(a)
\end{aligned}$$

es decir,

$$(f^{-1} \circ g^{-1}) \circ (g \circ f) = i_A \tag{8.2}$$

De (8.1), (8.2) y de 8.5.1 se sigue que

$$(g \circ f)^{-1} = f^{-1} \circ g^{-1}$$

■

Ejemplo 8.32

Verificar el teorema anterior para las funciones $f : A \longrightarrow B$ *y* $g : B \longrightarrow C$ *donde* $A = B = C = \mathbb{R}$ *y* $f(a) = 2a + 1$ *y* $g(b) = b/3$*, respectivamente.*

Solución

$$f : A \longrightarrow B \text{ tal que } f(a) = 2a + 1,\ \forall a \in A$$

$$g : B \longrightarrow C \text{ tal que } g(b) = \frac{b}{3},\ \forall b \in B$$

Cálculo de $g \circ f$.

Sea a cualquiera de A. Entonces,

$$(g \circ f)(a) = g\left[f(a)\right] = g(2a+1) = \frac{2a+1}{3}$$

es decir,

$$g \circ f : A \longrightarrow C \text{ tal que } (g \circ f)(a) = \frac{2a+1}{3},\ \forall a \in A$$

Cálculo de $(g \circ f)^{-1}$.

$$(g \circ f)^{-1} : C \longrightarrow A \text{ tal que } (g \circ f) \circ (g \circ f)^{-1} = i_C$$

Pues bien,

$$\begin{aligned}
(g \circ f) \circ (g \circ f)^{-1} = i_C &\iff \left((g \circ f) \circ (g \circ f)^{-1}\right)(c) = c,\ \forall c \in C \\
&\iff (g \circ f)\left[(g \circ f)^{-1}(c)\right] = c,\ \forall c \in C \\
&\iff \frac{2(g \circ f)^{-1}(c)+1}{3} = c,\ \forall c \in C \\
&\iff (g \circ f)^{-1}(c) = \frac{3c-1}{2},\ \forall c \in C
\end{aligned}$$

luego,

$$(g \circ f)^{-1} : C \longrightarrow A \text{ tal que } (g \circ f)^{-1}(c) = \frac{3c-1}{2},\ \forall c \in C$$

Cálculo de f^{-1}.

$$f^{-1} : B \longrightarrow A \text{ tal que } f \circ f^{-1} = i_B$$

Entonces,

$$\begin{aligned}
f \circ f^{-1} = i_B &\iff (f \circ f^{-1})(b) = i_B(b),\ \forall b \in B \\
&\iff f\left[f^{-1}(b)\right] = b \\
&\iff 2f^{-1}(b) + 1 = b \\
&\iff f^{-1}(b) = \frac{b-1}{2}
\end{aligned}$$

luego,

$$f^{-1} : B \longrightarrow A \text{ tal que } f^{-1}(b) = \frac{b-1}{2},\ \forall b \in B$$

Cálculo de g^{-1}.

$$g^{-1} : C \longrightarrow B \text{ tal que } g \circ f^{-1} = i_C$$

luego,

$$\begin{aligned}
g \circ g^{-1} = i_C &\iff (g \circ g^{-1})(c) = i_C(c),\ \forall c \in C \\
&\iff g\left[g^{-1}(c)\right] = c \\
&\iff \frac{g^{-1}(c)}{3} = c \\
&\iff g^{-1}(c) = 3c,\ \forall c \in C
\end{aligned}$$

es decir,

$$g^{-1} : C \longrightarrow B \text{ tal que } g^{-1}(c) = 3c,\ \forall c \in C$$

Cálculo de $f^{-1} \circ g^{-1}$.

$$f^{-1} \circ g^{-1} : C \longrightarrow A \text{ tal que } (f^{-1} \circ g^{-1})(c) \in A,\ \forall c \in C$$

Pues bien, sea c cualquiera de C. Entonces,

$$(f^{-1} \circ g^{-1})(c) = f^{-1}\left[g^{-1}(c)\right] = f^{-1}(3c) = \frac{3c-1}{2}$$

por tanto,

$$f^{-1} \circ g^{-1} : C \longrightarrow A \text{ tal que } (f^{-1} \circ g^{-1})(c) = \frac{3c-1}{2},\ \forall c \in C$$

Consecuentemente,

$$(f^{-1} \circ g^{-1})(c) = (g \circ f)^{-1}(c),\ \forall c \in C$$

de aquí que

$$(g \circ f)^{-1} = f^{-1} \circ g^{-1}$$

verificándose el teorema anterior.

■

Ejemplo 8.33

Sean $f : A \longrightarrow B$ y $g : B \longrightarrow A$. Verificar que $g = f^{-1}$ en los casos siguientes:

(a) $A = B = \mathbb{Z},\ f(a) = \dfrac{a+1}{2},\ g(b) = 2b-1$

(b) $A = \mathbb{R}_0^+,\ B = \{y : y \in \mathbb{R} \text{ e } y \geqslant -1\},\ f(a) = a^2 - 1,\ g(b) = \sqrt{b+1}$

(c) $A = B = \mathscr{P}(S)$, *donde S es un conjunto.* $f(X) = X^c,\ g(X) = X^c,\ \forall X \in \mathscr{P}(S)$

(d) $A = B = \{1,2,3,4\},\ f = \{(1,4),(2,1),(3,2),(4,3)\}$ y $g = \{(1,2),(2,3),(3,4),(4,1)\}$

Solución

Según hemos visto en 8.5.1, tendremos que probar, en cada uno de los casos, que

$$g \circ f = i_A \text{ y } f \circ g = i_B$$

(a) $A = B = \mathbb{Z},\ f(a) = \dfrac{a+1}{2},\ g(b) = 2b-1$

Sea $a \in A$, cualquiera. Entonces,

$$(g \circ f)(a) = g\left[f(a)\right] = g\left(\frac{a+1}{2}\right) = 2\frac{a+1}{2} - 1 = a = i_A(a)$$

Sea $b \in B$, cualquiera. Entonces,

$$(f \circ g)(b) = f\left[g(b)\right] = f\left(2b-1\right) = 2\frac{2b-1+1}{2} - 1 = b = i_B(b)$$

luego,

$$g \circ f = i_A \text{ y } f \circ g = i_B$$

y, consecuentemente, g es la inversa de f.

(b) $A = \mathbb{R}_0^+,\ B = \{y : y \in \mathbb{R} \text{ e } y \geqslant -1\},\ f(a) = a^2 - 1,\ g(b) = \sqrt{b+1}$
Para cada $a \in A$, se verifica:

$$(g \circ f)(a) = g\left[f(a)\right] = g(a^2 - 1) = \sqrt{a^2 - 1 + 1} = a = i_A(a)$$

y para cada $b \in B$,

$$(f \circ g)(b) = f\left[g(b)\right] = f\left(\sqrt{b+1}\right) = \left(\sqrt{b+1}\right)^2 - 1 = b = i_B(b)$$

luego,

$$g \circ f = i_A \text{ y } f \circ g = i_B$$

y $g = f^{-1}$.

(c) $A = B = \mathscr{P}(S)$, donde S es un conjunto. $f(X) = X^c,\ g(X) = X^c,\ \forall X \in \mathscr{P}(S)$
Para cada $X \in \mathscr{P}(S)$, tenemos

$$(g \circ f)(X) = g\left[f(X)\right] = g(X^c) = (X^c)^c = X = i_{\mathscr{P}(S)}(X)$$
$$(f \circ g)(X) = f\left[g(X)\right] = f(X^c) = (X^c)^c = X = i_{\mathscr{P}(S)}(X)$$

luego, $g = f^{-1}$.

(d) $A = B = \{1,2,3,4\},\ f = \{(1,4),(2,1),(3,2),(4,3)\}$ y $g = \{(1,2),(2,3),(3,4),(4,1)\}$

$$g \circ f = \{(1,1),(2,2),(3,3),(4,4)\} = i_A$$
$$f \circ g = \{(1,1),(2,2),(3,3),(4,4)\} = i_B$$

luego $g = f^{-1}$.

■

Unidad Temática IV

Ecuaciones de Recurrencia

Lección 9

Generalidades

> No existe nada más difícil de emprender, más peligroso de dirigir, ni de más incierto éxito que la iniciativa de la introducción de un nuevo orden de las cosas
>
> Niccolo Machiavelli. El Principe, 1513

9.1 Introducción

Brevemente, puede decirse que un algoritmo recursivo es aquél que se llama a si mismo. En general este tipo de algoritmos establece lo siguiente:

- acción que realiza cuando el conjunto de datos contiene un único elemento, es decir, cuando $n = 1$.

y también especifica lo que haría si n fuese mayor que 1 en función de dos cosas:

- la acción que realiza para conjuntos con menos de n datos, y
- la actividad necesaria para manejar el dato n-ésimo.

Por otra parte, en la práctica, un algoritmo y una función trabajan, en cierto modo, de forma similar; ambos tienen conjuntos de entrada, salidas que se corresponden con dichas entradas y una regla o conjunto de reglas que gobiernan la transformación de las entradas en salidas.

Desde este punto de vista, si $n \geqslant 1$, un algoritmo recursivo es como una ecuación de la forma

$$a_{n+1} = a_n + a$$

Esto es, a_{n+1} está determinada en función de a_n y una acción (en este caso añade a) para manejar el dato n-ésimo. Veamos un ejemplo de lo que decimos.

Ejemplo 9.1

Supongamos una recepción a la que asisten n diplomáticos y en el transcurso de la misma cada uno estrecha la mano de todos los demás exactamente una vez. ¿Cuántos apretones de manos tienen lugar?

Solución

Una primera forma de aproximarnos al problema podría ser la siguiente: supongamos que hay únicamente dos diplomáticos en la recepción. Entonces, el número de apretones de manos es, obviamente, uno.

Supongamos, ahora, que en la recepción hay n diplomáticos y sea a_n el número de apretones de manos que tienen lugar. Entonces, si llega un nuevo diplomático, tendrán lugar a_{n+1} apretones de manos.

El $n+1$-ésimo diplomático tendrá que estrechar la mano de los n restantes, por lo tanto el número total de apretones de manos es n más los a_n que han tenido lugar antes de su llegada. De esta forma,

$$a_{n+1} = a_n + n$$

Combinando estas observaciones, tendremos las ecuaciones

$$a_2 = 1$$
$$a_{n+1} = a_n + n,\ n \geqslant 2$$

si ahora damos valores a n, tendremos

$$a_3 = a_2 + 2 = 1 + 2$$
$$a_4 = a_3 + 3 = 1 + 2 + 3$$
$$a_5 = a_4 + 4 = 1 + 2 + 3 + 4$$

luego podemos inferir que, en general,

$$a_n = 1 + 2 + 3 + \cdots + (n-2) + (n-1) = \frac{1 + (n-1)}{2}(n-1) = \frac{n(n-1)}{2}$$

Obsérvese que la definición de a_{n+1} consta de dos partes: una ecuación que expresa a_{n+1} en términos de a_n y un valor para a_2.

■

9.1.1 Ecuación de Recurrencia

La ecuación que expresa a_{n+k} en términos de $a_{n+(k-1)}, a_{n+(k-2)}, \ldots\ldots, a_{n+2}, a_{n+1}, a_n$ se llama relación o ecuación de recurrencia.

Si además se dan uno o más valores para a_n, como $a_1, a_2, \ldots$, las llamaremos *condiciones iniciales o de contorno.*

En el ejemplo de la introducción, la ecuación de recurrencia es

$$a_{n+1} = a_n + n,\ n \geqslant 2$$

y la única condición inicial es

$$a_2 = 1$$

■

9.2 Solución de las Ecuaciones de Recurrencia

A continuación desarrollaremos teoremas y técnicas que nos permitirán resolver determinadas ecuaciones de recurrencia.

Comenzaremos dejando claro lo que se entiende por solución de una ecuación de recurrencia.

9.2.1 Sucesión

Una sucesión es una función real definida en el conjunto de los enteros positivos, $\mathbb{Z}^+$.

■

Ejemplo 9.2

(a) $1, 2, 3, 4, \ldots,$ *es la sucesión* $f : \mathbb{Z}^+ \longrightarrow \mathbb{R} : f(n) = n,\ \forall n \in \mathbb{Z}^+$ *que notaremos* $\{a_n\}$ *tal que* $a_n = n,\ \forall n,$ *ó simplemente* $\{n\}$.

(b) $0, 3, 8, 15, 24, 35, \ldots,$ *es la sucesión* f *tal que* $f(n) = n^2 - 1$ *ó* $\left\{n^2 - 1\right\}$.

■

9.2.2 Solución

Una solución de una ecuación de recurrencia es una sucesión tal que sus términos satisfacen la ecuación y sus condiciones iniciales.

Si no se especifican las condiciones iniciales, diremos que la sucesión es una solución de la ecuación de recurrencia si es solución para algún conjunto de condiciones iniciales.

■

Ejemplo 9.3

La sucesión $\{a_n\}$ *tal que* $a_n = n$ *es solución de la ecuación de recurrencia*

$$a_1 = 1$$
$$a_{n+1} = a_n + 1,\ n \geqslant 1$$

ya que $a_1 = 1$*, es decir satisface la condición inicial y*

$$a_{n+1} = n + 1 = a_n + 1,\ \forall n \geqslant 1$$

luego también satisface la ecuación.

■

Ejemplo 9.4

Probar que la sucesión $\{a_n\}$ tal que

$$a_n = \frac{n(n-1)}{2},\ \forall n \in \mathbb{Z}^+$$

es una solución para el problema del "apretón de manos" planteado en la introducción del tema.

Solución

Recordemos que la ecuación de recurrencia que obtuvimos en tal problema era

$$a_2 = 1$$
$$a_{n+1} = a_n + n,\ n \geqslant 2$$

Pues bien, comprobemos primero que satisface la condición inicial. En efecto,

$$a_n = \frac{n(n-1)}{2} \Longrightarrow a_2 = \frac{2 \cdot 1}{2} = 1$$

Para ver que $\{a_n\}$ satisface la ecuación, utilizaremos la inducción sobre n.

- Para $n = 2$, hemos comprobado que se satisface.
- Supongamos que la ecuación se verifica para $n = p$, con $p > 2$, es decir,

$$a_p = \frac{p(p-1)}{2}$$

- Veamos que también se verifica para $n = p + 1$. En efecto,

$$\begin{aligned} a_{p+1} &= a_p + p \\ &= \frac{p(p-1)}{2} + p \\ &= \frac{p(p-1) + 2p}{2} \\ &= \frac{p(p-1+2)}{2} \\ &= \frac{(p+1)p}{2} \end{aligned}$$

luego por el principio de inducción matemática, se verifica que

$$a_n = \frac{n(n-1)}{2}$$

y la sucesión $\{a_n\}$ es, por tanto, una solución del problema propuesto.

■

Lección 10

Ecuaciones de Recurrencia Lineales

10.1 Generalidades

10.1.1 Definición

Una ecuación de recurrencia se dice que es lineal si puede escribirse en la forma:

$$d_k(n)a_{n+k} + d_{k-1}(n)a_{n+(k-1)} + d_{k-2}(n)a_{n+(k-2)} + \cdots + d_2(n)a_{n+2} + d_1(n)a_{n+1} + d_0(n)a_n = b(n)$$

donde $\{a_n\}$ *es una sucesión, y*

$$d_0(n), d_1(n), \ldots, d_k(n) \text{ y } b(n)$$

son funciones de $\mathbb{Z}^+$ *en* $\mathbb{R}$ *llamados, respectivamente, coeficientes y término independiente de la ecuación.*

■

10.1.2 Orden de una Ecuación Lineal

Diremos que una ecuación de recurrencia lineal es de orden k*, si* k *es el mayor entero para el cual los coeficientes* $d_0(n)$ *y* $d_k(n)$ *son, ambos, distintos de cero cuando la ecuación está escrita en la forma definida anteriormente.*

■

10.1.3 Forma general de una ecuación de recurrencia lineal de orden k

Sea

$$d_k(n)a_{n+k} + d_{k-1}(n)a_{n+(k-1)} + d_{k-2}(n)a_{n+(k-2)} + \cdots + d_2(n)a_{n+2} + d_1(n)a_{n+1} + d_0(n)a_n = b(n)$$

una ecuación de recurrencia lineal de orden k*, es decir,* $d_k(n) \neq 0$ *y* $d_0(n) \neq 0$*. Si dividimos los dos miembros de la ecuación por* $d_k(n)$*, tendremos*

$$a_{n+k} + \frac{d_{k-1}(n)}{d_k(n)}a_{n+(k-1)} + \frac{d_{k-2}(n)}{d_k(n)}a_{n+(k-2)} + \cdots + \frac{d_2(n)}{d_k(n)}a_{n+2} + \frac{d_1(n)}{d_k(n)}a_{n+1} + \frac{d_0(n)}{d_k(n)}a_n = \frac{b(n)}{d_k(n)}$$

y tomando,

$$c_i(n) = \frac{d_i(n)}{d_k(n)} \text{ para } 0 \leqslant i \leqslant k-1 \text{ y } h(n) = \frac{b(n)}{d_k(n)}$$

resultaría

$$a_{n+k} + c_{k-1}(n)a_{n+(k-1)} + c_{k-2}(n)a_{n+(k-2)} + \cdots + c_2(n)a_{n+2} + c_1(n)a_{n+1} + c_0(n)a_n = h(n).$$

que es la forma más habitual de presentar una ecuación de este tipo.

■

Ejemplo 10.1

Decir el orden de las siguientes ecuaciones y escribirlas en su forma general.

(a) $2a_{n+3} = 4a_{n+2} + 6a_{n+1} - 4a_n$

(b) $a_{n+1} = 3 + a_n$

(c) $\dfrac{a_{n+1}}{5} = a_n$

Solución

(a) Los coeficientes de a_{n+3} y a_n son, respectivamente, 2 y -4, es decir la ecuación es lineal y de orden 3. Para escribir la ecuación en su forma general, bastará con pasar todos los términos al primer miembro y dividir por 2.

$$a_{n+3} - 2a_{n+2} - 3a_{n+1} + 2a_n = 0.$$

(b) Su forma general sería:

$$a_{n+1} - a_n = 3$$

es decir es una ecuación lineal de primer orden cuyo término independiente es 3.

(c) Ecuación lineal de primer orden cuya forma general es:

$$a_{n+1} - 5a_n = 0.$$

■

10.1.4 Clasificación

Clasificaremos las ecuaciones de recurrencia lineales según sus coeficientes y su término independiente.

⊛ *Homogéneas con coeficientes constantes.*

En este caso $h(n) = 0$ *para cada* n *y* $c_i(n) = c_i$*, para* $0 \leqslant i \leqslant k-1$ *y para cualquier* n*,*

$$a_{n+k} + c_{k-1}a_{n+(k-1)} + c_{k-2}a_{n+(k-2)} + \cdots + c_2a_{n+2} + c_1a_{n+1} + c_0a_n = 0.$$

⊛ *Homogéneas con coeficientes no constantes.*
En este caso $h(n) = 0$, para cada n.

$$a_{n+k} + c_{k-1}(n)a_{n+(k-1)} + c_{k-2}(n)a_{n+(k-2)} + \cdots + c_2(n)a_{n+2} + c_1(n)a_{n+1} + c_0(n)a_n = 0.$$

⊛ *No homogéneas con coeficientes constantes.*
En este caso $c_i(n) = c_i$, para $0 \leqslant i \leqslant k-1$ y para todo n,

$$a_{n+k} + c_{k-1}a_{n+(k-1)} + c_{k-2}a_{n+(k-2)} + \cdots + c_2a_{n+2} + c_1a_{n+1} + c_0a_n = h(n).$$

⊛ *No homogéneas con coeficientes no constantes. Este sería el caso más general.*

$$a_{n+k} + c_{k-1}(n)a_{n+(k-1)} + c_{k-2}(n)a_{n+(k-2)} + \cdots + c_2(n)a_{n+2} + c_1(n)a_{n+1} + c_0(n)a_n = h(n).$$

■

10.2 Soluciones

Como ya vimos en 9.2.2, una solución de una ecuación de recurrencia es una sucesión tal que sus términos satisfacen la ecuación y sus condiciones iniciales. Consideremos, por ejemplo, la ecuación de recurrencia lineal de segundo orden $a_{n+2} - 4a_{n+1} + 4a_n = 0$. Podemos comprobar fácilmente que las sucesiones

$$\{1, 2, 4, 8, 16, 32, 64, 128, 256, \ldots\ldots, \}$$

$$\{0, 1, 4, 12, 32, 80, 192, 448, 1024, \ldots\ldots, \}$$

$$\{2, 3, 4, 4, 0, -16, -64, -192, -512, \ldots\ldots, \}$$

son, las tres, solución de la ecuación propuesta. Si multiplicamos cualquiera de ellas por un número, obtendríamos otra solución

$$5 \cdot \{1, 2, 4, 8, 16, 32, 64, 128, 256, \ldots\ldots, \} = \{5, 10, 20, 40, 80, 160, 320, 640, 1280, \ldots\ldots, \}$$

y si, por ejemplo, sumamos las tres el resultado sería, también, una solución para la ecuación propuesta.

$$\begin{aligned} \{1, 2, 4, 8, 16, 32, 64, 128, 256, \ldots\ldots, \} &+ \{0, 1, 4, 12, 32, 80, 192, 448, 1024, \ldots\ldots, \} \\ &+ \{2, 3, 4, 4, 0, -16, -64, -192, -512, \ldots\ldots, \} \\ &= \{3, 6, 12, 24, 48, 96, 192, 384, 768, \ldots\ldots, \} \end{aligned}$$

Podemos concluir, por tanto, que la ecuación $a_{n+2} - 4a_{n+1} + 4a_n = 0$ tiene infinitas soluciones.

Ejemplo 10.2

¿Cuál de las siguientes ecuaciones tiene solución única?

(a)

$$\begin{aligned} a_1 &= 2 \\ a_{n+2} &= 4a_{n+1} - 4a_n, \ n \geqslant 1 \end{aligned}$$

(b)

$$\begin{aligned} a_1 &= 1 \\ a_2 &= 5 \\ a_{n+1} &= a_n + 3,\ n \geqslant 1 \end{aligned}$$

(c)

$$\begin{aligned} a_1 &= 0 \\ a_3 &= 1 \\ a_{n+2} &= a_{n+1} + a_n,\ n \geqslant 1 \end{aligned}$$

Solución

(a) Observemos lo siguiente:

$$\begin{array}{lllllll} n=1. & a_3 = 4(a_2-a_1) & = & 4a_2-8 & & \\ n=2. & a_4 = 4(a_3-a_2) & = & 4(3a_2-8) & = & 12a_2-32 \\ n=3. & a_5 = 4(a_4-a_3) & = & 4(8a_2-24) & = & 32a_2-96 \\ n=4. & a_6 = 4(a_5-a_4) & = & 4(20a_2-64) & = & 80a_2-256 \\ \vdots & \vdots & & \vdots & & \vdots \end{array}$$

La solución podría ser, por tanto, la sucesión

$$\{2, a_2, 4a_2-8, 12a_2-32, 32a_2-96, 80a_2-256, \ldots\ldots,\}$$

y bastaría tomar como a_2 cualquier número para obtener una solución. Consecuentemente, la solución no es única.

(b) Su forma general es:

$$a_{n+1} = a_n + 3 \Longleftrightarrow a_{n+1} - a_n = 3.$$

es decir, es una ecuación de recurrencia lineal de primer orden. La ecuación tiene dos condiciones iniciales ($a_1 = 1$ y $a_2 = 5$). Tomando $n = 1$ en la ecuación

$$a_2 = a_1 + 3 = 1 + 3 = 4$$

pero $a_2 = 5$, por lo tanto, la ecuación no es consistente con esta condición inicial. Así pues, no existen soluciones que satisfagan la ecuación y ambas condiciones iniciales.

(c) Escribiéndola en su forma general,

$$a_{n+2} = a_{n+1} + a_n \Longleftrightarrow a_{n+2} - a_{n+1} - a_n = 0$$

tendremos una ecuación de recurrencia lineal de segundo orden y con dos condiciones iniciales; sin embargo, las condiciones iniciales están definidas para $n = 1$ y $n = 3$, ahora bien, tomando $n = 1$ en la ecuación, obtendremos

$$a_3 = a_2 + a_1$$

y aplicando las condiciones iniciales, $1 = a_2 + 0$, luego $a_2 = 1$ y la única solución posible es:

$$\{0, 1, 1, 2, 3, 5, 8, 13, 21, 34, \ldots\ldots,\}$$

■

10.2.1 Existencia y unicidad de la solución

La ecuación de recurrencia lineal de orden k

$$a_{n+k} + c_{k-1}(n)a_{n+(k-1)} + c_{k-2}(n)a_{n+(k-2)} + \cdots + c_2(n)a_{n+2} + c_1(n)a_{n+1} + c_0(n)a_n = h(n),\ n \geqslant 1$$

tiene solución única si conocemos $a_1, a_2, \ldots, a_k$*, o sea si conocemos k condiciones iniciales.*

Demostración

En efecto, despejando a_{n+k} en la ecuación,

$$a_{n+k} = h(n) - c_{k-1}(n)a_{n+(k-1)} - c_{k-2}(n)a_{n+(k-2)} - \cdots - c_2(n)a_{n+2} - c_1(n)a_{n+1} - c_0(n)a_n$$

para $n \geqslant 1$ y la sucesión que satisface la ecuación, es decir la solución, se define inductivamente en la forma siguiente:

Para $n = 1$,

$$a_{k+1} = h(1) - c_{k-1}(1)a_k - c_{k-2}(1)a_{k-1} - \cdots - c_2(1)a_3 - c_1(1)a_2 - c_0(1)a_1$$

o sea, a_{k+1} viene dado en función $a_k, a_{k-1}, \ldots, a_3, a_2, a_1$, que son las condiciones iniciales. De esta forma, tenemos definido un valor de a_{k+1} que satisface la ecuación y que es, en efecto, el único valor posible que es consistente con la ecuación y las condiciones iniciales.

Para $n = 2$,

$$a_{k+2} = h(2) - c_{k-1}(2)a_{k+1} - c_{k-2}(2)a_k - \cdots - c_2(2)a_4 - c_1(2)a_3 - c_0(2)a_2$$

es decir,

$$a_{k+2} \text{ es función de } \left| \begin{array}{ll} a_{k+1} & \text{Calculado en el paso anterior.} \\ \text{y} & \\ a_k, a_{k-1}, \ldots, a_4, a_3, a_2 & \text{Condiciones iniciales.} \end{array} \right.$$

Para $n = 3$,

$$a_{k+3} = h(3) - c_{k-1}(3)a_{k+2} - c_{k-2}(3)a_{k+1} - \cdots - c_2(3)a_5 - c_1(3)a_4 - c_0(3)a_3$$

es decir,

$$a_{k+3} \text{ es función de } \left| \begin{array}{ll} a_{k+2}, a_{k+1} & \text{Calculados en los pasos anteriores.} \\ \text{y} & \\ a_k, a_{k-1}, \ldots, a_5, a_4, a_3 & \text{Condiciones iniciales.} \end{array} \right.$$

Seguimos así sucesivamente y para $n = k$,

$$a_{k+k} = h(k) - c_{k-1}(k)a_{k+(k-1)} - c_{k-2}(k)a_{k+(k-2)} - \cdots - c_2(k)a_{k+2} - c_1(k)a_{k+1} - c_0(k)a_k$$

Entonces,

$$a_{k+k} \text{ es función de } \left| \begin{array}{ll} a_{k+(k-1)}, a_{k+(k-2)}, \ldots, a_{k+2}, a_{k+1} & \text{Calculados en los pasos anteriores.} \\ \text{y} & \\ a_k & \text{Condición inicial.} \end{array} \right.$$

Y para $n = k + 1$,

$$\begin{aligned} a_{k+(k+1)} \;=\; h(k+1) \;&-\; c_{k-1}(k+1)a_{k+k} \;-\; c_{k-2}(k)a_{k+(k-1)} \;-\; \cdots\cdots \\ &-\; c_2(k+1)a_{k+3} \;-\; c_1(k+1)a_{k+2} \;-\; c_0(k)a_{k+1} \end{aligned}$$

es decir, $a_{k+(k+1)}$ es función de $a_{k+k}, a_{k+(k-1)}, \ldots, a_{k+3}, a_{k+2}, a_{k+1}$, calculados en los pasos anteriores.

Supongamos, ahora, que a_{n+k} está unívocamente determinado por la ecuación y las condiciones iniciales para cualquier $n = p$ con $p > k+1$, es decir,

$$a_{k+p} \text{ es función de } a_{k+(p-1)}, a_{k+(p-2)}, \ldots, a_{k+[p-(k-2)]}, a_{k+[p-(k-1)]}, a_{k+(p-k)}$$

o lo que es igual,

$$a_{k+p} \text{ es función de } a_{k+(p-1)}, a_{k+(p-2)}, \ldots, a_{p+2}, a_{p+1}, a_p.$$

Entonces,

$$\begin{aligned}
a_{k+(p+1)} &= h(p+1) - c_{k-1}(p+1)a_{k+p} - c_{k-2}(p+1)a_{k+(p-1)} \\
&- \cdots\cdots\cdots\cdots - c_2(p+1)a_{k+[p-(k-3)]} - c_1(p+1)a_{k+[p-(k-2)]} \\
&- c_0(p+1)a_{k+[p-(k-1)]} \\
&= h(p+1) - c_{k-1}(p+1)a_{k+p} - c_{k-2}(p+1)a_{k+(p-1)} \\
&- \cdots\cdots\cdots\cdots - c_2(p+1)a_{p+3} - c_1(p+1)a_{p+2} \\
&- c_0(p+1)a_{p+1}
\end{aligned}$$

determina un único valor para $a_{k+(p+1)}$ que es función de

$$a_{k+p}, a_{k+(p-1)}, \ldots, a_{p+3}, a_{p+2}, a_{p+1}$$

y, consecuentemente, la solución $\{a_n\}$ está unívocamente determinada para cada n.

■

Nota 10.1 Obsérvese que el teorema anterior puede modificarse con facilidad para aplicarlo a situaciones en las que las condiciones iniciales estén dadas por k puntos sucesivos, que no han de ser exactamente $n = 1, n = 2, \ldots$, etc.

Por otra parte, y como hemos visto en el ejemplo anterior al teorema, si no se especifican condiciones iniciales para una ecuación de recurrencia lineal, entonces la ecuación tiene infinitas soluciones.

10.3 Propiedades de la solución

Ahora veremos dos propiedades importantes de las soluciones y que usaremos para desarrollar métodos más poderosos para encontrar las soluciones que el de iteración.

10.3.1 Principio de superposición

Si las sucesiones $\{r_n\}$ y $\{s_n\}$ son, ambas, soluciones para una ecuación de recurrencia lineal y homogénea, entonces cualquier combinación lineal de ellas con coeficientes reales también es solución, es decir,

$$\{r_n\} \text{ y } \{s_n\} \text{ son soluciones} \Longrightarrow \{\alpha_1 \cdot r_n + \alpha_2 \cdot s_n\} \text{ con } \alpha_1 \text{ y } \alpha_2 \text{ reales, también lo es.}$$

Demostración

Sea la ecuación,

$$a_{n+k} + c_{k-1}(n)a_{n+(k-1)} + c_{k-2}(n)a_{n+(k-2)} + \cdots + c_1(n)a_{n+1} + c_0(n)a_n = 0$$

entonces, si $\{r_n\}$ y $\{s_n\}$ son soluciones, podemos decir que

$$r_{n+k} + c_{k-1}(n)r_{n+(k-1)} + c_{k-2}(n)r_{n+(k-2)} + \cdots + c_1(n)r_{n+1} + c_0(n)r_n = 0$$

y

$$s_{n+k} + c_{k-1}(n)s_{n+(k-1)} + c_{k-2}(n)s_{n+(k-2)} + \cdots + c_1(n)s_{n+1} + c_0(n)s_n = 0$$

para cada $n \in \mathbb{Z}^+$. Si ahora multiplicamos la primera ecuación por α_1 y la segunda por α_2, obtendremos

$$\alpha_1 r_{n+k} + \alpha_1 c_{k-1}(n)r_{n+(k-1)} + \alpha_1 c_{k-2}(n)r_{n+(k-2)} + \cdots + \alpha_1 c_1(n)r_{n+1} + \alpha_1 c_0(n)r_n = 0$$

y

$$\alpha_2 s_{n+k} + \alpha_2 c_{k-1}(n)s_{n+(k-1)} + \alpha_2 c_{k-2}(n)s_{n+(k-2)} + \cdots + \alpha_2 c_1(n)s_{n+1} + \alpha_2 c_0(n)s_n = 0.$$

Sumando y reagrupando términos, obtendremos

$$\begin{array}{lllll} \alpha_1 r_{n+k} & + \alpha_2 s_{n+k} & + c_{k-1}(n)\left(\alpha_1 r_{n+(k-1)} + \alpha_2 s_{n+(k-1)}\right) & + \cdots \\ & + c_1(n)\left(\alpha_1 r_{n+1} + \alpha_2 s_{n+1}\right) & + c_0(n)\left(\alpha_1 r_n + \alpha_2 s_n\right) & = 0 \end{array}$$

para cada $n \in \mathbb{Z}^+$. Por lo tanto, la sucesión

$$\alpha_1 \{r_n\} + \alpha_2 \{s_n\} = \{\alpha_1 \cdot r_n + \alpha_2 \cdot s_n\}$$

también es una solución de la ecuación.

■

10.3.2 Teorema

Si la sucesión $\{r_n\}$ es una solución de una ecuación de recurrencia no homogénea

$$a_{n+k} + c_{k-1}(n)a_{n+(k-1)} + c_{k-2}(n)a_{n+(k-2)} + \cdots + c_2(n)a_{n+2} + c_1(n)a_{n+1} + c_0(n)a_n = h(n)$$

y $\{s_n\}$ es solución de su ecuación reducida,

$$a_{n+k} + c_{k-1}(n)a_{n+(k-1)} + c_{k-2}(n)a_{n+(k-2)} + \cdots + c_2(n)a_{n+2} + c_1(n)a_{n+1} + c_0(n)a_n = 0$$

entonces la sucesión $\{r_n + s_n\}$ también es una solución de la ecuación no homogénea.

Demostración

En efecto, si $\{r_n\}$ es una solución de la ecuación. Entonces,

$$r_{n+k} + c_{k-1}(n)r_{n+(k-1)} + c_{k-2}(n)r_{n+(k-2)} + \cdots + c_2(n)r_{n+2} + c_1(n)r_{n+1} + c_0(n)r_n = h(n)$$

para cada $n \in \mathbb{Z}^+$. Por otra parte, si $\{s_n\}$ es solución de la ecuación reducida entonces,

$$s_{n+k} + c_{k-1}(n)s_{n+(k-1)} + c_{k-2}(n)s_{n+(k-2)} + \cdots + c_2(n)s_{n+2} + c_1(n)s_{n+1} + c_0(n)s_n = 0$$

Sumando ambas ecuaciones, obtenemos

$$r_{n+k} + s_{n+k} + c_{k-1}(n)\left(r_{n+(k-1)} + s_{n+(k-1)}\right) + \cdots + c_1(n)\left(r_{n+1} + s_{n+1}\right) + c_0(n)\left(r_n + s_n\right) = h(n)$$

De aquí que la sucesión $\{r_n + s_n\}$ también sea solución de la ecuación original.

■

Lección 11

Recurrencias Lineales Homogéneas

11.1 Primer Orden con Coeficientes Constantes

Según 10.1.4, una ecuación de este tipo puede escribirse en la forma

$$a_{n+1} + c_0 a_n = 0.$$

11.1.1 Solución única

Las ecuaciones de recurrencia lineales homogéneas de primer orden y con coeficientes constantes,

$$a_{n+1} + c_0 a_n = 0$$

son las más simples. Obtendremos una solución utilizando la iteración y luego probaremos que es única.

Demostración

Según vimos en 10.2.1 para que la ecuación tenga solución única necesitamos una condición inicial. Tomando como tal $a_1 = \alpha$, tendremos

$$\begin{aligned} a_1 &= \alpha \\ a_{n+1} + c_0 a_n &= 0,\ n \geqslant 1 \end{aligned}$$

la cual, despejando a_{n+1} y haciendo $c_0 = -\lambda$ quedaría en la forma:

$$\begin{aligned} a_1 &= \alpha \\ a_{n+1} &= \lambda a_n,\ n \geqslant 1 \end{aligned}$$

Pues bien,

$$\begin{aligned} a_1 &= \alpha \\ a_2 &= \lambda a_1 = \alpha\lambda \\ a_3 &= \lambda a_2 = \alpha\lambda^2 \\ a_4 &= \lambda a_3 = \alpha\lambda^3 \\ a_5 &= \lambda a_4 = \alpha\lambda^4 \\ &\vdots \quad\quad \vdots \quad\quad \vdots \end{aligned}$$

luego podemos inferir que la sucesión $\{a_n\}$ tal que $a_n = \alpha\lambda^{n-1},\ \forall n$ es solución de la ecuación. Probaremos, por inducción, que en efecto lo es.

– Para $n = 1$,

$$a_1 = \alpha\lambda^0 = \alpha$$

es decir, la solución propuesta satisface la condición inicial.

– Supongamos que es cierto para $n = p$, o sea, $a_p = \alpha\lambda^{p-1}$.

– Veamos que también lo es para $n = p + 1$. En efecto,

$$a_{p+1} = \lambda a_p = \lambda\alpha\lambda^{p-1} = \alpha\lambda^p$$

por lo tanto,

$$a_n = \alpha\lambda^{n-1},\ \forall n \in \mathbb{Z}^+$$

Así pues, la sucesión $\{a_n\}$ tal que $a_n = \alpha\lambda^{n-1},\ \forall n \in \mathbb{Z}^+$ es solución de la ecuación y además como hay una única condición inicial, por el teorema 10.2.1, la solución es única.

■

11.1.2 Solución general

Si en la ecuación anterior no hubiéramos establecido ninguna condición inicial, entonces la sucesión $\{a_n\}$ *tal que* $a_n = \alpha\lambda^{n-1}$ *sería solución para cualquier valor de* λ.

> *Como* a_1 *debe tener algún valor y además sabemos que la solución es única para cada uno de esos valores, la ecuación* $a_n = \alpha\lambda^{n-1}$ *deberá incluir todas las posibles soluciones de* $a_{n+1} = \lambda a_n$.
>
> *A* $a_n = \alpha\lambda^{n-1}$ *la llamaremos solución general de la ecuación, puesto que incluye cada posible solución como un caso particular.*

Una de las estrategias más utilizadas para resolver ecuaciones de recurrencia es encontrar, primero la solución general y luego usar las condiciones iniciales para resolver las constantes arbitrarias que aparecen en ella.

■

Ejemplo 11.1

Existen muchas situaciones regidas por ecuaciones de la forma $a_{n+1} = ra_n$. *Uno de los ejemplos más típicos es la función exponencial, cuya definición recursiva es*

$$a^1 = a$$
$$a^{n+1} = a \cdot a^n,\ n \geqslant 1$$

En este caso, la ecuación de recurrencia se utiliza para definir el significado de a^n. *Así, si escribimos*

$$a_1 = a$$
$$a_{n+1} = a \cdot a_n,\ n \geqslant 1$$

estaremos en el caso planteado en 11.1.1 con $\alpha = a$ *y* $\lambda = a$. *La solución sería, por tanto, la sucesión* $\{a_n\}$ *tal que* $a_n = a \cdot a^{n-1} = a^n$.

■

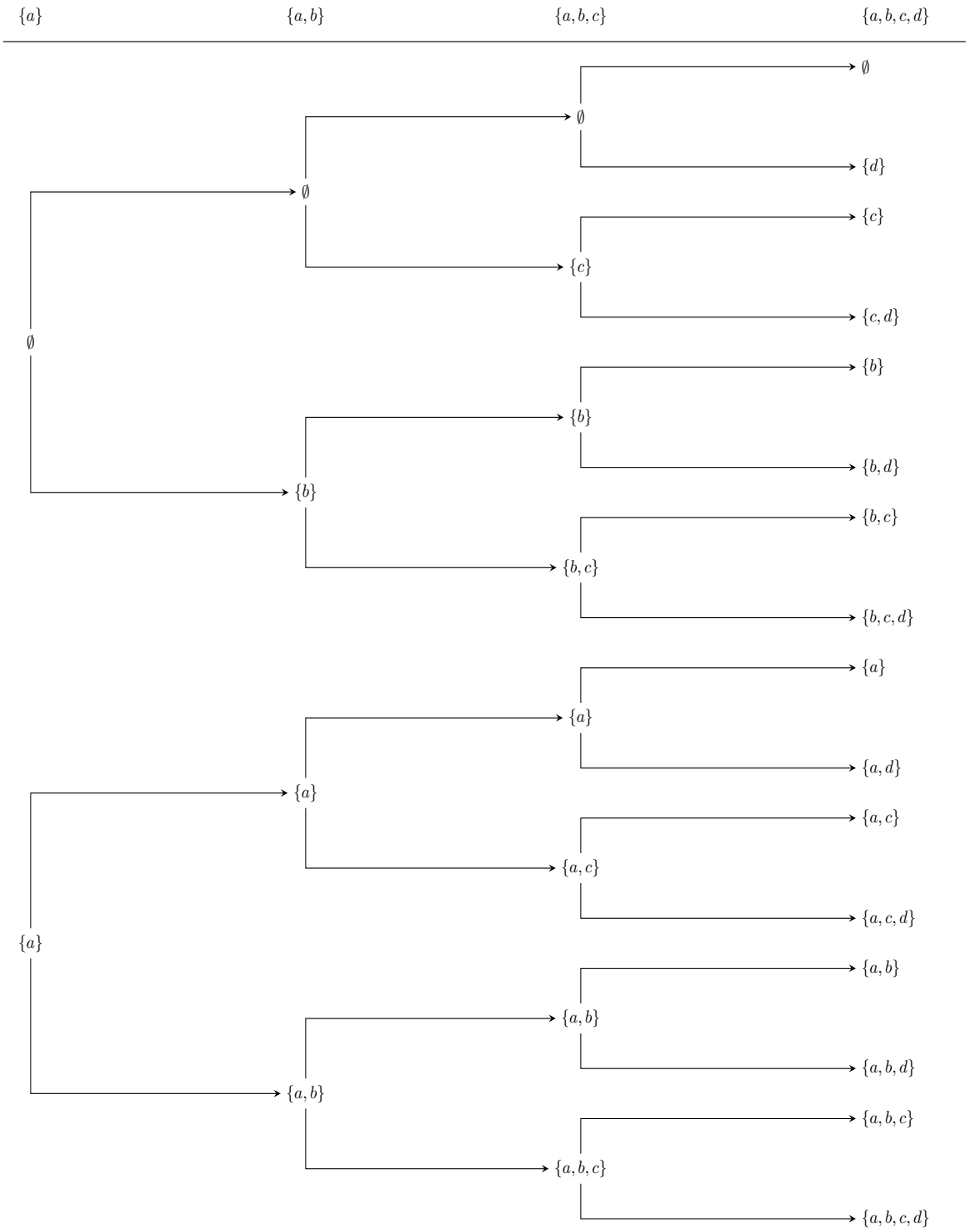
Ejemplo 11.2

Probar que el número de subconjuntos de un conjunto con n elementos es 2^n*, usando ecuaciones de recurrencia.*

Solución

Un conjunto con un elemento, $\{a\}$, tiene dos subconjuntos, el $\emptyset$, y el propio $\{a\}$.

Para obtener los subconjuntos de un conjunto con dos elementos, $\{a, b\}$, basta tener en cuenta que de cada uno de los subconjuntos anteriores podemos obtener dos: él mismo y el que resulta de unirlo con el nuevo elemento, b. Tendríamos pues, $\emptyset$, $\{b\}$, $\{a\}$ y $\{a, b\}$. En el cuadro siguiente vemos el proceso de obtención de los subconjuntos de un conjunto con 1, 2, 3 y 4 elementos.



Como puede verse, cada vez que añadimos un elemento al conjunto, el número de sus subconjuntos se multiplica por 2. De esta forma, si a_n es el número de subconjuntos de un conjunto con n elementos, tendremos que $a_{n+1} = 2a_n$, siendo $a_1 = 2$. Obtendríamos, pues, la siguiente ecuación de recurrencia:

$$\begin{aligned} a_1 &= 2 \\ a_{n+1} &= 2a_n, \quad n \geqslant 1 \end{aligned}$$

Aplicando 11.1.2, la solución general sería la sucesión $\{a_n\}$ tal que,

$$a_n = \alpha \cdot 2^{n-1}, \ \forall n$$

y aplicando la condición inicial,

$$\left.\begin{array}{rcl} a_1 & = & 2 \\ a_n & = & \alpha \cdot 2^{n-1} \end{array}\right\} \implies \alpha \cdot 2^0 = 2 \implies \alpha = 2.$$

Por lo tanto, la sucesión $\{a_n\}$ tal que

$$a_n = 2^n,\ n \geqslant 1$$

nos daría el número de subconjuntos que tiene un conjunto con n elementos.

■

Ejemplo 11.3

Resolver la ecuación de recurrencia,

$$\begin{array}{rcl} a_2 & = & 144 \\ a_{n+1} & = & 6a_n,\ n \geqslant 2 \end{array}$$

Solución

La ecuación propuesta es lineal homogénea de primer orden con coeficientes constantes. Aplicando los resultados obtenidos en 11.1.2, la solución general de la ecuación es la sucesión $\{a_n\}$ tal que

$$a_n = \alpha \cdot 6^{n-1}$$

y como la condición inicial es $a_2 = 144$, tendremos

$$\left.\begin{array}{rcl} a_2 & = & 144 \\ a_n & = & \alpha \cdot 6^{n-1} \implies a_2 = \alpha \cdot 6 \end{array}\right\} \implies 6\alpha = 144 \implies \alpha = 24$$

Por lo tanto, la sucesión $\{a_n\}$ tal que

$$a_n = 24 \cdot 6^{n-1};\ n \geqslant 1$$

es solución de la ecuación propuesta y además, por 11.1.1, es única.

■

Ejemplo 11.4

Se depositan 5000 *euros en un banco a un interés anual del* 7%*, con un interés compuesto mensual. ¿Cuánto dinero habrá depositado en el banco un año después?*

Solución

Si llamamos a_n al dinero que tenemos en el mes n, tendremos que el interés obtenido sobre a_n en ese mes, será

$$i = \frac{a_n \cdot 7 \cdot 1}{1200} = 0,006a_n$$

Pues bien, el dinero que habrá en depósito en un mes cualquiera será igual al que había el mes anterior más los intereses devengados por dicho capital, es decir,

$$a_{n+1} = a_n + 0,006a_n = 1,006a_n$$

y podemos tomar como a_1 los 5000 euros depositados como capital inicial, por lo tanto tendremos

$$\begin{aligned} a_1 &= 5000 \\ a_{n+1} &= 1,006a_n,\ n \geqslant 1. \end{aligned}$$

Hemos obtenido una ecuación de recurrencia lineal homogénea de primer orden con coeficientes constantes cuya solución general es, según 11.1.2,

$$a_n = \alpha \cdot 1,006^{n-1}$$

y como la condición inicial es $a_1 = 5000$,

$$\left.\begin{aligned} a_n &= \alpha \cdot 1,006^{n-1} \\ a_1 &= 5000 \end{aligned}\right\} \implies \alpha \cdot 1,006^0 = 5000 \implies \alpha = 5000$$

es decir, la solución es la sucesión $\{a_n\}$ tal que $a_n = 5000 \cdot 1,006^{n-1}$ y, consecuentemente, el dinero que habrá depositado en el banco al cabo de un año será:

$$a_{13} = 5000 \cdot 1,006^{12} = 5372,12 \text{ Euros.}$$

■

11.2 Segundo orden con Coeficientes Constantes

Según 10.1.4, una ecuación de este tipo puede escribirse en la forma

$$a_{n+2} + c_1 a_{n+1} + c_0 a_n = 0$$

sin más que hacer $k = 2$ en su forma más general.

Por ejemplo, consideremos la ecuación

$$a_{n+2} - a_{n+1} - a_n = 0$$

despejando a_{n+2}, tendremos

$$a_{n+2} = a_{n+1} + a_n$$

Según vimos en 10.2.1 para que la ecuación tenga una única solución necesitaremos dos condiciones iniciales. Tomando como tales $a_1 = \alpha_1$ y $a_2 = \alpha_2$, resulta

$$\begin{aligned} a_1 &= \alpha_1 \\ a_2 &= \alpha_2 \\ a_{n+2} &= a_{n+1} + a_n,\ n \geqslant 1. \end{aligned}$$

Entonces,

$$\begin{array}{lllllllll} a_1 & = & & & & & & & \alpha_1 \\ a_2 & = & & & & & \alpha_2 & & \\ a_3 & = & a_2 & + & a_1 & = & \alpha_2 & + & \alpha_1 \\ a_4 & = & a_3 & + & a_2 & = & 2\alpha_2 & + & \alpha_1 \\ a_5 & = & a_4 & + & a_3 & = & 3\alpha_2 & + & 2\alpha_1 \\ a_6 & = & a_5 & + & a_4 & = & 5\alpha_2 & + & 3\alpha_1 \\ \vdots & & \vdots & & \vdots & & \vdots & & \vdots \\ \vdots & & \vdots & & \vdots & & \vdots & & \vdots \end{array}$$

y aunque continuáramos no obtendríamos un patrón obvio, así que esta aproximación al problema no es muy útil. La estrategia que hemos seguido para resolver las ecuaciones de primer orden no funciona aquí. En su lugar usaremos una estrategia diferente. Para las ecuaciones de primer orden, encontramos que la solución era $a_n = \alpha\lambda^{n-1}$, es decir, una función exponencial. Lo que haremos es utilizar, también, una función exponencial como una posible solución para una ecuación de segundo orden. Esta conjetura acaba por ser buena para obtener una solución, aunque la comprobación de la misma es larga y tediosa. En su lugar probaremos que esta "buena conjetura" que se llama *método de las raíces características*, nos ofrece, en efecto, una solución general. Comenzaremos con un caso particular para, posteriormente, buscar una generalización.

Ejemplo 11.5

Resolver la ecuación de recurrencia

$$a_{n+2} = 2a_n - a_{n+1}$$

Solución

Supongamos que existe un $\lambda \neq 0$ tal que la sucesión $\{a_n\}$, con $a_n = \lambda^n$ es solución de la ecuación. Sustituyendo en la ecuación, tendremos

$$\left.\begin{array}{rcl} a_{n+2} & = & 2a_n - a_{n+1} \\ a_n & = & \lambda^n \end{array}\right\} \implies \lambda^{n+2} = 2\lambda^n - \lambda^{n+1}$$

$$\implies \lambda^{n+2} + \lambda^{n+1} - 2\lambda^n = 0$$

$$\implies \lambda^n\left(\lambda^2 + \lambda - 2\right) = 0$$

$$\overset{\lambda\neq 0}{\implies} \lambda^2 + \lambda - 2 = 0$$

$$\implies \lambda = \frac{-1 \pm \sqrt{1+8}}{2}$$

$$\implies \left\{\begin{array}{rcl} \lambda & = & 1 \\ \text{ó} & & \\ \lambda & = & -2 \end{array}\right.$$

de aquí que las sucesiones

$$\{(-2)^n\} \quad \text{y} \quad \{1^n\}$$

aparezcan como soluciones.

Comprobaremos este hecho, sustituyendo en el segundo miembro de la ecuación propuesta. En efecto,

Para $a_n = (-2)^n$,

$$\begin{array}{rcl} 2a_n - a_{n+1} & = & 2(-2)^n - (-2)^{n+1} \\ & = & -(-2)(-2)^n - (-2)^{n+1} \\ & = & -(-2)^{n+1} - (-2)^{n+1} \\ & = & (-2)(-2)^{n+1} \\ & = & (-2)^{n+2} \\ & = & a_{n+2} \end{array}$$

Para $a_n = 1^n$,

$$2a_n - a_{n+1} = 2 \cdot 1 - 1 = 1 = a_{n+2}$$

Por lo tanto, ambas sucesiones son soluciones. Por el *principio de superposición* (10.3.1), podemos concluir que la sucesión $\{a_n\}$ tal que

$$a_n = \alpha_1(-2)^n + \alpha_2 \cdot 1^n = \alpha_1(-2)^n + \alpha_2$$

es solución para cualquier par de constantes reales α_1 y α_2.

■

11.3 Orden k con Coeficientes Constantes

Generalizaremos esta técnica para cualquier ecuación de recurrencia lineal homogénea de orden k que tenga coeficientes constantes. Esto es, si tenemos una ecuación de la forma

$$a_{n+k} + c_{k-1}a_{n+(k-1)} + c_{k-2}a_{n+(k-2)} + \cdots + c_2a_{n+2} + c_1a_{n+1} + c_0a_n = 0$$

podemos suponer que una solución es la sucesión $\{a_n\}$ tal que $a_n = \lambda^n$, sustituir y resolver para λ.

11.3.1 Teorema

La sucesión $\{a_n\}$ tal que $a_n = \lambda^n$ para cada n, es una solución distinta de cero de la ecuación de recurrencia

$$a_{n+k} + c_{k-1}a_{n+(k-1)} + c_{k-2}a_{n+(k-2)} + \cdots + c_2a_{n+2} + c_1a_{n+1} + c_0a_n = 0$$

si y sólo si λ es una raíz de la ecuación

$$x^k + c_{k-1}x^{k-1} + c_{k-2}x^{k-2} + \cdots + c_2x^2 + c_1x + c_0 = 0.$$

Demostración

"*Sólo si*". Supongamos que la sucesión $\{a_n\}$ tal que $a_n = \lambda^n$ para cada n, es solución de la ecuación de recurrencia propuesta. Como $\lambda = 0$ se corresponde con la solución $a_n = 0$, podemos suponer que $\lambda \neq 0$. Entonces,

$$\lambda^{n+k} + c_{k-1}\lambda^{n+(k-1)} + c_{k-2}\lambda^{n+(k-2)} + \cdots + c_2\lambda^{n+2} + c_1\lambda^{n+1} + c_0\lambda^n = 0$$

y sacando factor común λ^n,

$$\lambda^n\left(\lambda^k + c_{k-1}\lambda^{k-1} + c_{k-2}\lambda^{k-2} + \cdots + c_2\lambda^2 + c_1\lambda + c_0\right) = 0$$

y al ser $\lambda \neq 0$, se sigue que

$$\lambda^k + c_{k-1}\lambda^{k-1} + c_{k-2}\lambda^{k-2} + \cdots + c_2\lambda^2 + c_1\lambda + c_0 = 0$$

por lo tanto, λ es una raíz de la ecuación $x^k + c_{k-1}x^{k-1} + c_{k-2}x^{k-2} + \cdots + c_2x^2 + c_1x + c_0 = 0$.

"*Si*". Recíprocamente, supongamos que λ sea una raíz de la ecuación

$$x^k + c_{k-1}x^{k-1} + c_{k-2}x^{k-2} + \cdots + c_2x^2 + c_1x + c_0 = 0.$$

Entonces,

$$\lambda^k + c_{k-1}\lambda^{k-1} + c_{k-2}\lambda^{k-2} + \cdots + c_2\lambda^2 + c_1\lambda + c_0 = 0$$

de donde se sigue, multiplicando por λ^n, que

$$\lambda^{n+k} + c_{k-1}\lambda^{n+(k-1)} + c_{k-2}\lambda^{n+(k-2)} + \cdots + c_2\lambda^{n+2} + c_1\lambda^{n+1} + c_0\lambda^n = 0$$

luego la sucesión $\{a_n\}$ tal que $a_n = \lambda^n,\ \forall n$ es una solución de la ecuación de recurrencia.

■

11.3.2 Ecuación Característica

La ecuación de grado k,

$$\lambda^k + c_{k-1}\lambda^{k-1} + c_{k-2}\lambda^{k-2} + \cdots + c_2\lambda^2 + c_1\lambda + c_0 = 0$$

se llama ecuación característica de la ecuación de recurrencia

$$a_{n+k} + c_{k-1}a_{n+(k-1)} + c_{k-2}a_{n+(k-2)} + \cdots + c_2a_{n+2} + c_1a_{n+1} + c_0a_n = 0.$$

Una solución de la ecuación se llama raíz de la misma.

Ejemplo 11.6

Resolver la ecuación de recurrencia,

$$a_{n+2} - 4a_{n+1} + 4a_n = 0,\ n \geqslant 0$$

Su ecuación característica (11.3.2) es:

$$\lambda^2 - 4\lambda + 4 = 0.$$

Entonces,

$$\begin{aligned} \lambda^2 - 4\lambda + 4 = 0 &\implies \lambda = \frac{\lambda \pm \sqrt{16 - 4 \cdot 1 \cdot 4}}{2} \\ &\implies \lambda = \frac{4}{2} \\ &\implies \lambda = 2 \end{aligned}$$

es decir, la ecuación característica tiene una raíz doble ($\lambda = 2$). Por el teorema 11.3.1, las sucesiones $\{2^n\}$ y $\{2^n\}$ son, ambas, solución de la ecuación. Por el *principio de superposición* (10.3.1), la sucesión $\{a_n\}$ tal que

$$a_n = \alpha_1 2^n + \alpha_2 2^n$$

es una solución, cualesquiera que sean las constantes α_1 y α_2. Observemos, sin embargo, lo siguiente:

$$a_n = \alpha_1 2^n + \alpha_2 2^n = (\alpha_1 + \alpha_2)\, 2^n$$

y tomando $\alpha = \alpha_1 + \alpha_2$,

$$a_n = \alpha \cdot 2^n$$

ya que α_1 y α_2 son constantes arbitrarias. Así pues, en este caso, nuestras dos soluciones se reducen a una sola.

Veamos que, además, existe otra solución. En efecto, la sucesión $\{n2^n\}$ también lo es. Sustituyendo,

$$\begin{aligned} 4a_{n+1} - 4a_n &= 4(n+1)2^{n+1} - 4n2^n \\ &= 2^2(n+1)2^{n+1} - 2^2n2^n \\ &= 2(n+1)2^{n+2} - n2^{n+2} \\ &= [2(n+1) - n]\, 2^{n+2} \\ &= (2n + 2 - n)2^{n+2} \\ &= (n+2)2^{n+2} \\ &= a_{n+2} \end{aligned}$$

es decir, $a_{n+2}-4a_{n+1}+4a_n=0$, luego la sucesión $\{n2^n\}$ también es solución. Nuevamente, por el *principio de superposición* (10.3.1), podemos concluir que la sucesión:

$$\beta_1\{2^n\}+\beta_2\{n2^n\}=\{\beta_1 2^n+\beta_2 n2^n\}$$

es solución cualesquiera que sean β_1 y β_2.

■

El resultado que sigue justifica la existencia de esta solución.

11.3.3 Teorema

Si la raíz, λ, de la ecuación característica de la ecuación de recurrencia,

$$a_{n+k}+c_{k-1}a_{n+(k-1)}+c_{k-2}a_{n+(k-2)}+\cdots+c_2a_{n+2}+c_1a_{n+1}+c_0a_n=0$$

tiene multiplicidad m, entonces las sucesiones $\{a_n\}$ tales que

$$a_n=n^q\lambda^n,\ 0\leqslant q\leqslant m-1,\ \forall n$$

son, todas, solución de la ecuación de recurrencia.

■

Ejemplo 11.7

Consideremos la ecuación de recurrencia

$$\begin{aligned} a_1 &= 1 \\ a_2 &= 1 \\ a_{n+2} &= a_{n+1}+a_n,\ n\geqslant 1 \end{aligned}$$

que define la sucesión de Fibonacci. *Resolvamos esta ecuación.*

Solución

Escribimos la ecuación en su forma general

$$a_{n+2}-a_{n+1}-a_n=0.$$

Su ecuación característica es

$$\lambda^2-\lambda-1=0.$$

Pues bien,

$$\begin{aligned} \lambda^2-\lambda-1=0 &\implies \lambda=\frac{1\pm\sqrt{1+4}}{2} \\ &\implies \lambda=\frac{1\pm\sqrt{5}}{2} \\ &\implies \begin{cases} \lambda = \dfrac{1+\sqrt{5}}{2} \\ \text{ó} \\ \lambda = \dfrac{1-\sqrt{5}}{2}. \end{cases} \end{aligned}$$

Es decir, la ecuación característica tiene dos raíces simples, o sea, de multiplicidad $m = 1$. Según el teorema anterior, 11.3.3, las sucesiones

$$\left\{\left(\frac{1+\sqrt{5}}{2}\right)^n\right\} \text{ y } \left\{\left(\frac{1-\sqrt{5}}{2}\right)^n\right\}$$

son, ambas, solución de la ecuación propuesta. Aplicando el *principio de superposición* (10.3.1), tendremos que la sucesión $\{a_n\}$ tal que:

$$a_n = \alpha_1\left(\frac{1+\sqrt{5}}{2}\right)^n + \alpha_2\left(\frac{1-\sqrt{5}}{2}\right)^n,\ n \geqslant 1,\ \alpha_1, \alpha_2 \in \mathbb{R}$$

es solución de la ecuación $a_{n+2} = a_{n+1} + a_n$. Como tenemos dos condiciones iniciales $a_1 = 1$ y $a_2 = 1$, podemos seleccionar los valores de las constantes, α_1 y α_2 de tal forma que a_n satisfaga dichas condiciones. Pues bien,

$$a_1 = 1 \Longrightarrow \alpha_1\left(\frac{1+\sqrt{5}}{2}\right)^1 + \alpha_2\left(\frac{1-\sqrt{5}}{2}\right)^1 = 1$$

y

$$a_2 = 1 \Longrightarrow \alpha_1\left(\frac{1+\sqrt{5}}{2}\right)^2 + \alpha_2\left(\frac{1-\sqrt{5}}{2}\right)^2 = 1$$

de aquí que

$$\left.\begin{array}{rcrcl} \alpha_1\left(1+\sqrt{5}\right) & + & \alpha_2\left(1-\sqrt{5}\right) & = & 2 \\ \alpha_1\left(1+\sqrt{5}\right)^2 & + & \alpha_2\left(1-\sqrt{5}\right)^2 & = & 4 \end{array}\right\}$$

Multiplicando la primera ecuación por $1+\sqrt{5}$,

$$\left.\begin{array}{rcrcl} \alpha_1\left(1+\sqrt{5}\right)^2 & + & \alpha_2(-4) & = & 2\left(1+\sqrt{5}\right) \\ \alpha_1\left(1+\sqrt{5}\right)^2 & + & \alpha_2\left(1-\sqrt{5}\right)^2 & = & 4 \end{array}\right\}$$

y restándolas,

$$\begin{aligned} \alpha_2\left[\left(1-\sqrt{5}\right)^2+4\right] = 4-2\left(1+\sqrt{5}\right) &\Longrightarrow \alpha_2\left(10-2\sqrt{5}\right) = 2-2\sqrt{5} \\ &\Longrightarrow \alpha_2 = \frac{1-\sqrt{5}}{5-\sqrt{5}} \\ &\Longrightarrow \alpha_2 = -\frac{\sqrt{5}}{5}. \end{aligned}$$

De la misma forma, si multiplicamos la primera ecuación por $1-\sqrt{5}$,

$$\left.\begin{array}{rcrcl} \alpha_1(-4) & + & \alpha_2\left(1-\sqrt{5}\right)^2 & = & 2\left(1-\sqrt{5}\right) \\ \alpha_1\left(1+\sqrt{5}\right)^2 & + & \alpha_2\left(1-\sqrt{5}\right)^2 & = & 4 \end{array}\right\}$$

y las restamos,

$$\begin{aligned} \alpha_1\left[\left(1+\sqrt{5}\right)^2+4\right] = 4-2\left(1-\sqrt{5}\right) &\Longrightarrow \alpha_1\left(10+2\sqrt{5}\right) = 2+2\sqrt{5} \\ &\Longrightarrow \alpha_1 = \frac{1+\sqrt{5}}{5+\sqrt{5}} \\ &\Longrightarrow \alpha_1 = \frac{\sqrt{5}}{5}. \end{aligned}$$

Por lo tanto, la sucesión $\{a_n\}$ tal que

$$a_n = \frac{\sqrt{5}}{5}\left[\left(\frac{1+\sqrt{5}}{2}\right)^n - \left(\frac{1-\sqrt{5}}{2}\right)^n\right];\ n \geqslant 1$$

es, por el teorema 10.2.1, la única solución de la ecuación.

■

Ejemplo 11.8

Resolver la ecuación

$$\begin{aligned} a_1 &= 2 \\ a_2 &= 3 \\ a_{n+2} &= 6a_{n+1} - 9a_n;\ n \geqslant 1 \end{aligned}$$

Solución

La ecuación escrita en su forma general es:

$$a_{n+2} - 6_{n+1} + 9a_n = 0$$

siendo su ecuación característica,

$$\lambda^2 - 6\lambda + 9 = 0$$

Pues bien,

$$\lambda^2 - 6\lambda + 9 = 0 \implies \lambda = \frac{6 \pm \sqrt{36-36}}{2} \implies \lambda = 3 \quad \text{(Doble)}.$$

Por lo tanto, y según el teorema 11.3.3, las sucesiones $\{3^n\}$ y $\{n3^n\}$ son, ambas, solución de la ecuación propuesta. Nuevamente, por el *principio de superposición* (10.3.1), la sucesión $\{a_n\}$ tal que

$$a_n = \alpha_1 3^n + \alpha_2 n 3^n;\ n \geqslant 1$$

es solución de la ecuación. Teniendo en cuenta las condiciones iniciales,

$$\left.\begin{aligned} a_1 &= 2 \\ a_2 &= 3 \\ a_n &= \alpha_1 3^n + \alpha_2 n 3^n \end{aligned}\right\} \implies \left.\begin{aligned} 3\alpha_1 + 3\alpha_2 &= 2 \\ 9\alpha_1 + 18\alpha_2 &= 3 \end{aligned}\right\}$$

$$\implies \left\{\begin{aligned} 18\alpha_1 + 18\alpha_2 &= 12 \\ 9\alpha_1 + 18\alpha_2 &= 3 \\ 9\alpha_1 + 9\alpha_2 &= 6 \\ 9\alpha_1 + 18\alpha_2 &= 3 \end{aligned}\right\}$$

$$\implies \left\{\begin{aligned} 9\alpha_1 &= 9 \\ 9\alpha_2 &= -3 \end{aligned}\right.$$

$$\implies \left\{\begin{aligned} \alpha_1 &= 1 \\ \alpha_2 &= -\frac{1}{3} \end{aligned}\right.$$

Sustituyendo, la sucesión $\{a_n\}$ tal que

$$a_n = 3^n - \frac{1}{3}n3^n = 3^n - n3^{n-1},\ n \geqslant 1$$

es solución única de la ecuación propuesta.

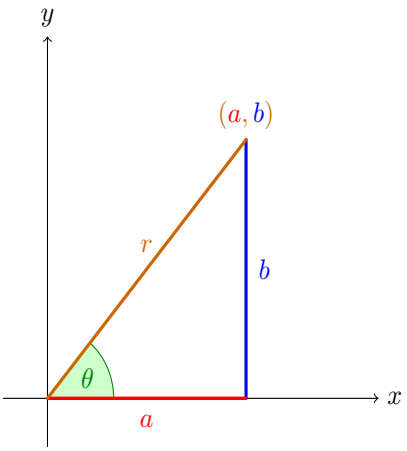
■

Tenemos, pues, una técnica para calcular la solución de la ecuación de recurrencia lineal homogénea de orden k con coeficientes constantes. Ésta incluye la resolución de una ecuación cuadrática y, si existen condiciones iniciales, resolver un par de ecuaciones simultáneas para dichas condiciones.

Sin embargo, hay una complicación que debemos tener en cuenta como es la posibilidad de que las raíces de la ecuación cuadrática sean complejas.

11.3.4 n-ésima Potencia de un Número Complejo

Dado un número complejo cualquiera $c = a + ib$, queremos calcular c^n, siendo $n \geqslant 0$



El número complejo $c = a + ib$ lo podemos representar geométricamente como el punto (a, b) en el plano cartesiano xy. Pues bien, según la figura,

$$\operatorname{sen}\theta = \frac{b}{r} \Longrightarrow b = r\operatorname{sen}\theta \quad \text{y} \quad \cos\theta = \frac{a}{r} \Longrightarrow a = r\cos\theta$$

luego, $a + ib = r\cos\theta + ir\operatorname{sen}\theta$, es decir,

$$c = r\left(\cos\theta + i\operatorname{sen}\theta\right)$$

siendo,

$$r = \sqrt{a^2 + b^2} \quad \text{y} \quad \operatorname{tag}\theta = \frac{b}{a},\ \text{para } a \neq 0.$$

Si $a = 0$, entonces

- Para $b > 0$, $c = ib = ib\operatorname{sen}\dfrac{\pi}{2} = b\left(\cos\dfrac{\pi}{2} + i\operatorname{sen}\dfrac{\pi}{2}\right)$
- Para $b < 0$, $c = ib = i|b|\operatorname{sen}\dfrac{3\pi}{2} = |b|\left(\cos\dfrac{3\pi}{2} + i\operatorname{sen}\dfrac{3\pi}{2}\right)$

En todos los casos, aplicando el teorema de DeMoivre,

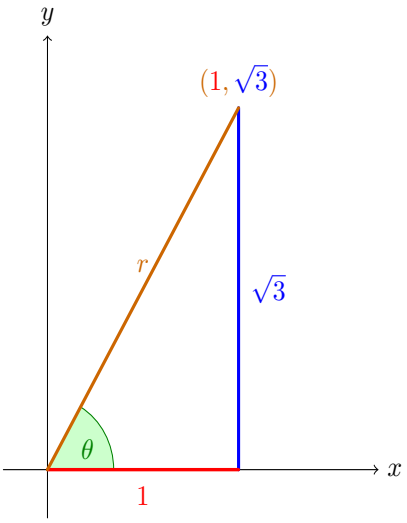
$$\begin{aligned} c = r\left(\cos\theta + i\operatorname{sen}\theta\right) &\Longrightarrow c^n = r^n\left(\cos\theta + i\operatorname{sen}\theta\right)^n \\ &\Longrightarrow c^n = r^n\left(\cos n\theta + i\operatorname{sen}n\theta\right),\ n \geqslant 0 \end{aligned}$$

■

Ejemplo 11.9

Calcular $\left(1+i\sqrt{3}\right)^{10}$

Solución



Directamente de la figura,

$$r = \sqrt{1^2+\left(\sqrt{3}\right)^2} = \sqrt{4} = 2$$

y

$$\text{tag}\theta = \frac{\sqrt{3}}{1} = \sqrt{3} \Longrightarrow \theta = \frac{\pi}{3}.$$

Por lo tanto,

$$1+i\sqrt{3} = 2\left(\cos\frac{\pi}{3}+i\,\text{sen}\,\frac{\pi}{3}\right)$$

Pues bien,

$$\begin{aligned}
\left(1+i\sqrt{3}\right)^{10} &= 2^{10}\left(\cos\frac{\pi}{3}+i\,\text{sen}\,\frac{\pi}{3}\right)^{10}\\
&= 2^{10}\left(\cos 10\frac{\pi}{3}+i\,\text{sen}\,10\frac{\pi}{3}\right)\\
&= 2^{10}\left(\cos\left(\frac{6\pi}{3}+\frac{4\pi}{3}\right)+i\,\text{sen}\left(\frac{6\pi}{3}+\frac{4\pi}{3}\right)\right)\\
&= 2^{10}\left(\cos\left(2\pi+\frac{4\pi}{3}\right)+i\,\text{sen}\left(2\pi+\frac{4\pi}{3}\right)\right)\\
&= 2^{10}\left(\cos\frac{4\pi}{3}+i\,\text{sen}\,\frac{4\pi}{3}\right)\\
&= 2^{10}\left(-\frac{1}{2}+i\left(-\frac{\sqrt{3}}{2}\right)\right)\\
&= -\frac{2^{10}}{2}\left(1+i\sqrt{3}\right)\\
&= -2^9\left(1+i\sqrt{3}\right)
\end{aligned}$$

■

Ejemplo 11.10

Resolver la ecuación de recurrencia

$$\begin{aligned}
a_1 &= 2\\
a_2 &= 2\\
a_{n+2} &= 2a_{n+1} - 2a_n,\ n \geqslant 1
\end{aligned}$$

Solución

La forma general de la ecuación propuesta es:

$$a_{n+2} - 2_{n+1} + 2a_n = 0$$

y su ecuación característica será,

$$\lambda^2 - 2\lambda + 2 = 0$$

Pues bien,

$$\begin{aligned}
\lambda^2 - 2\lambda + 2 = 0 \quad &\Longrightarrow \quad \lambda = \frac{2 \pm \sqrt{4 - 4 \cdot 2}}{2} \\
&\Longrightarrow \quad \lambda = \frac{2 \pm \sqrt{-4}}{2} \\
&\Longrightarrow \quad \lambda = \frac{2 \pm 2\sqrt{-1}}{2} \\
&\Longrightarrow \quad \lambda = 1 \pm i \\
&\Longrightarrow \quad \left\{ \begin{array}{lcl} \lambda & = & 1+i \\ \text{ó} & & \\ \lambda & = & 1-i \end{array} \right.
\end{aligned}$$

Por el teorema 11.3.3, las sucesiones $\{(1+i)^n\}$ y $\{(1-i)^n\}$ son, ambas, solución de la ecuación. Por el *principio de superposición* (10.3.1), la sucesión $\{a_n\}$ tal que

$$a_n = \alpha_1(1+i)^n + \alpha_2(1-i)^n;\ n \geqslant 1,\ \alpha_1, \alpha_2 \in \mathbb{R}$$

es solución de la ecuación propuesta. Ahora bien,

$$\begin{aligned}
1+i &= \sqrt{2}\left(\cos\frac{\pi}{4} + i\,\text{sen}\,\frac{\pi}{4}\right) \\
&\text{y} \\
1-i &= \sqrt{2}\left(\cos\left(-\frac{\pi}{4}\right) + i\,\text{sen}\left(-\frac{\pi}{4}\right)\right) = \sqrt{2}\left(\cos\frac{\pi}{4} - i\,\text{sen}\,\frac{\pi}{4}\right)
\end{aligned}$$

de aquí que

$$\begin{aligned}
a_n &= \alpha_1\left[\sqrt{2}\left(\cos\frac{\pi}{4} + i\,\text{sen}\,\frac{\pi}{4}\right)\right]^n + \alpha_2\left[\sqrt{2}\left(\cos\frac{\pi}{4} - i\,\text{sen}\,\frac{\pi}{4}\right)\right]^n \\
&= \alpha_1\left[\left(\sqrt{2}\right)^n\left(\cos\frac{n\pi}{4} + i\,\text{sen}\,\frac{n\pi}{4}\right)\right] + \alpha_2\left[\left(\sqrt{2}\right)^n\left(\cos\frac{n\pi}{4} - i\,\text{sen}\,\frac{n\pi}{4}\right)\right] \\
&= \left(\sqrt{2}\right)^n\left[(\alpha_1+\alpha_2)\cos\frac{n\pi}{4} + i\,(\alpha_1-\alpha_2)\,\text{sen}\,\frac{n\pi}{4}\right]
\end{aligned}$$

y tomando,

$$\begin{aligned}
\beta_1 &= \alpha_1 + \alpha_2 \\
\beta_2 &= i\,(\alpha_1 - \alpha_2)
\end{aligned}$$

tendremos que la sucesión $\{a_n\}$ tal que

$$a_n = \left(\sqrt{2}\right)^n\left(\beta_1\cos\frac{n\pi}{4} + \beta_2\,\text{sen}\,\frac{n\pi}{4}\right);\ n \geqslant 1,\ \beta_1, \beta_2 \in \mathbb{R}$$

es una solución de la ecuación $a_{n+2} = 2a_{n+1} - a_n$. Como tenemos dos condiciones iniciales $a_1 = 2$ y $a_2 = 2$, podemos calcular β_1 y β_2 de tal forma que a_n satisfaga dichas condiciones. En efecto,

$$\left.\begin{array}{lcl} a_1 & = & 2 \\ a_2 & = & 2 \\ a_n & = & \left(\sqrt{2}\right)^n\left(\beta_1\cos\frac{n\pi}{4} + \beta_2\,\text{sen}\,\frac{n\pi}{4}\right) \end{array}\right\}$$

de aquí que,

$$\left.\begin{array}{rcl} \sqrt{2}\left(\beta_1 \cos\dfrac{\pi}{4}+\beta_2 \operatorname{sen}\dfrac{\pi}{4}\right) & = & 2 \\ \left(\sqrt{2}\right)^2\left(\beta_1 \cos\dfrac{2\pi}{4}+\beta_2 \operatorname{sen}\dfrac{2\pi}{4}\right) & = & 2 \end{array}\right\} \Longrightarrow \left\{\begin{array}{rcrcl} \beta_1 & + & \beta_2 & = & 2 \\ & & 2\beta_2 & = & 2 \end{array}\right.$$

$$\Longrightarrow \left\{\begin{array}{rcl} \beta_1 & = & 1 \\ \beta_2 & = & 1 \end{array}\right.$$

y, consecuentemente, la sucesión $\{a_n\}$ tal que

$$a_n = \left(\sqrt{2}\right)^n \left(\cos\frac{n\pi}{4}+\operatorname{sen}\frac{n\pi}{4}\right),\ n \geqslant 1$$

es la única solución de la ecuación propuesta.

■

Lección 12

Recurrencias Lineales No Homogéneas

12.1 Generalidades

12.1.1 Forma General

Según 10.1.4, una ecuación de recurrencia lineal, no homogénea, de orden k y con coeficientes constantes puede escribirse en su forma general, como

$$a_{n+k} + c_{k-1}a_{n+(k-1)} + c_{k-2}a_{n+(k-2)} + \cdots + c_2a_{n+2} + c_1a_{n+1} + c_0a_n = h(n).$$

A la ecuación,

$$a_{n+k} + c_{k-1}a_{n+(k-1)} + c_{k-2}a_{n+(k-2)} + \cdots + c_2a_{n+2} + c_1a_{n+1} + c_0a_n = 0.$$

la llamaremos ecuación reducida homogénea asociada a la ecuación dada o, simplemente, ecuación reducida.

■

El siguiente teorema establece que si podemos encontrar una solución cualquiera de una ecuación no homogénea, podemos calcular cualquier otra solución sin más que añadir una solución de la ecuación reducida a la solución encontrada.

12.1.2 Teorema

Sea la ecuación de recurrencia lineal, no homogénea, de orden k y con coeficientes constantes:

$$a_{n+k} + c_{k-1}a_{n+(k-1)} + c_{k-2}a_{n+(k-2)} + \cdots + c_2a_{n+2} + c_1a_{n+1} + c_0a_n = h(n).$$

Si la sucesión $\left\{a_n^{(p)}\right\}$ es una solución particular de la ecuación dada y la sucesión $\left\{a_n^{(h)}\right\}$ es la solución general de su ecuación homogénea asociada, entonces la sucesión $\{a_n\}$ tal que

$$a_n = a_n^{(h)} + a_n^{(p)},\ \forall n$$

es la solución general de la ecuación propuesta.

Demostración

Sea $\{a_n\}$ cualquier solución de la ecuación dada. Entonces,

$$a_{n+k} + c_{k-1}a_{n+(k-1)} + c_{k-2}a_{n+(k-2)} + \cdots + c_2a_{n+2} + c_1a_{n+1} + c_0a_n = h(n)$$

y como $\left\{a_n^{(p)}\right\}$ es, por hipótesis, una solución de la ecuación,

$$a_{n+k}^{(p)} + c_{k-1}a_{n+(k-1)}^{(p)} + c_{k-2}a_{n+(k-2)}^{(p)} + \cdots + c_2a_{n+2}^{(p)} + c_1a_{n+1}^{(p)} + c_0a_n^{(p)} = h(n)$$

y restando ambas ecuaciones,

$$\begin{array}{rcccccccl} a_{n+k} & - & a_{n+k}^{(p)} & + & c_{k-1}\left(a_{n+(k-1)} - a_{n+(k-1)}^{(p)}\right) & + & c_{k-2}\left(a_{n+(k-2)} - a_{n+(k-2)}^{(p)}\right) & + & \\ & & & + & \cdots\cdots\cdots\cdots\cdots\cdots & + & c_0\left(a_n - a_n^{(p)}\right) & = & 0 \end{array}$$

Por tanto, si ahora tomamos

$$a_n^{(h)} = a_n - a_n^{(p)},\ \forall n$$

tendremos que $a_n^{(h)}$ es solución de la ecuación reducida y

$$a_n = a_n^{(h)} + a_n^{(p)},\ \forall n$$

luego $\{a_n\}$ es la solución general de la ecuación dada.

■

El único problema es, por tanto, la construcción de soluciones particulares, $\left\{a_n^{(p)}\right\}$, para la ecuación propuesta y éstas dependerán de la forma que tenga la función $h(n)$.

12.2 Método de los Coeficientes Indeterminados

Este método es, sin lugar a dudas, el más popular de los métodos que existen para resolver ecuaciones de recurrencia no homogéneas. Sea

$$a_{n+k} + c_{k-1}a_{n+(k-1)} + c_{k-2}a_{n+(k-2)} + \cdots + c_2a_{n+2} + c_1a_{n+1} + c_0a_n = h(n).$$

una ecuación de recurrencia lineal no homogénea de orden k.

En general, si $h(n)$ es de la forma r^n por un polinomio de grado t,

$$h(n) = r^n\left(p_0 + p_1n + p_2n^2 + \cdots + p_tn^t\right)$$

consideraremos dos casos:

1. Si r no es raíz de la ecuación característica de la ecuación de recurrencia homogénea asociada, entonces tomaremos como solución particular de la ecuación de recurrencia, la sucesión $\left\{a_n^{(p)}\right\}$ tal que $a_n^{(p)}$ es igual al producto de r^n por un polinomio del mismo grado, es decir,
$$a_n^{(p)} = r^n\left(A_0 + A_1n + A_2n^2 + \cdots + A_tn^t\right)$$
2. Si r es raíz con multiplicidad m de la ecuación característica de la ecuación de recurrencia homogénea asociada, entonces tomaremos como solución particular de la ecuación de recurrencia, la sucesión $\left\{a_n^{(p)}\right\}$ tal que $a_n^{(p)}$ es igual al producto de n^mr^n por un polinomio del mismo grado, es decir,
$$a_n^{(p)} = n^mr^n\left(A_0 + A_1n + A_2n^2 + \cdots + A_tn^t\right)$$

Siendo, en ambos casos, los coeficientes $A_0, A_1, A_2, \ldots, A_t$, desconocidos. Veremos según sea r y según sea el polinomio, algunos ejemplos de los distintos casos que pueden presentarse.

Ejemplo 12.1

Resolver la ecuación de recurrencia:

$$\begin{aligned} a_1 &= 1 \\ a_{n+1} &= 2a_n + 1,\ n \geqslant 1 \end{aligned}$$

Solución

La ecuación escrita en su forma general es,

$$\begin{aligned} a_1 &= 1 \\ a_{n+1} - 2a_n &= 1,\ n \geqslant 1 \end{aligned}$$

es decir, es una ecuación de recurrencia lineal, no homogénea, de primer orden y con coeficientes constantes.

Buscamos, primero, una solución para la ecuación de recurrencia homogénea asociada a la ecuación dada:

$$a_{n+1} - 2a_n = 0.$$

Su ecuación característica es $\lambda - 2 = 0$. Entonces,

$$\lambda - 2 = 0 \Longrightarrow \lambda = 2.$$

La solución general de la ecuación homogénea es, por 11.3.3, la sucesión $\left\{a_n^{(h)}\right\}$ tal que

$$a_n^{(h)} = \alpha \cdot 2^n,\ \alpha \in \mathbb{R},\ n \geqslant 1$$

Calculamos, ahora, una solución particular de la ecuación propuesta. Observemos que el término independiente es $h(n) = 1$, es decir es igual al producto de r^n por un polinomio de grado cero, o sea,

$$h(n) = r^n p_0$$

sin más que tomar $r = 1$ y $p_0 = 1$. Como la raíz de la ecuación característica asociada a la homogénea es distinta de 1, estamos en el primer caso de 12.2. Probaremos, por tanto, como solución particular la sucesión $\left\{a_n^{(p)}\right\}$ tal que

$$a_n^{(p)} = A_0,\ \text{con } A_0 \text{ constante.}$$

Sustituyendo en la ecuación,

$$a_{n+1}^{(p)} - 2a_n^{(p)} = 1 \quad \Longrightarrow \quad A_0 - 2A_0 = 1 \quad \Longrightarrow \quad A_0 = -1$$

luego

$$a_n^{(p)} = -1$$

y, consecuentemente, la solución general a la ecuación propuesta es:

$$a_n = a_n^{(h)} + a_n^{(p)} = \alpha \cdot 2^n - 1.$$

Teniendo en cuenta la condición inicial,

$$\left.\begin{aligned} a_1 &= 1 \\ a_n &= \alpha \cdot 2^n - 1 \end{aligned}\right\} \Longrightarrow 1 = 2\alpha - 1 \Longrightarrow \alpha = 1.$$

Por lo tanto, una solución a la ecuación de recurrencia propuesta es la sucesión $\{a_n\}$ tal que

$$a_n = 2^n - 1,\ n \geqslant 1$$

■

Ejemplo 12.2

Resolver la ecuación de recurrencia:

$$a_{n+2} - 2a_{n+1} + a_n = 1,\ n \geqslant 1$$

con las condiciones iniciales, $a_1 = 1$ *y* $a_2 = 0$.

Solución

La ecuación propuesta escrita en su forma general es,

$$\begin{array}{rcl} a_1 & = & 1 \\ a_2 & = & 0 \\ a_{n+2} - 2a_{n+1} + a_n & = & 1 \end{array}$$

o sea, es lineal, no homogénea, de segundo orden y con coeficientes constantes.

Primero, obtendremos una solución para la ecuación de recurrencia homogénea asociada a la ecuación dada:

$$a_{n+2} - 2a_{n+1} + a_n = 0.$$

En efecto, su ecuación característica es $\lambda^2 - 2\lambda + 1 = 0$. Resolviéndola,

$$\lambda^2 - 2\lambda + 1 = 0 \Longrightarrow \lambda = \frac{2 \pm \sqrt{4-4}}{2} \Longrightarrow \left\{ \begin{array}{rcl} \lambda_1 & = & 1 \\ \lambda_2 & = & 1 \end{array} \right.$$

Por lo tanto, según 11.3.3, la solución general de la ecuación reducida es la sucesión $\left\{a_n^{(h)}\right\}$ tal que

$$a_n^{(h)} = \alpha_1 \cdot 1^n + \alpha_2 \cdot n \cdot 1^n = \alpha_1 + n\alpha_2,\ n \geqslant 1.$$

Ahora, calculamos una solución particular de la ecuación dada. El término independiente es $h(n) = 1$, es decir es igual al producto de r^n por un polinomio de grado cero,

$$h(n) = r^n p_0$$

sin más que tomar $r = 1$ y $p_0 = 1$. Como $\lambda = 1$ y $r = 1$, quiere decir que r es raíz de la ecuación característica y estaremos, pues, en el segundo caso de 12.2 con multiplicidad $m = 2$, por lo que tomaremos la sucesión $\left\{a_n^{(p)}\right\}$ tal que

$$a_n^{(p)} = n^2 A_0, \text{ siendo } A_0 \text{ una constante}$$

como solución particular de la ecuación propuesta. Sustituyendo en la ecuación,

$$\begin{array}{rcl} a_{n+2}^{(p)} - 2a_{n+1}^{(p)} + a_n^{(p)} = 1 & \Longrightarrow & (n+2)^2 A_0 - 2(n+1)^2 A_0 + n^2 A_0 = 1 \\ & \Longrightarrow & (n^2 + 4n + 4)A_0 - 2(n^2 + 2n + 1)A_0 + n^2 A_0 = 1 \\ & \Longrightarrow & n^2 A_0 + 4nA_0 + 4A_0 - 2n^2 A_0 - 4nA_0 - 2A_0 + n^2 A_0 = 1 \\ & \Longrightarrow & 2A_0 = 1 \\ & \Longrightarrow & A_0 = \frac{1}{2}. \end{array}$$

Por lo tanto, la sucesión $\left\{a_n^{(p)}\right\}$ tal que,

$$a_n^{(p)} = \frac{1}{2}n^2,\ n \geqslant 1$$

será una solución particular de la ecuación propuesta.

Por el teorema 12.1.2 la solución general de la ecuación es la sucesión $\{a_n\}$ tal que

$$a_n = a_n^{(h)} + a_n^{(p)} = \alpha_1 + n\alpha_2 + \frac{1}{2}n^2,\ n \geqslant 1$$

Finalmente, si tenemos en cuenta las condiciones iniciales:

$$\left.\begin{array}{rcl} a_1 &=& 1 \\ a_2 &=& 0 \\ a_n &=& \alpha_1 + n\alpha_2 + \frac{1}{2}n^2 \end{array}\right\} \Longrightarrow \left\{\begin{array}{rcl} \alpha_1 + \alpha_2 + \frac{1}{2} &=& 1 \\ \alpha_1 + 2\alpha_2 + 2 &=& 0 \end{array}\right.$$

$$\Longrightarrow \left\{\begin{array}{rcl} \alpha_2 + \frac{3}{2} &=& -1 \\ -\alpha_1 + 1 &=& -2 \end{array}\right.$$

$$\Longrightarrow \left\{\begin{array}{rcl} \alpha_2 &=& -\frac{5}{2} \\ \alpha_1 &=& 3 \end{array}\right.$$

Consecuentemente, una solución a la ecuación propuesta es la sucesión $\{a_n\}$ tal que

$$a_n = 3 - \frac{5}{2}n + \frac{1}{2}n^2,\ n \geqslant 1$$

■

Ejemplo 12.3

Resolver la ecuación de recurrencia:

$$\begin{array}{rcl} a_1 &=& 1 \\ a_2 &=& 2 \\ a_{n+2} + 2a_{n+1} + a_n &=& 3^n,\ n \geqslant 1 \end{array}$$

Solución

La ecuación de recurrencia propuesta es lineal, no homogénea, de segundo orden y con coeficientes constantes.

Al igual que en los ejemplos anteriores, primero calcularemos una solución de la ecuación homogénea asociada a la dada

$$a_{n+2} + 2a_{n+1} + a_n = 0.$$

Su ecuación característica es $\lambda^2 + 2\lambda + 1 = 0$. Entonces,

$$\lambda^2 + 2\lambda + 1 = 0 \Longrightarrow \lambda = \frac{-2 \pm \sqrt{4-4}}{2} \Longrightarrow \left\{\begin{array}{rcl} \lambda &=& -1 \\ \text{ó} & & \\ \lambda &=& -1 \end{array}\right.$$

es decir, la raíz de la ecuación característica es $\lambda = -1$ con multiplicidad $m = 2$. Por 11.3.3, la solución general de la ecuación reducida será la sucesión $\left\{a_n^{(h)}\right\}$ tal que

$$a_n^{(h)} = \alpha_1 (-1)^n + \alpha_2 \cdot n \cdot (-1)^n,\ n \geqslant 1$$

Calcularemos, a continuación, una solución particular de la ecuación propuesta. El término independiente es $h(n) = 3^n$ es decir es de la forma r^n por un polinomio de grado cero,

$$h(n) = r^n p_0$$

con $r = 3$ y $p_0 = 1$. Tenemos, pues, que $\lambda = -1$ y $r = 3$ luego r no es raíz de la ecuación característica. Estamos en el primer caso de 12.2, de aquí que tomemos como solución particular de la ecuación la sucesión $\left\{a_n^{(p)}\right\}$ tal que

$$a_n^{(p)} = 3^n A_0,\ n \geqslant 1.$$

Pues bien, sustituyendo en al ecuación,

$$\begin{aligned} a_{n+2}^{(p)} + 2a_{n+1}^{(p)} + a_n^{(p)} = 3^n &\implies 3^{n+2}A_0 + 2\cdot 3^{n+1}A_0 + 3^n A_0 = 3^n \\ &\implies 9\cdot 3^n A_0 + 6\cdot 3^n A_0 + 3^n A_0 = 3^n \\ &\implies 16\cdot 3^n A_0 = 3^n \\ &\implies 16A_0 = 1 \\ &\implies A_0 = \frac{1}{16}. \end{aligned}$$

Por lo tanto, la sucesión $\left\{a_n^{(p)}\right\}$ tal que,

$$a_n^{(p)} = \frac{1}{16}3^n,\ n \geqslant 1$$

es una solución particular de la ecuación propuesta.

Por el teorema 12.1.2, la solución general de nuestra ecuación es la sucesión $\{a_n\}$ tal que

$$a_n = a_n^{(h)} + a_n^{(p)} = \alpha_1(-1)^n + \alpha_2\cdot n\cdot(-1)^n + \frac{1}{16}3^n$$

y teniendo en cuenta las condiciones iniciales,

$$\left.\begin{array}{rcl} a_1 &=& 2 \\ a_2 &=& 2 \\ a_n &=& \alpha_1(-1)^n + \alpha_2\cdot n\cdot(-1)^n + \frac{1}{16}3^n \end{array}\right\} \implies \left\{\begin{array}{rcccccl} -\alpha_1 & - & \alpha_2 & + & \frac{3}{16} & = & 1 \\ \alpha_1 & + & 2\alpha_2 & + & \frac{9}{16} & = & 2 \end{array}\right.$$

$$\implies \left\{\begin{array}{rcccccl} & & \alpha_2 & + & \frac{12}{16} & = & 1 \\ -\alpha_1 & & & + & \frac{15}{16} & = & 2 \end{array}\right.$$

$$\implies \left\{\begin{array}{rcl} \alpha_2 &=& \frac{9}{4} \\ \alpha_1 &=& -\frac{49}{16} \end{array}\right.$$

En consecuencia, una solución de la ecuación propuesta es la sucesión $\{a_n\}$ tal que

$$a_n = \left(-\frac{49}{16} + \frac{9}{4}\right)(-1)^n + \frac{3^n}{16},\ n \geqslant 1$$

■

Ejemplo 12.4

Resolver

$$a_{n+2} - 6a_{n+1} + 9a_n = 3^n,\ n \geqslant 1$$

con las condiciones iniciales $a_1 = 1$ *y* $a_2 = 2$.

Solución

La ecuación de recurrencia propuesta,

$$\begin{array}{rcl} a_1 & = & 1 \\ a_2 & = & 2 \\ a_{n+2} - 6a_{n+1} + 9a_n & = & 3^n,\ n \geqslant 1 \end{array}$$

es lineal, no homogénea, de segundo orden y con coeficientes constantes.

Obtendremos la solución general de la ecuación de recurrencia homogénea asociada a la ecuación dada,

$$a_{n+2} - 6a_{n+1} + 9a_n = 0,\ n \geqslant 1$$

Su ecuación característica es $\lambda^2 - 6\lambda + 9 = 0$. Entonces,

$$\lambda^2 - 6\lambda + 9 = 0 \implies \lambda = \frac{6 \pm \sqrt{36 - 4 \cdot 1 \cdot 9}}{2} \implies \left\{ \begin{array}{rcl} \lambda & = & 3 \\ \text{ó} & & \\ \lambda & = & 3 \end{array} \right.$$

o sea, la raíz de la ecuación característica es $\lambda = 3$ con multiplicidad $m = 2$. Por 11.3.3, la sucesión $\left\{a_n^{(h)}\right\}$ tal que

$$a_n^{(h)} = \alpha_1 \cdot 3^n + \alpha_2 \cdot n \cdot 3^n,\ \alpha_1, \alpha_2 \in \mathbb{R},\ n \geqslant 1$$

es la solución general de la ecuación homogénea asociada a la ecuación dada.

Calculamos, ahora, una solución particular de la ecuación propuesta. Como el término independiente es $h(n) = 3^n$ es de la forma r^n por un polinomio de grado cero,

$$h(n) = r^n p_0$$

con $r = 3$ y $p_0 = 1$. Como $\lambda = 3$ y $r = 3$, r es raíz de la ecuación característica. Estamos, pues, en el segundo caso de 12.2. Ensayamos, por tanto, como solución particular de la ecuación, la sucesión $\left\{a_n^{(p)}\right\}$ tal que,

$$a_n^{(p)} = n^2 3^n A_0,\ A_0 \text{ constante},\ n \geqslant 1.$$

Sustituyendo en la ecuación,

$$a_{n+2}^{(p)} - 6a_{n+1}^{(p)} + 9a_n^{(p)} = 3^n \implies (n+2)^2 3^{n+2} A_0 - 6(n+1)^2 3^{n+1} A_0 + 9n^2 3^n A_0 = 3^n$$

y haciendo operaciones,

$$\left(n^2 + 4n + 4\right) 3^n 9A_0 - 6\left(n^2 + 2n + 1\right) 3^n 3A_0 + 9n^2 3^n A_0 = 3^n$$

es decir,

$$\left(9A_0 n^2 + 36A_0 n + 36A_0 - 18A_0 n^2 - 36A_0 n - 18A + 9A_0 n^2\right) 3^n = 3^n$$

de aquí que

$$18A_0 3^n = 3^n$$

y, consecuentemente,

$$A_0 = \frac{1}{18}$$

Así pues, la sucesión $\left\{a_n^{(p)}\right\}$ tal que

$$a_n^{(p)} = \frac{1}{18}n^2 3^n,\ n \geqslant 1$$

es una solución particular de nuestra ecuación y, consecuentemente, la solución general de la ecuación dada es por 12.1.2, la sucesión $\{a_n\}$ tal que

$$a_n = a_n^{(h)} + a_n^{(p)} = \alpha_1 \cdot 3^n + \alpha_2 \cdot n \cdot 3^n + \frac{1}{18}n^2 \cdot 3^n$$

Si ahora tomamos en consideración las condiciones iniciales,

$$\left.\begin{array}{rcl} a_1 & = & 1 \\ a_2 & = & 2 \\ a_n & = & \alpha_1 \cdot 3^n + \alpha_2 \cdot n \cdot 3^n + \frac{1}{18}n^2 \cdot 3^n \end{array}\right\} \Longrightarrow \left\{\begin{array}{rcrcrcl} 3\alpha_1 & + & 3\alpha_2 & + & \frac{1}{18}\cdot 3 & = & 1 \\ 9\alpha_1 & + & 18\alpha_2 & + & \frac{1}{18}\cdot 4\cdot 9 & = & 2 \end{array}\right.$$

$$\Longrightarrow \left\{\begin{array}{rcrcl} 3\alpha_1 & + & 3\alpha_2 & = & 1 - \frac{1}{6} \\ 9\alpha_1 & + & 18\alpha_2 & = & 2 - 2 \end{array}\right.$$

$$\Longrightarrow \left\{\begin{array}{rcrcl} 3\alpha_1 & + & 3\alpha_2 & = & \frac{5}{6} \\ 9\alpha_1 & + & 18\alpha_2 & = & 0 \end{array}\right.$$

$$\Longrightarrow \left\{\begin{array}{rcrcll} & & 9\alpha_2 & = & -\frac{5}{2} & \{2^{\underline{a}} \text{ menos } 1^{\underline{a}} \times 3\} \\ -9\alpha_1 & = & -5 & & & \{2^{\underline{a}} \text{ menos } 1^{\underline{a}} \times 6\} \end{array}\right.$$

$$\Longrightarrow \left\{\begin{array}{rcl} \alpha_2 & = & -\frac{5}{18} \\ \alpha_1 & = & \frac{5}{9} \end{array}\right.$$

Por lo tanto, una solución de la ecuación de recurrencia propuesta es la sucesión $\{a_n\}$ tal que

$$\begin{array}{rcl} a_n & = & \frac{5}{9}3^n - \frac{5}{18}n3^n + \frac{1}{18}n^2 3^n \\ & = & \frac{1}{18}\left(n^2 - 5n + 10\right)3^n,\ n \geqslant 1 \end{array}$$

■

Ejemplo 12.5

Resolver la ecuación de recurrencia

$$a_{n+3} = 4a_{n+2} + 3a_{n+1} - 18a_n + 24n + 20,\ n \geqslant 1$$

con las condiciones iniciales $a_1 = 0$, $a_2 = 1$ *y* $a_3 = 2$.

Solución

La ecuación de recurrencia,

$$\begin{array}{rcl} a_1 & = & 0 \\ a_2 & = & 1 \\ a_3 & = & 2 \\ a_{n+3} - 4a_{n+2} - 3a_{n+1} + 18a_n & = & 24n + 20 \end{array}$$

Es lineal, no homogénea, de tercer orden y con coeficientes constantes.

Calcularemos la solución general de su ecuación de recurrencia homogénea asociada,

$$a_{n+3} - 4a_{n+2} - 3a_{n+1} + 18a_n = 0.$$

En efecto, su ecuación característica es $\lambda^3 - 4\lambda^2 - 3\lambda + 18 = 0$. Factorizamos el polinomio $\lambda^3 - 4\lambda^2 - 3\lambda + 18$ utilizando la Regla de Ruffini,

	1	-4	-3	18
3		3	-3	-18
	1	-1	-6	0
3		3	6	
	1	2	0	
-2		-2		
	1	0		

luego,

$$\lambda^2 - 4\lambda^2 - 3\lambda + 18 = 0 \implies (\lambda - 3)(\lambda - 3)(\lambda + 2) = 0 \implies \left\{ \begin{array}{rcl} \lambda & = & 3 \\ \text{ó} & & \\ \lambda & = & 3 \\ \text{ó} & & \\ \lambda & = & -2 \end{array} \right.$$

o sea, las raíces de la ecuación característica son $\lambda = 3$ con multiplicidad $m = 2$ y $\lambda = -2$ con multiplicidad 1. Por 11.3.3, su solución general es la sucesión $\left\{a_n^{(h)}\right\}$ tal que

$$a_n^{(h)} = \alpha_1 \cdot 3^n + \alpha_2 \cdot n \cdot 3^n + \alpha_3 (-2)^n, \ \alpha_1, \alpha_2, \alpha_3 \in \mathbb{R}, \text{ y } n \geqslant 1.$$

Calcularemos, a continuación, una solución particular de la ecuación propuesta. El término independiente es $h(n) = 24n + 20$, es decir es de la forma r^n por un polinomio de grado uno,

$$h(n) = r^n(p_0 + p_1 n)$$

sin más que tomar $r = 1$, $p_0 = 20$ y $p_1 = 24$. Como las raíces de la ecuación característica ($\lambda = 3$ y $\lambda = -2$) son, todas, distintas de r, ($r = 1$) estaríamos en el primer caso de 12.2. Probaremos, por tanto, como solución particular de la ecuación dada la sucesión $\left\{a_n^{(p)}\right\}$ tal que

$$a_n^{(p)} = A_0 + A_1 n, \ n \geqslant 1.$$

Sustituyendo en la ecuación,

$$a_{n+3}^{(p)} - 4a_{n+2}^{(p)} - 3a_{n+1}^{(p)} + 18a_n^{(p)} = 24n + 20$$

tendremos,

$$A_0 + A_1(n+3) - 4\left[A_0 + A_1(n+2)\right] - 3\left[A_0 + A_1(n+1)\right] + 18(A_0 + A_1 n) = 24n + 20$$

o sea,

$$A_0 + A_1 n + 3A_1 - 4A_0 - 4A_1 n - 8A_1 - 3A_0 - 3A_1 n - 3A_1 + 18A_0 + 18A_1 n = 24n + 20$$

y haciendo operaciones,

$$12A_1 n - 8A_1 + 12A_0 = 24n + 20.$$

Igualando coeficientes,

$$\begin{array}{rcrcl} 12A_1 & & & = & 24 \\ -8A_1 & + & 12A_0 & = & 20 \end{array}$$

y, consecuentemente,

$$A_0 = 3 \text{ y } A_1 = 2$$

luego,

$$a_n^{(p)} = 3 + 2n,\ n \geqslant 1.$$

De aquí se sigue que la solución general de la ecuación dada es la sucesión $\{a_n\}$ tal que

$$a_n = a_n^{(h)} + a_n^{(p)} = \alpha_1 \cdot 3^n + \alpha_2 \cdot n \cdot 3^n + \alpha_3(-2)^n + 3 + 2n$$

y aplicando las condiciones iniciales,

$$\left.\begin{array}{rcl} a_1 & = & 0 \\ a_2 & = & 1 \\ a_3 & = & 2 \\ a_n & = & \alpha_1 3^n + \alpha_2 n 3^n + \alpha_3(-2)^n + 3 + 2n \end{array}\right\}$$

de aquí que

$$\left.\begin{array}{rcrcrcrcl} 3\alpha_1 & + & 3\alpha_2 & - & 2\alpha_3 & + & 5 & = & 0 \\ 9\alpha_1 & + & 18\alpha_2 & + & 4\alpha_3 & + & 7 & = & 1 \\ 27\alpha_1 & + & 81\alpha_2 & - & 8\alpha_3 & + & 9 & = & 2 \end{array}\right\} \Longrightarrow \left\{\begin{array}{rcrcrcl} 3\alpha_1 & + & 3\alpha_2 & - & 2\alpha_3 & = & -5 \\ 9\alpha_1 & + & 18\alpha_2 & + & 4\alpha_3 & = & -6 \\ 27\alpha_1 & + & 81\alpha_2 & - & 8\alpha_3 & = & -7 \end{array}\right.$$

$$\left\{\begin{array}{l} 2^{\underline{a}} \text{ menos } 1^{\underline{a}} \times 3 \\ 3^{\underline{a}} \text{ menos } 1^{\underline{a}} \times 9 \end{array}\right\}$$

$$\Longrightarrow \left\{\begin{array}{rcrcrcl} 3\alpha_1 & + & 3\alpha_2 & - & 2\alpha_3 & = & -5 \\ & & 9\alpha_2 & + & 10\alpha_3 & = & 9 \\ & & 54\alpha_2 & + & 10\alpha_3 & = & 38 \end{array}\right.$$

$$\left\{\ 3^{\underline{a}} \text{ menos } 2^{\underline{a}} \times 6\ \right\}$$

$$\Longrightarrow \left\{\begin{array}{rcrcrcl} 3\alpha_1 & + & 3\alpha_2 & - & 2\alpha_3 & = & -5 \\ & & 9\alpha_2 & + & 10\alpha_3 & = & 9 \\ & & & - & 50\alpha_3 & = & -16 \end{array}\right.$$

$$\Longrightarrow \left\{\begin{array}{rcrcrcl} \alpha_1 & + & \alpha_2 & - & \frac{2}{3}\alpha_3 & = & -\frac{5}{3} \\ & & \alpha_2 & + & \frac{10}{9}\alpha_3 & = & 1 \\ & & & & \alpha_3 & = & \frac{8}{25} \end{array}\right.$$

$$\Longrightarrow \left\{\begin{array}{rcrcl} \alpha_1 & = & - & \frac{472}{225} & \\ \alpha_2 & = & & \frac{29}{45} & \\ \alpha_3 & = & & \frac{8}{25} & \end{array}\right.$$

Consecuentemente, una solución a la ecuación propuesta es la sucesión $\{a_n\}$ tal que

$$a_n = -\frac{472}{225} \cdot 3^n + \frac{29}{45} \cdot n \cdot 3^n + \frac{8}{25}(-2)^n + 2n + 3$$

■

Ejemplo 12.6

Encontrar una solución general para la ecuación de recurrencia,

$$\begin{aligned} a_1 &= 2 \\ a_{n+1} - a_n &= n+1,\ n \geqslant 1 \end{aligned}$$

Solución

La ecuación de recurrencia es lineal, no homogénea, de primer orden y con coeficientes constantes. Procederemos igual que en los ejercicios anteriores.

Sea

$$a_{n+1} - a_n = 0$$

la ecuación homogénea correspondiente a la ecuación dada y sea $\lambda - 1 = 0$ su ecuación característica. Entonces,

$$\lambda - 1 = 0 \Longrightarrow \lambda = 1$$

o sea, la raíz de la ecuación característica es $\lambda = 1$ con multiplicidad $m = 1$. La solución general de la ecuación homogénea será (11.3.3) la sucesión $\left\{a_n^{(h)}\right\}$ tal que

$$a_n^{(h)} = \alpha \cdot 1^n = \alpha,\ \alpha \in \mathbb{R},\ n \geqslant 1.$$

Calculamos, ahora, una solución particular para la ecuación propuesta. El término independiente es $h(n) = n + 1$, o sea es de la forma r^n por un polinomio de grado uno,

$$h(n) = r^n \left(p_0 + p_1 n\right)$$

con $r = 1$, $p_0 = 1$ y $p_1 = 1$. La raíz de la ecuación característica ($\lambda = 1$) y r son iguales ($r = 1$) por lo que estaremos en el segundo caso de 12.2 y probaremos como solución particular de nuestra ecuación la sucesión $\left\{a_n^{(p)}\right\}$ tal que

$$a_n^{(p)} = n\left(A_0 + A_1 n\right),\ n \geqslant 1.$$

Sustituyendo en la ecuación,

$$\begin{aligned}
a_{n+1}^{(p)} - a_n^{(p)} = n + 1 &\Longrightarrow (n+1)\left[A_0 + A_1(n+1)\right] - n\left(A_0 + A_1 n\right) = n + 1 \\
&\Longrightarrow A_0 n + A_0 + A_1(n+1)^2 - A_0 n - A_1 n^2 = n + 1 \\
&\Longrightarrow A_0 + A_1\left(n^2 + 2n + 1\right) - A_1 n^2 = n + 1 \\
&\Longrightarrow A_0 + A_1 + 2A_1 n = n + 1 \\
&\Longrightarrow \left\{\begin{array}{rcl} A_0 + A_1 & = & 1 \\ 2A_1 & = & 1 \end{array}\right. \\
&\Longrightarrow \left\{\begin{array}{rcl} A_0 & = & \dfrac{1}{2} \\ \text{y} & & \\ A_1 & = & \dfrac{1}{2} \end{array}\right.
\end{aligned}$$

luego,

$$a_n^{(p)} = n\left(\frac{1}{2} + \frac{1}{2}n\right) = \frac{1}{2}\left(n^2 + n\right).$$

La solución general de la ecuación dada será, por tanto, la sucesión $\{a_n\}$ tal que

$$a_n = a_n^{(h)} + a_n^{(p)} = \alpha + \frac{1}{2}\left(n^2 + n\right),\ n \geqslant 1$$

Teniendo en cuenta la condición inicial, tendremos:

$$\left.\begin{array}{rcl} a_1 & = & 2 \\ a_n & = & \alpha + \dfrac{1}{2}\left(n^2 + n\right) \end{array}\right\} \Longrightarrow \alpha + \frac{1}{2}\left(1^2 + 1\right) = 2 \Longrightarrow \alpha + 1 = 2 \Longrightarrow \alpha = 1.$$

Consecuentemente, una solución a la ecuación propuesta es la sucesión $\{a_n\}$ tal que

$$a_n = 1 + \frac{1}{2}\left(n^2 + n\right) = \frac{1}{2}\left(n^2 + n + 2\right),\ n \geqslant 1$$

■

Ejemplo 12.7

Resolver la ecuación de recurrencia:

$$\begin{aligned} a_1 &= 1 \\ a_2 &= 2 \\ a_{n+2} - 6a_{n+1} + 9a_n &= n \cdot 3^n,\ n \geqslant 1 \end{aligned}$$

Solución

La ecuación es lineal, no homogénea, de segundo orden y con coeficientes constantes. La ecuación homogénea asociada a la dada es

$$a_{n+2} - 6a_{n+1} + 9a_n = 0.$$

Su ecuación característica es $\lambda^2 - 6\lambda + 9 = 0$. Entonces,

$$\lambda^2 - 6\lambda + 9 = 0 \Longrightarrow \lambda = \frac{6 \pm \sqrt{36-36}}{2} \Longrightarrow \left\{ \begin{array}{lcl} \lambda & = & 3 \\ \text{ó} & & \\ \lambda & = & 3 \end{array} \right.$$

es decir, la raíz de la ecuación característica ($\lambda = 2$) es doble ($m = 2$). Por 11.3.3, la solución general de la ecuación reducida es la sucesión $\left\{a_n^{(h)}\right\}$ tal que

$$a_n^{(h)} = \alpha_1 \cdot 3^n + \alpha_2 \cdot n \cdot 3^n,\ \alpha_1, \alpha_2 \in \mathbb{R},\ n \geqslant 1$$

Por otra parte, el término independiente es $h(n) = n \cdot 3^n$, es decir es de la forma r^n por un polinomio de grado 1,

$$h(n) = r^n \left(p_0 + p_1 n\right)$$

con $r = 3$, $p_0 = 0$ y $p_1 = 1$. La raíz de la ecuación característica ($\lambda = 3$) y r son iguales ($r = 3$) por lo que siguiendo lo dicho en el segundo caso método de los coeficientes indeterminados (12.2), probaremos como solución particular de la ecuación propuesta la sucesión $\left\{a_n^{(p)}\right\}$ tal que

$$a_n^{(p)} = n^2 3^n (A_0 + A_1 n),\ n \geqslant 1.$$

Sustituyendo en la ecuación propuesta,

$$(n+2)^2 \cdot 3^{n+2} \left[A_0 + A_1(n+2)\right] - 6(n+1)^2 \cdot 3^{n+1} \left[A_0 + A_1(n+1)\right] + 9n^2 3^n (A_0 + A_1 n) = n \cdot 3^n$$

luego,

$$\begin{aligned} 9 \cdot 3^n \left[A_0(n+2)^2 + A_1(n+2)^3\right] &- 18 \cdot 3^n \left[A_0(n+1)^2 + A_1(n+1)^3\right] \\ &+ 9 \cdot 3^n \left(A_0 n^2 + A_1 n^3\right) = n \cdot 3^n \end{aligned}$$

desarrollando los cubos y los cuadrados,

$$\begin{aligned} &9 \cdot 3^n \left[A_0(n^2 + 4n + 4) + A_1(n^3 + 6n^2 + 12n + 8)\right] - \\ &18 \cdot 3^n \left[A_0(n^2 + 2n + 1) + A_1(n^3 + 3n^2 + 3n + 1)\right] + 9 \cdot 3^n \left(A_0 n^2 + A_1 n^3\right) = n \cdot 3^n \end{aligned}$$

haciendo operaciones,

$$\begin{aligned} 9 \cdot 3^n \big(&A_0 n^2 + 4A_0 n + 4A_0 + A_1 n^3 + 6A_1 n^2 + 12A_1 n \\ &+ 8A_1 - 2A_0 n^2 - 4A_0 n - 2A_0 - 2A_1 n^3 \\ &- 6A_1 n^2 - 6A_1 n - 2A_1 + A_0 n^2 + A_1 n^3\big) = n \cdot 3^n \end{aligned}$$

y simplificando, nos queda,

$$\begin{aligned} 9\cdot 3^n\left(6A_1n+6A_1+2A_0\right)=n\cdot 3^n &\implies 3^n\left(54A_1n+54A_1+18A_0\right)=n\cdot 3^n\\ &\implies 54A_1n+54A_1+18A_0=n\\ &\implies \left\{\begin{array}{rcl} 54A_1 & = & 1\\ 54A_1+18A_0 & = & 0\end{array}\right.\\ &\implies \left\{\begin{array}{rcl} A_1 & = & \dfrac{1}{54}\\ A_0 & = & -\dfrac{3}{54}\end{array}\right.\end{aligned}$$

Por lo tanto, la solución particular de la ecuación es la sucesión $\left\{a_n^{(p)}\right\}$ tal que

$$a_n^{(p)}=n^2\cdot 3^n\left(\frac{1}{54}n-\frac{3}{54}\right)=\frac{3^n}{54}\left(n^3-3n^2\right),\ n\geqslant 1$$

De aquí que la solución general a la ecuación propuesta, por 12.1.2, sea la sucesión $\{a_n\}$ tal que

$$a_n=a_n^{(h)}+a_n^{(p)}=\alpha_1\cdot 3^n+\alpha_2\cdot n\cdot 3^n+\frac{3^n}{54}\left(n^3-3n^2\right),\ n\geqslant 1.$$

Si ahora tenemos en cuenta las condiciones iniciales,

$$\left.\begin{array}{rcl} a_1 & = & 1\\ a_2 & = & 2\\ a_n & = & \alpha_1\cdot 3^n+\alpha_2\cdot n\cdot 3^n+\dfrac{3^n}{54}\left(n^3-3n^2\right)\end{array}\right\}$$

de aquí que

$$\left.\begin{array}{rcrcrcl} 3\alpha_1 & + & 3\alpha_2 & + & \dfrac{3}{54}2 & = & 1\\ 9\alpha_1 & + & 18\alpha_2 & + & \dfrac{9}{54}(-4) & = & 2\end{array}\right\} \implies \left\{\begin{array}{rcrcrcl} 3\alpha_1 & + & 3\alpha_2 & - & \dfrac{1}{9} & = & 1\\ 9\alpha_2 & + & 18\alpha_2 & - & \dfrac{2}{3} & = & 2\end{array}\right.$$

$$\implies \left\{\begin{array}{rcrcl} 3\alpha_1 & + & 3\alpha_2 & = & \dfrac{10}{9}\\ 9\alpha_2 & + & 18\alpha_2 & = & \dfrac{8}{3}\end{array}\right.$$

$$\implies \left\{\begin{array}{rcrcl} \alpha_1 & + & \alpha_2 & = & \dfrac{10}{27}\\ \alpha_1 & + & 2\alpha_2 & = & \dfrac{8}{27}\end{array}\right.$$

$$\implies \left\{\begin{array}{rcl} \alpha_2 & = & -\dfrac{2}{27}\\ \text{y} & & \\ \alpha_1 & = & \dfrac{12}{27}\end{array}\right.$$

Consecuentemente, una solución a la ecuación de recurrencia propuesta es la sucesión $\{a_n\}$ tal que:

$$\begin{aligned} a_n &= \frac{12}{27}3^n-\frac{2}{27}n\cdot 3^n+\frac{3^n}{54}\left(n^3-3n^2\right)\\ &= \frac{1}{54}\left(n^3-3n^2-4n+24\right)3^n,\ n\geqslant 1\end{aligned}$$

■

Unidad Temática V

Teoría de Números

Lección 13

Divisibilidad. Algoritmo de la División

Dios hizo los enteros, el resto es obra del hombre... Todos los resultados de la más profunda investigación matemática deben ser expresables en la sencilla forma de las propiedades de los enteros.

Leopold Kronecker (1823-1891)

13.1 Divisibilidad

Aunque el conjunto de los números enteros, $\mathbb{Z}$, no es cerrado para la división, hay muchos casos en los que un número entero divide a otro. Por ejemplo 2 divide a 12 y 3 divide a -27. La división es exacta y no existe resto. Así pues, el que 2 divida a 12 implica la existencia de un cociente, 6, tal que $12 = 2 \cdot 6$.

13.1.1 Definición

Sean a y b dos números enteros tales que $a \neq 0$. Diremos que "a" divide a "b" o "a" es divisor de "b" si existe un número entero q tal que $b = a \cdot q$. Suele notarse $a|b$, es decir,

$$a|b \Longleftrightarrow \exists q \in \mathbb{Z} : b = aq$$

■

Nota 13.1 Observemos lo siguiente:

$$a \text{ divide a } b \Longleftrightarrow b = aq;\ q \in \mathbb{Z} \Longleftrightarrow b \text{ es múltiplo de } a$$

y también,

$$\begin{aligned} a \text{ es divisor de } b &\iff b = aq;\ q \in \mathbb{Z} \\ &\iff \frac{b}{a} = q;\ q \in \mathbb{Z} \\ &\iff \frac{b}{a} \in \mathbb{Z} \\ &\iff b \text{ es divisible por } a \end{aligned}$$

luego las expresiones "a divide a b", "a es divisor de b", "b es múltiplo de a" y "b es divisible por a" significan, todas, lo mismo y se notan $a\,|b$.

■

Ejemplo 13.1

(a) 2 *divide a* 6 *ya que* $6 = 2 \cdot 3$*, con* $3 \in \mathbb{Z}$*.*

(b) 5 *divide a* -45 *ya que* $-45 = 5(-9)$*, con* $-9 \in \mathbb{Z}$*.*

(c) -4 *divide a* 64 *ya que* $64 = (-4)(-16)$*, con* $-16 \in \mathbb{Z}$*.*

(d) -7 *divide a* -21 *ya que* $-21 = (-7)3$*, con* $3 \in \mathbb{Z}$*.*

(e) 3 *no divide a* 5 *ya que no existe ningún número entero* q *tal que* $5 = 3 \cdot q$*.*

■

Obsérvese que la definición de divisibilidad nos permite hablar de división en $\mathbb{Z}$ sin ir a $\mathbb{Q}$.

Nota 13.2 Aunque nuestro objetivo no es el estudio de la estructura algebraica de los números enteros, es importante recordar que la suma y el producto de números enteros son operaciones asociativas y conmutativas, que $\{\mathbb{Z}, +\}$ es grupo abeliano y que se satisface la propiedad distributiva del producto respecto de la suma, por lo que $\{\mathbb{Z}, +, \cdot\}$ es un anillo conmutativo con elemento unidad (el 1) y sin divisores de cero.

■

13.1.2 Propiedades

Sean a*,* b *y* c *tres números enteros, siendo* a *y* b *distintos de cero. Se verifica:*

(i) El 1 *es divisor de cualquier número entero.*

(ii) El 0 *es múltiplo de cualquier número entero.*

(iii) Si "a" divide a "b" y "b" divide a "a", entonces $a = \pm b$*.*

(iv) Si "a" divide a "b" y "b" divide a "c", entonces "a" divide a "c".

(v) Si "a" divide a "b" y "a" divide a "c", entonces "a" divide a $pb+qc$*, cualesquiera que sean* p *y* q*, enteros. (A la expresión* $pb + qc$ *se le llama combinación lineal de* b *y* c *con coeficientes enteros).*

Demostración

(i) Sea a cualquier número entero distinto de cero. Entonces,

$$a = 1 \cdot a, \text{con } a \in \mathbb{Z}$$

luego, $1 \,|a\,.$

(ii) Sea a cualquier número entero. Entonces,

$$0 = a \cdot 0, \text{ con } 0 \in \mathbb{Z}$$

luego, $a \,|0$

(iii) $a\,|b$ y $b\,|a \iff |a| = |b|, \forall a, b \in \mathbb{Z} \setminus \{0\}$

Recordemos que si n es cualquier entero,

$$|n| = \begin{cases} n, \text{ si } n \geqslant 0 \\ -n, \text{ si } n < 0 \end{cases}$$

entonces,

$$|a| = |b| \iff \begin{cases} a = b, \text{ si } a \geqslant 0,\ b \geqslant 0 \\ a = -b, \text{ si } a \geqslant 0,\ b < 0 \\ -a = b, \text{ si } a < 0,\ b \geqslant 0 \\ -a = -b, \text{ si } a < 0,\ b < 0 \end{cases}$$

$$\iff \begin{cases} a = b \\ \text{o} \\ a = -b \end{cases}$$

Pues bien, veamos que $a\,|b$ y $b\,|a \implies |a| = |b|, \forall a, b \in \mathbb{Z} \setminus \{0\}$ En efecto,

$$\left.\begin{array}{l} a\,|b \iff \exists q_1 \in \mathbb{Z} : b = aq_1 \\ \text{y} \\ b\,|a \iff \exists q_2 \in \mathbb{Z} : a = bq_2 \end{array}\right\} \implies b = bq_1q_2 \implies b(1 - q_1q_2) = 0$$

y al ser $b \neq 0$ y no tener $\mathbb{Z}$ divisores de cero, se sigue que

$$1 - q_1q_2 = 0 \implies q_1q_2 = 1 \implies \begin{cases} q_1 = q_2 = 1 \\ \text{o} \\ q_1 = q_2 = -1 \end{cases}$$

luego,

$$\left.\begin{array}{l} \left.\begin{array}{l} b = aq_1 \\ a = bq_2 \\ q_1 = q_2 = 1 \end{array}\right\} \implies a = b \\ \text{o} \\ \left.\begin{array}{l} b = aq_1 \\ a = bq_2 \\ q_1 = q_2 = -1 \end{array}\right\} \implies a = -b \end{array}\right\} \implies |a| = |b|$$

Recíprocamente, veamos ahora que $|a| = |b| \implies a\,|b$ y $b\,|a$

En efecto,

$$|a| = |b| \implies \begin{cases} a = b \implies \begin{cases} a = b \cdot 1,\ 1 \in \mathbb{Z} \implies b|a \\ \text{y} \\ b = a \cdot 1,\ 1 \in \mathbb{Z} \implies a|b \end{cases} \\ \text{o} \\ a = -b \implies \begin{cases} a = b(-1),\ -1 \in \mathbb{Z} \implies b|a \\ \text{y} \\ b = a(-1),\ -1 \in \mathbb{Z} \implies a|b \end{cases} \end{cases}$$

(iv) $a\,|b$ y $b\,|c \Longrightarrow a\,|c$. En efecto,

$$\left.\begin{array}{l} a\,|b \iff \exists q_1 \in \mathbb{Z} : b = aq_1 \\ \text{y} \\ b\,|c \iff \exists q_2 \in \mathbb{Z} : c = bq_2 \end{array}\right\} \Longrightarrow \quad c = aq_1q_2, \text{ con } q_1q_2 \in \mathbb{Z} \quad \Longleftrightarrow \quad a|c$$

(v) $a\,|b$ y $a\,|c \Longrightarrow a\,|pb + qc\,,\ \forall p, q \in \mathbb{Z}$ En efecto,

$$\left.\begin{array}{l} a\,|b \iff \exists q_1 \in \mathbb{Z} : b = aq_1 \Longrightarrow pb = paq_1 \\ \text{y} \\ a\,|c \iff \exists q_2 \in \mathbb{Z} : c = aq_2 \Longrightarrow qc = qaq_2 \end{array}\right\} \Longrightarrow pb + qc = a(pq_1 + qq_2),\ pq_1 + qq_2 \in \mathbb{Z} \Longleftrightarrow a|pb + qc$$

■

Ejemplo 13.2

Probar que si un entero divide a otros dos, entonces divide a su suma y también a su diferencia.

Solución

En efecto, sean a, b y c tres enteros cualesquiera, siendo $a \neq 0$. Entonces,

$$\left.\begin{array}{l} a\,|b \\ \text{y} \\ a\,|c \end{array}\right\} \Longrightarrow \quad a|pb + qc,\ \forall p, q \in \mathbb{Z} \quad \{13.1.2\ (v)\}$$

$$\Longrightarrow \left\{\begin{array}{ll} a|b + c & \{\text{Tomando } p = q = 1\} \\ \text{y} & \\ a|b - c & \{\text{Tomando } p = 1 \text{ y } q = -1\} \end{array}\right.$$

■

Ejemplo 13.3

Sean a, b, c y d números enteros con $a \neq 0$ y $c \neq 0$. Demuéstrese que

(a) Si $a\,|b$ y $c\,|d$, entonces $ac\,|bd$.

(b) $ac\,|bc$ si, y sólo si $a\,|b$.

Solución

(a) Si $a\,|b$ y $c\,|d$, entonces $ac\,|bd$.
En efecto,

$$\left.\begin{array}{l} a\,|b \iff \exists q_1 \in \mathbb{Z} : b = aq_1 \\ \text{y} \\ c\,|d \iff \exists q_2 \in \mathbb{Z} : d = cq_2 \end{array}\right\} \Longrightarrow bd = acq_1q_2, \text{ con } q_1q_2 \in \mathbb{Z} \Longleftrightarrow ac|bd$$

(b) $ac\,|bc$ si, y sólo si $a\,|b$.

"Sólo si." En efecto, supongamos que $ac\,|bc$. Entonces, existirá un entero q tal que

$$bc = acq \Longrightarrow (b - aq)c = 0$$

pero $c \neq 0$ y $\mathbb{Z}$ no tiene divisores de cero, luego

$$b - aq = 0 \Longleftrightarrow b = aq, \text{ con } q \in \mathbb{Z}$$

es decir,

$$a\,|b$$

"Si." En efecto, si $a\,|b$, como $c\,|c$, por el apartado (a) se sigue que $ac\,|bc$.

■

Ejemplo 13.4

Sean a y b dos números enteros positivos. Probar que si $b\,|a$ y $b\,|(a+2)$, entonces $b = 1$ ó $b = 2$.

Solución

Aplicando el resultado obtenido en el ejemplo 13.2 ,

$$\left.\begin{array}{l} b\,|a \\ \text{y} \\ b\,|a+2 \end{array}\right\} \Longrightarrow b\,|a+2-a \Longrightarrow b\,|2 \Longrightarrow b = 1 \text{ ó } b = 2$$

■

Ejemplo 13.5

Probar que la suma de los cuadrados de dos enteros positivos e impares es múltiplo de 2 pero no de 4.

Solución

Sean a y b dos enteros positivos e impares cualesquiera.

⁕ Veamos que $a^2 + b^2$ es múltiplo de 2. En efecto,

$$\left.\begin{array}{l} a \in \mathbb{Z}^+ \\ a \text{ impar} \end{array}\right\} \Longrightarrow a = 2p+1, \text{ con } p \in \mathbb{Z}_0^+$$

$$\left.\begin{array}{l} b \in \mathbb{Z}^+ \\ b \text{ impar} \end{array}\right\} \Longrightarrow b = 2q+1, \text{ con } q \in \mathbb{Z}_0^+$$

Entonces,

$$\begin{aligned} a^2 + b^2 &= (2p+1)^2 + (2q+1)^2 \\ &= 4p^2 + 4p + 1 + 4q^2 + 4q + 1 \\ &= 2(2p^2 + 2q^2 + 2p + 2q + 1), \text{siendo } 2p^2 + 2q^2 + 2p + 2q + 1 \in \mathbb{Z}^+ \end{aligned}$$

luego,

$$2\,|a^2 + b^2$$

es decir, $a^2 + b^2$ es múltiplo de 2.

⋇ Comprobemos ahora que a^2+b^2 no es múltiplo de 4. En efecto, supongamos que lo contrario es cierto, es decir, a^2+b^2 es múltiplo de 4, o sea,

$$4 \,\big|\, a^2+b^2$$

Pues bien, tenemos que

$$\begin{aligned} a^2+b^2 = 4p^2+4p+1+4q^2+4q+1 \quad &\Longrightarrow \quad a^2+b^2-2 = 4(p^2+p+q^2+q), \\ &\quad \text{con } p^2+p+q^2+q \in \mathbb{Z}^+ \\ &\Longrightarrow \quad 4 \,\big|\, a^2+b^2-2\,. \end{aligned}$$

Así pues,

$$\left.\begin{array}{l} 4 \,\big|\, a^2+b^2 \\ \text{y} \\ 4 \,\big|\, (a^2+b^2)-2 \end{array}\right\} \overset{(13.2)}{\Longrightarrow} 4 \,\big|\, (a^2+b^2)-\big[(a^2+b^2)-2\big] \Longrightarrow 4 \,|\, 2$$

lo cual, obviamente, es falso y, por tanto, la suposición hecha no es cierta. Consecuentemente,

$$a^2+b^2 \text{ no es múltiplo de } 4$$

■

13.2 Algoritmo de la División

Estableceremos en este apartado el algoritmo de la división de dos números, comprobando que el cociente y el resto de la división son únicos.

13.2.1 Existencia y Unicidad de Cociente y Resto

Si a y b son dos números enteros con $b>0$, entonces existen otros dos números, q y r, enteros y únicos, tales que $a=bq+r$, con $0 \leqslant r < b$. A los números a, b, q y r se les suele llamar, respectivamente, dividendo, divisor, cociente y resto.

Demostración

Existencia de q y r.

Sean a y b dos números enteros cualesquiera con $b>0$. Encontraremos otros dos números enteros q y r que cumplan las condiciones exigidas, es decir, tales que $a=bq+r$ y $0 \leqslant r < b$. En efecto,

$$\left.\begin{array}{l} a = bq+r \\ \text{y} \\ 0 \leqslant r < b \end{array}\right\} \quad \Longrightarrow \quad \left.\begin{array}{l} r = a-bq \\ \text{y} \\ 0 \leqslant r < b \end{array}\right\}$$

$$\begin{aligned} &\Longrightarrow \quad 0 \leqslant a-bq < b \\ &\Longrightarrow \quad bq \leqslant a < b+bq \\ &\Longrightarrow \quad bq \leqslant a < b(q+1) \end{aligned}$$

Por lo tanto, q es un número entero tal que bq es el "mayor múltiplo de b menor o igual que a". Una vez obtenido el cociente q, podemos calcular el resto r sin más que hacer $r=a-bq$.

Unicidad de q y r.

Supongamos que no son únicos, es decir, supongamos que existen r_1, r_2, q_1 y q_2, enteros tales que verifican el teorema, o sea,

$$a = bq_1 + r_1 : 0 \leqslant r_1 < b$$
$$a = bq_2 + r_2 : 0 \leqslant r_2 < b.$$

Entonces,

$$\left.\begin{array}{l} a = bq_1 + r_1 \\ \text{y} \\ a = bq_2 + r_2 \end{array}\right\} \implies b(q_1 - q_2) = r_2 - r_1 \implies b\,|q_1 - q_2| = |r_2 - r_1|$$

por otra parte,

$$\left.\begin{array}{l} 0 \leqslant r_1 < b \\ \text{y} \\ 0 \leqslant r_2 < b \end{array}\right\} \implies \left.\begin{array}{l} -b < -r_1 \leqslant 0 \\ \text{y} \\ 0 \leqslant r_2 < b \end{array}\right\} \implies -b < r_2 - r_1 < b \implies |r_2 - r_1| < b$$

luego,

$$\left.\begin{array}{rcl} b\,|q_1 - q_2| & = & |r_2 - r_1| \\ \text{y} & & \\ |r_2 - r_1| & < & b \end{array}\right\} \implies b\,|q_1 - q_2| < b$$
$$\implies b\,|q_1 - q_2| - b < 0$$
$$\implies b\,(|q_1 - q_2| - 1) < 0$$
$$\overset{b>0}{\implies} |q_1 - q_2| - 1 < 0$$
$$\implies |q_1 - q_2| < 1$$
$$\overset{q_1 - q_2 \in \mathbb{Z}}{\implies} |q_1 - q_2| = 0$$
$$\implies q_1 = q_2$$

Además,

$$\left.\begin{array}{rcl} a & = & bq_1 + r_1 \\ \text{y} & & \\ a & = & bq_2 + r_2 \\ \text{y} & & \\ q_1 & = & q_2 \end{array}\right\} \implies r_1 - r_2 = 0 \implies r_1 = r_2$$

y la unicidad de q y r está comprobada.

■

13.2.2 Corolario

Si a y b son enteros, con $b \neq 0$, entonces existen otros dos números, q y r, enteros y únicos, tales que $a = bq + r$, donde $0 \leqslant r < |b|$.

Demostración

Si $b > 0$, entonces se cumplen las hipótesis del teorema anterior, luego se verifica el corolario.

Si $b < 0$, entonces $-b > 0$ y aplicando el teorema anterior, existirán dos enteros q_1 y r, únicos, tales que

$$a = (-b)q_1 + r, \text{ con } 0 \leqslant r < -b$$

de aquí que

$$a = b(-q_1) + r, \text{ con } 0 \leqslant r < -b = |b|$$

tomando $q = -q_1$, tendremos que

$$a = bq + r, \text{ con } 0 \leqslant r < |b|$$

siendo q y r únicos, ya que q_1 y r lo eran.

■

Ejemplo 13.6

1. *Sean* $a = 9$ *y* $b = 2$.

   El mayor múltiplo de 2 *menor o igual que* 9 *es* $2 \cdot 4$, *luego tomando* $q = 4$ *y* $r = 9 - 2 \cdot 4 = 1$, *tendremos que*

   $$9 = 2 \cdot 4 + 1, \text{ con } 0 \leqslant 1 < 2$$

2. *Sean* $a = 2$ *y* $b = 5$.

   El mayor múltiplo de 5 *menor o igual que* 2 *es* $5 \cdot 0$, *luego si* $q = 0$ *y* $r = 2 - 5 \cdot 0 = 2$, *se sigue que*

   $$2 = 5 \cdot 0 + 2, \text{ con } 0 \leqslant 2 < 5$$

3. *Sean* $a = -17$ *y* $b = 10$.

   El mayor múltiplo de 10 *menor o igual que* -17 *es* $10 \cdot (-2)$, *luego tomando* $q = -2$ *y* $r = -17 - 10 \cdot (-2) = 3$, *tendremos que*

   $$-17 = 10(-2) + 3, \text{ con } 0 \leqslant 3 < 10$$

4. *Sean* $a = -10$ *y* $b = 17$.

   El mayor múltiplo de 17 *menor o igual que* -10 *es* $17(-1)$, *luego si tomamos* $q = -1$ *y* $r = -10 - 17(-1) = 7$, *resulta que*

   $$-10 = 17(-1) + 7, \text{ con } 0 \leqslant 7 < 17$$

5. *Sean* $a = 61$ *y* $b = -7$.

   El mayor múltiplo de -7 *menor o igual que* 61 *es* $(-7)(-8)$, *así pues si tomamos* $q = -8$ *y* $r = 61 - (-7)(-8) = 61 - 56 = 5$, *tendremos que*

   $$61 = (-7)(-8) + 5, \text{ con } 0 \leqslant 5 < |-7| = 7$$

6. *Sean* $a = 7$ *y* $b = -61$.

   El mayor múltiplo de -61 *menor o igual que* 7 *es* $(-61) \cdot 0$, *por tanto tomando* $q = 0$ *y* $r = 7 - (-61) \cdot 0 = 7$, *resulta*

   $$7 = (-61) \cdot 0 + 7, \text{ con } 0 \leqslant 7 < |-61| = 61$$

7. *Sean* $a = -21$ *y* $b = -15$.

   El mayor múltiplo de -15 *menor o igual que* -21 *es* $(-15)(-2)$. *Tomando* $q = -2$ *y* $r = -21 - (-15)(-2) = 9$, *resulta*

   $$-21 = (-15)(-2) + 9, \text{ con } 0 \leqslant 9 < |-15| = 15$$

8. *Sean* $a = -15$ *y* $b = -21$.

   El mayor múltiplo de -21 *menor o igual que* -15 *es* $(-21) \cdot 1$, *así pues, si tomamos* $q = 1$ *y* $r = -15 - (-21) \cdot 1 = 6$, *tendremos*

   $$-15 = (-21) \cdot 1 + 6, \text{ con } 0 \leqslant 6 < |-21| = 21$$

■

Ejemplo 13.7

Demuéstrese que el cuadrado de cualquier número impar puede escribirse en la forma

(a) $4k+1$

(b) $8k+1$

Solución

En efecto, sea a cualquier número entero.

(a) Por el teorema de existencia y unicidad de cociente y resto, pueden encontrarse dos números enteros q y r, únicos, tales que

$$a = 2q + r, \text{ con } 0 \leqslant r < 2$$

es decir, $a = 2q + r$, con $r = 0$ ó $r = 1$. Pues bien,

Si $r = 0$, entonces $a = 2q$, es decir a es par.

Si $r = 1$, entonces $a = 2q + 1$, es decir a es impar, y

$$a^2 = (2q+1)^2 = 4q^2 + 4q + 1 = 4(q^2+q) + 1 = 4k + 1, \text{ con } k = q^2 + q \in \mathbb{Z}$$

(b) En el apartado anterior teníamos que

$$a^2 = 4(q^2+q) + 1, \text{ con } q \in \mathbb{Z}$$

o lo que es igual

$$a^2 = 4q(q+1) + 1, \text{ con } q \in \mathbb{Z}.$$

Pues bien, $q(q+1)$ es par ya que uno de los dos, q o $q+1$ será par, luego $q(q+1)$ puede escribirse en la forma $2k$, con k entero. De aquí que

$$a^2 = 4q(q+1) + 1 = 4 \cdot 2k + 1 = 8k + 1, \text{ con } k \in \mathbb{Z}.$$

■

Ejemplo 13.8

Demuéstrese que si un número entero es a la vez un cuadrado y un cubo, entonces puede escribirse en la forma $7k$ *ó* $7k+1$.

Solución

Sea n cualquier número entero. Entonces, si ha de ser a la vez un cuadrado y un cubo, quiere decir que pueden encontrarse a y b enteros, tales que

$$n = a^2 = b^3$$

Por el teorema 13.2.1, existirán q_1, q_2, r_1 y r_2, únicos, tales que

$$a = 7q_1 + r_1, \text{ con } 0 \leqslant r_1 < 7$$

$$b = 7q_2 + r_2, \text{ con } 0 \leqslant r_2 < 7$$

Pues bien,

$$a = 7q_1 + r_1 \Longrightarrow a^2 = 49q_1^2 + 14q_1r_1 + r_1^2 = 7(7q_1^2 + 2q_1r_1) + r_1^2 = 7k_1 + r_1^2,$$
$$\text{con } k_1 = 7q_1^2 + 2q_1r_1 \in \mathbb{Z}$$

$$b = 7q_2 + r_2 \Longrightarrow b^3 = 7(49q^3 + 21q_2^2r_2 + 21q_2^2r_2 + 3q_2r_2^2) + r_2^3 = 7k_2 + r_2^3, \text{ con } k_2 \in \mathbb{Z}$$

Entonces,

$$a^2 = b^3 \Longrightarrow 7k_1 + r_1^2 = 7k_2 + r_2^3, \text{ con } 0 \leqslant r_1, r_2 < 7$$

y, de nuevo por el teorema 13.2.1, $k_1 = k_2$ y $r_1^2 = r_2^3$. Los diferentes valores que pueden tomar r_1^2 y r_2^3 serán, $0, 1, 4, 9, 16, 25$ y 36 para r_1^2 y $0, 1, 8, 27, 64, 125$ y 216 para r_2^3 y las únicas opciones en las que coinciden es cuando r_1 y r_2 son los dos 0 ó los dos 1. O sea,

$$a^2 = b^3 \Longleftrightarrow a^2 \text{ y } b^3 \text{ son de la forma } 7k \text{ ó } 7k + 1$$

Por tanto,

$$n \text{ es cuadrado y cubo} \Longrightarrow n = 7k \text{ ó } n = 7k + 1$$

■

Ejemplo 13.9

Demostrar que

(a) El cuadrado de cualquier número entero es de la forma $3k$ ó $3k + 1$.

(b) El cubo de cualquier número entero es de la forma $9k$, $9k + 1$ ó $9k + 8$.

Solución

Sea a un entero cualquiera. Entonces, por 13.2.1, existen q y r tales que

$$a = 3q + r, \text{ con } 0 \leqslant r < 3$$

(a) El cuadrado de a es

$$a = 3q + r \Longrightarrow a^2 = (3q + r)^2 = 3(3q^2 + 2qr) + r^2 = 3k_1 + r^2, \text{ con } k_1 = 3q^2 + 2qr$$

Pues bien,

$$\text{Para } r = 0,\ a^2 = 3k, \text{ con } k = k_1$$
$$\text{Para } r = 1,\ a^2 = 3k + 1, \text{ con } k = k_1$$
$$\text{Para } r = 2,\ a^2 = 3k_1 + 4 = 3(k_1 + 1) + 1 = 3k + 1, \text{ con } k = k_1 + 1$$

(b) Veamos ahora como es el cubo de a.

$$\begin{aligned} a = 3q + r &\Longrightarrow a^3 = (3q + r)^3 \\ &\Longrightarrow a^3 = 27q^3 + 27q^2r + 27qr + r^3 \\ &\Longrightarrow a^3 = 9(3q^3 + 3q^2r + 3qr) + r^3 \\ &\Longrightarrow a^3 = 9k + r^3, \text{ con } k = 3q^3 + 3q^2r + 3qr \in \mathbb{Z}. \end{aligned}$$

Entonces,

$$\text{Para } r = 0,\ a^3 = 9k$$
$$\text{Para } r = 1,\ a^3 = 9k + 1$$
$$\text{Para } r = 2,\ a^3 = 9k + 8$$

■

Ejemplo 13.10

Probar que el producto de tres enteros consecutivos es múltiplo de 6.

Solución

Sea a cualquier número entero. El producto de tres enteros consecutivos, siendo a uno de ellos, presenta las siguientes opciones:

$a(a+1)(a+2)$

$(a-1)a(a+1)$

$(a-2)(a-1)a$

Por el teorema de existencia y unicidad de cociente y resto, (13.2.1), existirán q_1 y r, enteros y únicos tales que

$$a = 2q_1 + r,\ 0 \leqslant r < 2$$

y habrá, por tanto, dos opciones:

1 $a = 2q_1$.

En este caso,

$$\begin{aligned} a(a+1)(a+2) &= 2q_1(a+1)(a+2) &&= 2q_2, \text{ siendo } q_2 = q_1(a+1)(a+2) \in \mathbb{Z} \\ (a-1)a(a+1) &= (a-1)2q_1(a+1) &&= 2q_2, \text{ siendo } q_2 = (a-1)q_1(a+1) \in \mathbb{Z} \\ (a-2)(a-1)a &= (a-2)(a-1)2q_1 &&= 2q_2, \text{ siendo } q_2 = (a-2)(a-1)q_1 \in \mathbb{Z} \end{aligned}$$

2 $a = 2q_1 + 1$

En tal caso,

$$\begin{aligned} a(a+1)(a+2) &= (2q_1+1)(2q_1+2)(a+2) \\ &= 2(2q_1+1)(q_1+1)(a+2) \\ &= 2q_2, \text{ siendo } q_2 = (2q_1+1)(q_1+1)(a+2) \in \mathbb{Z} \\ (a-1)a(a+1) &= 2q_1(2q_1+1)(a+1) \\ &= 2q_2, \text{ siendo } q_2 = q_1(2q_1+1)(a+1) \in \mathbb{Z} \\ (a-2)(a-1)a &= (a-2)2q_1(2q_1+1) \\ &= 2q_2, \text{ siendo } q_2 = (a-2)q_1(2q_1+1) \in \mathbb{Z} \end{aligned}$$

Por lo tanto, el producto de tres enteros consecutivos es, siempre, múltiplo de 2.

De nuevo por el teorema de existencia y unicidad de cociente y resto, (13.2.1), existirán q_1 y r, enteros y únicos tales que

$$a = 3q_1 + r,\ 0 \leqslant r < 3$$

y tendremos, por tanto, tres opciones:

1 $a = 3q_1$.

En este caso,

$$\begin{aligned} a(a+1)(a+2) &= 3q_1(a+1)(a+2) = 3q_3, \text{ siendo } q_3 = q_1(a+1)(a+2) \in \mathbb{Z} \\ (a-1)a(a+1) &= (a-1)3q_1(a+1) = 3q_3, \text{ siendo } q_3 = (a-1)q_1(a+1) \in \mathbb{Z} \\ (a-2)(a-1)a &= (a-2)(a-1)3q_1 = 3q_3, \text{ siendo } q_3 = (a-2)(a-1)q_1 \in \mathbb{Z} \end{aligned}$$

2 $a = 3q_1 + 1$.

En este caso, tendremos,

$$\begin{aligned} a(a+1)(a+2) &= (3q_1+1)(a+1)(3q_1+3) \\ &= 3(3q_1+1)(a+1)(q_1+1) \\ &= 3q_3, \text{ siendo } q_3 = (3q_1+1)(a+1)(q_1+1) \in \mathbb{Z} \\ (a-1)a(a+1) &= 3q_1(3q_1+1)(a+1) \\ &= 3q_3, \text{ siendo } q_3 = q_1(3q_1+1)(a+1) \in \mathbb{Z} \\ (a-2)(a-1)a &= (a-2)3q_1(3q_1+1) \\ &= 3q_3, \text{ siendo } q_3 = (a-2)q_1(3q_1+1) \in \mathbb{Z} \end{aligned}$$

3 $a = 3q_1 + 2$.

En tal caso,

$$\begin{aligned} a(a+1)(a+2) &= (3q_1+2)(3q_1+3)(a+2) \\ &= 3(3q_1+2)(q_1+1)(a+2) = 3q_3, \text{ siendo } q_3 = (3q_1+2)(q_1+1)(a+2) \in \mathbb{Z} \\ (a-1)a(a+1) &= (a-1)(3q_1+2)(3q_1+3) \\ &= 3(a-1)(3q_1+2)(q_1+1) \\ &= 3q_3, \text{ siendo } q_3 = (a-1)(3q_1+2)(q_1+1)) \in \mathbb{Z} \\ (a-2)(a-1)a &= 3q_1(a-1)(3q_1+1) \\ &= 3q_3, \text{ siendo } q_3 = q_1(a-1)(3q_1+1) \in \mathbb{Z} \end{aligned}$$

Por lo tanto, y en cualquier caso, el producto de tres enteros consecutivos es, siempre, múltiplo de 3.

Pues bien, teniendo en cuenta que si un número es múltiplo de otros dos, entonces ha de ser múltiplo del mínimo común múltiplo de ambos,

$$\left.\begin{array}{l} a(a+1)(a+2) = 2q_2 \\ \text{y} \\ a(a+1)(a+2) = 3q_3 \end{array}\right\} \implies a(a+1)(a+2) = \text{m.c.m}(2,3)\cdot q \implies a(a+1)(a+2) = 6q,\ q \in \mathbb{Z}$$

$$\left.\begin{array}{l} (a-1)a(a+1) = 2q_2 \\ \text{y} \\ (a-1)a(a+1) = 3q_3 \end{array}\right\} \implies (a-1)a(a+1) = \text{m.c.m}(2,3)\cdot q \implies (a-1)a(a+1) = 6q,\ q \in \mathbb{Z}$$

$$\left.\begin{array}{l} (a-1)(a-2)a = 2q_2 \\ \text{y} \\ (a-1)(a-2)a = 3q_3 \end{array}\right\} \implies (a-1)(a-2)a = \text{m.c.m}(2,3)\cdot q \implies (a-1)(a-2)a = 6q,\ q \in \mathbb{Z}$$

Es decir, el producto de tres enteros consecutivos es múltiplo de 6.

■

Ejemplo 13.11

Probar que si a es un número entero, entonces $\dfrac{a(a+1)(2a+1)}{6}$ también lo es.

Solución

En efecto,

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

y según el ejemplo anterior, existirán q_1 y q_2, enteros tales que

$$\left.\begin{array}{l} (a-1)a(a+1)=6q_1 \\ \text{y} \\ a(a+1)(a+2)=6q_2 \end{array}\right\} \implies (a-1)a(a+1)+a(a+1)(a+2)=6(q_1+q_2)=6q,\ q=q_1+q_2\in\mathbb{Z}$$

Por lo tanto,

$$\frac{a(a+1)(2a+1)}{6}=\frac{(a-1)a(a+1)+a(a+1)(a+2)}{6}=\frac{6q}{6}=q,\ \text{siendo } q\in\mathbb{Z}$$

■

13.3 Sistemas de Numeración

Consideremos, por ejemplo, el entero positivo 7345. Normalmente leemos "siete mil trescientos cuarenta y cinco" y, dado que es lo habitual, entendemos que está escrito en el sistema decimal de numeración o en "base 10".

También sabemos que la última cifra, leyendo el número de derecha a izquierda, es la de las unidades, la siguiente es la cifra de las decenas, la que sigue de las centenas, y así sucesivamente. Observemos lo siguiente:

$$7345 = 5 + 40 + 300 + 7000$$

y si escribimos los números de la derecha como potencias de diez, tendremos

$$7345 = 5\cdot 10^0 + 4\cdot 10^1 + 3\cdot 10^2 + 7\cdot 10^3$$

y esto mismo puede hacerse con cualquier número entero positivo escrito en forma decimal, es decir si tal número es $a_k a_{k-1}\cdots a_2 a_1 a_0$, entonces

$$a_k a_{k-1}\cdots a_2 a_1 a_0 = a_0\cdot 10^0 + a_1\cdot 10^1 + a_2\cdot 10^2 + \cdots + a_{k-1}\cdot 10^{k-1} + a_k\cdot 10^k = \sum_{i=0}^{k} a_i 10^i$$

y esta forma de escribir el número se conoce como "representación polinómica" del mismo tomando como base el número 10.

Normalmente, se dice que a_0 es una unidad de primer orden, a_1 de segundo orden, a_2 de tercero y, en general, diremos que a_k es una unidad de orden $k+1$.

Consideramos ahora el número 35 y lo escribimos en la forma

$$35 = 1 \cdot 2^0 + 1 \cdot 2^1 + 0 \cdot 2^2 + 0 \cdot 2^3 + 0 \cdot 2^4 + 1 \cdot 2^5.$$

En tal caso tendríamos una "representación polinómica" del número 35 tomando como base el número 2.

Nada nos impide utilizar otro número como base para la representación polinómica del número 35. Por ejemplo, si tomamos el 3, tendríamos

$$35 = 2 \cdot 3^0 + 2 \cdot 3^1 + 0 \cdot 3^2 + 1 \cdot 3^3$$

y si tomáramos el 8,

$$35 = 3 \cdot 8^0 + 4 \cdot 8^1$$

El siguiente teorema matiza y aclara estas ideas.

13.3.1 Descomposición Polinómica de un Número

Dados dos números enteros positivos n y b (con $b \geqslant 2$) pueden encontrarse $k+1$ enteros no negativos, a_k, únicos, tales que

$$n = \sum_{i=0}^{k} a_i b^i$$

con $i \geqslant 0,\ 0 \leqslant a_i < b;\ i = 0, 1, \ldots, k$, siendo $a_k \neq 0$.

Demostración

En efecto, dados n y b, por 13.2.1, existirán q_1 y a_0, únicos, tales que

$$n = bq_1 + a_0,\ \text{con } 0 \leqslant a_0 < b \text{ y } q_1 < n.$$

Obtenido q_1 y aplicando de nuevo el *algoritmo de la división*, pueden encontrarse q_2 y a_1, únicos, tales que

$$q_1 = bq_2 + a_1 \text{ con } 0 \leqslant a_1 < b,\ \text{y } q_2 < q_1.$$

Reiterando el proceso,

$$q_2 = bq_3 + a_2 \text{ con } 0 \leqslant a_2 < b,\ \text{y } q_3 < q_2$$
$$q_3 = bq_4 + a_3 \text{ con } 0 \leqslant a_3 < b,\ \text{y } q_4 < q_3$$

y así sucesivamente.

Tendremos una sucesión de enteros positivos,

$$n, q_1, q_2, q_3, q_4, \ldots$$

tal que

$$n > q_1 > q_2 > q_3 > q_4 > \cdots$$

y que por el *principio del buen orden*, tiene un primer elemento q_k tal que

$$q_k = b \cdot 0 + a_k,\ \text{con } 0 \leqslant a_k < b$$

y a_k ha de ser distinto de cero ya que de lo contrario q_k sería cero, lo cual es imposible ya que es un entero positivo.

Pues bien, sustituyendo el valor de q_1 en n,

$$\left.\begin{array}{l} n = q_1 b + a_0 \\ q_1 = q_2 b + a_1 \end{array}\right\} \Longrightarrow n = (q_2 b + a_1)\, b + a_0 = q_2 b^2 + a_1 b + a_0$$

y sustituyendo en este resultado el valor de q_2,

$$\left.\begin{array}{l} n = q_2 b^2 + a_1 b + a_0 \\ q_2 = q_3 b + a_2 \end{array}\right\} \Longrightarrow n = (q_3 b + a_2)\, b^2 + a_1 b + a_0 = q_3 b^3 + a_2 b^2 + a_1 b + a_0.$$

Repitiendo el proceso para q_3,

$$\left.\begin{array}{l} n = q_3 b^3 + a_2 b^2 + a_1 b + a_0 \\ q_3 = q_4 b + a_3 \end{array}\right\} \begin{array}{rl} \Longrightarrow & n = (q_4 b + a_3)\, b^3 + a_2 b^2 + a_1 b + a_0 \\ \Longrightarrow & n = q_4 b^4 + a_3 b^3 + a_2 b^2 + a_1 b + a_0. \end{array}$$

Y siguiendo hasta q_k,

$$\left.\begin{array}{l} n = q_k b + \cdots + a_2 b^2 + a_1 b + a_0 \\ q_k = a_k \end{array}\right\} \Longrightarrow n = a_k b^k + \cdots + a_2 b^2 + a_1 b + a_0$$

donde por 13.2.1, los coeficientes a_k son únicos, $0 \leqslant a_i < b,\ i = 0, 1, \ldots, k$ y, como ya hemos visto, $a_k \neq 0$.

La expresión obtenida es la *descomposición polinómica* de n en la base b y se escribe $a_0 a_1 a_2 \cdots a_{k_{(b}}$.

■

Ejemplo 13.12

Escribir en forma decimal el número $1243_{(5}$.

Solución

Bastaría escribir la representación polinómica del número.

$$1243_{(5} = 3 + 4 \cdot 5 + 2 \cdot 5^2 + 1 \cdot 5^3 = 3 + 20 + 50 + 125 = 198$$

■

En el ejemplo siguiente veremos como puede utilizarse el teorema 13.2.1 para hacer lo contrario, es decir escribir la representación de números enteros en bases distintas de la decimal.

Ejemplo 13.13

Escribir el número 5346 *en base* 7.

Solución

El número dado en base 7 será:

$$5346 = a_k a_{k-1} a_{k-2} \cdots a_2 a_1 a_{0_{(7}}$$

y utilizando la representación polinómica del número,

$$\begin{aligned} 5346 &= a_k \cdot 7^k + a_{k-1} \cdot 7^{k-1} + a_{k-2} \cdot 7^{k-2} + \cdots + a_2 \cdot 7^2 + a_1 \cdot 7 + a_0 \\ &= 7\left(a_k \cdot 7^{k-1} + a_{k-1} \cdot 7^{k-2} + a_{k-2} \cdot 7^{k-3} + \cdots + a_2 \cdot 7 + a_1\right) + a_0. \end{aligned} \tag{13.1}$$

Por otra parte, por el 13.2.1,

$$5346 = 7 \cdot 763 + 5 \tag{13.2}$$

y por la unicidad del cociente y resto, de (13.1) y (13.2), se sigue que

$$\begin{aligned} a_0 &= 5 \\ \text{y} & \\ 763 &= a_k \cdot 7^{k-1} + a_{k-1} \cdot 7^{k-2} + a_{k-2} \cdot 7^{k-3} + \cdots + a_2 \cdot 7 + a_1. \end{aligned}$$

Entonces,

$$\begin{aligned} 763 &= a_k \cdot 7^{k-1} + a_{k-1} \cdot 7^{k-2} + \cdots + a_3 \cdot 7^2 + a_2 \cdot 7 + a_1 \\ &= 7\left(a_k \cdot 7^{k-2} + a_{k-1} \cdot 7^{k-3} + \cdots + a_3 \cdot 7 + a_2\right) + a_1. \end{aligned} \tag{13.3}$$

y por 13.2.1,

$$763 = 7 \cdot 109 + 0 \tag{13.4}$$

y, de nuevo, por la unicidad del cociente y el resto, de (13.3) y (13.3), tendremos que

$$\begin{aligned} a_1 &= 0 \\ \text{y} & \\ 109 &= a_k \cdot 7^{k-2} + a_{k-1} \cdot 7^{k-3} + \cdots + a_4 \cdot 7^2 + a_3 \cdot 7 + a_2. \end{aligned}$$

Repitiendo el proceso,

$$\begin{aligned} 109 &= 7\left(a_k \cdot 7^{k-3} + a_{k-1} \cdot 7^{k-4} + \cdots + a_4 \cdot 7 + a_3\right) + a_2 \\ \text{y} & \\ 109 &= 7 \cdot 15 + 4 \end{aligned}$$

luego,

$$\begin{aligned} a_2 &= 4 \\ \text{y} & \\ 15 &= a_k \cdot 7^{k-3} + a_{k-1} \cdot 7^{k-4} + \cdots + a_5 \cdot 7^2 + a_4 \cdot 7 + a_3. \end{aligned}$$

Repetimos de nuevo, y

$$\begin{aligned} 15 &= 7\left(a_k \cdot 7^{k-4} + a_{k-1} \cdot 7^{k-5} + \cdots + a_5 \cdot 7 + a_4\right) + a_3 \\ \text{y} & \\ 15 &= 7 \cdot 2 + 1 \end{aligned}$$

luego,

$$\begin{aligned} a_3 &= 1 \\ \text{y} & \\ 2 &= a_k \cdot 7^{k-4} + a_{k-1} \cdot 7^{k-5} + \cdots + a_6 \cdot 7^2 + a_5 \cdot 7 + a_4. \end{aligned}$$

Por última vez,

$$\begin{aligned} 2 &= 7\left(a_k \cdot 7^{k-5} + a_{k-1} \cdot 7^{k-6} + \cdots + a_6 \cdot 7 + a_5\right) + a_4 \\ \text{y} & \\ 2 &= 7 \cdot 0 + 2 \end{aligned}$$

luego,

$$\begin{aligned} a_4 &= 2 \\ \text{y} & \\ 0 &= a_k \cdot 7^{k-5} + a_{k-1} \cdot 7^{k-6} + \cdots + a_6 \cdot 7 + a_5. \end{aligned}$$

A partir de aquí todos los restos son cero, el proceso termina, y

$$5346 = 2 \cdot 7^4 + 1 \cdot 7^3 + 4 \cdot 7^2 + 0 \cdot 7 + 5 = 21405_{(7}.$$

En la práctica, este proceso de divisiones sucesivas suele hacerse en la forma

5346	7			
44	763	7		
26	06	109	7	
5	63	39	15	7
	0	4	1	2

y

$$5346 = 21405_{(7}$$

■

Nota 13.3 El sistema de numeración en base 2 o sistema binario es de vital importancia en la informática. Los únicos dígitos que pueden utilizarse son los *bits* 0 y 1.

Con los dígitos 0 y 1, el número de números de cuatro cifras que pueden construirse es

$$VR_{2,4} = 2^4 = 16$$

luego utilizando cuatro posiciones, con los *bits* 0 y 1 podemos representar 16 números enteros. La representación binaria de los dieciséis primeros números enteros es

0	0000
1	0001
2	0010
3	0011
4	0100
5	0101
6	0110
7	0111
8	1000
9	1001
10	1010
11	1011
12	1100
13	1101
14	1110
15	1111

Los ordenadores utilizan, normalmente, grupos de ocho dígitos (*octetos* o *bytes*) para almacenar información. Obsérvese que el número de octetos que pueden construirse con los dígitos 0 y 1 es

$$VR_{2,8} = 2^8 = 256$$

lo cual equivale a decir que puede almacenarse cualquier número entero entre 0 y 255 en formato binario.

Otro sistema de numeración muy utilizado en la informática es el de base 16 o hexadecimal. Además de los dígitos del 0 al 9, usaremos $A,\ B,\ C,\ D,\ E$ y F para los números 10, 11, 12, 13, 14 y 15, respectivamente.

En la primera y tercera columna de la tabla siguiente recogemos la expresión binaria y hexadecimal de los enteros entre el 0 y el 15.

Binario	Decimal	Hexadecimal
0000	0	0
0001	1	1
0010	2	2
0011	3	3
0100	4	4
0101	5	5
0110	6	6
0111	7	7
1000	8	8
1001	9	9
1010	10	A
1011	11	B
1100	12	C
1110	13	D
1110	14	E
1111	15	F

■

13.3.2 Representación Hexadecimal de un Octeto

Para escribir un octeto (número de ocho bits en binario) en forma hexadecimal, podemos escribirlo en base diez y, posteriormente, hallar su representación hexadecimal. Veremos un método para obtenerla directamente.

Según hemos visto, con los dígitos 0 y 1, podemos escribir un total de 256 octetos. La primera cuestión es saber cuantos dígitos hexadecimales tiene un octeto. En efecto, si x es dicho número, y a cada octeto le corresponde un número en hexadecimal y, dado que pueden escribirse un total de $VR_{16,x}$ números hexadecimales con x dígitos, tendremos que

$$VR_{16,x} = VR_{2,8}$$

de aquí que

$$16^x = 2^8 \Longrightarrow 2^{4x} = 2^8 \Longrightarrow 4x = 8 \Longrightarrow x = 2$$

luego a cada octeto le corresponde un número hexadecimal de dos cifras.

Pues bien, sea N un número cualquiera y sean

$$\begin{aligned} N &= a_7a_6a_5a_4a_3a_2a_1a_{0_{(2}} \\ \text{y} & \\ N &= b_1b_{0_{(16}} \end{aligned}$$

sus representaciones respectivas en binario (con ocho bits) y en hexadecimal. Entonces,

$$\begin{aligned} N &= a_0 + a_1 \cdot 2 + a_2 \cdot 2^2 + a_3 \cdot 2^3 + a_4 \cdot 2^4 + a_5 \cdot 2^5 + a_6 \cdot 2^6 + a_7 \cdot 2^7 \\ \text{y} & \\ N &= b_0 + b_1 \cdot 16 \end{aligned}$$

es decir,

$$\begin{aligned} N &= a_0 + a_1 \cdot 2 + a_2 \cdot 2^2 + a_3 \cdot 2^3 + 16(a_4 + a_5 \cdot 2 + a_6 \cdot 2^2 + a_7 \cdot 2^3) \\ \text{y} & \\ N &= b_0 + b_1 \cdot 16 \end{aligned}$$

y como el cociente y el resto de dividir N entre 16 son únicos, (13.2.1),

$$\begin{aligned} b_0 &= a_0 + a_1 \cdot 2 + a_2 \cdot 2^2 + a_3 \cdot 2^3 \\ \text{y} & \\ b_1 &= a_4 + a_5 \cdot 2 + a_6 \cdot 2^2 + a_7 \cdot 2^3 \end{aligned}$$

es decir,

$$\begin{aligned} b_{0_{(16}} &= a_3a_2a_1a_{0_{(2}} \\ \text{y} & \\ b_{1(16} &= a_7a_6a_5a_{4_{(2}} \end{aligned}$$

Así pues, para convertir un entero binario de ocho bits a base 16, basta descomponerlo en dos bloques de cuatro bits y representar cada uno de ellos en hexadecimal.

■

Ejemplo 13.14

Obtener la representación hexadecimal del número 01111100.

Solución

Descomponemos el número en dos de cuatro bits y, según la tabla anterior,

0111	1100
7	C

luego

$$01111100_{(2} = 7C_{(16}$$

■

13.3.3 Representación Binaria de un hexadecimal

Veamos ahora como puede escribirse directamente en binario un número hexadecimal de cuatro dígitos.

El número de representaciones hexadecimales con cuatro dígitos será $VR_{16,4}$. Si, al igual que en el apartado anterior, a cada uno de ellos le hacemos corresponder su representación en binario y x es el número de bits que tiene dicha representación, tendremos que

$$VR_{2,x} = VR_{16,4}$$

de aquí que

$$2^x = 16^4 \Longrightarrow 2^x = 2^{16} \Longrightarrow x = 16$$

es decir cada número de cuatro dígitos hexadecimales puede representarse por 16 dígitos binarios (dos octetos).

Pues bien, sea N un entero arbitrario y sean

$$\begin{aligned} N &= a_3a_2a_1a_{0_{(16}} \\ \text{y} & \\ N &= b_{15}b_{14}b_{13}b_{12}b_{11}b_{10}b_9b_8b_7b_6b_5b_4b_3b_2b_1b_{0_{(2}} \end{aligned}$$

sus representaciones en hexadecimal con 4 dígitos y en binario con 16 bits, respectivamente. Entonces,

$$\begin{aligned} N &= a_0 + a_1 \cdot 16 + a_2 \cdot 16^2 + a_3 \cdot 16^3 \\ \text{y} & \\ N &= b_0 + b_1 \cdot 2 + b_2 \cdot 2^2 + b_3 \cdot 2^3 + b_4 \cdot 2^4 + b_5 \cdot 2^5 + b_6 \cdot 2^6 + b_7 \cdot 2^7 + b_8 \cdot 2^8 + b_9 \cdot 2^9 + \\ & \quad b_{10} \cdot 2^{10} + b_{11} \cdot 2^{11} + b_{12} \cdot 2^{12} + b_{13} \cdot 2^{13} + b_{14} \cdot 2^{14} + b_{15} \cdot 2^{15} \end{aligned}$$

o sea,

$$\begin{aligned} N &= a_0 + a_1 \cdot 16 + a_2 \cdot 16^2 + a_3 \cdot 16^3 \\ \text{y} & \\ N &= b_0 + b_1 \cdot 2 + b_2 \cdot 2^2 + b_3 \cdot 2^3 \\ &+ 16\left(b_4 + b_5 \cdot 2 + b_6 \cdot 2^2 + b_7 \cdot 2^3\right) \\ &+ 16^2\left(b_8 + b_9 \cdot 2 + b_{10} \cdot 2^2 + b_{11} \cdot 2^3\right) \\ &+ 16^3\left(b_{12} + b_{13} \cdot 2 + b_{14} \cdot 2^2 + b_{15} \cdot 2^3\right) \end{aligned}$$

y como la descomposición polinómica de un número en una base dada es única,

$$\begin{aligned} a_0 &= b_0 + b_1 \cdot 2 + b_2 \cdot 2^2 + b_3 \cdot 2^3 \\ a_1 &= b_4 + b_5 \cdot 2 + b_6 \cdot 2^2 + b_7 \cdot 2^3 \\ a_2 &= b_8 + b_9 \cdot 2 + b_{10} \cdot 2^2 + b_{11} \cdot 2^3 \\ a_3 &= b_{12} + b_{13} \cdot 2 + b_{14} \cdot 2^2 + b_{15} \cdot 2^3 \end{aligned}$$

es decir,

$$\begin{aligned} a_{0_{(16}} &= b_3b_1b_2b_{0_{(2}} \\ a_{1_{(16}} &= b_7b_6b_5b_{4_{(2}} \\ a_{2_{(16}} &= b_{11}b_{10}b_9b_{8_{(2}} \\ a_{3_{(16}} &= b_{15}b_{14}b_{13}b_{12_{(2}} \end{aligned}$$

Así pues, para convertir un número hexadecimal de cuatro dígitos a binario, basta obtener la representación binaria con cuatro dígitos de cada uno de los símbolos hexadecimales.

■

Ejemplo 13.15

Obtener la representación binaria del número hexadecimal A8B3.

Solución

Según la tabla,

A	8	B	3
1010	1000	1011	0011

luego,

$$A8B3_{(16} = 1010100010110011_{(2}$$

■

13.4 Criterios de Divisibilidad

Ejemplo 13.16

Demostrar que un número entero positivo es divisible por 2 si, y sólo si lo es su última cifra.

Solución

Sea $n \in \mathbb{Z}^+$, cualquiera y sea

$$n = a_k 10^k + a_{k-1}10^{k-1} + \cdots + a_2 10^2 + a_1 10 + a_0 = \sum_{i=0}^{k} a_i 10^i$$

su representación decimal. Entonces,

$$\begin{aligned} 2\,|10 &\implies 2\,|10^i\ ;\ i = 1, 2, \ldots, k \\ &\implies 2\,|a_i 10^i\ ;\ i = 1, 2, \ldots, k \\ &\implies 2\left|\sum_{i=1}^{k} a_i 10^i\right. \\ &\implies 2\,|n - a_0\ . \end{aligned}$$

"Sólo si". En efecto, supongamos que n es divisible por 2. Entonces,

$$\left.\begin{array}{l} 2\,|n \\ 2\,|n - a_0 \end{array}\right\} \Longrightarrow 2\,|n - (n - a_0) \Longrightarrow 2\,|a_0$$

"Si". En efecto, supongamos ahora que la última cifra de n es divisible por 2, es decir $2\,|a_0$. Entonces

$$\left.\begin{array}{l} 2\,|a_0 \\ 2\,|n - a_0 \end{array}\right\} \Longrightarrow 2\,|a_0 + n - a_0 \Longrightarrow 2\,|n$$

Así pues,

un número entero positivo es divisible por 2 si, y sólo si su última cifra es 2 o múltiplo de 2.

■

13.4.1 Criterio General de Divisibilidad

Sea n un entero positivo, sea $\sum_{i=1}^{k} a_i 10^i$ su representación decimal, y sean r_i los restos de la división de 10^i por $p \geqslant 2,\ i = 1, 2, \ldots, k$.Entonces,

$$n \text{ es divisible por } p \text{ si, y sólo si lo es } \sum_{i=1}^{k} a_i r_i.$$

Demostración

Sea $p \geqslant 2$. Por el teorema 13.2.1, existirán q_i y $r_i,\ i = 1, 2, \ldots, k$ tales que

$$\begin{aligned} 10^0 &= q_0 p + r_0 \\ 10 &= q_1 p + r_1 \\ 10^2 &= q_2 p + r_2 \\ \ldots &\quad \ldots\ldots\ldots \\ 10^k &= q_k p + r_k \end{aligned}$$

es decir, $10^i = q_i p + r_i,\ i = 0, 1, \ldots, k$ donde $q_0 = 0$ y $r_0 = 1$. Entonces,

$$10^i - r_i = q_i p$$

luego,

$$p \,|10^i - r_i\ ,\ i = 0, 1, 2, \ldots, k$$

de aquí que

$$p \,|a_i \left(10^i - r_i\right)\ ,\ i = 0, 1, 2, \ldots, k$$

y, por lo tanto,

$$p \left| \sum_{i=0}^{k} a_i \left(10^i - r_i\right) \right.$$

luego,

$$p \left| \left(\sum_{i=0}^{k} a_i 10^i - \sum_{i=0}^{k} a_i r_i \right) \right.$$

es decir,

$$p \left| \left(n - \sum_{i=0}^{k} a_i r_i \right) \right.$$

"Sólo si". En efecto, si $p \,|n$, entonces,

$$\left.\begin{array}{l} p \,|n \\ \text{y} \\ p \left| \left(n - \sum_{i=0}^{k} a_i r_i \right) \right. \end{array}\right\} \Longrightarrow p \left| n - \left(n - \sum_{i=0}^{k} a_i r_i \right) \right. \Longrightarrow p \left| \sum_{i=0}^{k} a_i r_i \right.$$

"Si". En efecto, si $p \left| \sum_{i=0}^{k} a_i r_i \right.$, entonces,

$$\left.\begin{array}{l} p \left| \sum_{i=0}^{k} a_i r_i \right. \\ \text{y} \\ p \left| \left(n - \sum_{i=0}^{k} a_i r_i \right) \right. \end{array}\right\} \Longrightarrow p \left| \left(\sum_{i=0}^{k} a_i r_i + n - \sum_{i=0}^{k} a_i r_i \right) \right. \Longrightarrow p \,|n$$

■

Veamos de nuevo el ejemplo 13.16 .

Ejemplo 13.17

Demostrar que un número entero positivo es divisible por 2 si, y sólo si lo es su última cifra.

Solución

Sea $n \in \mathbb{Z}^+$, cualquiera, sea

$$n = a_k 10^k + a_{k-1} 10^{k-1} + \cdots + a_2 10^2 + a_1 10 + a_0 = \sum_{i=0}^{k} a_i 10^i$$

su representación decimal y sean r_i los restos de dividir 10^i entre 2 para $i = 0, 1, 2, \ldots, k$. Entonces,

$$\begin{array}{l} r_0 = 1 \\ \text{y} \\ r_i = 0, \;\; i = 1, 2, \ldots, k \end{array}$$

de aquí que

$$\sum_{i=1}^{k} a_i r^i = a_0$$

luego por el criterio anterior,

"n sea divisible por 2 si, y sólo si lo es su última cifra"

■

Ejemplo 13.18

Obtener una condición necesaria y suficiente para que un número entero positivo sea divisible por 3.

Solución

Sea $n \in \mathbb{Z}^+$, cualquiera, sea

$$n = a_k 10^k + a_{k-1}10^{k-1} + \cdots + a_2 10^2 + a_1 10 + a_0 = \sum_{i=0}^{k} a_i 10^i$$

su representación decimal y sean r_i los restos de dividir 10^i entre 3 para $i = 0, 1, 2, \ldots, k$. Por 13.2.1, existirá un entero positivo q tal que

$$10 = 3q + 1$$

luego,

$$10^i = (3q+1)^i$$

y desarrollando por el *teorema del binomio*,

$$\begin{aligned}
10^i &= (3q+1)^i \\
&= \sum_{k=0}^{i} \binom{i}{k} (3q)^k \\
&= 1 + \sum_{k=1}^{i} \binom{i}{k} 3^k q^k \\
&= 1 + 3\left[\sum_{k=1}^{i} \binom{i}{k} 3^{k-1} q^k\right] \\
&\quad \left\{\text{Tomando } q_i = \sum_{k=1}^{i} \binom{i}{k} 3^{k-1} q^k\right\} \\
&= 3q_i + 1,\ q_i \in \mathbb{Z}
\end{aligned}$$

es decir, los restos, r_i, de dividir 10^i entre 3 para $i = 0, 1, 2, \ldots, k$ son siempre iguales a 1, luego

$$\sum_{i=1}^{k} a_i r_i = \sum_{i=1}^{k} a_i$$

de aquí que por el *criterio general de divisibilidad*, (13.4.1), n es divisible por 3 si, y sólo si lo es la suma de sus cifras, o lo que es igual

> *"Una condición necesaria y suficiente para que un entero positivo sea divisible por* 3 *es que la suma de sus cifras sea múltiplo de* 3*".*

■

Ejemplo 13.19

Obtener un criterio de divisibilidad por 4.

Solución

Sea $n \in \mathbb{Z}^+$, cualquiera, sea

$$n = a_k 10^k + a_{k-1}10^{k-1} + \cdots + a_2 10^2 + a_1 10 + a_0 = \sum_{i=0}^{k} a_i 10^i$$

su representación decimal y sean r_i los restos de dividir 10^i entre 4 para $i = 0, 1, 2, \ldots, k$. Entonces, $r_0 = 1$ y $r_1 = 2$, y si tenemos en cuenta que

$$4 \,|100 \text{ , es decir, } 4 \,|10^2$$

tendremos que

$$4 \,|10^{i-2} \cdot 10^2 \text{ , } i = 2, 3, \ldots, k$$

es decir,

$$4 \,|10^i \text{ , } i = 2, 3, \ldots, k$$

luego,

$$r_i = 0, \ i = 2, 3, \ldots, k$$

de aquí que

$$\sum_{i=0}^{k} a_i r_i = a_0 + 2a_1$$

es decir,

> *"n es divisible por* 4 *si, y sólo si lo es la suma de la cifra de las unidades más dos veces la cifra de las decenas".*

■

Ejemplo 13.20

Obtener un criterio de divisibilidad por 5.

Solución

Sea $n \in \mathbb{Z}^+$, cualquiera, sea

$$n = a_k 10^k + a_{k-1}10^{k-1} + \cdots + a_2 10^2 + a_1 10 + a_0 = \sum_{i=0}^{k} a_i 10^i$$

su representación decimal y sean r_i los restos de dividir 10^i entre 5 para $i = 0, 1, 2, \ldots, k$. Entonces,

$$r_0 = 1$$

y

$$r_i = 0, \ i = 1, 2, \ldots, k$$

de aquí que

$$\sum_{i=1}^{k} a_i r^i = a_0$$

luego por el criterio general de divisibilidad,

"n sea divisible por 5 *si, y sólo si lo es su última cifra"*

■

Ejemplo 13.21

Obtener un criterio de divisibilidad por 8.

Solución

Sea $n \in \mathbb{Z}^+$, cualquiera, y sea

$$n = a_k 10^k + a_{k-1}10^{k-1} + \cdots + a_2 10^2 + a_1 10 + a_0 = \sum_{i=0}^{k} a_i 10^i$$

su representación polinómica en base decimal.

Si r_i son los restos de dividir 10^i entre 8 para $i = 0, 1, 2 \ldots, k$, entonces $r_0 = 1$, $r_1 = 2$ y $r_2 = 4$ y teniendo en cuenta que

$$8|1000, \text{ es decir, } 8 \left| 10^3 \right.$$

tendremos que

$$8 \left| 10^{i-3}10^3 \right. , \ i = 3, 4, \ldots, k$$

o sea,

$$8 \left| 10^i \right. , \ i = 3, 4, \ldots, k$$

de aquí que

$$r_i = 0, \ i = 3, 4, \ldots, k$$

y, consecuentemente,

$$\sum_{i=0}^{k} a_i r_i = a_0 + 2a_1 + 4a_2.$$

Aplicando el criterio general de divisibilidad,

> *"n es divisible por* 8 *si, y sólo lo es la suma de las cifras de sus unidades más dos veces la cifra de sus decenas más cuatro veces la cifra de sus centenas"*

■

13.5 Máximo Común Divisor

Siguiendo con la operación de división que desarrollamos anteriormente, centraremos ahora nuestra atención en los divisores comunes de un número finito de números enteros.

13.5.1 Definición

Dados los números enteros positivos a_1, a_2, a_3, ..., a_n, *llamaremos máximo común divisor de todos ellos al ínfimo del conjunto* $\{a_1, a_2, a_3, \ldots, a_n\}$ *ordenado con la relación de orden parcial de divisibilidad. Lo notaremos* $m.c.d.(a_1, a_2, a_3, \ldots, a_n)$

Ejemplo 13.22

Calcular, aplicando directamente la definición anterior,

$$m.c.d.\,(72, 108, 144, 216, 324, 288, 432, 648, 972, 864, 1296, 1944, 2592, 3888)$$

Solución

Según la definición de máximo común divisor de varios números, tendremos que calcular el Ínfimo del conjunto

$$A = \{72, 108, 144, 216, 324, 288, 432, 648, 972, 864, 1296, 1944, 2592, 3888\}$$

ordenado con la relación de orden de divisibilidad, es decir, si a y b son cualesquiera de A,

$$a \text{ es anterior a } b \text{ siempre y cuando } a \text{ divida a } b$$

o sea,

$$a \preccurlyeq b \Longleftrightarrow a|b$$

Recordemos que el ínfimo de A es el máximo del conjunto de sus cotas inferiores ordenado por la relación anterior. Vamos a calcular, pues, los elementos característicos de este conjunto.

Elementos Minimales. Por definición, un elemento m de A será minimal de A, respecto de la relación $\preccurlyeq$, si no hay en A elemento alguno que sea estrictamente anterior a él, es decir,

$$m \text{ es minimal de } A \iff \nexists x \in A : x \prec m$$

o lo que es igual,

$$m \text{ es minimal de } A \iff \nexists x \in A : x \preccurlyeq m \text{ y } x \neq m$$

y esto significa, teniendo en cuenta que la relación $\preccurlyeq$ es la de divisibilidad,

$$m \text{ es minimal de } A \iff \nexists x \in A : x \text{ divida a } m \text{ y } x \neq m$$

es decir,

$$m \text{ es minimal de } A \iff m \text{ no tiene en } A \text{ divisores distintos del propio } m.$$

Consecuentemente,

$$m \text{ es minimal de } A \iff m = 72 \text{ ó } m = 108$$

Obsérvese que al haber dos minimales no puede haber mínimo, ya que éste, caso de existir, ha de ser único y coincidir con el minimal.

Cotas Inferiores. Un elemento $i \in \mathbb{Z}^+$ es cota inferior de A, subconjunto de $\mathbb{Z}^+$, si es anterior a todos los elementos de A, o sea,

$$i \in \mathbb{Z}^+ \text{ es cota inferior de } A \subseteq \mathbb{Z}^+ \Longleftrightarrow \forall x\,(x \in A \Longrightarrow i \preccurlyeq x)$$

es decir,

$$i \in \mathbb{Z}^+ \text{ es cota inferior de } A \subseteq \mathbb{Z}^+ \Longleftrightarrow \forall x\,(x \in A \Longrightarrow i \text{ divide a } x)$$

Así pues,

$$i \in \mathbb{Z}^+ \text{ es cota inferior de } A \subseteq \mathbb{Z}^+ \iff i \text{ divide a todos los elementos de } A$$

y bastaría con que i dividiese a los minimales de A ya que por transitividad esto significaría que divide a todos los elementos de A. Por lo tanto,

$$i \in \mathbb{Z}^+ \text{ es cota inferior de } A \subseteq \mathbb{Z}^+ \iff i \text{ divide a los elementos minimales de } A.$$

Así pues,

$$\begin{aligned} i \in \mathbb{Z}^+ \text{ es cota inferior de } A \subseteq \mathbb{Z}^+ &\iff i \text{ divide a 72 y 108} \\ &\iff \begin{cases} i \text{ es divisor de 72} \\ \text{e} \\ i \text{ es divisor de 108} \end{cases} \\ &\iff \begin{cases} i \in \{1,2,4,8,3,6,12,24,9,18,36,72\} \\ \text{e} \\ i \in \{1,2,4,3,6,12,9,18,36,27,54,108\} \end{cases} \\ &\iff i \in \{1,2,4,3,6,12,9,18,36\} \end{aligned}$$

luego, si llamamos C_i al conjunto de las cotas inferiores, tendremos que

$$C_i = \{1,2,3,4,6,9,12,18,36\}$$

Ínfimo. Un elemento d de $\mathbb{Z}^+$ se dice que es el ínfimo de A, subconjunto de $\mathbb{Z}^+$, si es el máximo del conjunto de las cotas inferiores. Entonces,

$$d \in \mathbb{Z}^+ \text{ es el ínfimo de } A \subseteq \mathbb{Z}^+ \iff d \text{ es el máximo de } C_i$$

luego,

$$d \in \mathbb{Z}^+ \text{ es el ínfimo de } A \subseteq \mathbb{Z}^+ \iff d \text{ es posterior a todos los elementos de } C_i$$

o lo que es igual,

$$d \in \mathbb{Z}^+ \text{ es el ínfimo de } A \subseteq \mathbb{Z}^+ \iff d \text{ es múltiplo todos los elementos de } C_i.$$

Consecuentemente,

$$d \in \mathbb{Z}^+ \text{ es el ínfimo de } A \subseteq \mathbb{Z}^+ \iff d = 36.$$

Así pues, y según la definición de máximo común divisor,

$$\text{m.c.d.}\,(72,108,144,216,324,288,432,648,972,864,1296,1944,2592,3888) = 36$$

■

13.5.2 Proposición

Dados los números enteros a_1, a_2, a_3, …, a_n, se verifica:

$$m.c.d.\,(a_1,a_2,a_3,\ldots,a_n) = m.c.d.\,(a_1, m.c.d.\,(a_2,a_3,\ldots,a_n))$$

Demostración

Sea $d = \text{m.c.d.}\,(a_1,a_2,a_3,\ldots,a_n)$ y $d' = \text{m.c.d.}\,(a_1, \text{m.c.d.}\,(a_2,a_3,\ldots,a_n))$. Entonces, por definición

$$d = \text{m.c.d.}\,(a_1,a_2,a_3,\ldots,a_n) \implies d = \text{Ínf}\,\{a_1,a_2,a_3,\ldots,a_n\}$$

por lo tanto d será anterior (divisor) a todos los números, es decir,

$$d\,|a_1 \text{ y } d\,|a_2 \text{ y } d\,|a_3 \text{ y } \cdots \text{ y } d\,|a_n\,.$$

Pero si d es anterior (divisor) a varios números, entonces, por definición de ínfimo, será anterior (divisor) al ínfimo de todos ellos, es decir,

$$d\,|a_1 \ \text{ y } d\,\big|\text{Ínf}\,\{a_2, a_3, \ldots, a_n\}\ .$$

Nuevamente, por la definición de máximo común divisor,

$$d\,|a_1 \ \text{ y } d\,|\text{m.c.d.}\,(a_2, a_3, \ldots, a_n)$$

y, otra vez, por definición de ínfimo,

$$d\,\big|\text{Ínf}\,\{a_1, \text{m.c.d.}\,(a_2, a_3, \ldots, a_n)\}$$

y, finalizando, con la de máximo común divisor,

$$d\,|\text{m.c.d.}\,(a_1, \text{m.c.d.}\,(a_2, a_3, \ldots, a_n))$$

es decir,

$$d\,|d'$$

Por otra parte, por definición,

$$d' = \text{m.c.d.}\,(a_1, \text{m.c.d.}\,(a_2, a_3, \ldots, a_n)) \Longrightarrow d' = \text{Ínf}\,\{a_1, \text{m.c.d.}\,(a_2, a_3, \ldots, a_n)\}$$

y por ser d' el ínfimo de dos números, deberá ser anterior (divisor) a ambos, o sea,

$$d'\,|a_1 \ \text{ y } d'\,|\text{m.c.d.}\,(a_2, a_3, \ldots, a_n)$$

luego, por definición,

$$d'\,|a_1 \ \text{ y } d'\,\big|\text{Ínf}\,\{a_2, a_3, \ldots, a_n\}$$

y al ser d' anterior (divisor) al ínfimo de $a_2, a_3, \ldots, a_n$, tendrá que ser anterior (divisor) a todos ellos, es decir,

$$d'\,|a_1 \ \text{ y } d'\,|a_2 \ \text{ y } d'\,|a_3 \ \text{ y } \cdots \text{ y } d'\,|a_n$$

por tanto, d' ha de ser anterior (divisor) al ínfimo de todos,

$$d'\,\big|\text{Ínf}\,\{a_1, a_2, a_3, \ldots, a_n\}$$

y, nuevamente, por la definición de máximo común divisor,

$$d'\,|\text{m.c.d.}\,(a_1, a_2, a_3, \ldots, a_n)$$

es decir,

$$d'\,|d$$

Pues bien, como $d\,|d'$ y $d'\,|d$, por la antisimetría de la relación de divisibilidad, $d = d'$, es decir,

$$\text{m.c.d.}\,(a_1, a_2, a_3, \ldots, a_n) = \text{m.c.d.}\,(a_1, \text{m.c.d.}\,(a_2, a_3, \ldots, a_n))$$

■

Ejemplo 13.23

Calcular,

$$m.c.d.\,(576, 864, 1296, 1944)$$

aplicando la proposición anterior.

Solución

Aplicando reiteradamente la proposición anterior,

$$\begin{aligned}
\text{m.c.d.}\,(576, 864, 1296, 1944) &= \text{m.c.d.}\,(576, \text{m.c.d.}\,(864, 1296, 1944)) \\
&= \text{m.c.d.}\,(576, \text{m.c.d.}\,(864, \text{m.c.d.}\,(1296, 1944))) \\
&= \text{m.c.d.}\,(576, \text{m.c.d.}\,(864, 648)) \\
&= \text{m.c.d.}\,(576, 216) \\
&= 72
\end{aligned}$$

■

13.5.3 Máximo común divisor de dos números

Sean a y b dos números enteros. El entero $d > 0$ es el máximo común divisor de a y b siempre y cuando sea el máximo del conjunto de los divisores comunes a ambos ordenado por la relación de divisibilidad. Es decir,

$$d = m.c.d.(a, b) \iff \begin{cases} 1. \quad d|a \quad y \quad d|b \\ \quad y \\ 2. \quad c|a \quad y \quad c|b \implies c|d \end{cases}$$

Demostración

En efecto, según la definición, el máximo común divisor de dos números es el ínfimo del conjunto formado por ambos ordenado por la relación de divisibilidad. Entonces,

$$\begin{aligned}
d = \text{m.c.d.}\,(a, b) &\iff d = \text{Ínf}\,\{a, b\} \\
&\iff \begin{cases} 1. \quad d \text{ es cota inferior del conjunto } \{a, b\} \text{ en } \mathbb{Z}^+. \\ \quad \text{y} \\ 2. \quad \text{Si } c \text{ es otra cota inferior de } \{a, b\} \text{ en } \mathbb{Z}^+, \\ \quad \text{entonces } c \text{ es anterior a } d. \end{cases} \\
&\iff \begin{cases} 1. \quad d \text{ es anterior a } a \text{ y anterior a } b. \\ \quad \text{y} \\ 2. \quad \text{Si } c \text{ es anterior a } a \text{ y anterior a } b, \\ \quad \text{entonces } c \text{ es anterior a } d. \end{cases} \\
&\iff \begin{cases} 1. \quad d|a \quad \text{y} \quad d|b \\ \quad \text{y} \\ 2. \quad c|a \quad \text{y} \quad c|b \implies c|d \end{cases}
\end{aligned}$$

Nota 13.4 Obsérvese que si llamamos D_a y D_b a los conjuntos formados por los divisores de a y b, respectivamente, las condiciones 1. y 2. pueden escribirse, también, de la forma siguiente:

$$d = \text{m.c.d.}\,(a,b) \iff \left\{ \begin{array}{l} 1.\quad d \in D_a \quad \text{y} \quad d \in D_b \\ \quad \text{y} \\ 2.\quad c \in D_a \quad \text{y} \quad c \in D_b \implies c|d \end{array} \right.$$

$$\iff \left\{ \begin{array}{l} 1.\quad d \in (D_a \cap D_b) \\ \quad \text{y} \\ 2.\quad c \in (D_a \cap D_b) \implies c|d \end{array} \right.$$

$$\iff d = \text{Máx}\,(D_a \cap D_b)$$

es decir, d es el máximo del conjunto de los divisores comunes a a y a b.

■

13.5.4 Propiedades

Sean a y b enteros distintos de cero. Se Verifica:

(i) $m.c.d.\,(a,0) = |a|$

(ii) $m.c.d.\,(a,b) = m.c.d.\,(|a|\,,|b|)$

Demostración

(i) En efecto, sea a cualquier entero distinto de cero. Según hemos visto en la nota 13.4,

$$\text{m.c.d.}\,(a,0) = \text{Máx}\,(D_a \cap D_0)$$

es decir, el máximo común divisor de a y 0 es el máximo del conjunto de los divisores comunes a "a" y a "0" ordenado por la relación de divisibilidad. Pues bien, como todos los enteros son múltiplos de 0 ((ii) de 13.1.2), podemos considerar que todos los enteros dividen a 0. Entonces,

$$D_a \cap D_0 = D_a \cap \mathbb{Z} = D_a$$

por lo tanto,

$$\text{m.c.d.}\,(a,0) = \text{Máx}\,(D_a)$$

es decir, el máximo común divisor de a y 0 es el máximo del conjunto de los divisores de a, ordenado por la relación de divisibilidad. Recordemos que la relación de divisibilidad era de orden parcial y, esto es lo importante ahora, estaba definida sobre el conjunto de los enteros positivos. De esta forma si $a > 0$, no hay problema, y si a es menor que cero, tomamos $-a$ que es mayor que cero. Entonces,

$$\text{m.c.d.}(a,0) \;=\; \left\{ \begin{array}{ll} \text{Máx}\,(D_a)\,, & \text{si } a > 0 \\ \text{y} & \\ \text{Máx}\,(D_{-a})\,, & \text{si } a < 0 \end{array} \right\} \;=\; \text{Máx}\left(D_{|a|}\right) \;=\; |a|$$

(ii) Veamos, ahora, que m.c.d. (a,b) = m.c.d. $(|a|,|b|)$. En efecto,

$$\begin{aligned}
\text{m.c.d.}(a,b) &= \text{Máx}\,(D_a \cap D_b) \\
&= \begin{cases} \text{Máx}\,(D_a \cap D_b), & \text{si } a>0 \text{ y } b>0 \\ \text{Máx}\,(D_a \cap D_{-b}), & \text{si } a>0 \text{ y } b<0 \\ \text{Máx}\,(D_{-a} \cap D_b), & \text{si } a<0 \text{ y } b>0 \\ \text{Máx}\,(D_{-a} \cap D_{-b}), & \text{si } a<0 \text{ y } b<0 \end{cases} \\
&= \text{Máx}\left(D_{|a|} \cap D_{|b|}\right) \\
&= \text{m.c.d.}\,(|a|,|b|)
\end{aligned}$$

Obsérvese que de este resultado se sigue que si a y b son enteros positivos cualesquiera,

$$\begin{aligned}
\text{m.c.d.}(-a,b) &= \text{m.c.d.}\,(|-a|,|b|) &= \text{m.c.d.}(a,b) \\
\text{m.c.d.}(a,-b) &= \text{m.c.d.}\,(|a|,|-b|) &= \text{m.c.d.}(a,b) \\
\text{m.c.d.}(-a,-b) &= \text{m.c.d.}\,(|-a|,|-b|) &= \text{m.c.d.}(a,b)
\end{aligned}$$

por lo tanto,

$$\text{m.c.d.}(-a,b) = \text{m.c.d.}(a,-b) = \text{m.c.d.}(-a,-b) = \text{m.c.d.}(a,b)$$

■

13.5.5 Existencia y Unicidad del Máximo Común Divisor

Dados dos números enteros a y b distintos de cero, existe un único entero d que es el máximo común divisor de ambos

Demostración

Supondremos que a y b son enteros positivos, ya que según hemos visto en la nota de las propiedades del máximo común divisor, si uno de los dos, o ambos, fuera negativo, el máximo común divisor sería el mismo.

Existencia. Sea C el conjunto de todas las combinaciones lineales positivas con coeficientes enteros que puedan formarse con a y b, es decir,

$$C = \left\{ma + nb \in \mathbb{Z}^+ : m,n \in \mathbb{Z}\right\}$$

⊛ C no es vacío. En efecto, como a es positivo, podemos escribirlo en la forma

$$a = 1 \cdot a + 0 \cdot b, \text{ con 0 y 1 enteros}$$

y, al menos, a estaría en C. Así pues, C es un subconjunto no vacío de $\mathbb{Z}^+$ y aplicando el principio de la buena ordenación, C ha de tener primer elemento o elemento mínimo al que llamaremos d.

⊛ d es el máximo común divisor de a y b. En efecto,

$$d \in C \Longrightarrow d = sa + bt, \text{con } s \text{ y } t, \text{ enteros.}$$

1. d es divisor de a y de b.
   En efecto, supongamos lo contrario, es decir d no es divisor de a o d no es divisor de b. Entonces, si d no divide a a, por el teorema de existencia y unicidad de cociente y resto, podremos encontrar dos enteros q y r tales que $a = dq + r$, con $0 < r < d$. Pues bien,

$$\left.\begin{array}{rcrcl} a & = & dq & + & r \\ d & = & sa & + & tb \end{array}\right\} \implies a = (sa + tb)\, q + r$$

$$\implies r = a - (sa + tb)\, q$$

$$\implies r = (1 - sq)\, a + (-tq)\, b > 0, \quad \text{con } 1 - sq \text{ y } -tq \text{ enteros}$$

$$\implies r \in C.$$

   Tendremos, pues, que $r \in C$ y $r < d$ lo cual contradice el que d sea el mínimo de C. La suposición hecha es, por lo tanto, falsa y, consecuentemente, $d|a$.
   Con un razonamiento idéntico se prueba que $d|b$.
2. d es el máximo de los divisores comunes a a y b.
   En efecto, si el entero c es otro divisor de a y b, entonces por (v) de las propiedades de la divisibilidad (13.1.2), dividirá a cualquier combinación lineal con coeficientes enteros de a y b, es decir,

$$c\,|pa + qb\,, \text{ con } p \text{ y } q \text{ enteros},$$

   en particular $c\,|sa + tb$, luego $c|d$.

De 1. y 2. se sigue que $d = \text{m.c.d.}(a, b)$.

Unicidad. En efecto, supongamos que el máximo común divisor de a y b no fuese único.

En tal caso habría, al menos, otro entero d' que también sería máximo común divisor de a y b. Entonces,

$$d \text{ es el máximo de los divisores comunes a } a \text{ y } b.$$

y

$$d' \text{ es un divisor común de } a \text{ y } b$$

por lo tanto,

$$d'\,|d$$

Por otra parte,

$$d' \text{ es el máximo de los divisores comunes a } a \text{ y } b.$$

y

$$d \text{ es un divisor común de } a \text{ y } b$$

por lo tanto,

$$d\,|d'$$

Así pues, tenemos que

$$d'\,|d \quad \text{y} \quad d\,|d'$$

aplicamos (iii) de las propiedades de la divisibilidad (13.1.2) y,

$$d = d'$$

ya que, por definición, tanto d como d' son mayores que cero.

■

13.5.6 Corolario

Si d es el máximo común divisor de a y b, entonces d es el menor entero positivo que puede escribirse como combinación lineal de a y b con coeficientes enteros.

$$d = m.c.d.(a,b) \Longrightarrow \exists p, q \in \mathbb{Z} : d = pa + qb$$

Demostración

Se sigue directamente del teorema anterior.

■

Nota 13.5 ¿Será cierto el recíproco?. Es decir, si $d > 0$ puede escribirse como combinación lineal con coeficientes enteros de dos números dados a y b, ¿será $d = \text{m.c.d.}(a,b)$?

Veamos que, en general, no tiene porque serlo. En efecto,

$$6 = 2 \cdot 27 + (-8) \cdot 6$$

y, sin embargo,

$$\text{m.c.d.}\,(27,6) = 3 \neq 6.$$

En la proposición siguiente veremos que si añadimos la hipótesis de que d sea un divisor común de a y de b, entonces si se verifica el recíproco.

■

13.5.7 Proposición

Si d es el menor entero positivo que puede escribirse como combinación lineal con coeficientes enteros de dos enteros dados a y b y es divisor común de ambos, entonces d es el máximo común divisor de a y de b.

Demostración

En efecto, supongamos que

$$d = pa + qb, \text{ con } p, q \in \mathbb{Z}$$

y

$$d|a \text{ y } d|b$$

Entonces,

1 d es divisor de a y de b. Directamente de la hipótesis.

2 d es el máximo. En efecto, sea c otro de los divisores comunes de a y b. Entonces,

$$\left.\begin{array}{l} c|a \\ \text{y} \\ c|b \end{array}\right\} \Longrightarrow c|pa + qb, \text{ con } p \text{ y } q \text{ enteros} \Longrightarrow c|d.$$

Por lo tanto, $d = \text{m.c.d.}(a,b)$.

■

Veamos ahora como un corolario a la proposición anterior que en el caso de que el máximo común divisor de a y b sea 1, se verifica el recíproco sin necesidad de añadirle ninguna hipótesis al número d.

13.5.8 Corolario

Si a y b son dos enteros distintos de cero, entonces m.c.d. $(a,b)=1$ si, y sólo si existen dos números enteros p y q tales que $pa+qb=1$.

Demostración

"Sólo si." Si m.c.d. $(a,b)=1$, entonces por el corolario 13.5.6, pueden encontrarse dos números enteros p y q tales que $pa+qb=1$.

"Si." Sean p y q dos números enteros tales que $pa+qb=1$. Como 1 es divisor de cualquier número entero, $1|a$ y $1|b$. Aplicamos la proposición anterior y m.c.d. $(a,b)=1$.

■

Ejemplo 13.24

Demuéstrese que si m.c.d. $(a,b)=1$ y m.c.d. $(a,c)=1$, entonces m.c.d. $(a,bc)=1$.

Solución

Aplicando el corolario anterior, tendremos

$$\text{m.c.d.}\,(a,b)=1 \iff \exists p,q\in\mathbb{Z}: pa+qb=1$$
$$\text{m.c.d.}\,(a,c)=1 \iff \exists r,s\in\mathbb{Z}: ra+sc=1$$

y multiplicando término a término, se sigue que

$$(pa+qb)(ra+sc)=1 \iff a(pra+psc+qrb)+(qs)bc=1$$

con $pra+psc+qrb$ y bc enteros. Aplicamos de nuevo el corolario anterior, y

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

■

13.5.9 Más Propiedades

Sean a y b dos números enteros. Se verifica:

(i) *Si m.c.d. $(a,b)=d$, entonces m.c.d. $\left(\frac{a}{d},\frac{b}{d}\right)=1$.*

(ii) *m.c.d. $(ka,kb)=k\cdot$ m.c.d. (a,b), $\forall k\in\mathbb{Z}^+$.*

Demostración

(i) Si $\text{m.c.d.}\,(a,b)=d$, entonces $\text{m.c.d.}\left(\frac{a}{d},\frac{b}{d}\right)=1$

En efecto,

$$\begin{aligned} d=\text{m.c.d.}(a,b) &\implies \exists p,q\in\mathbb{Z}: pa+qb=d && \{\text{Corolario 13.5.6}\}\\ &\implies \exists p,q\in\mathbb{Z}: p\frac{a}{d}+q\frac{b}{d}=1 \\ &\iff \text{m.c.d.}\left(\frac{a}{d},\frac{b}{d}\right)=1 && \{\text{Corolario 13.5.8}\}\end{aligned}$$

(ii) $\text{m.c.d.}\,(ka,kb)=k\text{m.c.d.}\,(a,b)\,,\ \forall k\in\mathbb{Z}^+$

En efecto, supongamos que $\text{m.c.d.}\,(a,b)=d$. Entonces,

$$\begin{aligned} d=\text{m.c.d.}(a,b) &\implies \exists p,q\in\mathbb{Z}: pa+qb=d && \{\text{Corolario 13.5.6}\}\\ &\implies \exists p,q\in\mathbb{Z}: pka+qkb=kd\end{aligned}$$

Veamos que kd es el máximo común divisor de ka y kb.

1. kd es divisor de ka y kb.
   En efecto,
   $$d=\text{m.c.d.}\,(a,b)\implies\begin{cases} d\,|a\implies kd\,|ka\\ \text{y}\\ d\,|b\implies kd\,|kb\end{cases}$$
2. Sea c cualquier otro divisor común de ka y kb. Entonces,
   $$\left.\begin{array}{c} c\,|ka\\ \text{y}\\ c\,|kb\end{array}\right\}\implies c\,|pka+qkb\ \text{ con } p,q\in\mathbb{Z}\implies c\,|kd$$

Luego,

$$\text{m.c.d.}\,(ka,kb)=kd=k\text{m.c.d.}\,(a,b)$$

■

Ejemplo 13.25

Demostrar que si m.c.d. $(a,b)=1$, *entonces m.c.d.* $(a+b,a-b)=1$ *ó* 2.

Solución

Sea $d=\text{m.c.d.}\,(a+b,a-b)$. Entonces,

$$\left.\begin{array}{l} d\,|a+b\\ \text{y}\\ d\,|a-b\end{array}\right\}\implies d\,|(a+b)+(a-b)\implies d\,|2a$$

también

$$\left.\begin{array}{l} d\,|a+b\\ \text{y}\\ d\,|a-b\end{array}\right\}\implies d\,|(a+b)-(a-b)\implies d\,|2b$$

y si $d\,|2a$ y $d\,|2b$, entonces d divide al máximo común divisor de $2a$ y $2b$, es decir,

$$d\,|\text{m.c.d.}\,(2a, 2b) \Longrightarrow d\,|2 \cdot \text{m.c.d.}\,(a, b) \Longrightarrow d\,|2$$

pero los únicos divisores positivos de 2 son 1 y 2, luego

$$d = 1 \text{ ó } d = 2$$

o sea,

$$\text{m.c.d.}\,(a + b, a - b) = 1 \text{ ó } 2$$

■

Ejemplo 13.26

Demuéstrese que $d = m.c.d.\,(a, b)$ *si, y sólo si* $d\,|a\,, d\,|b$ *y* $m.c.d.\left(\frac{a}{d}, \frac{b}{d}\right) = 1$.

Solución

"Sólo si". Esta demostración la hicimos en (i) de 13.5.9. Ahora la haremos utilizando (ii) de dicha proposición.

Si $d = \text{m.c.d.}\,(a, b)$, es obvio que $d\,|a$ y $d\,|b$, entonces $\frac{a}{d}$ y $\frac{b}{d}$ son números enteros. Escribimos,

$$a = d \cdot \frac{a}{d} \text{ y } b = d \cdot \frac{b}{d}$$

luego,

$$\begin{aligned} \text{m.c.d.}\,(a, b) = d &\Longrightarrow \text{m.c.d.}\left(d \cdot \frac{a}{d}, d \cdot \frac{b}{d}\right) = d \\ &\Longrightarrow d \cdot \text{m.c.d.}\left(\frac{a}{d}, \frac{b}{d}\right) = d \\ &\Longrightarrow \text{m.c.d.}\left(\frac{a}{d}, \frac{b}{d}\right) = 1 \end{aligned}$$

Veamos ahora que la hipótesis de que $d\,|a$ y $d\,|b$, permite probar el recíproco también.

"Si". En efecto, como $d\,|a$ y $d\,|b$, al igual que antes, se sigue que $\frac{a}{d}$ y $\frac{b}{d}$ son números enteros, por tanto,

$$\begin{aligned} \text{m.c.d.}\,(a, b) &= \text{m.c.d.}\left(d \cdot \frac{a}{d}, d \cdot \frac{b}{d}\right) \\ &= d \cdot \text{m.c.d.}\left(\frac{a}{d}, \frac{b}{d}\right) \\ &= d \cdot 1 \\ &= d \end{aligned}$$

■

Ejemplo 13.27

Probar que si $d|a$ y $d|b$, entonces m.c.d. $\left(\frac{a}{d}, \frac{b}{d}\right) = \frac{1}{d} \cdot m.c.d.(a, b)$.

Solución

Por hipótesis $d|a$ y $d|b$ luego $\frac{a}{d}$ y $\frac{b}{d}$ son números enteros y existe m.c.d. $\left(\frac{a}{d}, \frac{b}{d}\right)$. Pues bien, aplicando (ii) de 13.5.9,

$$d \cdot \text{m.c.d.}\left(\frac{a}{d}, \frac{b}{d}\right) = \text{m.c.d.}\left(d \cdot \frac{a}{d}, d \cdot \frac{b}{d}\right) \implies d \cdot \text{m.c.d.}\left(\frac{a}{d}, \frac{b}{d}\right) = \text{m.c.d.}\,(a, b)$$

Por lo tanto,

$$\text{m.c.d.}\left(\frac{a}{d}, \frac{b}{d}\right) = \frac{1}{d} \cdot \text{m.c.d.}\,(a, b)$$

Ejemplo 13.28

Se han plantado árboles igualmente espaciados en el contorno de un campo triangular cuyos lados miden $144m.$, $180m.$ *y* $240m.$ *respectivamente. Sabiendo que hay un árbol en cada vértice y que la distancia entre dos árboles consecutivos está comprendida entre* 5 *y* 10 *metros. Calcular el número de árboles plantados.*

Solución

Sea d la distancia entre dos árboles consecutivos. Entonces d de ser un divisor de 144, 180 y 240 luego ha de ser divisor de su máximo común divisor.

Pues bien, calculemos el máximo común divisor de 144, 180 y 240. Los conjuntos de divisores positivos de los tres números son:

$$D_{144} = \{1, 2, 4, 8, 16, 3, 6, 12, 24, 48, 9, 18, 36, 72, 144\}$$

y

$$D_{180} = \{1, 2, 4, 3, 6, 12, 9, 18, 36, 5, 10, 20, 15, 30, 60, 45, 90, 180\}$$

y

$$D_{240} = \{1, 2, 4, 8, 16, 3, 6, 12, 24, 48, 5, 10, 20, 40, 80, 15, 30, 60, 120, 240\}$$

Por lo tanto, el conjunto de los divisores comunes a los tres números será

$$D_{144} \cap D_{180} \cap D_{240} = \{1, 2, 4, 3, 6, 12\}$$

y un diagrama de Hasse que represente la ordenación de este conjunto por la relación de divisibilidad es:

Como puede apreciarse claramente el máximo es el 12, por lo tanto,

$$\text{m.c.d.}(144, 180, 240) = 12.$$

Así pues, d ha de ser un divisor de 12 y como éstos son 1, 2, 3, 4, 6 y 12, y d ha de estar comprendido entre 5 y 10, se sigue que

$$d = 6$$

El número total de árboles plantados será, pues

$$N = \frac{144}{6} + \frac{180}{6} + \frac{240}{6} = 94$$

■

13.6 Algoritmo de Euclides

Desarrollaremos un método para calcular el máximo común divisor de dos números conocido como el *Algoritmo de Euclides*[1]. Este método es más sencillo que el de calcular todos los divisores de ambos números cuando se trata de calcular el máximo común divisor de dos números y éstos son muy grandes.

Veamos un teorema previo que sustenta teóricamente el algoritmo.

13.6.1 Teorema

El máximo común divisor del dividendo y del divisor de una división es el mismo que el máximo común divisor del divisor y el resto.

Demostración

Sean a y b dos números enteros cualesquiera con $b \neq 0$. Por el teorema de existencia y unicidad de cociente y resto, existirán dos números enteros, únicos, q y r tales que

$$a = bq + r : 0 \leqslant r < b$$

Probaremos que el máximo común divisor de a y b es el mismo que el de b y r.

En efecto, sea $d = \text{m.c.d.}\,(a, b)$. Entonces, d es un divisor común a a y a b, luego por (v) de 13.1.2,

$$d \,|a + (-q)b$$

es decir,

$$d \,|r\ .$$

Por lo tanto,

$$d \,|b \ \text{ y } d \,|r\ . \tag{13.5}$$

Veamos ahora que es el máximo de los divisores comunes de b y r. En efecto, si c es otro divisor común a b y r, nuevamente por (iv) de 13.1.2,

$$c \,|bq + r$$

es decir,

$$c \,|a$$

luego,

$$c \,|a \ \text{ y } c \,|b$$

[1] Matemático griego del siglo III antes de Cristo. Se sabe que enseñaba matemáticas en Alejandría, donde fundó la escuela más célebre de la antigüedad. Es sobre todo conocido por sus *Elementos*, que continúan siendo considerados como el libro de geometría por excelencia. En el principio de esta obra, importante por su gran claridad y rigor, hay la definición de las "nociones comunes", a las que Euclides recurre casi constantemente en las páginas que siguen, y entre las cuales figura su famoso postulado. A continuación va desarrollando, en un orden lógico, los diversos teoremas. El conjunto consta de trece libros, a los que suele unirse otros dos atribuidos a Hipsicles, matemático de Alejandría que vivió probablemente en el siglo II antes de Cristo. Los cuatro primeros libros tratan de la geometría del plano y estudian las razones y las proporciones. La teoría de los números enteros es el objeto de los libros VII, VIII y IX. El libro X, más largo, y considerado también como el más perfecto de todos, está consagrado al estudio de los irracionales algebraicos más simples. La última parte trata de la geometría del espacio. Los *Cálculos*, especie de complemento de los *Elementos*, tienen una forma más analítica. Una obra perdida, la de los *Lugares de la superficie*, debía tener por objeto el estudio de las secciones planas de las superficies de revolución de segundo grado. Los textos de Proclo y de Papo nos han transmitido los *Porismas* sobre los cuales se ha discutido mucho, pero que, según Chasles, contienen en germen las tres teorías modernas de la razón anarmónica, de las divisiones homográficas y de la involución. En fin, en su *Optica*, Euclides procede como en geometría, poniendo en cabeza algunas proposiciones fundamentales, la más importante de las cuales admite la propagación de los rayos luminosos en línea recta.

y, consecuentemente, ha de dividir al máximo común divisor de a y b, es decir,

$$c \,|d\,. \tag{13.6}$$

De (13.5) y (13.6) se sigue que

$$\text{m.c.d.}\,(b,r) = d$$

y, por lo tanto,

$$\text{m.c.d.}\,(a,b) = \text{m.c.d.}\,(b,r)$$

■

13.6.2 Algoritmo de Euclides

El teorema anterior es el fundamento del algoritmo de Euclides, proceso de divisiones sucesivas que permite calcular el máximo común divisor de dos números.

Demostración

Sean a y b dos números enteros que supondremos mayores que cero y tales que $a \neq b$.

Obsérvese que al ser

$$\text{m.c.d.}\,(a,b) = \text{m.c.d.}\,(|a|\,,|b|)$$

el suponer que $a > 0$ y $b > 0$ no significa pérdida de generalidad alguna y lo mismo ocurre con suponer que $a \neq b$ ya que $\text{m.c.d.}(a,a) = a$. Como $a \neq b$, será $a > b$ ó $a < b$. Supondremos que $a > b$.

Por el teorema 13.2.1, existirán dos enteros q_1 y r_1, únicos, tales que

$$a = bq_1 + r_1 : 0 \leqslant r_1 < b$$

y por el teorema anterior,

$$\text{m.c.d.}(a,b) = \text{m.c.d.}(b,r_1).$$

Ahora pueden ocurrir dos cosas:

- Si $r_1 = 0$, entonces,
$$\text{m.c.d.}(a,b) = \text{m.c.d.}(b,r_1) = \text{m.c.d.}(b,0) = b$$
y el proceso para obtener el máximo común divisor termina.
- Si $r_1 \neq 0$, entonces aplicando de nuevo 13.2.1, obtenemos q_2 y r_2 tales que
$$b = r_1q_2 + r_2 : 0 \leqslant r_2 < r_1$$
y por el teorema previo,
$$\text{m.c.d.}(b,r_1) = \text{m.c.d.}(r_1,r_2)$$
y, nuevamente, pueden ocurrir dos cosas:
  - Si $r_2 = 0$, entonces
$$\text{m.c.d.}(b,r_1) = \text{m.c.d.}(r_1,r_2) = \text{m.c.d.}(r_1,0) = r_1$$
y, consecuentemente,
$$\text{m.c.d.}(a,b) = \text{m.c.d.}(b,r_1) = \text{m.c.d.}(r_1,r_2) = r_1$$
terminando el proceso.

– Si $r_2 \neq 0$, entonces el teorema 13.2.1 permite, de nuevo, obtener q_3 y r_3 tales que

$$r_1 = r_2 q_3 + r_3 : 0 \leqslant r_3 < r_2$$

y por el teorema previo,

$$\text{m.c.d.}(r_1, r_2) = \text{m.c.d.}(r_2, r_3)$$

y, otra vez,

– Si $r_3 = 0$, entonces

$$\text{m.c.d.}(r_1, r_2) = \text{m.c.d.}(r_2, r_3) = \text{m.c.d.}(r_2, 0) = r_2$$

por lo tanto,

$$\text{m.c.d.}(a, b) = \text{m.c.d.}(b, r_1) = \text{m.c.d.}(r_1, r_2) = \text{m.c.d.}(r_2, 0) = r_2$$

y el proceso acaba.

– Si $r_3 \neq 0$, entonces ¿qué harías?

Procediendo así sucesivamente, obtendríamos

$$r_1 > r_2 > r_3 > \cdots\cdots > r_k > \cdots\cdots$$

y todos y cada uno de los números $r_1, r_2, \ldots\ldots, r_k$ son mayores que cero, luego el conjunto de todos ellos no puede tener infinitos elementos.

En algún momento y después de un número finito de pasos, aparecerá un resto igual a cero. Supongamos que dicho resto es r_{n+1}, entonces aplicando sucesivamente el teorema previo, tendremos

$$\text{m.c.d.}\,(a, b) = \text{m.c.d.}\,(b, r_1) = \text{m.c.d.}\,(r_1, r_2) = \cdots = \text{m.c.d.}\,(r_{n-1}, r_n) = \text{m.c.d.}\,(r_n, r_{n+1})$$

y al ser $r_{n+1} = 0$, será

$$\text{m.c.d.}\,(r_n, r_{n+1}) = \text{m.c.d.}\,(r_n, 0) = r_n$$

y, por tanto,

$$\text{m.c.d.}\,(a, b) = r_n$$

finalizando el proceso de obtener el máximo común divisor de los números a y b.

En la práctica los cálculos suelen disponerse en la forma siguiente:

	q_1	q_2	q_3	q_4	$\cdots$	$\cdots$	$\cdots$	$\cdots$	q_n	q_{n+1}
a	b	r_1	r_2	r_3	$\cdots$	$\cdots$	$\cdots$	$\cdots$	r_{n-1}	$r_n = \text{m.c.d.}(a, b)$
r_1	r_2	r_3	r_4	$\cdots$	$\cdots$	$\cdots$	$\cdots$	r_n	$r_{n+1} = 0$	

■

Ejemplo 13.29

Hallar el máximo común divisor de 1369 *y* 2597 *y expresarlo como una combinación lineal con coeficientes enteros de ellos.*

Solución

Lo haremos de forma práctica, disponiendo los cálculos en una tabla

	1	1	8	1	2	2	3	1	1	2
2597	1369	1228	141	100	41	18	5	3	2	1
1228	141	100	41	18	5	3	2	1	0	

luego,

$$\text{m.c.d.}(2597, 1369) = 1$$

Según vimos en 13.5.6,

Si $d = \text{m.c.d.}(a, b)$, entonces podemos encontrar dos enteros p y q tales que $d = pa + qb$.

Es decir, podemos escribir d como combinación lineal, con coeficientes enteros, de a y b y nuestro problema es encontrar dichos coeficientes, para lo cual utilizaremos de nuevo el Algoritmo de Euclides aunque haciendo

las "cuentas" hacia atrás.

$$\left.\begin{array}{r} 1 = 3 - 1 \cdot 2 \\ 2 = 5 - 1 \cdot 3 \end{array}\right\} \Longrightarrow \begin{array}{rcl} 1 & = & 3 - 1(5 - 3 \cdot 1) \\ & = & (-1) \cdot 5 + 2 \cdot 3 \end{array}$$

$$\left.\begin{array}{r} 1 = (-1) \cdot 5 + 2 \cdot 3 \\ 3 = 18 - 3 \cdot 5 \end{array}\right\} \Longrightarrow \begin{array}{rcl} 1 & = & (-1)5 + 2(18 - 3 \cdot 5) \\ & = & 2 \cdot 18 + (-7) \cdot 5 \end{array}$$

$$\left.\begin{array}{r} 1 = 2 \cdot 18 + (-7) \cdot 5 \\ 5 = 41 - 2 \cdot 18 \end{array}\right\} \Longrightarrow \begin{array}{rcl} 1 & = & 2 \cdot 18 + (-7)(41 - 2 \cdot 18) \\ & = & (-7) \cdot 41 + 16 \cdot 18 \end{array}$$

$$\left.\begin{array}{r} 1 = (-7) \cdot 41 + 16 \cdot 18 \\ 18 = 100 - 2 \cdot 41 \end{array}\right\} \Longrightarrow \begin{array}{rcl} 1 & = & (-7) \cdot 41 + 16(100 - 2 \cdot 41) \\ & = & 16 \cdot 100 + (-39) \cdot 41 \end{array}$$

$$\left.\begin{array}{r} 1 = 16 \cdot 100 + (-39) \cdot 41 \\ 41 = 141 - 1 \cdot 100 \end{array}\right\} \Longrightarrow \begin{array}{rcl} 1 & = & 16 \cdot 100 + (-39)(141 - 1 \cdot 100) \\ & = & (-39) \cdot 141 + 55 \cdot 100 \end{array}$$

$$\left.\begin{array}{r} 1 = (-39) \cdot 141 + 55 \cdot 100 \\ 100 = 1228 - 8 \cdot 141 \end{array}\right\} \Longrightarrow \begin{array}{rcl} 1 & = & (-39) \cdot 141 + 55(1228 - 8 \cdot 141) \\ & = & 55 \cdot 1228 + (-479) \cdot 141 \end{array}$$

$$\left.\begin{array}{r} 1 = 55 \cdot 1228 + (-479) \cdot 141 \\ 141 = 1369 - 1 \cdot 1228 \end{array}\right\} \Longrightarrow \begin{array}{rcl} 1 & = & 55 \cdot 1228 + (-479)(1369 - 1 \cdot 1228) \\ & = & (-479) \cdot 1369 + 534 \cdot 1228 \end{array}$$

$$\left.\begin{array}{r} 1 = (-479) \cdot 1369 + 534 \cdot 1228 \\ 1228 = 2597 - 1 \cdot 1369 \end{array}\right\} \Longrightarrow \begin{array}{rcl} 1 & = & (-479) \cdot 1369 + 534(2597 - 1 \cdot 1369) \\ & = & 534 \cdot 2597 + (-1013) \cdot 1369 \end{array}$$

De aquí que los coeficientes que buscábamos sean $p = 534$ y $q = -1013$ y la expresión del máximo común divisor como combinación lineal de 2597 y 1369 con esos coeficientes sea:

$$1 = 534 \cdot 2597 + (-1013) \cdot 1369$$

Obsérvese que esta expresión no es única. En efecto, para cualquier $k \in \mathbb{Z}$, tendremos

$$\begin{array}{rcl} 1 & = & 534 \cdot 2597 + (-1013) \cdot 1369 \\ & = & 534 \cdot 2597 + (-1013) \cdot 1369 + (-1369k) \cdot 2597 + (2597k) \cdot 1369 \\ & = & (534 - 1369k)2597 + (-1013 + 2597k)1369 \end{array}$$

Obsérvese también que

$$\text{m.c.d.}\,(-1369, 2597) = 1$$
$$\text{m.c.d.}\,(1369, -2597) = 1$$
$$\text{m.c.d.}\,(-1369, -2597) = 1$$

y en tales casos las combinaciones lineales con coeficientes enteros serían:

$$\begin{array}{rcl} 1 & = & 1013 \cdot (-1369) + 534 \cdot 2597 \\ 1 & = & (-1013) \cdot 1369 + (-534)(-2597) \\ 1 & = & 1013 \cdot (-1369) + (-534)(-2597) \end{array}$$

■

Ejemplo 13.30

Calcular el máximo común divisor de 231 y 1820. Expresar dicho número como una combinación lineal con coeficientes enteros de ellos dos.

Solución

	7	1	7	4
1820	231	203	28	7
203	28	7	0	

Ahora calcularemos los coeficientes de la combinación lineal siguiendo, al igual que hicimos en el ejemplo anterior, el proceso inverso.

$$\left.\begin{array}{rcrcr} 7 & = & 203 & - & 7\cdot 28 \\ 28 & = & 231 & - & 1\cdot 203 \end{array}\right\} \Longrightarrow 7 = 203 - 7(231 - 1\cdot 203)$$

$$\Longrightarrow 7 = (-7)\cdot 231 + 8\cdot 203$$

$$\left.\begin{array}{rcrcr} 7 & = & (-7)\cdot 231 & + & 8\cdot 203 \\ 203 & = & 1820 & - & 7\cdot 231 \end{array}\right\} \Longrightarrow 7 = (-7)\cdot 231 + 8(1820 - 7\cdot 231)$$

$$\Longrightarrow 7 = 8\cdot 1820 + (-63)\cdot 231$$

es decir, la combinación lineal pedida es

$$7 = 8\cdot 1820 + (-63)\cdot 231$$

■

Ejemplo 13.31

¿Cuál es el mayor número que al emplearlo como divisor de 68130 *y* 107275 *origina los restos* 27 *y* 49*, respectivamente?*

Solución

Sea a el número que buscamos. Entonces, por el 13.2.1, existirán q_1 y q_2, enteros, tales que

$$\left.\begin{array}{rcrcr} 68130 & = & aq_1 & + & 27 \\ \text{y} & & & & \\ 107275 & = & aq_2 & + & 49 \end{array}\right\} \Longrightarrow \left.\begin{array}{rcl} 68103 & = & aq_1, \text{ con } q_1 \in \mathbb{Z} \\ \text{y} & & \\ 107226 & = & aq_2, \text{ con } q_2 \in \mathbb{Z} \end{array}\right\}$$

$$\Longrightarrow a\,|68103 \text{ y } a\,|107226$$

luego a es un divisor común a 68103 y 107226 y como tiene que ser el mayor, será

$$a = \text{m.c.d.}\,(68103, 107226)$$

y utilizando el Algoritmo de Euclides para el cálculo del máximo común divisor,

	1	1	1	1	0	1	1	6
107226	68103	39123	28980	10143	18837	10143	8694	1449
39123	28980	10143	18837	10143	8694	1449	0	

luego, $a = 1449$

■

Ejemplo 13.32

Halla dos números cuyo máximo común divisor es 7 *y tales que los cocientes obtenidos en su determinación por el algoritmo de Euclides son, en orden inverso,* 7, 2, 3 *y* 36.

Solución

Presentando los cálculos en la forma práctica que vimos antes, si los números buscados son a y b, tendremos

	36	3	2	7
a	b	r_1	r_2	r_3
r_1	r_2	r_3	0	

por tanto,

$$\text{m.c.d.}\,(a, b) = \text{m.c.d.}\,(r_3, 0) = r_3$$

y como según el enunciado $\text{m.c.d.}\,(a, b) = 7$, tendremos que $r_3 = 7$. Sustituyendo en el algoritmo nos quedaría,

	36	3	2	7
a	b	r_1	r_2	7
r_1	r_2	7	0	

Volviendo hacia atrás podemos calcular r_1. En efecto,

$$0 = r_2 - 7 \cdot 7 \Longrightarrow r_2 = 49$$

y sustituyendo, de nuevo, en el algoritmo,

	36	3	2	7
a	b	r_1	49	7
r_1	49	7	0	

Calculamos, ahora, r_1.

$$7 = r_1 - 2 \cdot 49 \Longrightarrow r_1 = 105$$

y el algoritmo quedaría,

	36	3	2	7
a	b	105	49	7
105	49	7	0	

Ya podemos calcular b.

$$49 = b - 3 \cdot 105 \Longrightarrow b = 364$$

y

	36	3	2	7
a	364	105	49	7
105	49	7	0	

con lo que,

$$105 = a - 36 \cdot 364 \Longrightarrow a = 13209$$

es decir, los números buscados son $a = 13209$ y $b = 364$.

■

13.7 Mínimo Común Múltiplo

Estudiaremos en esta sección los múltiplos comunes a un par de números enteros.

13.7.1 Definición

Dados los números enteros positivos $a_1, a_2, a_3, \ldots, a_n$, llamaremos mínimo común múltiplo de todos ellos al supremo del conjunto $\{a_1, a_2, a_3, \ldots, a_n\}$ ordenado con la relación de orden parcial de divisibilidad. Lo notaremos m.c.m.$(a_1, a_2, a_3, \ldots, a_n)$

Ejemplo 13.33

Calcular, aplicando directamente la definición anterior,

$$m.c.m.\,(72, 108, 144, 216, 324, 288, 432, 648, 972, 864, 1296, 1944, 2592, 3888)$$

Solución

Según la definición de mínimo común múltiplo de varios números, tendremos que calcular el Supremo del conjunto

$$A = \{72, 108, 144, 216, 324, 288, 432, 648, 972, 864, 1296, 1944, 2592, 3888\}$$

ordenado con la relación de orden de divisibilidad, es decir, si a y b son cualesquiera de A,

$$b \text{ es posterior a } a \text{ siempre y cuando } b \text{ sea múltiplo de } a$$

o sea,

$$a \preccurlyeq b \Longleftrightarrow a|b \Longrightarrow b = a \cdot q, \text{ con } q \text{ entero.}$$

Recordemos que el supremo de A es el mínimo del conjunto de sus cotas superiores ordenado por la relación anterior. Vamos a calcular, pues, los elementos característicos de este conjunto.

Elementos Maximales. Por definición, un elemento m de A será maximal de A, respecto de la relación $\preccurlyeq$, si no hay en A elemento alguno que sea estrictamente posterior a él, es decir,

$$m \text{ es maximal de } A \iff \nexists x \in A : m \prec x$$

o lo que es igual,

$$m \text{ es maximal de } A \iff \nexists x \in A : m \preccurlyeq x \text{ y } m \neq x$$

y esto significa, teniendo en cuenta que la relación $\preccurlyeq$ es la de divisibilidad,

$$m \text{ es maximal de } A \iff \nexists x \in A : m \text{ sea múltiplo de } x \text{ y } m \neq x$$

es decir,

$$m \text{ es maximal de } A \iff m \text{ no tiene en } A \text{ múltiplos distintos del propio } m.$$

Consecuentemente,

$$m \text{ es maximal de } A \iff m = 2592 \text{ ó } m = 3888$$

Obsérvese que al haber dos maximales no puede haber máximo, ya que éste, caso de existir, ha de ser único y coincidir con el maximal.

Cotas Superiores. Un elemento $s \in \mathbb{Z}^+$ es cota superior de A, subconjunto de $\mathbb{Z}^+$, si es posterior a todos los elementos de A, o sea,

$$s \in \mathbb{Z}^+ \text{ es cota superior de } A \text{ en } \mathbb{Z}^+ \Longleftrightarrow \forall x, (x \in A \Longrightarrow x \preccurlyeq s)$$

es decir,

$$s \in \mathbb{Z}^+ \text{ es cota superior de } A \text{ en } \mathbb{Z}^+ \Longleftrightarrow \forall x, (x \in A \Longrightarrow s \text{ es múltiplo de } x)$$

Así pues,

$$s \in \mathbb{Z}^+ \text{ es cota superior de } A \text{ en } \mathbb{Z}^+ \iff s \text{ es múltiplo de todos los elementos de } A$$

y bastaría con que s fuese múltiplo de los maximales de A ya que por transitividad esto significaría que es múltiplo de todos los elementos de A. Por lo tanto,

$$s \in \mathbb{Z}^+ \text{ es cota superior de } A \text{ en } \mathbb{Z}^+ \iff s \text{ es múltiplo de los elementos maximales de } A.$$

Así pues,

$$\begin{aligned} s \in \mathbb{Z}^+ \text{ es cota superior de } A \subseteq \mathbb{Z}^+ &\iff s \text{ es múltiplo de 2592 y 3888} \\ &\iff \begin{cases} s \text{ es múltiplo de 2592} \\ \text{y} \\ s \text{ es múltiplo de 3888} \end{cases} \\ &\iff \begin{cases} s \text{ es múltiplo de } 2^5 \cdot 3^3 \\ \text{y} \\ s \text{ es múltiplo de } 2^4 \cdot 3^5 \end{cases} \\ &\iff s = 2^5 \cdot 3^5 \cdot k,\ k \in \mathbb{Z}^+ \end{aligned}$$

luego, si llamamos C_s al conjunto de las cotas inferiores, tendremos que

$$C_s = \left\{2^5 \cdot 3^5 \cdot k,\ k \in \mathbb{Z}^+\right\}$$

Supremo. Un elemento m de $\mathbb{Z}^+$ se dice que es el supremo de A, subconjunto de $\mathbb{Z}^+$, si es el mínimo del conjunto de las cotas superiores. Entonces,

$$m \in \mathbb{Z}^+ \text{ es el supremo de } A \subseteq \mathbb{Z}^+ \iff m \text{ es el mínimo de } C_s$$

luego,

$$m \in \mathbb{Z}^+ \text{ es el supremo de } A \subseteq \mathbb{Z}^+ \iff m \text{ es anterior a todos los elementos de } C_s$$

o lo que es igual,

$$m \in \mathbb{Z}^+ \text{ es el supremo de } A \subseteq \mathbb{Z}^+ \iff m \text{ es divisor de todos los elementos de } C_s.$$

Consecuentemente,

$$m \in \mathbb{Z}^+ \text{ es el supremo de } A \subseteq \mathbb{Z}^+ \iff m = 2^5 \cdot 3^5 = 7776.$$

Así pues, y según la definición de mínimo común múltiplo,

$$\text{m.c.m.}\,(72, 108, 144, 216, 324, 288, 432, 648, 972, 864, 1296, 1944, 2592, 3888) = 7776$$

■

13.7.2 Proposición

Dados los números enteros a_1, a_2, a_3, ..., a_n, se verifica:

$$m.c.m.\,(a_1, a_2, a_3, \ldots, a_n) = m.c.m.\,(a_1, m.c.m.\,(a_2, a_3, \ldots, a_n))$$

Demostración

Sea $m = \text{m.c.m.}\,(a_1, a_2, a_3, \ldots, a_n)$ y $m' = \text{m.c.m.}\,(a_1, \text{m.c.m.}\,(a_2, a_3, \ldots, a_n))$. Entonces, por definición

$$m = \text{m.c.m.}\,(a_1, a_2, a_3, \ldots, a_n) \implies m = \text{Sup}\,\{a_1, a_2, a_3, \ldots, a_n\}$$

por lo tanto m será posterior (múltiplo) de todos los números, es decir,

$$a_1 \,|m \;\text{ y } a_2 \,|m \;\text{ y } a_3 \,|m \;\text{ y } \cdots \text{ y } a_n \,|m \,.$$

Pero si m es posterior (múltiplo) de varios números, entonces, por definición de supremo, será posterior (múltiplo) al supremo de todos ellos, es decir,

$$a_1 \,|m \;\text{ y } \operatorname{Sup}\{a_2, a_3, \ldots, a_n\} \,|m \,.$$

Nuevamente, por la definición de mínimo común múltiplo,

$$a_1 \,|m \;\text{ y } \text{m.c.m.}\,(a_2, a_3, \ldots, a_n) \,|m$$

y, otra vez, por definición de supremo,

$$\operatorname{Sup}\{a_1, \text{m.c.m.}\,(a_2, a_3, \ldots, a_n)\} \,|m$$

y, finalizando, con la de mínimo común múltiplo,

$$\text{m.c.m.}\,(a_1, \text{m.c.m.}\,(a_2, a_3, \ldots, a_n)) \,|m$$

es decir,

$$m' \,|m$$

Por otra parte, por definición,

$$m' = \text{m.c.m.}\,(a_1, \text{m.c.m.}\,(a_2, a_3, \ldots, a_n)) \Longrightarrow m' = \operatorname{Sup}\{a_1, \text{m.c.m.}\,(a_2, a_3, \ldots, a_n)\}$$

y por ser m' el supremo de dos números, deberá ser posterior (múltiplo) de ambos, o sea,

$$a_1 \,|m' \;\text{ y } \text{m.c.m.}\,(a_2, a_3, \ldots, a_n) \,|m'$$

luego, por definición,

$$a_1 \,|m' \;\text{ y } \operatorname{Sup}\{a_2, a_3, \ldots, a_n\} \,|m'$$

y al ser m' posterior (múltiplo) del supremo de $a_2, a_3, \ldots, a_n$, tendrá que ser posterior (múltiplo) de todos ellos, es decir,

$$a_1 \,|m' \;\text{ y } a_2 \,|m' \;\text{ y } a_3 \,|m' \;\text{ y } \cdots \text{ y } a_n \,|m'$$

por tanto, m' ha de ser posterior (múltiplo) del supremo de todos,

$$\operatorname{Sup}\{a_1, a_2, a_3, \ldots, a_n\} \,|m'$$

y, nuevamente, por la definición de mínimo común múltiplo,

$$\text{m.c.m.}\,(a_1, a_2, a_3, \ldots, a_n) \,|m'$$

es decir,

$$m \,|m'$$

Pues bien, como $m \,|m' \;\text{ y } m' \,|m$, por la antisimetría de la relación de divisibilidad, $m = m'$, es decir,

$$\text{m.c.m.}\,(a_1, a_2, a_3, \ldots, a_n) = \text{m.c.m.}\,(a_1, \text{m.c.m.}\,(a_2, a_3, \ldots, a_n))$$

■

13.7.3 Mínimo común múltiplo de dos números

Sean a y b dos números enteros. El entero $m > 0$ es el mínimo común múltiplo de a y b siempre y cuando sea el mínimo del conjunto de los múltiplos comunes a ambos ordenado por la relación de divisibilidad. Es decir,

$$m = m.c.m.(a,b) \iff \begin{cases} 1. \quad a|m \quad y \quad b|m \\ \quad y \\ 2. \quad a|c \quad y \quad b|c \quad \Longrightarrow \quad m|c \end{cases}$$

Demostración

En efecto, según la definición, el mínimo común múltiplo de dos números es el supremo del conjunto formado por ambos ordenado por la relación de divisibilidad. Entonces,

$$\begin{aligned} m = \text{m.c.m.}\,(a,b) &\iff m = \text{Sup}\,\{a,b\} \\ &\iff \begin{cases} 1. \quad m \text{ es cota superior del conjunto } \{a,b\} \text{ en } \mathbb{Z}^+. \\ \text{y} \\ 2. \quad \text{Si } c \text{ es otra cota superior de } \{a,b\} \text{ en } \mathbb{Z}^+, \\ \quad \text{entonces } c \text{ es posterior a } m. \end{cases} \\ &\iff \begin{cases} 1. \quad m \text{ es posterior a } a \text{ y posterior a } b. \\ \text{y} \\ 2. \quad \text{Si } c \text{ es posterior a } a \text{ y posterior a } b, \\ \quad \text{entonces } c \text{ es posterior a } m. \end{cases} \\ &\iff \begin{cases} 1. \quad a|m \quad \text{y} \quad b|m \\ \text{y} \\ 2. \quad a|c \quad \text{y} \quad b|c \quad \Longrightarrow \quad m|c \end{cases} \end{aligned}$$

Nota 13.6 Obsérvese que si llamamos M_a y M_b a los conjuntos formados por los múltiplos de a y b, respectivamente, las condiciones 1. y 2. pueden escribirse, también, de la forma siguiente:

$$\begin{aligned} m = \text{m.c.m.}\,(a,b) &\iff \begin{cases} 1. \quad m \in M_a \quad \text{y} \quad m \in M_b \\ \text{y} \\ 2. \quad c \in M_a \quad \text{y} \quad c \in M_b \quad \Longrightarrow \quad m|c \end{cases} \\ &\iff \begin{cases} 1. \quad m \in (M_a \cap M_b) \\ \text{y} \\ 2. \quad c \in (M_a \cap M_b) \quad \Longrightarrow \quad m|c \end{cases} \\ &\iff m = \text{Mín}\,(M_a \cap M_b) \end{aligned}$$

es decir, m es el mínimo del conjunto de los múltiplos comunes a a y a b.

■

Ejemplo 13.34

Calcular, utilizando la definición, el mínimo común múltiplo de 12 *y* 15.

Solución

Según la nota anterior,

$$m = \text{Mín}\,(M_{12} \cap M_{15})$$

donde M_{12} y M_{15} son los conjuntos integrados, respectivamente, por los múltiplos de 12 y de 15. Pues bien, sea a cualquier entero positivo. Entonces

$$\begin{aligned}
a \in M_{12} \cap M_{15} &\iff \left\{ \begin{array}{l} a \in M_{12} \\ \text{y} \\ a \in M_{15} \end{array} \right. \\
&\iff \left\{ \begin{array}{l} \exists q_1 \in \mathbb{Z} : a = 12 \cdot q_1 \\ \text{y} \\ \exists q_2 \in \mathbb{Z}^+ : a = 15 \cdot q_2 \end{array} \right. \\
&\implies 12q_1 = 15q_2 \\
&\iff \frac{q_1}{q_2} = \frac{15}{12} \\
&\qquad \left. \begin{array}{l} \left\{ \begin{array}{l} \text{m.c.d.}(q_1, q_2) = q \\ \text{y} \\ \text{m.c.d.}(15, 12) = 3 \end{array} \right. \end{array} \right\} \\
&\iff \frac{\frac{q_1}{q}}{\frac{q_2}{q}} = \frac{\frac{15}{3}}{\frac{12}{3}} \\
&\implies \frac{\frac{q_1}{q}}{\frac{q_2}{q}} = \frac{5}{4} \\
&\iff \left\{ \begin{array}{lll} \dfrac{q_1}{q} & = & 5 \\ \text{y} & & \{\text{Fracciones Irreducibles}\} \\ \dfrac{q_2}{q} & = & 4 \end{array} \right. \\
&\iff \left\{ \begin{array}{lll} q_1 & = & 5q,\ q \in \mathbb{Z}^+ \\ \text{y} & & \\ q_2 & = & 4q,\ q \in \mathbb{Z}^+ \end{array} \right. \\
&\implies \left\{ \begin{array}{l} \exists q \in \mathbb{Z}^+ : a = 12 \cdot 5q \\ \text{y} \\ \exists q \in \mathbb{Z}^+ : a = 15 \cdot 4q \end{array} \right. \\
&\iff \exists q \in \mathbb{Z}^+ : a = 60q
\end{aligned}$$

Como a era cualquiera, hemos probado que

$$M_{12} \cap M_{15} \subseteq \left\{n : n = 60q, q \in \mathbb{Z}^+\right\}$$

Veamos la inclusión contraria. En efecto,

$$\begin{aligned}
a \in \{n : n = 60q, q \in \mathbb{Z}^+\} &\iff \exists q \in \mathbb{Z}^+ : a = 60q \\
&\iff \exists q \in \mathbb{Z}^+ : \begin{cases} a = 12(5q) \\ \text{y} \\ a = 15(4q) \end{cases} \\
&\implies \begin{cases} a = 12q_1, \text{ con } q_1 = 5q \in \mathbb{Z}^+ \\ \text{y} \\ a = 15q_2, \text{ con } q_2 = 4q \in \mathbb{Z}^+ \end{cases} \\
&\iff \begin{cases} a \in M_{12} \\ \text{y} \\ a \in M_{15} \end{cases} \\
&\iff a \in M_{12} \cap M_{15}
\end{aligned}$$

Por lo tanto,

$$\left\{n : n = 60q, q \in \mathbb{Z}^+\right\} \subseteq M_{12} \cap M_{15}$$

y por la doble inclusión,

$$M_{12} \cap M_{15} = \left\{n : n = 60q, \ q \in \mathbb{Z}^+\right\}$$

y

$$m = \text{Mín}\left(M_{12} \cap M_{15}\right) = \text{Mín}\left\{n : n = 60q, \ q \in \mathbb{Z}^+\right\} = 60$$

■

13.7.4 Propiedades

Sean a y b dos números enteros positivos. Se verifica:

(a) Si m.c.d.$(a, b) = 1$, entonces m.c.m.$(a, b) = a \cdot b$.

(b) m.c.m.$(ka, kb) = k \cdot$ m.c.m.(a, b), $\forall k \in \mathbb{Z}^+$

(c) m.c.d.$(a, b) \cdot$ m.c.m.$(a, b) = a \cdot b$

Demostración

(a) Si m.c.d.$(a, b) = 1$, entonces m.c.m.$(a, b) = a \cdot b$.

En efecto, sean a y b dos enteros positivos cualesquiera primos entre sí. Según 13.6, $\text{m.c.m.}(a,b) = \text{Mín}\,(M_a \cap M_b)$. Pues bien, sea c cualquier entero positivo. Entonces,

$$
\begin{aligned}
c \in (M_a \cap M_b) &\iff \begin{cases} c \in M_a \\ \text{y} \\ c \in M_b \end{cases} \\
&\iff \begin{cases} \exists q_1 \in \mathbb{Z}^+ : c = aq_1 \\ \text{y} \\ \exists q_2 \in \mathbb{Z}^+ : c = bq_2 \end{cases} \\
&\implies aq_1 = bq_2 \\
&\iff \frac{q_1}{q_2} = \frac{b}{a} \\
&\qquad \left.\begin{cases} \exists q \in \mathbb{Z}^+ : \text{m.c.d.}(q_1, q_2) = q \\ \text{m.c.d.}(a,b) = 1 \end{cases}\right\} \\
&\iff \frac{\frac{q_1}{q}}{\frac{q_2}{q}} = \frac{b}{a} \\
&\iff \begin{cases} \dfrac{q_1}{q} = b \\ \text{y} \qquad \{\text{Fracciones irreducibles}\} \\ \dfrac{q_2}{q} = a \end{cases} \\
&\iff \begin{cases} \exists q \in \mathbb{Z}^+ : q_1 = bq \\ \text{y} \\ \exists q \in \mathbb{Z}^+ : q_2 = aq \end{cases} \\
&\implies \begin{cases} \exists q \in \mathbb{Z}^+ : c = abq \\ \text{y} \\ \exists q \in \mathbb{Z}^+ : c = baq \end{cases} \\
&\iff c \in \{n : n = abq, q \in \mathbb{Z}^+\}
\end{aligned}
$$

De la arbitrariedad de c se sigue que

$$M_a \cap M_b \subseteq \left\{n : n = abq, q \in \mathbb{Z}^+\right\}$$

Recíprocamente,

$$\begin{aligned} c \in \{n : n = abq, q \in \mathbb{Z}^+\} &\iff \exists q \in \mathbb{Z}^+ : c = abq \\ &\iff \exists q \in \mathbb{Z}^+ : \begin{cases} c = a(bq) \\ \text{y} \\ c = b(aq) \end{cases} \\ &\implies \begin{cases} c = aq_1, \text{ con } q_1 = bq \in \mathbb{Z}^+ \\ \qquad\qquad\qquad\qquad \text{y} \\ c = bq_2, \text{ con } q_2 = aq \in \mathbb{Z}^+ \end{cases} \\ &\iff \begin{cases} c \in M_a \\ \text{y} \\ c \in M_b \end{cases} \\ &\iff c \in (M_a \cap M_b) \end{aligned}$$

luego,

$$\left\{n : n = abq, q \in \mathbb{Z}^+\right\} \subseteq (M_a \cap M_b)$$

y de la doble inclusión se sigue que

$$M_a \cap M_b = \left\{n : n = abq, q \in \mathbb{Z}^+\right\}$$

y, por tanto,

$$\text{m.c.m.}(a, b) = \text{Mín}\,(M_a \cap M_b) = \text{Mín}\left\{n : n = abq, q \in \mathbb{Z}^+\right\} = ab$$

(b) $\text{m.c.m.}(ka, kb) = k \cdot \text{m.c.m.}(a, b),\ \forall k \in \mathbb{Z}^+$.

En efecto, sea $m = \text{m.c.m.}\,(a, b)$. Entonces,

1. $$m = \text{m.c.m.}\,(a, b) \implies \begin{cases} a \,|m \implies ka \,|km \\ \text{y} \\ b \,|m \implies kb \,|km \end{cases}$$

   es decir, km es múltiplo común de ka y kb.

2. Veamos que km es el mínimo de los múltiplos comunes a ka y kb. En efecto, supongamos que c es otro múltiplo común de ka y kb. Entonces,

   $$\begin{aligned} &ka \,|c \iff \exists q_1 \in \mathbb{Z} : c = ka \cdot q_1 \implies \frac{c}{k} = a \cdot q_1 \iff a \left| \frac{c}{k} \right. \\ &\text{y} \\ &kb \,|c \iff \exists q_2 \in \mathbb{Z} : c = kb \cdot q_2 \implies \frac{c}{k} = b \cdot q_2 \iff b \left| \frac{c}{k} \right. \end{aligned}$$

   o sea, $\dfrac{c}{k}$ es un múltiplo común de a y b, luego ha de serlo también de su mínimo común múltiplo, m, luego

   $$m \left| \frac{c}{k} \right. \iff \exists q \in \mathbb{Z} : \frac{c}{k} = m \cdot q \iff c = km \cdot q \iff km \,|c$$

   y por lo tanto, c es múltiplo de km.

De 1. y 2. se sigue que

$$\text{m.c.m.}(ka, kb) = km = k \cdot \text{m.c.m.}(a, b)$$

(c) $\text{m.c.d.}(a,b)\cdot\text{m.c.m.}(a,b)=a\cdot b$.

En efecto, por (i) de 13.5.9, si $d=\text{m.c.d.}(a,b)$, entonces $\frac{a}{d}$ y $\frac{b}{d}$ han de ser primos entre sí, es decir, $\text{m.c.d.}\left(\frac{a}{d},\frac{b}{d}\right)=1$, luego por (a),

$$\text{m.c.m.}\left(\frac{a}{d},\frac{b}{d}\right)=\frac{a}{d}\cdot\frac{b}{d}$$

y por (b),

$$\text{m.c.m.}(a,b)=\text{m.c.m.}\left(\frac{d\cdot a}{d},\frac{d\cdot b}{d}\right)=d\cdot\text{m.c.m.}\left(\frac{a}{d},\frac{b}{d}\right)$$

Pues bien,

$$\text{m.c.d.}(a,b)\cdot\text{m.c.m.}(a,b)=d\cdot d\cdot\text{m.c.m.}\left(\frac{a}{d},\frac{b}{d}\right)=d\cdot d\cdot\frac{a}{d}\cdot\frac{b}{d}=a\cdot b$$

■

Ejemplo 13.35

Sean a y b enteros positivos. Demostrar que las tres condiciones siguientes son equivalentes:

(i) $a\,|b$

(ii) $m.c.d.(a,b)=a$

(iii) $m.c.m.(a,b)=b$

Solución

$(i)\Longrightarrow(ii)$.

En efecto, $a\,|a$ y como, por hipótesis, $a\,|b$, tendremos que a es divisor común a a y a b, luego ha de dividir a su máximo común divisor, es decir,

$$a\,|\text{m.c.d.}(a,b)\ .$$

Por otro lado,

$$\text{m.c.d.}(a,b)\,|a$$

y por la antisimetría de la relación de divisibilidad,

$$\text{m.c.d.}(a,b)=a$$

$(ii)\Longrightarrow(iii)$.

En efecto, si $\text{m.c.d.}(a,b)=a$, entonces aplicando (iii) de 13.7.4, tendremos

$$\begin{aligned}\text{m.c.d.}(a,b)\cdot\text{m.c.m.}(a,b)=a\cdot b &\Longrightarrow a\cdot\text{m.c.m.}(a,b)=a\cdot b\\ &\Longrightarrow \text{m.c.m.}(a,b)=b\end{aligned}$$

$(iii)\Longrightarrow(i)$.

En efecto, si $\text{m.c.m.}(a,b)=b$, entonces b es el mínimo de los múltiplos comunes a a y a b, es decir b es múltiplo de a o lo que es lo mismo, a es divisor de b, por lo tanto,

$$a\,|b$$

■

Ejemplo 13.36

Determinar el máximo común divisor y el mínimo común múltiplo de las siguientes parejas de números y expresar, en cada caso, el máximo común divisor como una combinación lineal de ellos.

(a) 2689 *y* 4001

(b) 7982 *y* 7983

Solución

(a) Hallamos el máximo común divisor de 2689 y 4001 mediante el algoritmo de Euclides.

	1	2	20	5	2	2	2
4001	2689	1312	65	12	5	2	1
1312	65	12	5	2	1	0	

luego,

$$\text{m.c.d.}\,(4001, 2689) = 1$$

y, por tanto,

$$\text{m.c.m.}\,(4001, 2689) = 4001 \cdot 2689 = 10758689$$

Expresamos ahora el máximo común divisor como una combinación lineal con coeficientes enteros de 4001 y 2689.

$$\left.\begin{array}{r} 1 = 5 - 2 \cdot 2 \\ 2 = 12 - 2 \cdot 5 \end{array}\right\} \implies \begin{array}{rcl} 1 & = & 5 - 2(12 - 2 \cdot 5) \\ & = & (-2) \cdot 12 + 5 \cdot 5 \end{array}$$

$$\left.\begin{array}{r} 1 = (-2) \cdot 12 + 5 \cdot 5 \\ 5 = 65 - 5 \cdot 12 \end{array}\right\} \implies \begin{array}{rcl} 1 & = & (-2) \cdot 12 + 5(65 - 5 \cdot 12) \\ & = & 5 \cdot 65 + (-27) \cdot 12 \end{array}$$

$$\left.\begin{array}{r} 1 = 5 \cdot 65 + (-27) \cdot 12 \\ 12 = 1312 - 20 \cdot 65 \end{array}\right\} \implies \begin{array}{rcl} 1 & = & 5 \cdot 65 + (-27)(1312 - 20 \cdot 65) \\ & = & (-27) \cdot 1312 + 545 \cdot 65 \end{array}$$

$$\left.\begin{array}{r} 1 = (-27) \cdot 1312 + 545 \cdot 65 \\ 65 = 2689 - 2 \cdot 1312 \end{array}\right\} \implies \begin{array}{rcl} 1 & = & -27 \cdot 1312 + 545(2689 - 2 \cdot 1312) \\ & = & 545 \cdot 2689 + (-1117) \cdot 1312 \end{array}$$

$$\left.\begin{array}{r} 1 = 545 \cdot 2689 + (-1117) \cdot 1312 \\ 1312 = 4001 - 1 \cdot 2689 \end{array}\right\} \implies \begin{array}{rcl} 1 & = & 545 \cdot 2689 + \\ & & (-1117)(4001 - 1 \cdot 2689) \\ & = & (-1117) \cdot 4001 + 1662 \cdot 2689 \end{array}$$

luego la combinación lineal buscada es

$$1 = (-1117) \cdot 4001 + 1662 \cdot 2689$$

(b) Al igual que en el apartado anterior, utilizamos el algoritmo de Euclides para hallar el máximo común divisor de 7982 y 7983.

	1	7982
7983	7982	1
1	0	

luego,

$$\text{m.c.d.}\,(7983, 7982)) = 1$$

y

$$\text{m.c.m.}\,(7983, 7982) = 7983 \cdot 7982 = 63720306$$

La combinación lineal buscada será, por tanto,

$$1 = 7983 + (-1) \cdot 7982$$

■

Ejemplo 13.37

Para cada $a \in \mathbb{Z}^+$, ¿Cuál es el mínimo común múltiplo y el máximo común divisor de a y $a+1$?

Solución

Obsérvese lo siguiente:

Si a es par(impar), entonces $a+1$ es impar(par), luego el único divisor común positivo que tienen es el 1, de aquí que

$$\text{m.c.d.}\,(a, a+1) = 1$$

Si empleamos el algoritmo de Euclides

	1	a
$a+1$	a	1
1	0	

o sea,

$$\text{m.c.d.}\,(a, a+1) = 1$$

De

$$\text{m.c.d.}\,(a, a+1) \cdot \text{m.c.m.}\,(a, a+1) = a(a+1)$$

se sigue que

$$\text{m.c.m.}\,(a, a+1) = a(a+1)$$

■

Ejemplo 13.38

Sean a, b y c tres números enteros positivos tales que a y b son primos entre sí. Probar que si $a\,|c$ y $b\,|c$, entonces $ab\,|c$. ¿Se verifica también si a y b no son primos entre sí?

Solución

En efecto,

$$\left.\begin{array}{l} a\,|c \iff c \text{ es múltiplo de } a \\ \text{y} \\ b\,|c \iff c \text{ es múltiplo de } b \end{array}\right\} \implies c \text{ es múltiplo del m.c.m.}\,(a,b)$$

$$\{\text{m.c.m.}\,(a,b) = ab\}$$

$$\implies c \text{ es múltiplo de } ab$$

$$\iff ab\,|c$$

Si a y b no son primos entre sí, no se verifica la proposición. Por ejemplo

$$4\,|16 \quad \text{y } 8\,|16$$

sin embargo 32 no divide a 16.

■

Ejemplo 13.39

El mínimo común múltiplo de los términos de una fracción es 340. *Determinar dicha fracción sabiendo que no altera su valor si se suma* 20 *al numerador y* 25 *al denominador.*

Solución

Sean a y b el numerador y del denominador de la fracción buscada y sea d el máximo común divisor de ambos números, entonces

$$\frac{a}{b} = \frac{a+20}{b+25} \iff ab + 25a = ab + 20b \iff \frac{a}{b} = \frac{20}{25}$$

y si dividimos numerador y denominador de ambas fracciones por su máximo común divisor, tendremos

$$\frac{\frac{a}{d}}{\frac{b}{d}} = \frac{\frac{20}{5}}{\frac{25}{5}} \implies \frac{\frac{a}{d}}{\frac{b}{d}} = \frac{4}{5} \iff \left\{\begin{array}{l} \dfrac{a}{d} = 4 \\ \text{y} \\ \dfrac{b}{d} = 5 \end{array}\right.$$

Por otra parte,

$$\text{m.c.d.}\,(a,b) \cdot \text{m.c.m.}\,(a,b) = a \cdot b$$

luego,

$$d \cdot 340 = a \cdot b$$

de aquí que

$$\frac{a}{d} = \frac{340}{b} \quad \text{y} \quad \frac{b}{d} = \frac{340}{a}$$

y comparando estas igualdades con las anteriores, tendremos

$$\left.\begin{array}{l} \dfrac{a}{d} = 4 \\ \text{y} \\ \dfrac{a}{d} = \dfrac{340}{b} \end{array}\right\} \implies \frac{340}{b} = 4 \Longrightarrow b = \frac{340}{4} \Longrightarrow b = 85$$

$$\left.\begin{array}{l} \dfrac{b}{d} = 5 \\ \text{y} \\ \dfrac{b}{d} = \dfrac{340}{a} \end{array}\right\} \implies \frac{340}{a} = 5 \Longrightarrow a = \frac{340}{5} \Longrightarrow a = 68$$

■

Ejemplo 13.40

Probar que si dos enteros positivos son primos entre sí, entonces su suma y su producto también lo son.

Solución

Sean a y b enteros positivos cualesquiera. Probaremos que:

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

En efecto, como m.c.d.$(a, b) = 1$, aplicando 13.5.8, podremos encontrar dos enteros p y q tales que

$$pa + qb = 1$$

de aquí que

$$\begin{array}{lcll} pa^2 & + & qab & = & a \\ \text{y} & & & & \\ pab & + & qb^2 & = & b \end{array}$$

Pues bien, sea d un divisor común a ab y $a+b$. Entonces,

$$\left.\begin{array}{l} d\,|ab \\ \text{y} \\ d\,|a+b \implies d\,|a\,(a+b) \end{array}\right\} \implies d\,|ab \text{ y } d\,|a\,(a+b)-ab$$

$$\implies d\,|ab \text{ y } d\,|a^2+ab-ab$$
$$\implies d\,|ab \text{ y } d\,|a^2$$
$$\implies d\,|pa^2+qab$$
$$\implies d\,|a$$

Por otro lado,

$$\left.\begin{array}{l} d\,|ab \\ \text{y} \\ d\,|a+b \implies d\,|b\,(a+b) \end{array}\right\} \implies d\,|ab \text{ y } d\,|b\,(a+b)-ab$$

$$\implies d\,|ab \text{ y } d\,|b^2+ab-ab$$
$$\implies d\,|ab \text{ y } d\,|b^2$$
$$\implies d\,|pab+qb^2$$
$$\implies d\,|b$$

Por tanto, d es un divisor común a a y b, luego será divisor del máximo común divisor de ambos, es decir,

$$d\,|\text{m.c.d.}(a,b) \implies d\,|1 \implies d=1$$

por lo tanto,

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

■

Ejemplo 13.41

Hallar dos números, sabiendo que su suma es 240 *y su mínimo común múltiplo es* 1768.

Solución

Sean a y b los números buscados y sea d su máximo común divisor. Entonces,

$$\text{m.c.d.}(a,b)\cdot\text{m.c.m.}(a,b)=ab \iff d\cdot 1768=ab \implies \frac{ab}{d^2}=\frac{1768d}{d^2} \implies \frac{ab}{d^2}=\frac{1768}{d}$$

Además,

$$a+b=240 \implies \frac{a+b}{d}=\frac{240}{d}$$

luego,

$$\frac{\dfrac{ab}{d^2}}{\dfrac{a+b}{d}}=\frac{1768}{240}$$

Por otra parte, por el ejemplo anterior, (13.40),

$$\text{m.c.d.}(a,b)=d \Longrightarrow \text{m.c.d.}\left(\frac{a}{d},\frac{b}{d}\right)=1 \Longrightarrow \text{m.c.d.}\left(\frac{a}{d}\cdot\frac{a}{d},\frac{a}{d}+\frac{a}{d}\right)=1 \Longrightarrow \text{mc.d.}\left(\frac{ab}{d^2},\frac{a+b}{d}\right)=1$$

Entonces,

$$\begin{aligned}
\frac{\frac{ab}{d^2}}{\frac{a+b}{d}}=\frac{1768}{240} &\Longrightarrow \frac{\frac{ab}{d^2}}{\frac{a+b}{d}}=\frac{\frac{1768}{8}}{\frac{240}{8}} \quad \{\text{m.c.d.}(1768,240)=8\}\\
&\Longrightarrow \frac{\frac{ab}{d^2}}{\frac{a+b}{d}}=\frac{221}{30}\\
&\Longrightarrow \begin{cases} \dfrac{ab}{d^2}=221 \\ \text{y} \qquad\qquad \{\text{Fracciones irreducibles}\} \\ \dfrac{a+b}{d}=30 \end{cases}\\
&\Longrightarrow \begin{cases} \dfrac{a}{d}\cdot\dfrac{b}{d}=13\cdot 17 \\ \text{y} \\ a+b=30d \end{cases}\\
&\Longrightarrow \begin{cases} \dfrac{a}{d}=13 \text{ y } \dfrac{b}{d}=17 \\ \text{o} \\ \dfrac{a}{d}=17 \text{ y } \dfrac{b}{d}=13 \\ \text{y} \\ d=\dfrac{240}{30} \end{cases}\\
&\Longrightarrow \begin{cases} a=13d \text{ y } b=17d \\ \text{o} \\ a=17d \text{ y } b=13d \\ \text{y} \\ d=8 \end{cases}\\
&\Longrightarrow \begin{cases} a=104 \text{ y } b=136 \\ \text{o} \\ a=136 \text{ y } b=104 \end{cases}
\end{aligned}$$

de aquí que los números buscados sean 104 y 136.

■

Lección 14

Teorema Fundamental de la Aritmética

El concepto de número primo se remonta a la antigüedad. Los griegos poseían dicho concepto, así como una larga lista de teoremas y propiedades relacionados con él. Los cuatro ejemplos siguientes aparecen en los *Elementos de Euclides*:

- Todo entero positivo distinto de 1 es un producto de números primos.
- Teorema fundamental de la Aritmética: "Todo entero positivo puede descomponerse de manera única como un producto de números primos".
- Existen infinitos números primos.
- Podemos obtener una lista de los números primos por medio del método conocido como la *Criba de Eratóstenes*.

14.1 Números Primos

Observemos que si a es cualquier número entero mayor que 1, entonces

$$a = a \cdot 1, \text{ con } 1 \in \mathbb{Z}, \text{ es decir, } a \text{ es un divisor de } a.$$

$$a = 1 \cdot a, \text{ con } a \in \mathbb{Z}, \text{ es decir, } 1 \text{ es un divisor de } a.$$

luego todo número entero $a > 1$ tiene, al menos, dos divisores, el 1 y el propio a.

14.1.1 Primos

Diremos que el número entero positivo p es primo si tiene, exactamente, dos divisores positivos, el 1 y el mismo p. Si un número entero no es primo, lo llamaremos compuesto.

En el conjunto de los cien primeros enteros positivos son primos 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89 y 97.

■

14.1.2 Compuestos

Diremos que un número entero positivo es compuesto si tiene más de dos divisores.

En el conjunto de los diez primeros números enteros positivos son compuestos 4, 6, 8, 9 y 10.

■

Nota 14.1 Obsérvese que de la definición de número primo se sigue que

$$p \text{ es primo si, y sólo si es imposible escribir } p = ab \text{ con } a, b \in \mathbb{Z} \text{ y } 1 < a, b < p.$$

■

14.1.3 Proposición

Todo número compuesto posee, al menos, un divisor primo.

Demostración

Probaremos que

$$\forall a \in \mathbb{Z}^+, (a \text{ es compuesto} \Longrightarrow a \text{ tiene, al menos, un divisor primo})$$

Lo haremos por contradicción, es decir supondremos que la proposición anterior es falsa o lo que es igual que su negación es verdadera, o sea,

$$\exists a \in \mathbb{Z}^+ : a \text{ es compuesto y, sin embargo, no tiene divisores primos}$$

En efecto, si llamamos C el conjunto formado por todos los enteros positivos que son compuestos y no tienen divisores primos, entonces C es no vacío ya que, al menos, a estará en C, luego C es un subconjunto no vacío de $\mathbb{Z}^+$. Aplicando el "principio de la buena ordenación" C tendrá mínimo o primer elemento y que llamaremos m. Pues bien,

$$\begin{aligned}
m \in C \Longrightarrow & \begin{cases} m \text{ es compuesto.} \\ \text{y} \\ m \text{ no tiene divisores primos.} \end{cases} \\
\Longrightarrow & \begin{cases} m \text{ tiene más de 2 divisores.} \\ \text{y} \\ m \text{ no tiene divisores primos.} \end{cases} \\
\Longrightarrow & \begin{cases} \text{Hay, al menos, un } m_1 \in \mathbb{Z}^+, \text{ divisor de } m \text{ y distinto de 1 y de } m. \\ \text{y} \\ m_1 \text{ no es primo.} \end{cases} \\
\Longrightarrow & \text{ Hay, al menos, un } m_1 \in \mathbb{Z}^+, \text{ compuesto tal que } m_1 | m \text{ y } 1 < m_1 < m.
\end{aligned}$$

Veamos ahora que m_1 tiene que tener divisores primos.

En efecto, si m_1 no tuviera divisores primos, entonces m_1 sería un entero positivo compuesto y sin divisores primos, es decir, $m_1 \in C$, siendo $m_1 < m$, lo cual es imposible ya que m es el mínimo de C, por lo tanto m_1 ha de tener, al menos, un divisor primo, p. Pero,

$$\left.\begin{array}{l} p|m_1 \\ \text{y} \\ m_1|m \end{array}\right\} \Longrightarrow p|m$$

es decir m tiene un divisor primo lo cual es una contradicción ya que $m \in C$, es decir no tiene divisores primos.

Consecuentemente, la suposición hecha es falsa, y, por lo tanto, si un número es compuesto, entonces ha de tener, al menos, un divisor primo.

■

Euclides demostró en el libro IX de los Elementos que existían infinitos números primos. La argumentación que utilizó ha sido considerada desde siempre como un modelo de elegancia matemática.

14.1.4 Teorema

Existen infinitos números primos.

Demostración

Supongamos lo contrario, es decir la cantidad de números primos existente es finita, pongamos, por ejemplo, que sólo hay k números primos,

$$p_1, p_2, \ldots\ldots, p_k.$$

Pues bien, sea m el producto de todos ellos más 1, es decir,

$$m = p_1 \cdot p_2 \cdot \cdots\cdots \cdot p_k + 1$$

Entonces, obviamente,

$$m > 1, \text{ y } m \neq p_i, \ i = 1, 2, \ldots, k$$

es decir es distinto de todos los primos que existen, luego no puede ser primo, de aquí que sea compuesto y, por el teorema anterior, tendrá, al menos, un divisor primo que tendrá que ser uno de los existentes, o sea, existe p_j con $j \in \{1, 2, \ldots\ldots, k\}$ tal que

$$p_j \,|m$$

y como

$$p_j \,|p_1 \cdot p_2 \cdot \cdots\cdots \cdot p_k$$

entonces dividirá a la diferencia de ambos,

$$p_j \,|m - p_1 \cdot p_2 \cdot \cdots\cdots \cdot p_k$$

luego,

$$p_j \,|1$$

de aquí que $p_j = 1$ ó $p_j = -1$ y esto es imposible ya que p_j es primo.

De la contradicción a la que hemos llegado, se sigue que la suposición hecha es falsa y, por tanto, existen infinitos números primos.

■

Ejemplo 14.1

Demostrar

(a) Todo cuadrado perfecto es de la forma $4k$ ó $4k+1$, con $k \in \mathbb{Z}$.

(b) Ningún número entero de la forma $p_1 \cdot p_2 \cdot \cdots \cdot p_n + 1$ es un cuadrado perfecto (p_n es el $n-$ésimo número primo).

Solución

Antes que nada digamos que un número entero es un cuadrado perfecto, si su raíz cuadrada es entera, es decir,

$$a \in \mathbb{Z} \text{ es cuadrado perfecto} \Longleftrightarrow \sqrt{a} \in \mathbb{Z}$$

Por ejemplo, $1, 4, 9, 16, 25, 36, \cdots$ son cuadrados perfectos.

(a) Probaremos que

$$\forall n \in \mathbb{Z}, (n \text{ es cuadrado perfecto} \longrightarrow \exists q \in \mathbb{Z} : a = 4q \text{ ó } a = 4q+1)$$

En efecto, sea a cualquier entero.

$$\begin{aligned}
a \text{ cuadrado perfecto} &\iff \sqrt{a} \in \mathbb{Z} \\
&\Longrightarrow \exists q_1, r \in \mathbb{Z} : \sqrt{a} = 2q_1 + r, \text{ con } r = 0 \text{ ó } r = 1 \ (13.2.1) \\
&\iff \exists q_1, r \in \mathbb{Z} : a = (2q_1 + r)^2, \text{ con } r = 0 \text{ ó } r = 1 \\
&\iff \exists q_1, r \in \mathbb{Z} : a = 4q_1^2 + 4q_1 r + r^2, \text{ con } r = 0 \text{ ó } r = 1 \\
&\iff \exists q_1, r \in \mathbb{Z} : a = 4\left(q_1^2 + q_1 r\right) + r^2, \text{ con } r = 0 \text{ ó } r = 1 \\
&\quad \left\{\text{Tomando } q \in \mathbb{Z} \text{ tal que } q = q_1^2 + q_1 r\right\} \\
&\iff \exists q \in \mathbb{Z} : \begin{cases} a = 4q \\ \text{o} \\ a = 4q+1 \end{cases}
\end{aligned}$$

luego en cualquier caso, a puede escribirse en la forma $4q$ ó $4q+1$.

(b) Probemos ahora que ningún entero de la forma $p_1 \cdot p_2 \cdot p_3 \cdot \cdots \cdot p_n + 1$ es un cuadrado perfecto (p_n es el $n-$ésimo número primo).

En el apartado (a), hemos probado que

$$\forall n, (n \text{ es cuadrado perfecto} \longrightarrow \exists q \in \mathbb{Z} : a = 4q \text{ ó } a = 4q+1)$$

lo que, usando el contrarrecíproco, equivale a decir

$$\forall n, (n \neq 4q \text{ y } n \neq 4q+1, \forall q \in \mathbb{Z} \longrightarrow n \text{ no es un cuadrado perfecto})$$

y si a es cualquier entero, esto significa que

$$a \neq 4q \text{ y } a \neq 4q+1, \forall q \in \mathbb{Z} \Longrightarrow a \text{ no es un cuadrado perfecto} \tag{14.1}$$

Pues bien, los p_i, para $1 \leqslant i \leqslant n$, son números primos, luego todos, excepto p_1, que es 2, son impares, y como el producto de dos números impares es impar, $p_2 \cdot p_3 \cdots p_n$ es impar, luego.

$$\begin{aligned}
\exists q \in \mathbb{Z} : p_2 \cdot p_3 \cdots p_n = 2q+1 &\Longrightarrow \exists q \in \mathbb{Z} : p_1 \cdot p_2 \cdot p_3 \cdots p_n + 1 = 2(2q+1) + 1 \\
&\Longrightarrow \exists q \in \mathbb{Z} : p_1 \cdot p_2 \cdot p_3 \cdots p_n + 1 = 4q + 3
\end{aligned}$$

Por lo tanto,

$$a = p_1 \cdot p_2 \cdot p_3 \cdots p_n + 1 \Longrightarrow \exists q \in \mathbb{Z} : a = 4q + 3$$

es decir, el resto de dividir a entre 4 es 3 y, al ser único el resto, tendremos que

$$\exists q \in \mathbb{Z} : a = 4q + 3 \Longrightarrow a \neq 4q \text{ y } a \neq 4q + 1, \ \forall q \in \mathbb{Z}$$

y combinando ambos resultados,

$$a = p_1 \cdot p_2 \cdot p_3 \cdots p_n + 1 \Longrightarrow a \neq 4q \text{ y } a \neq 4q + 1, \ \forall q \in \mathbb{Z}$$

y teniendo en cuenta (14.1),

$$a = p_1 \cdot p_2 \cdot p_3 \cdots p_n + 1 \Longrightarrow a \text{ no es un cuadrado perfecto}$$

es decir ningún número entero de la forma $p_1 \cdot p_2 \cdot p_3 \cdots p_n + 1$ es un cuadrado perfecto.

■

14.2 Criba de Eratóstenes

Una vez conocida la existencia de infinitos números primos, se plantea un nuevo problema cual es la forma en que dichos números están distribuidos en el conjunto de los números naturales. Este problema es complicado y se conocen sólo resultados parciales. Un primer método para resolver esta cuestión fue establecido en el siglo III a.c. por Eratóstenes[1]; recibe el nombre de *Criba de Eratóstenes* en honor a su autor y es consecuencia del siguiente teorema cuya primera demostración rigurosa se debe a Fermat.

14.2.1 Teorema

Si un número entero mayor que 1 *no tiene divisores primos menores o iguales que su raíz, entonces es primo.*

Demostración

Sea a entero estrictamente mayor que 1. Utilizamos el método de demostración por la contrarrecíproca, es decir veremos que

si a no es primo, entonces existe, al menos, un divisor primo de a menor o igual que su raíz.

[1] Astrónomo, geógrafo, matemático y filósofo griego (Cirene 284 a.c.-Alejandría 192 a.c.). Vivió durante mucho tiempo en Atenas, antes de ser llamado a Alejandría (245 a.c.) por Tolomeo III, quien le confió la educación de sus hijos y luego la dirección de la biblioteca. Sus aportaciones a los diversos campos de la ciencia fueron muy importantes, pero sobre todo es conocido como matemático, por su célebre *criba* -que conserva su nombre- para encontrar los números primos, y por el *mesolabio*, instrumento de cálculo para resolver el problema de la media proporcional. Fue el primero en medir de un modo exacto la longitud de la circunferencia de la Tierra. Para ello determinó la amplitud del arco meridiano entre Siena y Alejandría: sabiendo que en el solsticio de verano el sol en Siena se hallaba en la vertical del lugar, ya que los rayos penetraban en los pozos más profundos, midió, con la ayuda de la sombra proyectada por un gnomon, el ángulo formado, en Alejandría, por los rayos solares con la vertical. En razón de la propagación rectilínea de los rayos solares y del paralelismo existente entre ellos, el ángulo así medido correspondía al ángulo formado en el centro de la Tierra por el radio terrestre de Siena y el de Alejandría, obteniendo así la amplitud del arco interceptado por estas dos ciudades sobre el meridiano. Luego midió sobre el terreno la dimensión de este arco. Obtuvo para la circunferencia entera, es decir, para el meridiano, 252000 estadios, o sea, casi 40 millones de m. Luego repitió este cálculo, basándose en la distancia de Siena a Méroe, que creyó estaba también sobre el mismo meridiano, y obtuvo un resultado concorde.

En efecto, si a no es primo, entonces es compuesto luego,

$$a = bc, \text{ siendo } 1 < b < a \text{ y } 1 < c < a$$

Pues bien, uno de los divisores de a, b ó c ha de ser menor o igual que la raíz de a. Es decir, $b \leqslant \sqrt{a}$ ó $c \leqslant \sqrt{a}$ ya que si no fuera así tendríamos que

$$\left.\begin{array}{l} b > \sqrt{a} \\ \text{y} \\ c > \sqrt{a} \end{array}\right\} \implies bc > \sqrt{a}\sqrt{a} \implies a > a$$

lo cual, obviamente, es imposible. Supondremos, sin pérdida de generalidad, que $b \leqslant \sqrt{a}$. Ahora puede ocurrir lo siguiente:

- Si b es primo, entonces el teorema estará demostrado ya que

  $$b \text{ es divisor primo de } a \text{ y } b \leqslant \sqrt{a}$$

- Si b no es primo, entonces por la proposición 14.1.2, b tendrá, al menos, un divisor primo p. Entonces,

  $$\left.\begin{array}{l} p|b \\ \text{y} \\ b|a \end{array}\right\} \implies p|a$$

  luego hemos encontrado

  $$p \text{ divisor primo de } a \text{ y } p \leqslant \sqrt{a}$$

  es decir, el teorema estaría probado.

■

14.2.2 Eratóstenes

Veamos como se utiliza el teorema anterior para construir la criba de Eratóstenes y encontrar números primos.

Solución

Partiremos de que los enteros 2 y 3 son primos.

Sea a un número entero mayor que 1 que esté entre los cuadrados de los dos primeros números primos sin que pueda ser el segundo, es decir, $2^2 \leqslant a < 3^2$. Entonces,

$$2^2 \leqslant a < 3^2 \Longrightarrow 2 \leqslant \sqrt{a} < 3$$

luego el único número primo menor o igual que $\sqrt{a}$ sería el 2. Particularizando el teorema anterior, tendríamos

si un número entero entre 4 y 8 no es múltiplo de 2, entonces es primo.

La forma de proceder en la práctica es la siguiente:

⁕ Escribimos todos los números enteros entre 4 y 8.

4 5 6 7 8

- Tachamos los que sean múltiplos de 2.

~~4~~ 5 ~~6~~ 7 ~~8~~

- Los números que no están tachados no son múltiplos de 2, luego son primos, así que ya tenemos todos los números primos que hay entre 2 y 8.

2 3 ~~4~~ 5 ~~6~~ 7 ~~8~~

Tomemos ahora a tal que $3^2 \leqslant a < 5^2$. Entonces,

$$3^2 \leqslant a < 5^2 \Longrightarrow 3 \leqslant \sqrt{a} < 5$$

luego los números primos menores o iguales que la raíz de a son 2 y 3. Particularizando, al igual que antes, el teorema anterior:

si un entero entre 9 y 24 no es múltiplo de 2 ni de 3, entonces es primo.

Procediendo, en la práctica, igual que antes

- Escribimos todos los números enteros entre 9 y 24.

9 10

11 12 13 14 15 16 17 18 19 20

21 22 23 24

- Tachamos los que sean múltiplos de 2.

9 ~~10~~

11 ~~12~~ 13 ~~14~~ 15 ~~16~~ 17 ~~18~~ 19 ~~20~~

21 ~~22~~ 23 ~~24~~

- Tachamos los que sean múltiplos de 3.

9 ~~10~~

11 ~~12~~ 13 ~~14~~ ~~15~~ ~~16~~ 17 ~~18~~ 19 ~~20~~

~~21~~ ~~22~~ 23 ~~24~~

⁕ Los que quedan sin tachar no son múltiplos de 2 ni de 3, por lo tanto, son primos. Añadimos los que teníamos entre 2 y 8 y tendremos todos los números primos entre 2 y 24.

~~2~~ ~~3~~ ~~4~~ ~~5~~ ~~6~~ ~~7~~ ~~8~~ ~~9~~ ~~10~~

~~11~~ ~~12~~ ~~13~~ ~~14~~ ~~15~~ ~~16~~ ~~17~~ ~~18~~ ~~19~~ ~~20~~

~~21~~ ~~22~~ ~~23~~ ~~24~~

Elegimos ahora a tal que $5^2 \leqslant a < 7^2$. Entonces,

$$5^2 \leqslant a < 7^2 \Longrightarrow 5 \leqslant \sqrt{a} < 7$$

luego los números primos menores o iguales que la raíz de a son 2, 3 y 5. Particularizando, de nuevo, el teorema anterior:

si un entero entre 25 y 48 no es múltiplo de 2, ni de 3, ni de 5, entonces es primo.

Procediendo, en la práctica, igual que en los casos anteriores

⁕ Escribimos todos los números enteros entre 25 y 48.

~~25~~ ~~26~~ ~~27~~ ~~28~~ ~~29~~ ~~30~~

~~31~~ ~~32~~ ~~33~~ ~~34~~ ~~35~~ ~~36~~ ~~37~~ ~~38~~ ~~39~~ ~~40~~

~~41~~ ~~42~~ ~~43~~ ~~44~~ ~~45~~ ~~46~~ ~~47~~ ~~48~~

⁕ Tachamos los que sean múltiplos de 2.

25 ~~26~~ 27 ~~28~~ 29 ~~30~~

31 ~~32~~ 33 ~~34~~ 35 ~~36~~ 37 ~~38~~ 39 ~~40~~

41 ~~42~~ 43 ~~44~~ 45 ~~46~~ 47 ~~48~~

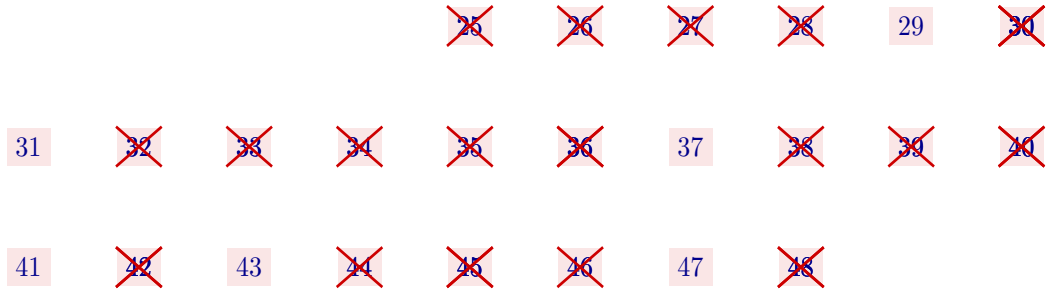
⁕ Tachamos los que sean múltiplos de 3.

25 ~~26~~ ~~27~~ ~~28~~ 29 ~~30~~

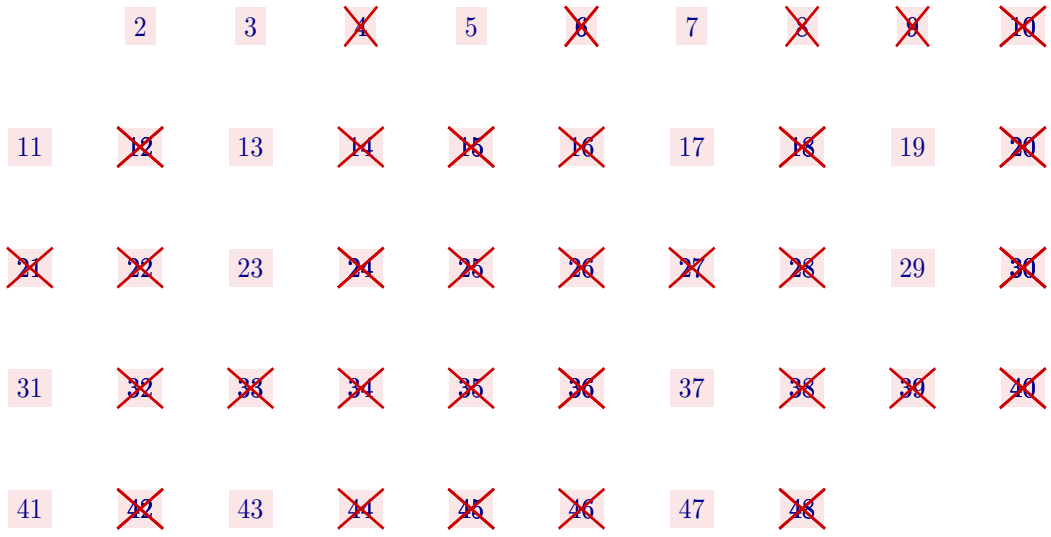
31 ~~32~~ ~~33~~ ~~34~~ 35 ~~36~~ 37 ~~38~~ ~~39~~ ~~40~~

41 ~~42~~ 43 ~~44~~ ~~45~~ ~~46~~ 47 ~~48~~

⁕ Tachamos los que sean múltiplos de 5.



⁕ Los que quedan sin tachar no son múltiplos de 2, ni de 3, ni de 5 y, consecuentemente, son primos. Añadimos los que teníamos entre 2 y 24 y tendremos todos los números primos entre 2 y 48.



El número a estará, ahora, entre 7^2 y 11^2. Pues bien,

$$7^2 \leqslant a < 11^2 \Longrightarrow 7 \leqslant \sqrt{a} < 11$$

luego los números primos menores o iguales que la raíz de a son 2, 3, 5 y 7. Particularizando, de nuevo, el teorema anterior:

si un entero entre 49 y 120 no es múltiplo de 2, ni de 3, ni de 5, ni de 7, entonces es primo.

Procediendo, en la práctica, igual que en los casos anteriores

⁕ Escribimos todos los números enteros entre 49 y 120.

								49	50
51	52	53	54	55	56	57	58	59	60
61	62	63	64	65	66	67	68	69	70
71	72	73	74	75	76	77	78	79	80
81	82	83	84	85	86	87	88	89	90
91	92	93	94	95	96	97	98	99	100
101	102	103	104	105	106	107	108	109	110
111	112	113	114	115	116	117	118	119	120

⋇ Tachamos los que sean múltiplos de 2.

								49	~~50~~
51	~~52~~	53	~~54~~	55	~~56~~	57	~~58~~	59	~~60~~
61	~~62~~	63	~~64~~	65	~~66~~	67	~~68~~	69	~~70~~
71	~~72~~	73	~~74~~	75	~~76~~	77	~~78~~	79	~~80~~
81	~~82~~	83	~~84~~	85	~~86~~	87	~~88~~	89	~~90~~
91	~~92~~	93	~~94~~	95	~~96~~	97	~~98~~	99	~~100~~
101	~~102~~	103	~~104~~	105	~~106~~	107	~~108~~	109	~~110~~
111	~~112~~	113	~~114~~	115	~~116~~	117	~~118~~	119	~~120~~

⁎ Tachamos los que sean múltiplos de 3.

								49	~~50~~
~~51~~	~~52~~	53	~~54~~	55	~~56~~	~~57~~	~~58~~	59	~~60~~
61	~~62~~	~~63~~	~~64~~	65	~~66~~	67	~~68~~	~~69~~	~~70~~
71	~~72~~	73	~~74~~	~~75~~	~~76~~	77	~~78~~	79	~~80~~
~~81~~	~~82~~	83	~~84~~	85	~~86~~	~~87~~	~~88~~	89	~~90~~
91	~~92~~	~~93~~	~~94~~	95	~~96~~	97	~~98~~	~~99~~	~~100~~
101	~~102~~	103	~~104~~	~~105~~	~~106~~	107	~~108~~	109	~~110~~
~~111~~	~~112~~	113	~~114~~	115	~~116~~	~~117~~	~~118~~	119	~~120~~

⁎ Tachamos los que sean múltiplos de 5.

								49	~~50~~
~~51~~	~~52~~	53	~~54~~	~~55~~	~~56~~	~~57~~	~~58~~	59	~~60~~
61	~~62~~	~~63~~	~~64~~	~~65~~	~~66~~	67	~~68~~	~~69~~	~~70~~
71	~~72~~	73	~~74~~	~~75~~	~~76~~	77	~~78~~	79	~~80~~
~~81~~	~~82~~	83	~~84~~	~~85~~	~~86~~	~~87~~	~~88~~	89	~~90~~
91	~~92~~	~~93~~	~~94~~	~~95~~	~~96~~	97	~~98~~	~~99~~	~~100~~
101	~~102~~	103	~~104~~	~~105~~	~~106~~	107	~~108~~	109	~~110~~
~~111~~	~~112~~	113	~~114~~	~~115~~	~~116~~	~~117~~	~~118~~	119	~~120~~

⁎ Tachamos los que sean múltiplos de 7.

~~49~~ ~~50~~

~~51~~ ~~52~~ 53 ~~54~~ ~~55~~ ~~56~~ ~~57~~ ~~58~~ 59 ~~60~~

61 ~~62~~ ~~63~~ ~~64~~ ~~65~~ ~~66~~ 67 ~~68~~ ~~69~~ ~~70~~

71 ~~72~~ 73 ~~74~~ ~~75~~ ~~76~~ ~~77~~ ~~78~~ 79 ~~80~~

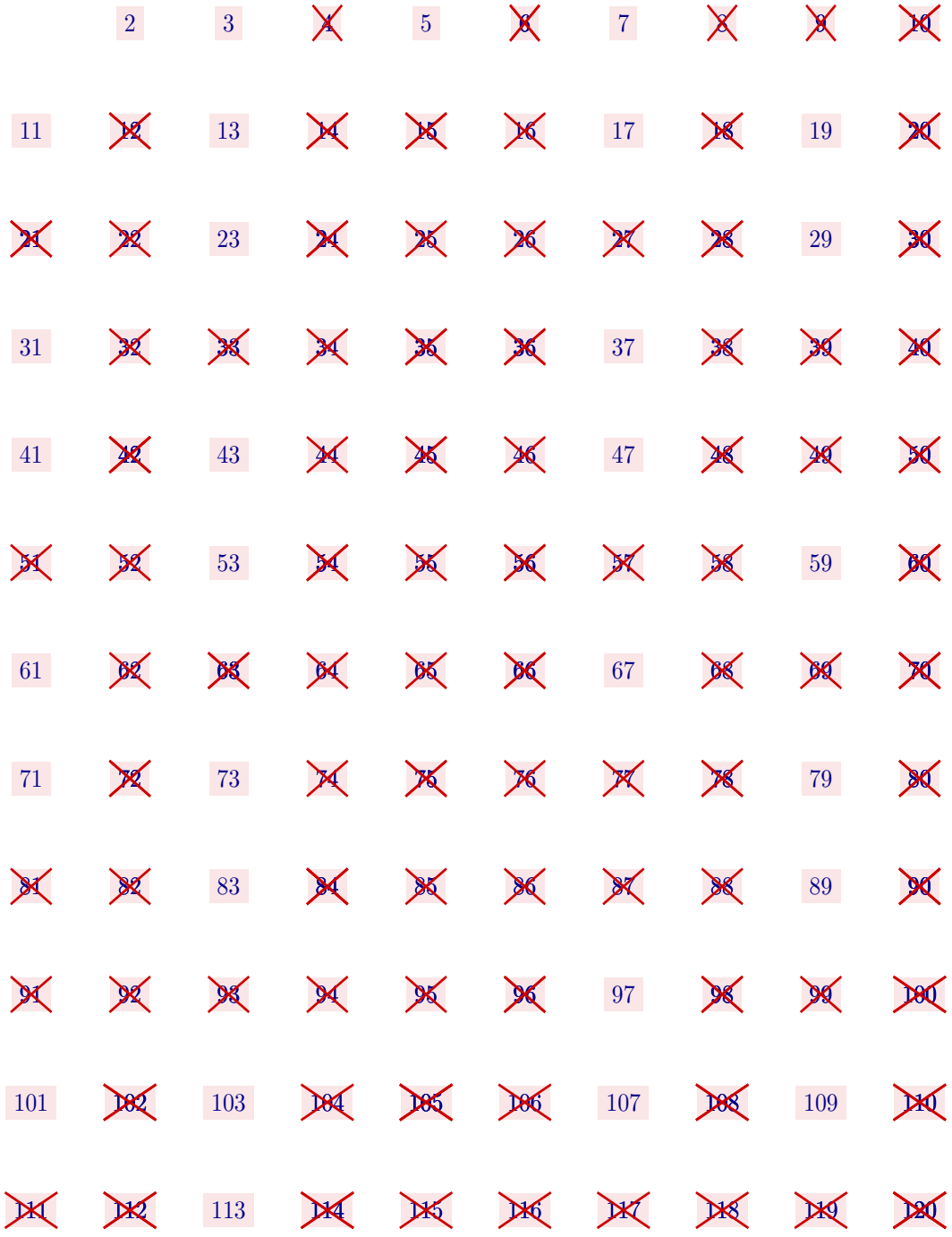
~~81~~ ~~82~~ 83 ~~84~~ ~~85~~ ~~86~~ ~~87~~ ~~88~~ 89 ~~90~~

~~91~~ ~~92~~ ~~93~~ ~~94~~ ~~95~~ ~~96~~ 97 ~~98~~ ~~99~~ ~~100~~

101 ~~102~~ 103 ~~104~~ ~~105~~ ~~106~~ 107 ~~108~~ 109 ~~110~~

~~111~~ ~~112~~ 113 ~~114~~ ~~115~~ ~~116~~ ~~117~~ ~~118~~ ~~119~~ ~~120~~

⁎ Los que quedan sin tachar no son múltiplos de 2, ni de 3, ni de 5, ni de 7 y, por lo tanto, son primos. Añadimos los que teníamos entre 2 y 48 y tendremos todos los números primos entre 2 y 120.



Nota 14.2 Observemos lo siguiente:

(1) Para obtener los números primos entre 4 y 8 hemos eliminado, únicamente, los múltiplos de 2, luego no hay, entre 4 y 8, ningún múltiplo de 3 que no sea, también, múltiplo de 2 ya que si lo hubiera, al no haberlo tachado, sería primo y eso es imposible.

(2) Para encontrar los primos entre 9 y 24, hemos tachado los múltiplos de 2 y de 3, luego entre 9 y 24 no hay, por la misma razón que en el punto anterior, ningún múltiplo de 5 que no sea también, múltiplo de 2, de 3 ó de ambos.

De (1) y (2) se deduce que si queremos obtener los números primos entre 2 y 24 de una sola vez, bastaría con eliminar todos los múltiplos de 2, excepto el 2 y todos los de 3, excepto el 3.

Este mismo razonamiento puede ampliarse a cualquier entero a de forma que si queremos obtener todos los números primos que hay entre 2 y a, bastaría con eliminar los múltiplos de todos los números primos p, excepto el propio p, que sean menores o iguales que la raíz de a, o lo que es igual de cualquier primo p tal que $p^2 \leqslant \sqrt{a}$.

■

Ejemplo 14.2

Obtener todos los números primos que hay entre 2 *y* 200.

Solución

Seguiremos el procedimiento visto en la nota anterior paso a paso.

Primer paso. Escribimos todos los números entre 1 y 200.

	2	3	4	5	6	7	8	9	10
11	12	13	14	15	16	17	18	19	20
21	22	23	24	25	26	27	28	29	30
31	32	33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48	49	50
51	52	53	54	55	56	57	58	59	60
61	62	63	64	65	66	67	68	69	70
71	72	73	74	75	76	77	78	79	80
81	82	83	84	85	86	87	88	89	90
91	92	93	94	95	96	97	98	99	100
101	102	103	104	105	106	107	108	109	110
111	112	113	114	115	116	117	118	119	120
121	122	123	124	125	126	127	128	129	130
131	132	133	134	135	136	137	138	139	140
141	142	143	144	145	146	147	148	149	150
151	152	153	154	155	156	157	158	159	160
161	162	163	164	165	166	167	168	169	170
171	172	173	174	175	176	177	178	179	180
181	182	183	184	185	186	187	188	189	190
191	192	193	194	195	196	197	198	199	200

Segundo paso. $2^2 \leqslant 200$. Eliminamos, por tanto, todos los múltiplos de 2 excepto el 2.

	2	3	~~4~~	5	~~6~~	7	~~8~~	9	~~10~~
11	~~12~~	13	~~14~~	15	~~16~~	17	~~18~~	19	~~20~~
21	~~22~~	23	~~24~~	25	~~26~~	27	~~28~~	29	~~30~~
31	~~32~~	33	~~34~~	35	~~36~~	37	~~38~~	39	~~40~~
41	~~42~~	43	~~44~~	45	~~46~~	47	~~48~~	49	~~50~~
51	~~52~~	53	~~54~~	55	~~56~~	57	~~58~~	59	~~60~~
61	~~62~~	63	~~64~~	65	~~66~~	67	~~68~~	69	~~70~~
71	~~72~~	73	~~74~~	75	~~76~~	77	~~78~~	79	~~80~~
81	~~82~~	83	~~84~~	85	~~86~~	87	~~88~~	89	~~90~~
91	~~92~~	93	~~94~~	95	~~96~~	97	~~98~~	99	~~100~~
101	~~102~~	103	~~104~~	105	~~106~~	107	~~108~~	109	~~110~~
111	~~112~~	113	~~114~~	115	~~116~~	117	~~118~~	119	~~120~~
121	~~122~~	123	~~124~~	125	~~126~~	127	~~128~~	129	~~130~~
131	~~132~~	133	~~134~~	135	~~136~~	137	~~138~~	139	~~140~~
141	~~142~~	143	~~144~~	145	~~146~~	147	~~148~~	149	~~150~~
151	~~152~~	153	~~154~~	155	~~156~~	157	~~158~~	159	~~160~~
161	~~162~~	163	~~164~~	165	~~166~~	167	~~168~~	169	~~170~~
171	~~172~~	173	~~174~~	175	~~176~~	177	~~178~~	179	~~180~~
181	~~182~~	183	~~184~~	185	~~186~~	187	~~188~~	189	~~190~~
191	~~192~~	193	~~194~~	195	~~196~~	197	~~198~~	199	~~200~~

Tercer paso. $3^2 \leqslant 200$. Eliminamos, por tanto, todos los múltiplos de 3 excepto el 3.

	2	3	4	5	6	7	8	9	10
11	12	13	14	15	16	17	18	19	20
21	22	23	24	25	26	27	28	29	30
31	32	33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48	49	50
51	52	53	54	55	56	57	58	59	60
61	62	63	64	65	66	67	68	69	70
71	72	73	74	75	76	77	78	79	80
81	82	83	84	85	86	87	88	89	90
91	92	93	94	95	96	97	98	99	100
101	102	103	104	105	106	107	108	109	110
111	112	113	114	115	116	117	118	119	120
121	122	123	124	125	126	127	128	129	130
131	132	133	134	135	136	137	138	139	140
141	142	143	144	145	146	147	148	149	150
151	152	153	154	155	156	157	158	159	160
161	162	163	164	165	166	167	168	169	170
171	172	173	174	175	176	177	178	179	180
181	182	183	184	185	186	187	188	189	190
191	192	193	194	195	196	197	198	199	200

Cuarto paso. $5^2 \leqslant 200$. Eliminamos, por tanto, todos los múltiplos de 5 excepto el 5.

	2	3	4	5	6	7	8	9	10
11	12	13	14	15	16	17	18	19	20
21	22	23	24	25	26	27	28	29	30
31	32	33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48	49	50
51	52	53	54	55	56	57	58	59	60
61	62	63	64	65	66	67	68	69	70
71	72	73	74	75	76	77	78	79	80
81	82	83	84	85	86	87	88	89	90
91	92	93	94	95	96	97	98	99	100
101	102	103	104	105	106	107	108	109	110
111	112	113	114	115	116	117	118	119	120
121	122	123	124	125	126	127	128	129	130
131	132	133	134	135	136	137	138	139	140
141	142	143	144	145	146	147	148	149	150
151	152	153	154	155	156	157	158	159	160
161	162	163	164	165	166	167	168	169	170
171	172	173	174	175	176	177	178	179	180
181	182	183	184	185	186	187	188	189	190
191	192	193	194	195	196	197	198	199	200

Quinto paso. $7^2 \leqslant 200$. Eliminamos, por tanto, todos los múltiplos de 7 excepto el 7.

	2	3	4	5	6	7	8	9	10
11	12	13	14	15	16	17	18	19	20
21	22	23	24	25	26	27	28	29	30
31	32	33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48	49	50
51	52	53	54	55	56	57	58	59	60
61	62	63	64	65	66	67	68	69	70
71	72	73	74	75	76	77	78	79	80
81	82	83	84	85	86	87	88	89	90
91	92	93	94	95	96	97	98	99	100
101	102	103	104	105	106	107	108	109	110
111	112	113	114	115	116	117	118	119	120
121	122	123	124	125	126	127	128	129	130
131	132	133	134	135	136	137	138	139	140
141	142	143	144	145	146	147	148	149	150
151	152	153	154	155	156	157	158	159	160
161	162	163	164	165	166	167	168	169	170
171	172	173	174	175	176	177	178	179	180
181	182	183	184	185	186	187	188	189	190
191	192	193	194	195	196	197	198	199	200

Sexto paso. $11^2 \leqslant 200$. Eliminamos, por tanto, todos los múltiplos de 11 excepto el 11.

	2	3	4	5	6	7	8	9	10
11	12	13	14	15	16	17	18	19	20
21	22	23	24	25	26	27	28	29	30
31	32	33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48	49	50
51	52	53	54	55	56	57	58	59	60
61	62	63	64	65	66	67	68	69	70
71	72	73	74	75	76	77	78	79	80
81	82	83	84	85	86	87	88	89	90
91	92	93	94	95	96	97	98	99	100
101	102	103	104	105	106	107	108	109	110
111	112	113	114	115	116	117	118	119	120
121	122	123	124	125	126	127	128	129	130
131	132	133	134	135	136	137	138	139	140
141	142	143	144	145	146	147	148	149	150
151	152	153	154	155	156	157	158	159	160
161	162	163	164	165	166	167	168	169	170
171	172	173	174	175	176	177	178	179	180
181	182	183	184	185	186	187	188	189	190
191	192	193	194	195	196	197	198	199	200

Séptimo paso. $13^2 \leqslant 200$. Eliminamos todos los múltiplos de 13 excepto el 13.

	2	3	4	5	6	7	8	9	10
11	12	13	14	15	16	17	18	19	20
21	22	23	24	25	26	27	28	29	30
31	32	33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48	49	50
51	52	53	54	55	56	57	58	59	60
61	62	63	64	65	66	67	68	69	70
71	72	73	74	75	76	77	78	79	80
81	82	83	84	85	86	87	88	89	90
91	92	93	94	95	96	97	98	99	100
101	102	103	104	105	106	107	108	109	110
111	112	113	114	115	116	117	118	119	120
121	122	123	124	125	126	127	128	129	130
131	132	133	134	135	136	137	138	139	140
141	142	143	144	145	146	147	148	149	150
151	152	153	154	155	156	157	158	159	160
161	162	163	164	165	166	167	168	169	170
171	172	173	174	175	176	177	178	179	180
181	182	183	184	185	186	187	188	189	190
191	192	193	194	195	196	197	198	199	200

Octavo paso. $17^2 > 200$. Se acabó. Los números primos entre 1 y 200 son los que no están tachados.

■

14.3 Teorema Fundamental de la Aritmética

En este apartado veremos que cualquier entero a mayor que 1 es primo o puede escribirse como un producto de números primos.

Este resultado, que tiene un equivalente en el libro IX de los *Elementos* de Euclides, se conoce con el nombre de "*Teorema fundamental de la aritmética*".

14.3.1 Lema de Euclides

Si un número entero divide al producto de otros dos y es primo con uno de ellos, entonces divide al tercero.

Demostración

Sean a, b y c tres números enteros cualesquiera. Probaremos que

$$a\,|bc \text{ y m.c.d.}(a,b) = 1 \Longrightarrow a\,|c$$

En efecto, como m.c.d. $(a,b) = 1$, por el corolario 13.5.8, existirán dos números enteros p y q tales que

$$pa + qb = 1$$

Por otra parte, si a divide a bc, como a divide a a, dividirá a cualquier combinación lineal con coeficientes enteros de a y bc. En particular,

$$a|pac + qbc$$

es decir,

$$a|(pa + qb)c$$

luego,

$$\left.\begin{array}{l} a|(pa+qb)c \\ \text{y} \\ pa+qb=1 \end{array}\right\} \Longrightarrow \quad a|c$$

■

14.3.2 Corolario

Una condición necesaria y suficiente para que un número entero mayor que 1 *sea primo es que si divide a un producto de dos enteros, entonces ha de dividir a uno de los dos.*

Demostración

La condición es *suficiente*.

Probaremos que si p es cualquier entero mayor que 1,

$$p \text{ es primo} \Longrightarrow \forall a, b \in \mathbb{Z}\,(p\,|ab \Longrightarrow p\,|a \text{ ó } p\,|b)$$

por contradicción. En efecto, supongamos que la proposición es falsa o lo que es igual, que su negación es verdad. Es decir,

$$p \text{ es primo y } \exists a, b \in \mathbb{Z} : p\,|ab \text{ y } p\not|a \text{ y } p\not|b$$

Sea, pues, p un entero mayor que 1, primo, y a y b, enteros, tales que

$$p\,|ab \text{ y } p\not|a \text{ y } p\not|b$$

Entonces,

$$\begin{aligned}
p \text{ es primo y } p\,|ab \text{ y } p\not|a \text{ y } p\not|b \quad &\Longrightarrow \quad \left\{\begin{array}{l} p \text{ es primo} \\ \text{y} \\ p \text{ no es divisor de } a \\ \text{y} \\ p\,|ab \\ \text{y} \\ p\not|b \end{array}\right. \\
&\Longrightarrow \quad \left\{\begin{array}{l} \text{el único divisor común de } p \text{ y } a \text{ es 1} \\ \text{y} \\ p\,|ab \\ \text{y} \\ p\not|b \end{array}\right. \\
&\Longrightarrow \quad \left\{\begin{array}{l} \text{m.c.d.}(a,b) = 1 \\ \text{y} \\ p\,|ab \\ \text{y} \\ p\not|b \end{array}\right. \\
&\Longrightarrow \quad \left\{\begin{array}{l} p\,|b \quad \{\text{Lema de Euclides}\} \\ \text{y} \\ p\not|b \end{array}\right. \\
&\Longrightarrow \quad \text{Contradicción}
\end{aligned}$$

Si utilizamos la condición de que p no divide a b, la conclusión hubiera sido, p divide a a y p no divide a a y hubiéramos llegado, también, a una contradicción.

La condición es *necesaria*.

Sea p cualquier entero mayor que 1, probaremos que

$$\forall a, b \in \mathbb{Z}\,(p\,|ab \Longrightarrow p\,|a \text{ ó } p\,|b) \Longrightarrow p \text{ es primo}$$

demostrando el contrarrecíproco, es decir,

$$p \text{ no es primo} \Longrightarrow \exists a, b \in \mathbb{Z} : p\,|ab \text{ y } p\not|a \text{ y } p\not|b$$

En efecto,

$$\begin{aligned} p \text{ no es primo} &\implies p \text{ es compuesto} \\ &\implies \exists a \in \mathbb{Z} : a \,|p\,, \text{ con } 1 < a < p \\ &\implies \exists a, b \in \mathbb{Z} : p = ab, \text{ con } 1 < a < p \text{ y } 1 < b < p \\ &\implies p \,|ab \end{aligned}$$

Además, p no puede dividir a a ni a b, ya que

- si p divide a a, entonces
$$p \,|a \implies p \,|a \text{ y } a \,|p \implies p = a$$
lo cual es imposible ya que $a \neq p$.
- si p divide a b, entonces
$$p \,|b \implies p \,|b \text{ y } b \,|p \implies p = b$$
lo cual es imposible ya que $b \neq p$.

luego, si p no es primo, hemos encontrado dos enteros a y b tales que p divide a ab y no divide a a ni a b.

■

14.3.3 Corolario

Si un número primo divide al producto de varios números enteros, entonces ha de dividir, al menos, a uno de ellos.

Demostración

Sea p cualquier número primo, probaremos que

$$p|a_1 \cdot a_2 \cdot a_3 \cdot \cdots \cdot a_n \implies \exists a_i : p|a_i,\ 1 \leqslant i \leqslant n$$

En efecto, supongamos que

$$p \,|a_1 \cdot a_2 \cdot a_3 \cdot \cdots \cdot a_n$$

entonces,

$$p \,|a_1 \cdot (a_2 \cdot a_3 \cdot \cdots \cdot a_n)$$

y aplicando el corolario anterior

$$p \,|a_1 \text{ ó } p \,|a_2 \cdot a_3 \cdot \cdots \cdot a_n$$

- Si $p \,|a_1$, el corolario está demostrado, de lo contrario
$$p \,|a_2 \cdot a_3 \cdot \cdots \cdot a_n$$
luego,
$$p \,|a_2 \cdot (a_3 \cdot \cdots \cdot a_n)$$
y, nuevamente por el corolario anterior,
$$p \,|a_2 \text{ ó } p \,|a_3 \cdot a_4 \cdot \cdots \cdot a_n$$
- Si $p \,|a_2$, el corolario está demostrado, de lo contrario
$$p \,|a_3 \cdot a_4 \cdot \cdots \cdot a_n$$
luego,
$$p \,|a_3 \cdot (a_4 \cdot \cdots \cdot a_n)$$

Repitiendo el proceso un número finito de veces, encontraremos, al menos, un a_i, $1 \leqslant i \leqslant n$, tal que $p \,|a_i$.

■

Ejemplo 14.3

Demostrar que si $p, q_1, q_2, \ldots, q_r$ son primos y $p \,|q_1 \cdot q_2 \cdots q_r$, entonces existe algún $i = 1, 2, \ldots, r$ tal que $p = q_i$

Solución

En efecto, por el corolario 14.3.3 p divide a q_i para algún i entre 1 y r. Ahora bien, como q_i es primo, los únicos divisores que tiene son el 1 y el mismo q_i, y al ser $p > 1$, tendrá que ser necesariamente $p = q_i$.

■

Ejemplo 14.4

Demostrar que el número $\sqrt{2}$ es irracional.

Solución

Si $\sqrt{2}$ fuese racional, entonces podría expresarse como un cociente de dos enteros a y b primos entre sí (fracción irreducible), es decir,

$$\sqrt{2} = \frac{a}{b} : \text{m.c.d.}\,(a, b) = 1$$

Pues bien, elevando al cuadrado ambos miembros de esta igualdad, resulta:

$$\sqrt{2} = \frac{a}{b} \Longrightarrow 2 = \frac{a^2}{b^2} \Longrightarrow a^2 = 2b^2 \Longrightarrow 2 \,|a \cdot a$$

luego por el corolario 14.3.3

$$2 \,|a$$

y, consecuentemente, existe un entero q tal que

$$a = 2q$$

entonces,

$$a = 2q \Longrightarrow a^2 = 4q^2 \Longrightarrow 2b^2 = 4q^2 \Longrightarrow b^2 = 2q^2 \Longrightarrow 2 \,|b^2 \Longrightarrow 2 \,|b \cdot b$$

y, nuevamente por el corolario 14.3.3, se sigue que

$$2 \,|b$$

Así pues, 2 es un divisor común de a y b, lo cual es una contradicción ya que estos dos números son primos entre sí, luego la suposición hecha es falsa y $\sqrt{2}$ es irracional.

■

Ejemplo 14.5

Demostrar que la $\sqrt[3]{5}$ es un número irracional.

Solución

En efecto, supongamos que no lo fuese, entonces existirán dos números enteros a y b primos entre sí tales que

$$\sqrt[3]{5} = \frac{a}{b}$$

elevando al cubo ambos miembros de la igualdad, tendremos

$$5 = \frac{a^3}{b^3} \Longrightarrow a^3 = 5b^3 \Longrightarrow 5 \,|a^3$$

de donde se sigue, al ser 5 un número primo, que

$$5 \,|a$$

luego existe un número entero q tal que

$$a = 5q \Longrightarrow a^3 = 5^3q^3 \Longrightarrow 5b^3 = 5^3q^3 \Longrightarrow b^3 = 5^2q^3 \Longrightarrow 5 \,|b^3$$

por tanto,

$$5 \,|b$$

Concluimos, pues, que 5 es un divisor común de a y de b, lo cual contradice el hecho de que estos dos números sean primos entre sí, luego la suposición hecha es falsa y $\sqrt[3]{5}$ es un número irracional.

■

Ejemplo 14.6

Probar que si a no es la k-ésima potencia de ningún número entero, entonces $\sqrt[k]{a}$ es irracional cualesquiera que sean a y k enteros positivos.

Solución

Sean a y k enteros positivos cumpliendo las condiciones del enunciado y supongamos que $\sqrt[k]{a}$ es un número racional.

Entonces, podrá expresarse como un cociente de dos números enteros primos entre sí, es decir, existirán b y c de $\mathbb{Z}$, tales que

$$\sqrt[k]{a} = \frac{b}{c}, \text{ con m.c.d. } (b, c) = 1$$

elevando a k ambos miembros de esta igualdad, resulta

$$\sqrt[k]{a} = \frac{b}{c} \Longrightarrow a = \frac{b^k}{c^k} \Longrightarrow b^k = a \cdot c^k \Longrightarrow a \,|b^k \,.$$

Si

$$a = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \cdots \cdot p_t^{\alpha_t}$$

es la descomposición de a en factores primos, ha de existir un i entre 1 y t tal que α_i no sea múltiplo de k ya que por hipótesis a no es la k-ésima potencia de un número entero.

Pues bien, como $a \,|b^k$, b^k ha de tener todos los factores primos de a con exponentes iguales o mayores, luego tendremos que

$$p_i^{\alpha_i} \,|b^k$$

y p_i debe aparecer en la descomposición en factores primos de b, luego

$$a = p_i^s q$$

donde q y p_i son primos entre sí y $\alpha_i < k \cdot s$ ya que como vimos anteriormente, α_i no es múltiplo de k, por tanto,

$$b^k = p_i^{ks} \cdot q^k$$

Así pues,

$$\begin{aligned} ac^k = b^k &\implies p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \cdots\cdots p_t^{\alpha_t} \cdot b^k = p_i^{ks} \cdot q^k \\ &\implies p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \cdots\cdots p_{i-1}^{\alpha_i - 1} p_{i+1}^{\alpha_i + 1} \cdot \cdots\cdots p_t^{\alpha_t} \cdot b^k = p_i^{ks-\alpha_i} \cdot q^k \end{aligned}$$

luego,

$$p_i \,|p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \cdots\cdots p_{i-1}^{\alpha_i - 1} p_{i+1}^{\alpha_i + 1} \cdot \cdots\cdots p_t^{\alpha_t} \cdot b^k$$

y como p_i no divide a $p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \cdots\cdots p_t^{\alpha_t}$, entonces

$$p_i \,|c^k$$

y al ser p_i un número primo, se sigue que

$$p_i \,|c$$

y como

$$p_i \,|b$$

tendremos que $p_i \neq 1$ es un divisor común de b y c lo cual contradice el hecho de que b y c sean primos entre sí, por tanto la suposición hecha es falsa y $\sqrt[k]{a}$ es irracional.

■

14.3.4 Teorema Fundamental de la Aritmética

Cualquier número entero mayor que 1 *puede escribirse de manera única, salvo el orden, como un producto de números primos.*

Demostración

Sea a un número entero mayor que 1. Probaremos, primero, que a puede escribirse como un producto de números primos y, posteriormente, veremos que esa descomposición es, salvo en el orden de los factores, única.

⁕ *Descomposición.*

- Si a es primo, consideramos el número como un producto de un sólo factor y el teorema está demostrado.
- Si a no es primo, entonces es compuesto, y la proposición 14.1.3 asegura que tendrá, al menos, un divisor primo.

Sea p_1 el menor divisor primo de a. Entonces existirá un entero a_1 tal que

$$a = p_1 a_1$$

- Si a_1 es primo, entonces el teorema está demostrado.

– Si a_1 no es primo, será compuesto y aplicando de nuevo la proposición 14.1.3 tendrá, al menos, un divisor primo.

Sea p_2 el menor divisor primo de a_1, entonces existirá un entero a_2 tal que

$$a_1 = p_2 a_2, \text{ con } a_1 > a_2$$

sustituyendo esta igualdad en la anterior, tendremos que

$$a = p_1 p_2 a_2$$

Repitiendo el proceso un número finito de veces, obtendremos

$$a_1 > a_2 > a_3 > \cdots > a_{k-1}$$

con

$$a = p_1 p_2 p_3 \cdots p_{k-1} a_{k-1}$$

donde a_{k-1} es primo o es la unidad, entonces tomando $a_{k-1} = p_k$, si es primo o $a_{k-1} = 1$, se sigue que

$$a = p_1 p_2 p_3 \cdots p_{k-1}$$

ó

$$a = p_1 p_2 p_3 \cdots p_{k-1} p_k$$

y a está escrito como un producto de factores primos.

⁕ *Unicidad.* Supongamos lo contrario, es decir a puede descomponerse en producto de factores primos de dos formas distintas:

$$a = p_1 p_2 p_3 \cdots p_k, \text{ siendo los } p_i \text{ primos para } 1 \leqslant i \leqslant k$$

y

$$a = q_1 q_2 q_3 \cdots q_r, \text{ siendo los } q_j \text{ primos para } 1 \leqslant j \leqslant r.$$

Supondremos, también, que el número de factores es distinto, o sea, $k \neq r$. Tomaremos, sin perder generalidad por ello, $k < r$. Pues bien,

$$\begin{aligned} a = p_1(p_2 p_3 \cdots p_k) &\implies p_1 \,|a \\ &\implies p_1 \,|q_1 q_2 q_3 \cdots q_r \\ &\implies p_1 \,|q_j \text{ para algún } j \text{ entre 1 y } r. \text{ \{Corolario 14.3.3\}} \\ &\implies p_1 = q_j, \text{ ya que } q_j \text{ es primo y } p_1 \neq 1. \end{aligned}$$

Podemos suponer que $j = 1$. Si no lo fuese bastaría con cambiar el orden de los factores. Tendremos, pues, que $p_1 = q_1$ y

$$p_1 p_2 p_3 \cdots p_k = p_1 q_2 q_3 \cdots q_r$$

de donde, al ser $p_1 \neq 0$, se sigue que

$$p_2 p_3 \cdots p_k = q_2 q_3 \cdots q_r$$

Sea ahora

$$a_1 = p_2 p_3 \cdots p_k$$

y

$$a_1 = q_2 q_3 \cdots q_r.$$

Entonces $a_1 < a$, y

$$\begin{aligned} a_1 = p_2(p_3p_4\cdots p_k) &\implies p_2 \,|a_1 \\ &\implies p_2 \,|q_2q_3q_4\cdots q_r \\ &\implies p_2 \,|q_j \text{ para algún } j \text{ entre 2 y } r. \text{ \{Corolario 14.3.3\}} \\ &\implies p_2 = q_j, \text{ ya que } q_j \text{ es primo y } p_2 \neq 1. \end{aligned}$$

Y, ahora, podemos suponer que $j = 2$. Bastaría cambiar el orden de los factores si no fuese así. Tendríamos que $p_2 = q_2$ y, por lo tanto,

$$p_2p_3\cdots p_k = p_2q_3\cdots q_r$$

y, al ser $p_2 \neq 0$, tendremos que

$$p_3p_4\cdots p_k = q_3q_4\cdots q_r$$

y llamando

$$a_2 = p_3p_4\cdots p_k$$

y

$$a_2 = q_3q_4\cdots q_r.$$

se tiene que $a_2 < a_1 < a$.

Como $k < r$, si repetimos el proceso $k-1$ veces, tendremos que

$$a_{k-1} = p_k$$

y

$$a_{k-1} = q_kq_{k+1}\cdots q_r.$$

siendo $a_{k-1} < a_{k-2} < \cdots < a_2 < a_1 < a$. Entonces,

$$\begin{aligned} a_{k-1} = p_k &\implies p_k \,|a_{k-1} \\ &\implies p_k \,|q_kq_{k+1}q_{k+2}\cdots q_r \\ &\implies p_k \,|q_j \text{ para algún } j \text{ entre } k \text{ y } r. \text{ \{Corolario 14.3.3\}} \\ &\implies p_k = q_j, \text{ ya que } q_j \text{ es primo y } p_k \neq 1 \end{aligned}$$

y, razonando igual que en los pasos anteriores, podemos suponer que $j = k$, o sea, $p_k = q_k$ y,

$$p_k = q_k \cdot q_{k+1} \cdot \cdots \cdot q_r$$

y al ser $p_k \neq 0$, tendremos

$$1 = q_{k+1} \cdot q_{k+2} \cdot \cdots \cdot q_r$$

de donde se sigue que

$$q_{k+1} = q_{k+2} = \cdots = q_r = 1$$

lo cual es imposible ya que estos números son primos, por tanto, $k = r$ y

$$a = p_1p_2 \cdot p_3\cdots p_k$$

siendo, pues, la descomposición única.

■

14.3.5 Corolario

Sea a un número entero tal que $|a| > 1$, entonces a tiene una factorización única de la forma:

$$a = \pm p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$$

siendo $k \geqslant 1$, los p_k primos distintos con $p_1 < p_2 < \cdots < p_k$ y $\alpha_i \geqslant 1$ para $1 \leqslant i \leqslant k$.

Demostración

Si $|a| > 1$, entonces $a > 1$ ó $a < -1$. Pues bien,

- Si $a > 1$, por el *Teorema fundamental de la aritmética*, a puede descomponerse en factores primos. Agrupamos todos los primos iguales a p_1 en el factor $p_1^{\alpha_1}$, hacemos igual con p_2, p_3, y así sucesivamente hasta p_k, obteniendo así la descomposición pedida.
- Si $a < -1$, entonces $-a > 1$ aplicamos el razonamiento anterior a $-a$ y

$$-a = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k} \Longrightarrow a = -p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$$

■

Ejemplo 14.7

Descomponer en factores primos el número 720.

Solución

Obtendremos una descomposición del tipo anterior.

- Empezamos buscando el divisor más pequeño de 720.
  Como
  $$720 = 2 \cdot 360$$
  dicho divisor es, obviamente, el 2.
- Hacemos lo mismo con el 360.
  Dado que
  $$360 = 2 \cdot 180$$
  el divisor más pequeño de 360 es 2.
- Repetimos el proceso sucesivamente, y

$$\begin{aligned} 180 &= 2 \cdot 90 \\ 90 &= 2 \cdot 45 \\ 45 &= 3 \cdot 15 \\ 15 &= 3 \cdot 5 \\ 5 &= 1 \cdot 5 \end{aligned}$$

Ahora bastaría sustituir cada igualdad en la igualdad anterior, y resultaría

$$720 = 2 \cdot 2 \cdot 2 \cdot 2 \cdot 3 \cdot 3 \cdot 5 = 2^4 \cdot 3^2 \cdot 5$$

En la práctica suelen disponerse los cálculos en la forma siguiente:

720	2
360	2
180	2
90	2
45	3
15	3
5	5
1	

Ahora sólo habrá que contar los números que hay de cada factor, y

$$720 = 2^4 \cdot 3^2 \cdot 5$$

■

14.4 Divisores de un número

14.4.1 Lema

Si a y b son dos números enteros tales que $|a| > 1$ y $|b| > 1$, entonces pueden encontrarse k números primos $p_1, p_2, \ldots, p_k$ y k números enteros $\alpha_i \geqslant 0$ y $\beta_i \geqslant 0$, $1 \leqslant i \leqslant k$ tales que

$$a = \pm p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$$

y

$$b = \pm p_1^{\beta_1} p_2^{\beta_2} \cdots p_k^{\beta_k}$$

siendo $p_1 < p_2 < \cdots < p_k$.

Demostración

La descomposición de a y b se sigue directamente del corolario 14.3.5.

Si hay algún factor primo de a que no lo sea de b se introduce en la factorización de éste con exponente cero y análogamente se hace con los factores de b que no lo sean de a.

■

Ejemplo 14.8

Descomponer $a = 270$ y $b = 368$ en factores primos según el lema anterior.

Solución

$$\begin{array}{r|l} 270 & 2 \\ 135 & 3 \\ 45 & 3 \\ 15 & 3 \\ 5 & 5 \\ 1 & \end{array} \quad \Longrightarrow \quad 270 = 2 \cdot 3^3 \cdot 5$$

$$\begin{array}{r|l} 368 & 2 \\ 184 & 2 \\ 92 & 2 \\ 46 & 2 \\ 23 & 23 \\ 1 & \end{array} \quad \Longrightarrow \quad 368 = 2^4 \cdot 23$$

Ahora bastaría escribir,

$$270 = 2^2 \cdot 3^2 \cdot 5 \cdot 23^0$$
$$368 = 2^4 \cdot 3^0 \cdot 5^0 \cdot 23$$

para tener los números en la forma descrita en el lema.

■

14.4.2 Criterio General de Divisibilidad

Sean a y b dos números enteros tales que $|a|, |b| > 1$. Se verifica que a es divisible por b si, y sólo si a tiene, al menos, todos los factores primos de b con exponentes iguales o mayores.

Demostración

Sean a y b dos enteros cualesquiera de valor absoluto mayor que 1. Observemos lo siguiente:

$$\left.\begin{array}{l} |a| > 1 \\ \text{y} \\ |b| > 1 \end{array}\right\} \Longrightarrow \left\{\begin{array}{l} a > 1 \quad \text{ó} \quad a < -1 \\ \text{y} \\ b > 1 \quad \text{ó} \quad b < -1 \end{array}\right.$$

$$\Longrightarrow \left\{\begin{array}{l} 1. \quad a > 1 \quad \text{y} \quad b > 1 \\ \text{ó} \\ 2. \quad a > 1 \quad \text{y} \quad b < -1 \\ \text{ó} \\ 3. \quad a < -1 \quad \text{y} \quad b > 1 \\ \text{ó} \\ 4. \quad a < -1 \quad \text{y} \quad b < -1 \end{array}\right.$$

1. $a > 1$ y $b > 1$.

"Sólo si". En efecto, supongamos que a es divisible por b. Entonces

$$\begin{aligned} a \text{ es divisible por } b &\iff \frac{a}{b} \in \mathbb{Z} \\ &\iff \exists q \in \mathbb{Z} : \frac{a}{b} = q \\ &\iff \exists q \in \mathbb{Z} : a = b \cdot q \end{aligned}$$

Aplicamos el lema anterior (14.4.1) y podemos escribir b y q en la forma,

$$b = p_1^{\beta_1} p_2^{\beta_2} \cdots p_k^{\beta_k}, \text{con } \beta_i \geqslant 0,\ 1 \leqslant i \leqslant k \tag{14.2}$$

$$q = p_1^{\gamma_1} p_2^{\gamma_2} \cdots p_k^{\gamma_k}, \text{con } \gamma_i \geqslant 0,\ 1 \leqslant i \leqslant k$$

donde en las factorizaciones anteriores se verifica:

$\beta_i = 0$, si p_i no está en la descomposición en factores primos de q,

y

$\gamma_i = 0$, si p_i no está en la descomposición en factores primos de b

y, por lo tanto,

$$\left.\begin{array}{l} \beta_i = 0 \text{ en } b \implies \gamma_i \geqslant 1 \text{ en } q \\ \text{y} \\ \gamma_i = 0 \text{ en } q \implies \beta_i \geqslant 1 \text{ en } b \end{array}\right\} \implies \beta_i + \gamma_i \geqslant 1,\ 1 \leqslant i \leqslant k$$

Entonces,

$$a = p_1^{\beta_1+\gamma_1} p_2^{\beta_2+\gamma_2} \cdots p_k^{\beta_k+\gamma_k}, \text{con } \beta_i + \gamma_i \geqslant 1,\ 1 \leqslant i \leqslant k$$

y tomando $\alpha_i = \beta_i + \gamma_i$ para cada $i = 1, 2, \cdots, k$, tendremos

$$a = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}, \text{con } \alpha_i \geqslant 1,\ 1 \leqslant i \leqslant k$$

siendo,

$$\alpha_i = \beta_i + \gamma_i,\ \text{con } \gamma_i \geqslant 0 \Longrightarrow \alpha_i \geqslant \beta_i,\ \text{para } 1 \leqslant i \leqslant k$$

y a tiene, al menos, todos los factores primos de b ya que en la factorización (14.2) puede haber algún(os) β_i iguales a cero.

"Si". En efecto, supongamos que a tiene, al menos, todos los factores primos de b con exponentes iguales o mayores. Entonces, si la descomposición en factores primos de b (14.3.5) es:

$$b = p_1^{\beta_1} p_2^{\beta_2} \cdots p_j^{\beta_j}, \text{con } \beta_i \geqslant 0,\ 1 \leqslant i \leqslant j$$

la factorización de a debe ser:

$$a = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_j^{\alpha_j} \cdot p_{j+1}^{\alpha_{j+1}} \cdots p_k^{\alpha_k}, \text{con} \begin{cases} \alpha_i \geqslant \beta_i, \text{ si } 1 \leqslant i \leqslant j \\ \text{y} \\ \alpha_i \geqslant 0, \text{ si } j+1 \leqslant i \leqslant k \end{cases}$$

si ahora completamos la descomposición de b añadiendo, con exponente cero, los factores primos de a que le faltan,

$$b = p_1^{\beta_1} p_2^{\beta_2} \cdots p_j^{\beta_j} \cdot p_{j+1}^{\beta_{j+1}} \cdots p_k^{\beta_k}, \text{con} \begin{cases} \beta_i \geqslant 1, \text{ si } 1 \leqslant i \leqslant j \\ \text{y} \\ \beta_i = 0, \text{ si } j+1 \leqslant i \leqslant k \end{cases}$$

y finalmente, dividimos a entre b,

$$\frac{a}{b} = \frac{p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}}{p_1^{\beta_1} p_2^{\beta_2} \cdots p_k^{\beta_k}} = p_1^{\alpha_1-\beta_1} p_2^{\alpha_2-\beta_2} \cdots p_k^{\alpha_k-\beta_k}$$

y como

$$\alpha_i \geqslant \beta_i \Longrightarrow \alpha_i - \beta_i \geqslant 0, \text{ para } 1 \leqslant i \leqslant k$$

tendremos que $\frac{a}{b}$ es un número entero y, consecuentemente, a es divisible por b.

2. $a > 1$ y $b < -1$. Como $-b > 1$ bastaría aplicar la demostración anterior a a y a $-b$.
3. $a < -1$ y $b > 1$. Al ser $-a > 1$, aplicaríamos la demostración anterior a $-a$ y a b.
4. $a < -1$ y $b < -1$. Como $-a > 1$ y $-b > 1$, al igual que en los casos anteriores, bastaría con aplicar la demostración anterior a $-a$ y a $-b$.

■

14.4.3 Divisores de un número

Obtendremos los divisores de cualquier entero de valor absoluto mayor que 1.

Demostración

Sea a cualquier entero tal que $|a| > 1$. Entonces,

$$|a| > 1 \implies \begin{cases} 1.\ a > 1 \\ \text{ó} \\ 2.\ a < -1 \end{cases}$$

Estudiaremos ambos casos.

1. $a > 1$. Por el corolario 14.3.5, a admite una descomposición única,

   $$a = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \cdots \cdot p_k^{\alpha_k}$$

   siendo $k \geqslant 1$, los p_k primos distintos con $p_1 < p_2 < \cdots < p_k$ y $\alpha_i \geqslant 1$ para $1 \leqslant i \leqslant k$. Pues bien, sea b cualquier entero distinto de cero. Entonces,

   $$b \neq 0 \implies \begin{cases} 1.\ b > 0 \\ \text{ó} \\ 2.\ b < 0 \end{cases}$$

   Analizaremos, también, ambos casos.

   1.1 $b > 0$. Sea, pues, D_a el conjunto formado por los divisores de a. Entonces,

   $$\begin{aligned} b \in D_a &\iff b \text{ es divisor de } a \\ &\iff a \text{ es divisible por } b \\ &\iff \begin{cases} a \text{ tiene en su descomposición, al menos, todos los factores} \\ \text{primos de } b \text{ con exponentes iguales o mayores.} \end{cases} \\ &\iff \begin{cases} b \text{ tiene en su descomposición, a lo sumo, todos los factores} \\ \text{primos de } a \text{ con exponentes iguales o menores.} \end{cases} \\ &\iff b = p_1^{\beta_1} \cdot p_2^{\beta_2} \cdot \cdots \cdot p_k^{\beta_k}, \text{con } 0 \leqslant \beta_i \leqslant \alpha_i,\ 1 \leqslant i \leqslant k \end{aligned}$$

y como b es entero, los β_i han de ser no negativos. Por tanto,

$$D_a = \left\{ p_1^{\beta_1} \cdot p_2^{\beta_2} \cdot \cdots\cdots \cdot p_k^{\beta_k}, \text{con } 0 \leqslant \beta_i \leqslant \alpha_i,\ 1 \leqslant i \leqslant k \right\}$$

será el conjunto de los divisores positivos de a.

1.2 $b < 0$. En este caso $-b > 0$, aplicamos a $-b$ lo que acabamos de hacer y,

$$D_a = \left\{ -p_1^{\beta_1} \cdot p_2^{\beta_2} \cdot \cdots\cdots \cdot p_k^{\beta_k}, \text{con } 0 \leqslant \beta_i \leqslant \alpha_i,\ 1 \leqslant i \leqslant k \right\}$$

es el conjunto formado por los divisores negativos de a.

El conjunto de todos los divisores de a será, por tanto,

$$D_a = \left\{ \pm p_1^{\beta_1} \cdot p_2^{\beta_2} \cdot \cdots\cdots \cdot p_k^{\beta_k}, \text{con } 0 \leqslant \beta_i \leqslant \alpha_i,\ 1 \leqslant i \leqslant k \right\}$$

2. $a < -1$. En este caso,

$$a < -1 \Longrightarrow -a > 1$$

aplicamos todo lo que hicimos en el caso anterior a $-a$ y tendremos:

$$D_{-a} = \left\{ \pm p_1^{\beta_1} \cdot p_2^{\beta_2} \cdot \cdots\cdots \cdot p_k^{\beta_k}, \text{con } 0 \leqslant \beta_i \leqslant \alpha_i,\ 1 \leqslant i \leqslant k \right\}$$

De 1. y 2. se sigue que:

$$D_{|a|} = \left\{ \pm p_1^{\beta_1} \cdot p_2^{\beta_2} \cdot \cdots\cdots \cdot p_k^{\beta_k}, \text{con } 0 \leqslant \beta_i \leqslant \alpha_i,\ 1 \leqslant i \leqslant k \right\}$$

■

14.4.4 Método para la obtención de todos los divisores de un número

Expondremos un método basado en el apartado anterior para calcular todos los divisores de cualquier entero de valor absoluto mayor que 1.

Demostración

Sea a un entero tal que $|a| > 1$. Según hemos visto en el apartado anterior,

$$D_{|a|} = \left\{ \pm p_1^{\beta_1} \cdot p_2^{\beta_2} \cdot \cdots\cdots \cdot p_k^{\beta_k}, \text{con } 0 \leqslant \beta_i \leqslant \alpha_i,\ 1 \leqslant i \leqslant k \right\}$$

Calcularemos, únicamente, los divisores positivos ya que sólo hay que cambiar el signo a éstos para obtener los negativos. Haremos una tabla con todos los divisores procediendo de la forma siguiente:

⁕ Divisores de la forma $p_1^{\beta_1} \cdot p_2^0 \cdot p_3^0 \cdot \cdots\cdots \cdot p_k^0$ con $0 \leqslant \beta_1 \leqslant \alpha_1$. Escribimos todas las potencias de p_1.

p_1^0	p_1	p_1^2	$\cdots\cdots$	$p_1^{\alpha_1}$

⁕ Divisores de la forma $p_1^{\beta_1} \cdot p_2^{\beta_2} \cdot p_3^0 \cdot \cdots \cdot p_k^0$ con $0 \leqslant \beta_1 \leqslant \alpha_1$ y $0 \leqslant \beta_2 \leqslant \alpha_2$. Bastaría multiplicar cada uno de los anteriores por todas las potencias de p_2 a partir de p_2^1.

	p_1^0	p_1	p_1^2	$\cdots\cdots$	$p_1^{\alpha_1}$
$\times p_2$	$p_1^0 p_2$	$p_1 p_2$	$p_1^2 p_2$	$\cdots\cdots$	$p_1^{\alpha_1} p_2$
$\times p_2^2$	$p_1^0 p_2^2$	$p_1 p_2^2$	$p_1^2 p_2^2$	$\cdots\cdots$	$p_1^{\alpha_1} p_2^2$
$\times p_2^3$	$p_1^0 p_2^3$	$p_1 p_2^3$	$p_1^2 p_2^3$	$\cdots\cdots$	$p_1^{\alpha_1} p_2^3$
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots \quad \vdots$	$\vdots$
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots \quad \vdots$	$\vdots$
$\times p_2^{\alpha_2}$	$p_1^0 p_2^{\alpha_2}$	$p_1 p_2^{\alpha_2}$	$p_1^2 p_2^{\alpha_2}$	$\cdots\cdots$	$p_1^{\alpha_1} p_2^{\alpha_2}$

⁕ Divisores de la forma $p_1^{\beta_1} \cdot p_2^{\beta_2} \cdot p_3^{\beta_3} \cdot p_4^0 \cdot \cdots \cdot p_k^0$ con

$$0 \leqslant \beta_1 \leqslant \alpha_1,\ 0 \leqslant \beta_2 \leqslant \alpha_2 \text{ y } 0 \leqslant \beta_3 \leqslant \alpha_3.$$

Multiplicamos cada uno de los anteriores por todas las potencias de p_3 desde p_3^1.

	p_1^0	p_1	p_1^2	$\cdots\cdots$	$p_1^{\alpha_1}$
$\times p_2$	$p_1^0 p_2$	$p_1 p_2$	$p_1^2 p_2$	$\cdots\cdots$	$p_1^{\alpha_1} p_2$
$\times p_2^2$	$p_1^0 p_2^2$	$p_1 p_2^2$	$p_1^2 p_2^2$	$\cdots\cdots$	$p_1^{\alpha_1} p_2^2$
$\times p_2^3$	$p_1^0 p_2^3$	$p_1 p_2^3$	$p_1^2 p_2^3$	$\cdots\cdots$	$p_1^{\alpha_1} p_2^3$
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots \quad \vdots$	$\vdots$
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots \quad \vdots$	$\vdots$
$\times p_2^{\alpha_2}$	$p_1^0 p_2^{\alpha_2}$	$p_1 p_2^{\alpha_2}$	$p_1^2 p_2^{\alpha_2}$	$\cdots\cdots$	$p_1^{\alpha_1} p_2^{\alpha_2}$
$\times p_3$	$p_1^0 p_3$	$p_1 p_3$	$p_1^2 p_3$	$\cdots\cdots$	$p_1^{\alpha_1} p_3$
	$p_1^0 p_2 p_3$	$p_1 p_2 p_3$	$p_1^2 p_2 p_3$	$\cdots\cdots$	$p_1^{\alpha_1} p_2 p_3$
	$p_1^0 p_2^2 p_3$	$p_1 p_2^2 p_3$	$p_1^2 p_2^2 p_3$	$\cdots\cdots$	$p_1^{\alpha_1} p_2^2 p_3$
	$p_1^0 p_2^3 p_3$	$p_1 p_2^3 p_3$	$p_1^2 p_2^3 p_3$	$\cdots\cdots$	$p_1^{\alpha_1} p_2^3 p_3$
	$\vdots$	$\vdots$	$\vdots$	$\vdots \quad \vdots$	$\vdots$
	$\vdots$	$\vdots$	$\vdots$	$\vdots \quad \vdots$	$\vdots$
	$p_1^0 p_2^{\alpha_2} p_3$	$p_1 p_2^{\alpha_2} p_3$	$p_1^2 p_2^{\alpha_2} p_3$	$\cdots\cdots$	$p_1^{\alpha_1} p_2^{\alpha_2} p_3$
$\times p_3^2$	$p_1^0 p_3^2$	$p_1 p_3^2$	$p_1^2 p_3^2$	$\cdots\cdots$	$p_1^{\alpha_1} p_3^2$
	$p_1^0 p_2 p_3^2$	$p_1 p_2 p_3^2$	$p_1^2 p_2 p_3^2$	$\cdots\cdots$	$p_1^{\alpha_1} p_2 p_3^2$
	$p_1^0 p_2^2 p_3^2$	$p_1 p_2^2 p_3^2$	$p_1^2 p_2^2 p_3^2$	$\cdots\cdots$	$p_1^{\alpha_1} p_2^2 p_3^2$
	$p_1^0 p_2^3 p_3^2$	$p_1 p_2^3 p_3^2$	$p_1^2 p_2^3 p_3^2$	$\cdots\cdots$	$p_1^{\alpha_1} p_2^3 p_3^2$
	$\vdots$	$\vdots$	$\vdots$	$\vdots \quad \vdots$	$\vdots$
	$\vdots$	$\vdots$	$\vdots$	$\vdots \quad \vdots$	$\vdots$
	$p_1^0 p_2^{\alpha_2} p_3^2$	$p_1 p_2^{\alpha_2} p_3^2$	$p_1^2 p_2^{\alpha_2} p_3^2$	$\cdots\cdots$	$p_1^{\alpha_1} p_2^{\alpha_2} p_3^2$
	$\vdots$	$\vdots$	$\vdots$	$\vdots \quad \vdots$	$\vdots$
	$\vdots$	$\vdots$	$\vdots$	$\vdots \quad \vdots$	$\vdots$
$\times p_3^{\alpha_3}$	$p_1^0 p_3^{\alpha_3}$	$p_1 p_3^{\alpha_3}$	$p_1^2 p_3^{\alpha_3}$	$\cdots\cdots$	$p_1^{\alpha_1} p_3^{\alpha_3}$
	$p_1^0 p_2 p_3^{\alpha_3}$	$p_1 p_2 p_3^{\alpha_3}$	$p_1^2 p_2 p_3^{\alpha_3}$	$\cdots\cdots$	$p_1^{\alpha_1} p_2 p_3^{\alpha_3}$
	$p_1^0 p_2^2 p_3^{\alpha_3}$	$p_1 p_2^2 p_3^{\alpha_3}$	$p_1^2 p_2^2 p_3^{\alpha_3}$	$\cdots\cdots$	$p_1^{\alpha_1} p_2^2 p_3^{\alpha_3}$
	$p_1^0 p_2^3 p_3^{\alpha_3}$	$p_1 p_2^3 p_3^{\alpha_3}$	$p_1^2 p_2^3 p_3^{\alpha_3}$	$\cdots\cdots$	$p_1^{\alpha_1} p_2^3 p_3^{\alpha_3}$
	$\vdots$	$\vdots$	$\vdots$	$\vdots \quad \vdots$	$\vdots$
	$\vdots$	$\vdots$	$\vdots$	$\vdots \quad \vdots$	$\vdots$
	$p_1^0 p_2^{\alpha_2} p_3^{\alpha_3}$	$p_1 p_2^{\alpha_2} p_3^{\alpha_3}$	$p_1^2 p_2^{\alpha_2} p_3^{\alpha_3}$	$\cdots\cdots$	$p_1^{\alpha_1} p_2^{\alpha_2} p_3^{\alpha_3}$

⋇ Así sucesivamente hasta obtener todos los divisores de la forma

$$p_1^{\beta_1} \cdot p_2^{\beta_2} \cdot p_3^{\beta_3} \cdots p_k^{\beta_k}$$

siendo,

$$\begin{array}{l} 0 \leqslant \beta_1 \leqslant \alpha_1 \\ 0 \leqslant \beta_2 \leqslant \alpha_2 \\ 0 \leqslant \beta_3 \leqslant \alpha_3 \\ \cdots\cdots\cdots \\ 0 \leqslant \beta_k \leqslant \alpha_k \end{array}$$

■

Ejemplo 14.9

Calcular todos los divisores de 604800.

Solución

Descomponemos el número dado en factores primos.

$$\begin{array}{r|l} 604800 & 2 \\ 302400 & 2 \\ 151200 & 2 \\ 75600 & 2 \\ 37800 & 2 \\ 18900 & 2 \\ 9450 & 2 \\ 4725 & 3 \\ 1575 & 3 \\ 525 & 3 \\ 175 & 5 \\ 35 & 5 \\ 7 & 7 \\ 1 & \end{array} \quad \Longrightarrow \quad 604800 = 2^7 \cdot 3^3 \cdot 5^2 \cdot 7$$

Hacemos una tabla con todos los divisores de 604800 utilizando el método visto en el apartado anterior.

	1	2	4	8	16	32	64	128
$\times 3$	3	6	12	24	48	96	192	384
$\times 3^2$	9	18	36	72	144	288	576	1152
$\times 3^3$	27	54	108	216	432	864	1728	3456
$\times 5$	5	10	20	40	80	160	320	640
	15	30	60	120	240	480	960	1920
	45	90	180	360	720	1440	2880	5760
	135	270	540	1080	2160	4320	8640	17280
$\times 5^2$	25	50	100	200	400	800	1600	3200
	75	150	300	600	1200	2400	4800	9600
	225	450	900	1800	3600	7200	14400	28800
	675	1350	2700	5400	10800	21600	43200	86400
$\times 7$	7	14	28	56	112	224	448	896
	21	42	84	168	336	672	1344	2688
	63	126	252	504	1008	2016	4032	8064
	189	378	756	1512	3024	6048	12096	24192
	35	70	140	280	560	1120	2240	4480
	105	210	420	840	1680	3360	6720	13440
	315	630	1260	2520	5040	10080	20160	40320
	945	1890	3780	7560	15120	30240	60480	120960
	175	350	700	1400	2800	5600	11200	22400
	525	1050	2100	4200	8400	16800	33600	67200
	1575	3150	6300	12600	25200	50400	100800	201600
	4725	9450	18900	37800	75600	151200	302400	604800

■

14.4.5 Número de divisores de un número compuesto

Si a es un entero de valor absoluto mayor que 1 y $a = p_1^{\alpha_1} p_2^{\alpha_2} \cdot \cdots \cdot p_k^{\alpha_k}$ es su descomposición en factores primos, entonces el número de divisores de a es

$$N_a = (\alpha_1 + 1)(\alpha_2 + 1) \cdot \cdots \cdot (\alpha_k + 1)$$

Demostración

En efecto, según vimos en 14.4.3, los divisores de a son los elementos del conjunto

$$D_a = \left\{ p_1^{\beta_1} \cdot p_2^{\beta_2} \cdot \cdots \cdot p_k^{\beta_k}, \text{con } 0 \leqslant \beta_i \leqslant \alpha_i,\ 1 \leqslant i \leqslant k \right\}.$$

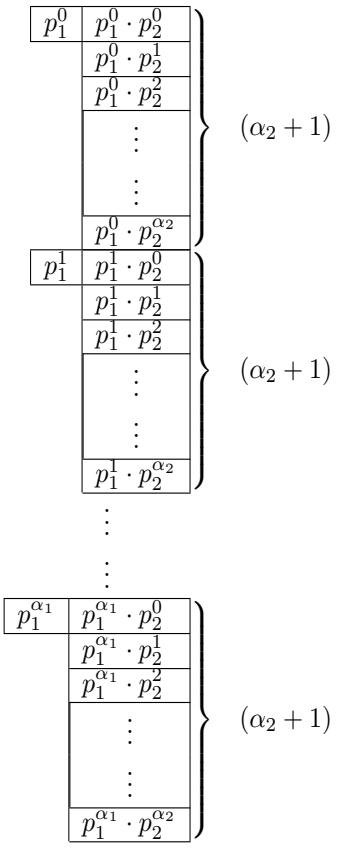
Veamos cuántos elementos tiene este conjunto.

⊛ Los divisores de la forma $p_1^{\beta_1}$, con $0 \leqslant \beta_1 \leqslant \alpha_1$ serán

$$\left.\begin{array}{|c|}\hline p_1^0 \\ \hline p_1^1 \\ \hline p_1^2 \\ \hline \vdots \\ \\ \vdots \\ \hline p_1^{\alpha_1} \\ \hline \end{array}\right\} (\alpha_1 + 1)$$

es decir habrá un total de $\alpha_1 + 1$ de estos divisores.

⊛ Los divisores de la forma $p_1^{\beta_1}\cdot p_2^{\beta_2},\ \text{con } 0\leqslant\beta_2\leqslant\alpha_2$ son:



Por lo tanto, el número total de los divisores de la forma

$$p_1^{\beta_1}\cdot p_2^{\beta_2},\ \text{con}\begin{cases}0\leqslant\beta_1\leqslant\alpha_1\\ 0\leqslant\beta_2\leqslant\alpha_2\end{cases}$$

será

$$(\alpha_1+1)\,(\alpha_2+1)$$

⊛ Para obtener todos los divisores de la forma $p_1^{\beta_1}\cdot p_2^{\beta_2}\cdot p_3^{\beta_3}$ multiplicamos cada uno de los anteriores por $p_3^{\beta_3},\ 0\leqslant\beta_3\leqslant\alpha_3$. por lo tanto el número total de divisores de la forma

$$p_1^{\beta_1}\cdot p_2^{\beta_2}\cdot p_3^{\beta_3},\ \text{con}\begin{cases}0\leqslant\beta_1\leqslant\alpha_1\\ 0\leqslant\beta_2\leqslant\alpha_2\\ 0\leqslant\beta_3\leqslant\alpha_3\end{cases}$$

es

$$(\alpha_1+1)\,(\alpha_2+1)\,(\alpha_3+1)$$

⊛ Seguimos así sucesivamente y supongamos que hemos obtenido todos los divisores de la forma $p_1^{\beta_1}\cdot p_2^{\beta_2}\cdot p_3^{\beta_3}\cdots p_{k-1}^{\beta_{k-1}}$, es decir,

$$p_1^{\beta_1}\cdot p_2^{\beta_2}\cdot p_3^{\beta_3}\cdots p_{k-1}^{\beta_{k-1}},\ \text{con}\begin{cases}0\leqslant\beta_1\leqslant\alpha_1\\ 0\leqslant\beta_2\leqslant\alpha_2\\ 0\leqslant\beta_3\leqslant\alpha_3\\ \qquad\vdots\\ 0\leqslant\beta_{k-1}\leqslant\alpha_{k-1}\end{cases}$$

cuyo número es

$$(\alpha_1+1)\,(\alpha_2+1)\,(\alpha_3+1)\cdot\cdots\cdot(\alpha_{k-1}+1)$$

⊛ Para obtener todos los divisores de la forma $p_1^{\beta_1}\cdot p_2^{\beta_2}\cdot p_3^{\beta_3}\cdots p_{k-1}^{\beta_{k-1}}\cdot p_k^{\beta_k}$, multiplicamos todos los anteriores por $p_k^{\beta_k},\ 0\leqslant\beta_k\leqslant\alpha_k$ y obtendremos

$$p_1^{\beta_1}\cdot p_2^{\beta_2}\cdot p_3^{\beta_3}\cdots p_{k-1}^{\beta_{k-1}}\cdot p_k^{\beta_k},\ \text{con}\begin{cases}0\leqslant\beta_1\leqslant\alpha_1\\0\leqslant\beta_2\leqslant\alpha_2\\0\leqslant\beta_3\leqslant\alpha_3\\\qquad\vdots\\0\leqslant\beta_{k-1}\leqslant\alpha_{k-1}\\0\leqslant\beta_k\leqslant\alpha_k\end{cases}$$

cuyo número es

$$(\alpha_1+1)\,(\alpha_2+1)\,(\alpha_3+1)\cdot\cdots\cdot(\alpha_{k-1}+1)\,(\alpha_k+1)$$

Por lo tanto, el número total de divisores de a es:

$$N_a=(\alpha_1+1)\,(\alpha_2+1)\,(\alpha_3+1)\cdot\cdots\cdot(\alpha_{k-1}+1)\,(\alpha_k+1)$$

■

Ejemplo 14.10

¿Cuántos divisores positivos tiene el número 604800*?*

Solución

En un ejemplo anterior teníamos que

$$604800=2^7\cdot3^3\cdot5^2\cdot7$$

por lo tanto, según el apartado anterior,

$$N_{604800}=(7+1)(3+1)(2+1)(1+1)=8\cdot4\cdot3\cdot2=192$$

es decir, el número 604800 tiene 192 divisores positivos.

■

14.4.6 Suma de los divisores de un número compuesto

Si a es un entero de valor absoluto mayor que 1 y $a=p_1^{\alpha_1}p_2^{\alpha_2}p_3^{\alpha_3}\cdots\cdots p_k^{\alpha_k}$ es su descomposición en factores primos, entonces la suma de todos los divisores de a es

$$S_a=\frac{p_1^{\alpha_1+1}-1}{p_1-1}\cdot\frac{p_2^{\alpha_2+1}-1}{p_2-1}\cdot\frac{p_3^{\alpha_3+1}-1}{p_3-1}\cdot\cdots\cdot\frac{p_k^{\alpha_k+1}-1}{p_k-1}$$

Demostración

En efecto, según vimos en 14.4.3, los divisores de a son los elementos del conjunto

$$D_a = \left\{ p_1^{\beta_1} \cdot p_2^{\beta_2} p_3^{\alpha_3} \cdot \cdots \cdot p_k^{\beta_k}, \text{con } 0 \leqslant \beta_i \leqslant \alpha_i,\ 1 \leqslant i \leqslant k \right\}.$$

Calculemos su suma.

$$\begin{aligned}
S_a &= \sum_{\beta_1=0}^{\alpha_1} \sum_{\beta_2=0}^{\alpha_2} \sum_{\beta_3=0}^{\alpha_3} \cdots \cdots \sum_{\beta_k=0}^{\alpha_k} p_1^{\beta_1} \cdot p_2^{\beta_2} \cdot p_3^{\beta_3} \cdots \cdots p_k^{\beta_k} \\
&= \sum_{\beta_1=0}^{\alpha_1} \sum_{\beta_2=0}^{\alpha_2} \sum_{\beta_3=0}^{\alpha_3} p_1^{\beta_1} \cdot p_2^{\beta_2} \cdot p_3^{\beta_3} \cdots \cdots \sum_{\beta_k=0}^{\alpha_k} p_k^{\beta_k} \\
&= \sum_{\beta_1=0}^{\alpha_1} \sum_{\beta_2=0}^{\alpha_2} p_1^{\beta_1} \cdot p_2^{\beta_2} \sum_{\beta_3=0}^{\alpha_3} \cdot p_3^{\beta_3} \cdots \cdots \sum_{\beta_k=0}^{\alpha_k} p_k^{\beta_k} \\
&= \sum_{\beta_1=0}^{\alpha_1} p_1^{\beta_1} \sum_{\beta_2=0}^{\alpha_2} p_2^{\beta_2} \sum_{\beta_3=0}^{\alpha_3} p_3^{\beta_3} \cdots \cdots \sum_{\beta_k=0}^{\alpha_k} p_k^{\beta_k} \\
&= \left(p_1^0 + p_1^1 + p_1^2 + \cdots + p_1^{\alpha_1}\right) \left(p_2^0 + p_2^1 + p_2^2 + \cdots + p_2^{\alpha_2}\right) \\
&\qquad \left(p_3^0 + p_3^1 + p_3^2 + \cdots + p_3^{\alpha_3}\right) \\
&\qquad \cdots\cdots\cdots\cdots\cdots\cdots \\
&\qquad \left(p_k^0 + p_k^1 + p_k^2 + \cdots + p_k^{\alpha_k}\right) \\
&= \frac{p_1^{\alpha_1+1} - 1}{p_1 - 1} \cdot \frac{p_2^{\alpha_2+1} - 1}{p_2 - 1} \cdot \frac{p_3^{\alpha_3+1} - 1}{p_3 - 1} \cdots\cdots \frac{p_k^{\alpha_k+1} - 1}{p_k - 1}
\end{aligned}$$

ya que cada uno de los paréntesis es, respectivamente, la suma de los $\alpha_1+1, \alpha_2+1, \alpha_3+1 \cdots \alpha_k+1$ términos de una progresión geométrica de razones $p_1, p_2, p_3, \cdots, p_k$.

■

Ejemplo 14.11

Determinar dos enteros positivos cuyo máximo común divisor es 18*, sabiendo que uno de ellos tiene* 21 *divisores y el otro tiene* 10*.*

Solución

Sean a y b los números que buscamos. Por el corolario 14.3.5, existirán $p_1, p_2, \ldots, p_k$ y $q_1, q_2, \ldots, q_m$, primos distintos y $\alpha_i \geqslant 1,\ 1 \leqslant i \leqslant k$, $\beta_j \geqslant 1,\ 1 \leqslant j \leqslant m$, enteros, con $p_1 < p_2 < \cdots < p_k$ y $q_1 < q_2 < \cdots < q_m$ tales que

$$a = p_1^{\alpha_1} p_2^{\alpha_2} p_3^{\alpha_3} \cdots\cdots p_k^{\alpha_k}$$

y

$$b = q_1^{\beta_1} q_2^{\beta_2} q_3^{\beta_3} \cdots\cdots q_m^{\beta_m}$$

Pues bien, según el enunciado, m.c.d.$(a, b) = 18$, es decir, 18 es divisor de a y de b luego por 14.4.2 tanto a como b deberán tener en su factorización, al menos, todos los factores primos de 18 con exponentes iguales

o mayores. Pues bien, como $18 = 2 \cdot 3^2$,

$$\text{m.c.d.}(a,b) = 18 \implies \begin{cases} 18 \,|a \\ \text{y} \\ 18 \,|b \end{cases} \implies \begin{cases} 2 \cdot 3^2 \,|a \\ \text{y} \\ 2 \cdot 3^2 \,|b \end{cases} \implies \begin{cases} \begin{cases} p_1 = 2 \text{ y } \alpha_1 \geqslant 1 \\ \text{y} \\ p_2 = 3 \text{ y } \alpha_2 \geqslant 2 \end{cases} \\ \text{y} \\ \begin{cases} q_1 = 2 \text{ y } \beta_1 \geqslant 1 \\ \text{y} \\ q_2 = 3 \text{ y } \beta_2 \geqslant 2 \end{cases} \end{cases}$$

Por otra parte, el número de divisores de a es 21. Entonces, utilizando el resultado de 14.4.5,

$$\begin{aligned} N_a = 21 &\implies (\alpha_1 + 1)(\alpha_2 + 1)(\alpha_3 + 1) \cdot \cdots \cdot (\alpha_k + 1) = 21 \\ &\implies \alpha_i + 1 \text{ es divisor de 21, para } 1 \leqslant i \leqslant k \\ &\quad \left[\; 21 = 3 \cdot 7 \implies D_{21} = \{1,3,7,21\} \; \right] \\ &\implies \alpha_i + 1 \in \{1,3,7,21\}\,, \; 1 \leqslant i \leqslant k \end{aligned}$$

Ahora bien,

$$\left.\begin{array}{l} \alpha_1 \geqslant 1 \implies \alpha_1 + 1 \geqslant 2 \\ \text{y} \\ \alpha_2 \geqslant 2 \implies \alpha_2 + 1 \geqslant 3 \\ \text{y} \\ \alpha_i + 1 \in \{1,3,7,21\}\,, \; 1 \leqslant i \leqslant k \end{array}\right\} \implies \begin{cases} \alpha_1 + 1 \in \{3,7,21\} \\ \text{y} \\ \alpha_2 + 1 \in \{3,7,21\} \\ \text{y} \\ \alpha_i + 1 \in \{1,3,7,21\}\,, \; 3 \leqslant i \leqslant k \end{cases}$$

Además,

$$\alpha_i + 1 \neq 21, \; 1 \leqslant i \leqslant k$$

ya que si alguno de ellos fuera igual a 21, todos los demás deberían ser iguales a 1 y eso es imposible porque $\alpha_1 + 1$ y $\alpha_2 + 1$ son, ambos, distintos de 1. Entonces,

$$\left.\begin{array}{l} \alpha_1 + 1 \in \{3,7,21\} \\ \text{y} \\ \alpha_2 + 1 \in \{3,7,21\} \\ \text{y} \\ \alpha_i + 1 \in \{1,3,7,21\} \;\; 3 \leqslant i \leqslant k \\ \text{y} \\ \alpha_i + 1 \neq 21, \; 1 \leqslant i \leqslant k \end{array}\right\} \implies \begin{cases} \alpha_1 + 1 \in \{3,7\} \\ \text{y} \\ \alpha_2 + 1 \in \{3,7\} \\ \text{y} \\ \alpha_i + 1 \in \{1,3,7\} \;\; 3 \leqslant i \leqslant k \end{cases}$$

Pues bien,

$$\alpha_1+1\in\{3,7\} \implies \begin{cases} \alpha_1+1=3 \\ \text{ó} \\ \alpha_1+1=7 \end{cases}$$

Estudiemos ambos casos:

$$\left.\begin{array}{l} \alpha_1+1=3 \\ \text{y} \\ (\alpha_1+1)(\alpha_2+1)(\alpha_3+1)\cdot\cdots\cdot(\alpha_k+1)=21 \end{array}\right\} \implies \alpha_i+1\neq 3,\ 2\leqslant i\leqslant k$$

y

$$\left.\begin{array}{l} \alpha_i+1\neq 3,\ 2\leqslant i\leqslant k \\ \text{y} \\ \alpha_2+1\in\{3,7\} \\ \text{y} \\ \alpha_i+1\in\{1,3,7\},\ 3\leqslant i\leqslant k \end{array}\right\} \implies \begin{cases} \alpha_2+1=7 \\ \text{y} \\ \alpha_i+1\in\{1,7\},\ 3\leqslant i\leqslant k \end{cases}$$

y

$$\left.\begin{array}{l} \alpha_2+1=7 \\ \text{y} \\ \alpha_i+1\in\{1,7\},\ 3\leqslant i\leqslant k \\ \text{y} \\ (\alpha_1+1)(\alpha_2+1)(\alpha_3+1)\cdot\cdots\cdot(\alpha_k+1)=21 \end{array}\right\} \implies \alpha_i+1=1,\ 3\leqslant i\leqslant k$$

Por lo tanto, en este caso, tenemos:

$$\begin{array}{l} \alpha_1+1=3 \\ \text{y} \\ \alpha_2+1=7 \\ \text{y} \\ \alpha_i+1=1,\ 3\leqslant i\leqslant k \end{array}$$

Veamos ahora que ocurre si $\alpha_1+1=7$.

$$\left.\begin{array}{l} \alpha_1+1=7 \\ \text{y} \\ (\alpha_1+1)(\alpha_2+1)(\alpha_3+1)\cdot\cdots\cdot(\alpha_k+1)=21 \end{array}\right\} \implies \alpha_i+1\neq 7,\ 2\leqslant i\leqslant k$$

y

$$\left.\begin{array}{l} \alpha_i+1\neq 7,\ 2\leqslant i\leqslant k \\ \text{y} \\ \alpha_2+1\in\{3,7\} \\ \text{y} \\ \alpha_i+1\in\{1,3,7\},\ 3\leqslant i\leqslant k \end{array}\right\} \implies \begin{cases} \alpha_2+1=3 \\ \text{y} \\ \alpha_i+1\in\{1,3\},\ 3\leqslant i\leqslant k \end{cases}$$

y

$$\left.\begin{array}{l}\alpha_2+1=3\\ \text{y}\\ \alpha_i+1\in\{1,3\},\ 3\leqslant i\leqslant k\\ \text{y}\\ (\alpha_1+1)(\alpha_2+1)(\alpha_3+1)\cdot\cdots\cdot(\alpha_k+1)=21\end{array}\right\}\implies \alpha_i+1=1,\ 3\leqslant i\leqslant k$$

Luego,

$$\begin{array}{l}\alpha_1+1=7\\ \text{y}\\ \alpha_2+1=3\\ \text{y}\\ \alpha_i+1=1,\ 3\leqslant i\leqslant k\end{array}$$

Reuniendo ambos casos:

$$\left.\begin{array}{l}\alpha_1+1=3\\ \text{y}\\ \alpha_2+1=7\\ \text{y}\\ \alpha_i+1=1,\ 3\leqslant i\leqslant k\end{array}\right\}\implies\left.\begin{array}{l}\alpha_1=2\\ \text{y}\\ \alpha_2=6\\ \text{y}\\ \alpha_i=0,\ 3\leqslant i\leqslant k\end{array}\right\}\implies a=2^2\cdot 3^6$$

ó

$$\left.\begin{array}{l}\alpha_1+1=7\\ \text{y}\\ \alpha_2+1=3\\ \text{y}\\ \alpha_i+1=1,\ 3\leqslant i\leqslant k\end{array}\right\}\implies\left.\begin{array}{l}\alpha_1=6\\ \text{y}\\ \alpha_2=2\\ \text{y}\\ \alpha_i=0,\ 3\leqslant i\leqslant k\end{array}\right\}\implies a=2^6\cdot 3^2$$

Un razonamiento análogo puede hacerse para b. En efecto, el número de divisores de b es 10, luego

$$\begin{array}{rl}N_b=10 & \implies (\beta_1+1)(\beta_2+1)(\beta_3+1)\cdot\cdots\cdot(\beta_m+1)=10\\ & \implies \beta_j+1 \text{ es divisor de 10, para } 1\leqslant j\leqslant m\\ & \quad\left[\ 10=2.5\implies D_{10}=\{1,2,5,10\}\ \right]\\ & \implies \beta_j+1\in\{1,2,5,10\},\ 1\leqslant j\leqslant m\end{array}$$

Ahora bien,

$$\left.\begin{array}{l}\beta_1\geqslant 1\implies\beta_1+1\geqslant 2\\ \text{y}\\ \beta_2\geqslant 2\implies\beta_2+1\geqslant 3\\ \text{y}\\ \beta_j+1\in\{1,2,5,10\}\ \ 1\leqslant j\leqslant m\end{array}\right\}\implies\left\{\begin{array}{l}\beta_1+1\in\{2,5,10\}\\ \text{y}\\ \beta_2+1\in\{5,10\}\\ \text{y}\\ \beta_j+1\in\{1,2,5,10\},\ 3\leqslant j\leqslant m\end{array}\right.$$

además,

$$\beta_j+1\neq 10,\ 1\leqslant j\leqslant m.$$

En efecto, si alguno de ellos fuera igual a 10, todos los demás serían iguales a 1 y eso es imposible ya que β_1+1 y β_2+1 son, ambos, distintos de 1. Entonces,

$$\left.\begin{array}{l}\beta_1+1\in\{2,5,10\}\\ \text{y}\\ \beta_2+1\in\{5,10\}\\ \text{y}\\ \beta_j+1\in\{1,2,5,10\},\ 3\leqslant j\leqslant m\\ \text{y}\\ \beta_j+1\neq 10,\ 1\leqslant j\leqslant m\end{array}\right\}\Longrightarrow\left\{\begin{array}{l}\beta_1+1\in\{2,5\}\\ \text{y}\\ \beta_2+1=5\\ \text{y}\\ \beta_j+1\in\{1,2,5\},\ 3\leqslant j\leqslant m\end{array}\right.$$

$$\left[\left.\begin{array}{l}\beta_2+1=5\\ \text{y}\\ (\beta_1+1)(\beta_2+1)\cdots(\beta_m+1)=10\end{array}\right\}\Longrightarrow\ \beta_j+1\neq 5,\ \text{para cualquier } j\neq 2\right]$$

$$\Longrightarrow\left\{\begin{array}{l}\beta_1+1=2\\ \text{y}\\ \beta_2+1=5\\ \text{y}\\ \beta_j+1\in\{1,2\},\ 3\leqslant j\leqslant m\end{array}\right.$$

$$\left[\left.\begin{array}{l}\beta_1+1=2\\ \text{y}\\ \beta_2+1=5\\ \text{y}\\ (\beta_1+1)(\beta_2+1)(\beta_3+1)\cdots\cdots(\beta_m+1)=10\end{array}\right\}\Longrightarrow\ \beta_j+1\neq 2,\ 3\leqslant j\leqslant m\right]$$

$$\Longrightarrow\left\{\begin{array}{l}\beta_1+1=2\\ \text{y}\\ \beta_2+1=5\\ \text{y}\\ \beta_j+1=1,\ 3\leqslant j\leqslant m\end{array}\right.$$

$$\Longrightarrow\left\{\begin{array}{l}\beta_1=1\\ \text{y}\\ \beta_2=4\\ \text{y}\\ \beta_j+1=0,\ 3\leqslant j\leqslant m\end{array}\right.$$

$$\Longrightarrow\ b=2\cdot 3^4$$

Tenemos, pues, dos soluciones:

$$\left(a = 2^2 \cdot 3^6 \text{ ó } a = 2^6 \cdot 3^2\right) \text{ y } b = 2 \cdot 3^4 \implies \begin{cases} 1.\ a = 2^2 \cdot 3^6 \text{ y } b = 2 \cdot 3^4 \\ \text{ó} \\ 2.\ a = 2^6 \cdot 3^2 \text{ y } b = 2 \cdot 3^4 \end{cases}$$

Veamos cual de las dos es la que buscamos.

1. $a = 2^2 \cdot 3^6$ y $b = 2 \cdot 3^4$. Según 14.4.3,

$$\begin{aligned} D_a &= \{2^{\gamma_1}3^{\gamma_2} :\ 0 \leqslant \gamma_1 \leqslant 2 \text{ y } 0 \leqslant \gamma_2 \leqslant 6\} \\ &\text{y} \\ D_b &= \left\{2^{\delta_1}3^{\delta_2} :\ 0 \leqslant \delta_1 \leqslant 1 \text{ y } 0 \leqslant \delta_2 \leqslant 4\right\} \end{aligned}$$

   luego entonces los divisores comunes son:

$$\begin{aligned} D_a \cap D_b &= \left\{ 2^{\min\{\gamma_1,\delta_1\}}3^{\min\{\gamma_2,\delta_2\}} \ : \begin{array}{l} 0 \leqslant \min\{\gamma_1,\delta_1\} \leqslant \min\{2,1\} \\ \text{y} \\ 0 \leqslant \min\{\gamma_2,\delta_2\} \leqslant \min\{6,4\} \end{array} \right\} \\ &= \left\{ 2^{\min\{\gamma_1,\delta_1\}}3^{\min\{\gamma_2,\delta_2\}} \ : \begin{array}{l} 0 \leqslant \min\{\gamma_1,\delta_1\} \leqslant 1 \\ \text{y} \\ 0 \leqslant \min\{\gamma_2,\delta_2\} \leqslant 4 \end{array} \right\} \end{aligned}$$

   y el máximo de todos ellos,

$$\begin{aligned} \max(D_a \cap D_b) &= \left\{ 2^{\min\{\gamma_1,\delta_1\}}3^{\min\{\gamma_2,\delta_2\}} \ : \begin{array}{l} 0 \leqslant \min\{\gamma_1,\delta_1\} \leqslant 1 \\ \text{y} \\ 0 \leqslant \min\{\gamma_2,\delta_2\} \leqslant 4 \end{array} \right\} \\ &= 2 \cdot 3^4 \\ &= 162 \end{aligned}$$

   es decir,

$$\text{m.c.d.}(a,b) = 162$$

   y esto es imposible ya que, según el enunciado, el máximo común divisor de a y b era 18.

2. $a = 2^6 \cdot 3^2$ y $b = 2 \cdot 3^4$.

   Al igual que en el caso anterior, por 14.4.3,

$$\begin{aligned} D_a &= \{2^{\gamma_1}3^{\gamma_2} :\ 0 \leqslant \gamma_1 \leqslant 6 \text{ y } 0 \leqslant \gamma_2 \leqslant 2\} \\ &\text{y} \\ D_b &= \left\{2^{\delta_1}3^{\delta_2} :\ 0 \leqslant \delta_1 \leqslant 1 \text{ y } 0 \leqslant \delta_2 \leqslant 4\right\} \end{aligned}$$

   luego entonces los divisores comunes son:

$$\begin{aligned} D_a \cap D_b &= \left\{ 2^{\min\{\gamma_1,\delta_1\}}3^{\min\{\gamma_2,\delta_2\}} \ : \begin{array}{l} 0 \leqslant \min\{\gamma_1,\delta_1\} \leqslant \min\{6,1\} \\ \text{y} \\ 0 \leqslant \min\{\gamma_2,\delta_2\} \leqslant \min\{2,4\} \end{array} \right\} \\ &= \left\{ 2^{\min\{\gamma_1,\delta_1\}}3^{\min\{\gamma_2,\delta_2\}} \ : \begin{array}{l} 0 \leqslant \min\{\gamma_1,\delta_1\} \leqslant 1 \\ \text{y} \\ 0 \leqslant \min\{\gamma_2,\delta_2\} \leqslant 2 \end{array} \right\} \end{aligned}$$

y el máximo de todos ellos,

$$\begin{aligned}\max\left(D_a \cap D_b\right) &= \left\{ 2^{\min\{\gamma_1,\delta_1\}}3^{\min\{\gamma_2,\delta_2\}} \;:\; \begin{array}{l} 0 \leqslant \min\{\gamma_1,\delta_1\} \leqslant 1 \\ \text{y} \\ 0 \leqslant \min\{\gamma_2,\delta_2\} \leqslant 2 \end{array} \right\} \\ &= 2 \cdot 3^2 \\ &= 162\end{aligned}$$

es decir,

$$\text{m.c.d.}(a,b) = 18$$

lo que coincide con el dato proporcionado por el enunciado.

La solución correcta del ejercicio es, pues,

$$a = 576 \text{ y } b = 162$$

■

Ejemplo 14.12

Hallar un número entero positivo sabiendo que tiene 2 *factores primos,* 8 *divisores y que la suma de éstos es* 320.

Solución

Sea a el número buscado, p_1 y p_2 sus factores primos y α_1 y α_2, respectivamente, el número de veces que se repiten. Entonces,

$$a = p_1^{\alpha_1} p_2^{\alpha_2},\ \alpha_1 \geqslant 1 \text{ y } \alpha_2 \geqslant 1$$

Como tiene 8 divisores, $N_a = 8$, luego,

$$\begin{aligned} N_a = 8 &\implies (\alpha_1 + 1)(\alpha_2 + 1) = 8 \\ &\implies \alpha_1 + 1 \text{ y } \alpha_2 + 1 \text{ son, ambos, divisores de } 8 \\ &\quad \left[\ 8 = 2^3 \implies D_8 = \{1,2,4,8\}\ \right] \\ &\implies \left\{ \begin{array}{l} \alpha_1 + 1 \in \{1,2,4,8\} \\ \text{y} \\ \alpha_2 + 1 \in \{1,2,4,8\} \end{array} \right.\end{aligned}$$

Representamos las posibles opciones en la tabla siguiente:

$\alpha_1 + 1$	1	2	4	8
$\alpha_2 + 1$	8	4	2	1

Si α_1+1 toma cualquier valor de la primera fila, como $(\alpha_1+1)(\alpha_2+1)=8$, entonces α_2+1 ha de tomar el valor que figura en la segunda fila y en la misma columna que α_1+1 y viceversa, es decir, si α_2+1 toma cualquier valor en la segunda fila, entonces α_1+1 ha de tomar el valor de su misma columna en la primera fila. Por ejemplo,

$$\begin{aligned}&\alpha_1+1=2 \implies \alpha_2+1=4\\ &\text{y}\\ &\alpha_2+1=8 \implies \alpha_1+1=1\end{aligned}$$

Pues bien,

$$\alpha_1 \geqslant 1 \Longrightarrow \alpha_1+1 \geqslant 2$$

luego los valores de α_1+1 y α_2+1 en la primera columna no son posibles, o sea,

α_1+1	~~1~~	2	4	8
α_2+1	~~8~~	4	2	1

también,

$$\alpha_2 \geqslant 1 \Longrightarrow \alpha_2+1 \geqslant 2$$

luego los valores de α_1+1 y α_2+1 en la cuarta columna no son posibles, es decir,

α_1+1	~~1~~	2	4	~~8~~
α_2+1	~~8~~	4	2	~~1~~

Las opciones que nos quedan son:

1. $\alpha_1+1=2$ y $\alpha_2+1=4$. Entonces,

$$\left.\begin{aligned}&\alpha_1+1=2 \implies \alpha_1=1\\ &\text{y}\\ &\alpha_2+1=4 \implies \alpha_2=3\end{aligned}\right\} \implies a=p_1p_2^3$$

2. $\alpha_1+1=4$ y $\alpha_2+1=2$. Entonces,

$$\left.\begin{aligned}&\alpha_1+1=4 \implies \alpha_1=3\\ &\text{y}\\ &\alpha_2+1=1 \implies \alpha_2=1\end{aligned}\right\} \implies a=p_1^3p_2$$

Tenemos, pues, dos posibles soluciones. Estudiaremos cada una de ellas.

1. $a=p_1p_2^3$.

   Según el enunciado, la suma de los divisores de a es 320. Pues bien, por 14.4.3,

$$D_a=\left\{p_1^\alpha p_2^\beta : 0 \leqslant \alpha \leqslant 1 \text{ y } 0 \leqslant \beta \leqslant 3\right\}$$

y podemos escribirlos todos utilizando el método que vimos en 14.4.4, es decir,

	1	p_1
$\times p_2$	p_2	p_1p_2
$\times p_2^2$	p_2^2	$p_1p_2^2$
$\times p_2^3$	p_2^3	$p_1p_2^3$

Calculamos ahora la suma de todos ellos, S_a. En efecto, sumando por columnas,

$$\begin{aligned} S_a &= 1+p_2+p_2^2+p_2^3+p_1+p_1p_2+p_1p_2^2+p_1p_2^3 \\ &= (1+p_1)\left(1+p_2+p_2^2+p_2^3\right) \end{aligned}$$

y, entonces,

$$S_a = 320 \implies (1+p_1)\left(1+p_2+p_2^2+p_2^3\right) = 320$$

$$\implies \begin{cases} 1+p_1 \text{ es divisor de } 320 \\ \text{y} \\ 1+p_2+p_2^2+p_2^3 \text{ es divisor de } 320 \end{cases}$$

y como $320 = 2^6 \cdot 5$, de nuevo por 14.4.3, tendremos que

$$D_{320} = \left\{2^\gamma 3^\delta : 0 \leqslant \gamma \leqslant 6 \text{ y } 0 \leqslant \delta \leqslant 1\right\}$$

y por 14.4.4,

	1	2	4	8	16	32	64
$\times 5$	5	10	20	40	80	160	320

luego,

$$D_{320} = \{1,2,4,8,16,32,64,5,10,20,40,80,160,320\}$$

y

$$\begin{cases} 1+p_1 \in \{1,2,4,8,16,32,64,5,10,20,40,80,160,320\} \\ \text{y} \\ 1+p_2+p_2^2+p_2^3 \in \{1,2,4,8,16,32,64,5,10,20,40,80,160,320\} \\ \text{y} \\ (1+p_1)\left(1+p_2+p_2^2+p_2^3\right) = 320 \end{cases}$$

Ahora, al igual que hicimos antes, representamos las distintas opciones en una tabla:

$1+p_1$	1	2	4	5	8	10	16	20	32	40	64	80	160	320
$1+p_2+p_2^2+p_2^3$	320	160	80	64	40	32	20	16	10	8	5	4	2	1

Veamos cuales son las posibles soluciones.

- p_1 es primo $\implies p_1 \geqslant 2 \implies 1+p_1 \geqslant 3$, luego entonces las opciones representadas en la primera y segunda columna son imposibles.

$1+p_1$	1	2	4	5	8	10	16	20	32	40	64	80	160	320
$1+p_2+p_2^2+p_2^3$	320	160	80	64	40	32	20	16	10	8	5	4	2	1

⁕ p_2 es primo $\Longrightarrow p_2 \geqslant 2 \Longrightarrow 1+p_2+p_2^2+p_2^3 \geqslant 15$, luego entonces las opciones representadas de la novena columna en adelante también son imposibles.

$1+p_1$	1	2	4	5	8	10	16	20	32	40	64	80	160	320
$1+p_2+p_2^2+p_2^3$	320	160	80	64	40	32	20	16	10	8	5	4	2	1

⁕ De la cuarta columna se sigue que

$$1+p_1=5 \Longrightarrow p_1=4. \text{ Imposible, ya que } p_1 \text{ es primo.}$$

En la sexta columna,

$$1+p_1=10 \Longrightarrow p_1=9. \text{ Imposible, ya que } p_1 \text{ es primo,}$$

y en la séptima,

$$1+p_1=16 \Longrightarrow p_1=15. \text{ Imposible, ya que } p_1 \text{ es primo.}$$

Eliminamos, por tanto, las opciones representadas en las columnas cuarta, sexta y séptima.

$1+p_1$	1	2	4	5	8	10	16	20	32	40	64	80	160	320
$1+p_2+p_2^2+p_2^3$	320	160	80	64	40	32	20	16	10	8	5	4	2	1

⁕ En la tercera columna,

$$\begin{aligned} 1+p_2+p_2^2+p_2^3=80 &\Longrightarrow p_2\left(1+p_2+p_2^2\right)=79 \\ &\Longrightarrow p_2 \text{ es divisor de } 79 \end{aligned}$$

y esto, al ser 79 un número primo, es imposible. Por lo tanto, eliminamos, también, la tercera columna.

$1+p_1$	1	2	4	5	8	10	16	20	32	40	64	80	160	320
$1+p_2+p_2^2+p_2^3$	320	160	80	64	40	32	20	16	10	8	5	4	2	1

⁕ En la octava columna tenemos que

$$1+p_2+p_2^2+p_2^3=16 \Longrightarrow p_2\left(1+p_2+p_2^2\right)=15$$

y esto tampoco es posible ya que al ser $15=3\cdot 5$, tendríamos,

$$\left.\begin{array}{l} 15=3\cdot 5 \\ \text{y} \\ p_2\left(1+p_2+p_2^2\right)=15 \\ \text{y} \\ p_2 \text{ es primo} \end{array}\right\} \Longrightarrow \left\{\begin{array}{lll} p_2=3 & \Longrightarrow & 1+p_2+p_2^2=13\neq 5 \\ \text{ó} & & \\ p_2=5 & \Longrightarrow & 1+p_2+p_2^2=31\neq 3 \end{array}\right.$$

Eliminamos, por tanto, la octava columna.

$1+p_1$	1	2	4	5	8	10	16	20	32	40	64	80	160	320
$1+p_2+p_2^2+p_2^3$	320	160	80	64	40	32	20	16	10	8	5	4	2	1

⁎ Nos queda como única opción posible las representadas en la quinta columna. Pues bien,

$$1+p_1=8 \Longrightarrow p_1=7$$

y

$$1+p_2+p_2^2+p_2^3=40 \implies p_2\left(1+p_2+p_2^2\right)=39$$

Entonces,

$$\left.\begin{array}{l} 39=3\cdot 13 \\ \text{y} \\ p_2\left(1+p_2+p_2^2\right)=39 \\ \text{y} \\ p_2 \text{ es primo} \end{array}\right\} \implies \left\{\begin{array}{lll} p_2=3 & \Longrightarrow & 1+p_2+p_2^2=13 \\ \text{ó} & & \\ p_2=13 & \Longrightarrow & 1+p_2+p_2^2=183\neq 3 \end{array}\right.$$

y, consecuentemente, $p_2=3$.

Así pues, la primera solución es:

$$\left.\begin{array}{l} a=p_1p_2^3 \\ \text{y} \\ p_1=7 \\ \text{y} \\ p_2=3 \end{array}\right\} \implies a=7\cdot 3^3=189$$

2. $a=p_1^3p_2$

Seguiremos los mismos pasos que en el caso anterior. Según el enunciado, la suma de los divisores de a es 320. Pues bien, por 14.4.3,

$$D_a=\left\{p_1^\alpha p_2^\beta : 0\leqslant \alpha\leqslant 3 \text{ y } 0\leqslant \beta\leqslant 1\right\}$$

y podemos escribirlos todos utilizando el método que vimos en 14.4.4, es decir,

	1	p_1	p_1^2	p_1^3
$\times p_2$	p_2	p_1p_2	$p_1^2p_2$	$p_1^3p_2$

Calculamos ahora la suma de todos ellos, S_a. En efecto, sumando por filas,

$$\begin{aligned} S_a &= 1+p_1+p_1^2+p_1^3+p_2+p_1p_2+p_1^2p_2+p_1^3p_2 \\ &= \left(1+p_1+p_1^2+p_1^3\right)(1+p_2) \end{aligned}$$

y, entonces,

$$S_a=320 \implies \left(1+p_1+p_1^2+p_1^3\right)(1+p_2)=320$$

$$\implies \left\{\begin{array}{l} 1+p_1+p_1^2+p_1^3 \text{ es divisor de } 320 \\ \text{y} \\ 1+p_2 \text{ es divisor de } 320 \end{array}\right.$$

y como $320 = 2^6 \cdot 5$, de nuevo por 14.4.3, tendremos que

$$D_{320} = \left\{2^\gamma 3^\delta : 0 \leqslant \gamma \leqslant 6 \text{ y } 0 \leqslant \delta \leqslant 1\right\}$$

Representando, ahora, al igual que en el caso anterior, las distintas opciones en una tabla:

$1+p_2$	1	2	4	5	8	10	16	20	32	40	64	80	160	320
$1+p_1+p_1^2+p_1^3$	320	160	80	64	40	32	20	16	10	8	5	4	2	1

obtendremos los mismos resultados que antes, sin más que intercambiar p_1 y p_2, luego,

$$\left.\begin{array}{l} a = p_1^3 p_2 \\ \text{y} \\ p_1 = 3 \\ \text{y} \\ p_2 = 7 \end{array}\right\} \implies a = 3^3 \cdot 7 = 189$$

es decir, la solución es la misma.

El ejercicio tiene, pues, una solución única, y el número pedido es el 189.

■

Ejemplo 14.13

Hallar un número entero que en su descomposición no tiene más factores primos que 2, 5 *y* 7, *sabiendo que al multiplicarlo por* 5 *el número de sus divisores se incrementa en* 8 *y al multiplicarlo por* 8 *éste número se incrementa en* 18. *Calcular también la suma de todos los divisores de* a.

Solución

Sea a el número buscado y sean α_1, α_2 y α_3 las veces que se repiten, respectivamente, los números primos 2, 5 y 7 en la factorización de a. Entonces,

$$a = 2^{\alpha_1} 5^{\alpha_2} 7^{\alpha_3}, \text{ con } \alpha_1 \geqslant 1,\ \alpha_2 \geqslant 1,\ \alpha_3 \geqslant 1$$

Pues bien,

$$a = 2^{\alpha_1} 5^{\alpha_2} 7^{\alpha_3} \implies \left\{\begin{array}{rcl} 5a & = & 2^{\alpha_1} 5^{\alpha_2+1} 7^{\alpha_3} \\ \text{y} & & \\ 8a & = & 2^{\alpha_1+3} 5^{\alpha_2} 7^{\alpha_3} \end{array}\right.$$

$$\implies \left\{\begin{array}{rcl} N_a & = & (\alpha_1+1)(\alpha_2+1)(\alpha_3+1) \\ \text{y} & & \\ N_{5a} & = & (\alpha_1+1)(\alpha_2+2)(\alpha_3+1) \\ \text{y} & & \\ N_{8a} & = & (\alpha_1+4)(\alpha_2+1)(\alpha_3+1) \end{array}\right.$$

y por los datos del enunciado,

$$\left.\begin{array}{rcl} N_{5a} & = & N_a + 8 \\ \text{y} & & \\ N_{8a} & = & N_a + 18 \end{array}\right\}$$

es decir,

$$\left.\begin{array}{rcl} (\alpha_1+1)(\alpha_2+2)(\alpha_3+1) & = & (\alpha_1+1)(\alpha_2+1)(\alpha_3+1)+8 \\ \text{y} & & \\ (\alpha_1+4)(\alpha_2+1)(\alpha_3+1) & = & (\alpha_1+1)(\alpha_2+1)(\alpha_3+1)+18 \end{array}\right\}$$

y haciendo operaciones,

$$\left.\begin{array}{rcl} (\alpha_1+1)(\alpha_3+1)(\alpha_2+2-\alpha_2-1) & = & 8 \\ \text{y} & & \\ (\alpha_2+1)(\alpha_3+1)(\alpha_1+4-\alpha_1-1) & = & 18 \end{array}\right\} \Longrightarrow \left\{\begin{array}{rcl} (\alpha_1+1)(\alpha_3+1) & = & 8 \\ \text{y} & & \\ (\alpha_2+1)(\alpha_3+1) & = & 6 \end{array}\right.$$

$$\Longrightarrow \left\{\begin{array}{l} \alpha_3+1 \text{ es divisor de } 8 \\ \text{y} \\ \alpha_3+1 \text{ es divisor de } 6 \end{array}\right.$$

$$\left[\begin{array}{rcl} D_8 & = & \{1,2,4,8\} \\ \text{y} & & \\ D_6 & = & \{1,2,3,6\} \end{array}\right]$$

$$\Longrightarrow \left\{\begin{array}{l} \alpha_3+1 \in \{1,2,4,8\} \\ \text{y} \\ \alpha_3+1 \in \{1,2,3,6\} \end{array}\right.$$

$$\Longrightarrow \left\{\begin{array}{l} \alpha_3+1=1 \\ \text{ó} \\ \alpha_3+1=2 \end{array}\right.$$

$$\Longrightarrow \left\{\begin{array}{l} \alpha_3=0. \text{ Imposible, ya que } \alpha_3 \geqslant 1 \\ \text{ó} \\ \alpha_3=1 \end{array}\right.$$

Además,

$$\left.\begin{array}{rcl} (\alpha_1+1)(\alpha_3+1) & = & 8 \\ \text{y} & & \\ (\alpha_3+1) & = & 2 \end{array}\right\} \Longrightarrow \alpha_1+1=4 \Longrightarrow \alpha_1=3$$

y

$$\left.\begin{array}{rcl} (\alpha_2+1)(\alpha_3+1) & = & 8 \\ \text{y} & & \\ (\alpha_3+1) & = & 2 \end{array}\right\} \Longrightarrow \alpha_2+1=3 \Longrightarrow \alpha_2=2$$

por lo tanto el número buscado es:

$$\left.\begin{array}{l}\alpha_1 = 3\\ \text{y}\\ \alpha_2 = 2\\ \text{y}\\ \alpha_3 = 1\\ \text{y}\\ a = 2^{\alpha_1}5^{\alpha_2}7^{\alpha_3}\end{array}\right\} \Longrightarrow a = 2^3 5^2 7 \implies a = 1400$$

Veamos ahora la suma de todos sus divisores. Por 14.4.6,

$$S = \frac{2^{3+1}-1}{2-1}\cdot\frac{5^{2+1}-1}{5-1}\cdot\frac{7^{1+1}-1}{7-1} = 3720$$

■

Ejemplo 14.14

Un número tiene 24 *divisores, su mitad* 18 *divisores y su triple* 28 *divisores. Hallar el número y sus divisores.*

Solución

Sea a el número buscado y supongamos que su descomposición en factores primos es

$$a = p_1^{\alpha_1}p_2^{\alpha_2}p_3^{\alpha_3}\cdots p_k^{\alpha_k}.$$

Como su mitad tiene 18 divisores, a ha de ser divisible por 2, luego uno de los factores primos, pongamos p_1, ha de ser 2, es decir,

$$a = 2^{\alpha_1}p_2^{\alpha_2}p_3^{\alpha_3}\cdots p_k^{\alpha_k}$$

y

$$\frac{a}{2} = 2^{\alpha_1-1}p_2^{\alpha_2}p_3^{\alpha_3}\cdots p_k^{\alpha_k}.$$

Entonces,

$$N_a = 24 \implies (\alpha_1+1)(\alpha_2+1)(\alpha_3+1)\cdots(\alpha_k+1) = 24$$

y

$$N_{a/2} = 18 \implies (\alpha_1-1+1)(\alpha_2+1)(\alpha_3+1)\cdots(\alpha_k+1) = 18.$$

Dividiendo miembro a miembro,

$$\frac{\alpha_1+1}{\alpha_1} = \frac{24}{18} \Longrightarrow \frac{\alpha_1+1}{\alpha_1} = \frac{4}{3} \Longrightarrow \alpha_1 = 3.$$

Así pues,

$$a = 2^3 p_2^{\alpha_2}p_3^{\alpha_3}\cdots p_k^{\alpha_k}$$

y si ninguno de los restantes factores primos es 3, entonces,

$$3a = 3\cdot 2^3 p_2^{\alpha_2}p_3^{\alpha_3}\cdots p_k^{\alpha_k}$$

luego,

$$N_{3a} = 28 \Longrightarrow (3+1)(\alpha_2+1)\cdots(\alpha_k+1)(1+1) = 28 \Longrightarrow 2(\alpha_2+1)\cdots(\alpha_k+1) = 7$$

y esto es imposible ya que 7 es primo. Por lo tanto uno de los factores primos de la descomposición de a, digamos p_2, ha de ser 3. Entonces,

$$a = 2^3 3^{\alpha_2} p_3^{\alpha_3}\cdots p_k^{\alpha_k},\ \text{con } \alpha_2 \geqslant 1$$

y

$$3a = 2^3 3^{\alpha_2+1} p_3^{\alpha_3}\cdots p_k^{\alpha_k}$$

luego,

$$\begin{aligned}
N_{3a} = 28 \quad &\Longrightarrow \quad (3+1)(\alpha_2+2)(\alpha_3+1)\cdots(\alpha_k+1) = 28\\
&\Longrightarrow \quad (\alpha_2+2)(\alpha_3+1)\cdots(\alpha_k+1) = 7\\
&\Longrightarrow \quad \begin{cases} \alpha_2+2 \text{ es divisor de } 7\\ \text{y}\\ \alpha_i+1 \text{ es divisor de } 7,\ 3 \leqslant i \leqslant k \end{cases}\\
&\qquad [p_2 \text{ es primo} \Longrightarrow D_7 = \{1,7\}]\\
&\Longrightarrow \quad \begin{cases} \alpha_2+2 \in \{1,7\}\\ \text{y}\\ \alpha_i+1 \in \{1,7\},\ 3 \leqslant i \leqslant k \end{cases}\\
&\qquad [\alpha_2 \geqslant 1 \Longrightarrow \alpha_2+2 \geqslant 3]\\
&\Longrightarrow \quad \begin{cases} \alpha_2+2 \in \{1,7\} \text{ y } \alpha_2+2 \geqslant 3\\ \text{y}\\ \alpha_i+1 \in \{1,7\},\ 3 \leqslant i \leqslant k \end{cases}\\
&\Longrightarrow \quad \begin{cases} \alpha_2+2 = 7\\ \text{y}\\ \alpha_i+1 \in \{1,7\},\ 3 \leqslant i \leqslant k \end{cases}\\
&\qquad [(\alpha_2+2)(\alpha_3+1)\cdots(\alpha_k+1) = 7]\\
&\Longrightarrow \quad \begin{cases} \alpha_2+2 = 7\\ \text{y}\\ \alpha_i+1 = 1,\ 3 \leqslant i \leqslant k \end{cases}\\
&\Longrightarrow \quad \begin{cases} \alpha_2 = 5\\ \text{y}\\ \alpha_i = 0,\ 3 \leqslant i \leqslant k \end{cases}
\end{aligned}$$

y como 7 es primo, el producto anterior tiene un sólo factor resultando, en consecuencia,

$$\alpha_2+2 = 7 \Longrightarrow \alpha_2 = 5$$

es decir el número pedido es

$$a = 2^3 \cdot 3^5 = 8 \cdot 243 = 1944.$$

Veamos ahora cuales son sus divisores. Utilizando el método 14.4.4,

	1	2	4	8
$\times 3^1$	3	6	12	24
$\times 3^2$	9	18	36	72
$\times 3^3$	27	54	108	216
$\times 3^4$	81	162	324	648
$\times 3^5$	243	486	972	1944

■

14.5 Reglas para el cálculo del máximo común divisor y el mínimo común múltiplo de dos números

Estableceremos un método alternativo al algoritmo de Euclides para el cálculo del máximo común divisor de dos números. Está basado en el Teorema Fundamental de la Aritmética.

14.5.1 Máximo común divisor

El máximo común divisor de dos números enteros es igual al producto de los factores primos comunes a ambos, elevados a los menores exponentes con que aparezcan en sus respectivas descomposiciones en factores primos.

Demostración

Sean a y b enteros cualesquiera. Recordemos que la relación de orden parcial de divisibilidad es:

$$a \preccurlyeq b \iff a \text{ es divisor de } b$$

Pues bien, por el corolario 14.3.5, tanto a como b admiten una descomposición única en factores primos y según vimos en 14.4.3,

$$a \text{ es divisor de } b \iff \begin{cases} a \text{ tiene en su descomposición, a lo sumo, todos los factores} \\ \text{primos de } b \text{ con exponentes iguales o menores.} \end{cases}$$

Ahora bien, por el lema 14.4.1, podemos escribir a y b en la forma:

$$a = p_1^{\alpha_1} p_2^{\alpha_2} \cdot \cdots \cdot p_k^{\alpha_k},\ \alpha_i \geqslant 0,\ 1 \leqslant i \leqslant k$$

y

$$b = p_1^{\beta_1} p_2^{\beta_2} \cdot \cdots \cdot p_k^{\beta_k},\ \beta_i \geqslant 0,\ 1 \leqslant i \leqslant k$$

siendo $\alpha_i = 0$, si el factor primo p_i de la descomposición de b no aparece en la de a y $\beta_i = 0$ si el p_i de la descomposición de a no aparece en la de b. Podemos pues, escribir de nuevo la relación de divisibilidad en estos términos,

$$\begin{aligned} a \preccurlyeq b &\iff a \text{ es divisor de } b \\ &\iff \left\{ \begin{array}{l} a \text{ tiene en su factorización todos los factores} \\ \text{primos de } b \text{ con exponentes iguales o menores.} \end{array} \right. \\ &\iff \alpha_i \leqslant \beta_i, \forall i, 1 \leqslant i \leqslant k \end{aligned}$$

Supongamos que a y b son dos enteros cualesquiera de valor absoluto mayor que 1.

- Si a divide a b, entonces m.c.d.$(a, b) = a$.
- Si b divide a a, entonces m.c.d.$(a, b) = b$.

Supondremos, por tanto, que a no divide a b ni b divide a a.

Por definición de máximo común divisor,

$$\text{m.c.d.}(a, b) = \inf\{a, b\} = \max\left(C_{\inf}\left(\{a, b\}\right)\right).$$

siendo $C_{\inf}\left(\{a, b\}\right)$ el conjunto de las cotas inferiores del conjunto $\{a, b\}$ ordenado por la relación de orden parcial de divisibilidad.

Pues bien, sea c cualquiera de $\mathbb{Z}^+$. Aplicando el lema 14.4.1, podemos escribir c en la forma:

$$c = p_1^{\gamma_1} p_2^{\gamma_2} \cdot \cdots \cdot p_k^{\gamma_k}$$

Pues bien,

$$\begin{aligned} c \in C_{\inf}\left(\{a, b\}\right) &\iff c \preccurlyeq x, \forall x \in \{a, b\} \\ &\iff \left\{ \begin{array}{l} c \preccurlyeq a \\ \text{y} \\ c \preccurlyeq b \end{array} \right. \\ &\iff \left\{ \begin{array}{l} \gamma_i \leqslant \alpha_i,\ 1 \leqslant i \leqslant k \\ \text{y} \\ \gamma_i \leqslant \beta_i,\ 1 \leqslant i \leqslant k \end{array} \right. \\ &\iff \gamma_i \leqslant \min\{\alpha_i, \beta_i\},\ 1 \leqslant i \leqslant k \end{aligned}$$

Por lo tanto,

$$C_{\inf}\left(\{a, b\}\right) = \left\{p_1^{\gamma_1} p_2^{\gamma_2} \cdot \cdots \cdot p_k^{\gamma_k} : \gamma_i \leqslant \min\{\alpha_i, \beta_i\},\ 1 \leqslant i \leqslant k\right\}.$$

Entonces,

$$\begin{aligned} \text{m.c.d.}(a, b) &= \inf\left(\{a, b\}\right) \\ &= \max\left(C_{\inf}\left(\{a, b\}\right)\right) \\ &= \max\left\{p_1^{\gamma_1} p_2^{\gamma_2} \cdot \cdots \cdot p_k^{\gamma_k} : \gamma_i \leqslant \min\{\alpha_i, \beta_i\},\ 1 \leqslant i \leqslant k\right\} \\ &= p_1^{\min\{\alpha_1, \beta_1\}} p_2^{\min\{\alpha_1, \beta_2\}} \cdot \cdots \cdot p_k^{\min\{\alpha_k, \beta_k\}} \end{aligned}$$

Ahora, para cada i entre 1 y k, puede ocurrir lo siguiente:

$$\min\{\alpha_i, \beta_i\} = 0 \implies \begin{cases} \alpha_i = 0 \\ \text{ó} \\ \beta_i = 0 \end{cases}$$

$$\implies \begin{cases} p_i \text{ no está en la descomposición en factores primos de } a. \\ \text{ó} \\ p_i \text{ no está en la descomposición en factores primos de } b. \end{cases}$$

$$\implies \text{El factor primo } p_i \text{ no es común a } a \text{ y a } b$$

ó

$$\min\{\alpha_i, \beta_i\} \neq 0 \implies \begin{cases} \alpha_i \neq 0 \\ \text{y} \\ \beta_i \neq 0 \end{cases}$$

$$\implies \begin{cases} p_i \text{ está en la descomposición en factores primos de } a. \\ \text{y} \\ p_i \text{ está en la descomposición en factores primos de } b. \end{cases}$$

$$\implies \text{El factor primo } p_i \text{ es común a } a \text{ y a } b$$

Por lo tanto, el máximo común divisor de dos números es el producto de los factores primos comunes a ambos elevados a sus menores exponentes.

■

Ejemplo 14.15

Calcular el máximo común divisor de 1548 *y* 18900.

Solución

Lo calcularemos siguiendo los pasos del apartado anterior.

Descomponemos ambos números en factores primos.

$$\begin{array}{r|l} 1584 & 2 \\ 792 & 2 \\ 396 & 2 \\ 198 & 2 \\ 99 & 3 \\ 33 & 3 \\ 11 & 11 \\ 1 & \end{array} \quad \Longrightarrow \quad 1584 = 2^4 \cdot 3^2 \cdot 11$$

$$\begin{array}{r|l} 18900 & 2 \\ 9450 & 2 \\ 4725 & 3 \\ 1575 & 3 \\ 525 & 3 \\ 175 & 5 \\ 35 & 5 \\ 7 & 7 \\ 1 & \end{array} \quad \Longrightarrow \quad 18900 = 2^2 \cdot 3^3 \cdot 5^2 \cdot 7$$

Completamos la descomposición en factores primos de los dos números, añadiendo a cada uno de ellos los factores primos que no tenga del otro, con exponente cero (lema 14.4.1).

$$\begin{aligned} 1584 &= 2^4 \cdot 3^2 \cdot 5^0 \cdot 7^0 \cdot 11 \\ 18900 &= 2^2 \cdot 3^3 \cdot 5^2 \cdot 7 \cdot 11^0 \end{aligned}$$

Entonces,

$$\begin{aligned} \text{m.c.d.}(1548, 18900) &= 2^{\min\{4,2\}} 3^{\min\{2,3\}} 5^{\min\{0,2\}} 7^{\min\{0,1\}} 11^{\min\{1,0\}} \\ &= 2^2 \cdot 3^2 \cdot 5^0 \cdot 7^0 \cdot 11^0 \\ &= 2^2 \cdot 3^2 \\ &= 36 \end{aligned}$$

es decir, los factores primos comunes a ambos números (2 y 3) con sus menores exponentes (2 y 2).

■

14.5.2 Mínimo común múltiplo

El mínimo común múltiplo de dos números enteros es igual al producto de los factores primos comunes y no comunes a ambos, elevados a los mayores exponentes con que aparezcan en sus respectivas descomposiciones en factores primos.

Demostración

Sean a y b son dos enteros cualesquiera de valor absoluto mayor que 1.

Al igual que en el apartado anterior, el lema 14.4.1 nos permite escribir a y b en la forma:

$$a = p_1^{\alpha_1} p_2^{\alpha_2} \cdot \cdots \cdot p_k^{\alpha_k},\ \alpha_i \geqslant 0,\ 1 \leqslant i \leqslant k$$

y

$$b = p_1^{\beta_1} p_2^{\beta_2} \cdot \cdots \cdot p_k^{\beta_k},\ \beta_i \geqslant 0,\ 1 \leqslant i \leqslant k$$

siendo $\alpha_i = 0$, si el factor primo p_i de la descomposición de b no aparece en la de a y $\beta_i = 0$ si el p_i de la descomposición de a no aparece en la de b. Podemos pues, escribir de nuevo la relación de divisibilidad en estos términos,

$$\begin{aligned} a \preccurlyeq b &\iff a \text{ es divisor de } b \\ &\iff \begin{cases} a \text{ tiene en su factorización todos los factores} \\ \text{primos de } b \text{ con exponentes iguales o menores.} \end{cases} \\ &\iff \alpha_i \leqslant \beta_i, \forall i, 1 \leqslant i \leqslant k \end{aligned}$$

- Si a divide a b, entonces $\text{m.c.m.}(a,b) = b$.
- Si b divide a a, entonces $\text{m.c.m.}(a,b) = a$.

Supondremos, por tanto, que a no divide a b ni b divide a a.

Por definición de mínimo común múltiplo,

$$\text{m.c.m.}(a,b) = \sup\{a,b\} = \min\left(C_{\sup}\left(\{a,b\}\right)\right).$$

siendo $C_{\sup}\left(\{a,b\}\right)$ el conjunto de las cotas superiores del conjunto $\{a,b\}$ ordenado por la relación de orden parcial de divisibilidad.

Sea s cualquiera de $\mathbb{Z}^+$. Aplicando el lema 14.4.1, podemos escribir s en la forma:

$$s = p_1^{\gamma_1} p_2^{\gamma_2} \cdot \cdots \cdot p_k^{\gamma_k}$$

Pues bien,

$$\begin{aligned} s \in C_{\sup}\left(\{a,b\}\right) &\iff x \preccurlyeq s, \forall x \in \{a,b\} \\ &\iff \begin{cases} a \preccurlyeq s \\ \text{y} \\ b \preccurlyeq s \end{cases} \\ &\iff \begin{cases} \alpha_i \leqslant \gamma_i,\ 1 \leqslant i \leqslant k \\ \text{y} \\ \beta_i \leqslant \gamma_i,\ 1 \leqslant i \leqslant k \end{cases} \\ &\iff \gamma_i \geqslant \max\{\alpha_i, \beta_i\},\ 1 \leqslant i \leqslant k \end{aligned}$$

Luego,

$$C_{\sup}\left(\{a,b\}\right) = \{p_1^{\gamma_1} p_2^{\gamma_2} \cdot \cdots \cdot p_k^{\gamma_k} : \gamma_i \geqslant \max\{\alpha_i, \beta_i\},\ 1 \leqslant i \leqslant k\}$$

Entonces,

$$\begin{aligned} \text{m.c.m.}(a,b) &= \min\left(C_{\sup}\left(\{a,b\}\right)\right) \\ &= \min\{p_1^{\gamma_1} p_2^{\gamma_2} \cdot \cdots \cdot p_k^{\gamma_k} : \gamma_i \geqslant \max\{\alpha_i, \beta_i\},\ 1 \leqslant i \leqslant k\} \\ &= p_1^{\max\{\alpha_1,\beta_1\}} p_2^{\max\{\alpha_1,\beta_2\}} \cdot \cdots \cdot p_k^{\max\{\alpha_k,\beta_k\}} \end{aligned}$$

Ahora, para cada i entre 1 y k, puede ocurrir lo siguiente:

$$\left.\begin{array}{l}\alpha_i = 0\\ \text{y}\\ \beta_i \neq 0\end{array}\right\} \Longrightarrow \text{El factor primo } p_i \text{ no es común a } a \text{ y a } b \text{ y } \max\{\alpha_i, \beta_i\} = \beta_i$$

ó

$$\left.\begin{array}{l}\alpha_i \neq 0\\ \text{y}\\ \beta_i = 0\end{array}\right\} \Longrightarrow \text{El factor primo } p_i \text{ no es común a } a \text{ y a } b \text{ y } \max\{\alpha_i, \beta_i\} = \alpha_i$$

ó

$$\left.\begin{array}{l}\alpha_i \neq 0\\ \text{y}\\ \beta_i \neq 0\end{array}\right\} \Longrightarrow \text{El factor primo } p_i \text{ es común a } a \text{ y a } b$$

Por lo tanto, el mínimo común múltiplo de dos números es igual al productos de los factores primos comunes y no comunes a ambos elevados a sus mayores exponentes.

■

Ejemplo 14.16

Calcular el mínimo común múltiplo de 1548 *y* 18900.

Solución

Según el ejemplo anterior,

$$\begin{aligned} 1584 &= 2^4 \cdot 3^2 \cdot 11 \\ 18900 &= 2^2 \cdot 3^3 \cdot 5^2 \cdot 7 \end{aligned}$$

Completamos la descomposición en factores primos de los dos números, añadiendo a cada uno de ellos los factores primos que no tenga del otro, con exponente cero (lema 14.4.1).

$$\begin{aligned} 1584 &= 2^4 \cdot 3^2 \cdot 5^0 \cdot 7^0 \cdot 11 \\ 18900 &= 2^2 \cdot 3^3 \cdot 5^2 \cdot 7 \cdot 11^0 \end{aligned}$$

Entonces,

$$\begin{aligned} \text{m.c.m.}(1548, 18900) &= 2^{\max\{4,2\}} 3^{\max\{2,3\}} 5^{\max\{0,2\}} 7^{\max\{0,1\}} 11^{\max\{1,0\}} \\ &= 2^4 \cdot 3^3 \cdot 5^2 \cdot 7^1 \cdot 11^1 \\ &= 831600 \end{aligned}$$

es decir, los factores primos comunes y no comunes de ambos números con sus mayores exponentes.

■

Lección 15

Ecuaciones Diofánticas

15.1 Generalidades

Estas ecuaciones reciben este nombre en honor a Diofanto[1], matemático que trabajó en Alejandría a mediados del siglo III a.c. Fue uno de los primeros en introducir la notación simbólica en matemáticas y escribió seis libros sobre problemas en las que consideraba la representación de números anterior como suma de cuadrados.

15.1.1 Definición

Una ecuación diofántica es una ecuación lineal con coeficientes enteros y que exige soluciones también enteras.

15.2 Solución de una Ecuación Diofántica

Veremos un teorema que nos permite saber cuando una ecuación de este tipo tiene solución y aporta un método para calcular una solución particular de la misma.

15.2.1 Solución Particular

Sean a, b y c tres números enteros. La ecuación lineal $ax + by = c$ tiene solución entera si, y sólo si el máximo común divisor de a y b divide a c.

Demostración

[1] Matemático griego de la escuela de Alejandría (a.c. 325-a.c. 410). Dejó trece libros de aritmética, de los cuales sólo los seis primeros nos han llegado, y otro sobre los Números angulares. Aunque tomó como ejemplo para sus métodos los trabajos de Hiparco, su teoría completamente nueva de ecuaciones de primer grado y la resolución que dio a las de segundo hacen de él un innovador en este campo. Sus obras han constituido tema de meditación de sus contemporáneos griegos, y de los árabes, y, más tarde, de los geómetras del renacimiento. El mismo Viete en su obra capital, reproduce sus proposiciones, aunque sustituye los problemas abstractos por cuestiones de geometría resolubles por álgebra.

"Sólo si". En efecto, supongamos que los enteros x_0 e y_0 son solución de la ecuación $ax + by = c$, es decir, $ax_0 + by_0 = c$. Pues bien, si $d = \text{m.c.d.}(a, b)$, entonces

$$d = \text{m.c.d.}(a, b) \implies d|a \text{ y } d|b \implies d|ax_0 + by_0 \implies d|c$$

"Si". Recíprocamente, supongamos que $d = \text{m.c.d.}(a, b)$ es divisor de c. Entonces,

$$\begin{aligned} \text{m.c.d.}(a, b) = d &\implies \text{m.c.d.}\left(\frac{a}{d}, \frac{b}{d}\right) = 1 \\ &\iff \exists p, q \in \mathbb{Z} : \frac{a}{d}p + \frac{b}{d}q = 1 \\ &\implies a\frac{cp}{d} + b\frac{cq}{d} = c \end{aligned}$$

siendo $\dfrac{c}{d}$ entero ya que, por hipótesis, d es divisor de c. Ahora bastaría tomar

$$x_0 = \frac{cp}{d} \text{ e } y_0 = \frac{cq}{d}$$

y tendríamos que

$$ax_0 + by_0 = c$$

es decir los enteros x_0 e y_0 son solución de la ecuación.

La solución encontrada se llamará *solución particular* del sistema.

■

Obsérvese que este teorema además de asegurar la existencia de solución para una ecuación de este tipo, ofrece un método para calcularla. El siguiente ejemplo aclarará estas cuestiones.

Ejemplo 15.1

Encontrar una solución para la ecuación diofántica $525x + 100y = 50$

Solución

♢ Veamos si existe solución entera para la ecuación.

Calculamos el máximo común divisor de 525 y 100 mediante el algoritmo de Euclides.

	5	4
525	100	25
25	0	

es decir,

$$\text{m.c.d.}\,(525, 100) = 25$$

y como 25 divide a 50, el teorema anterior asegura la existencia de solución entera para la ecuación.

♢ Calculamos una solución para la ecuación.

Siguiendo el método indicado en la demostración del teorema, hallamos los coeficientes de la combinación lineal del máximo común divisor de 525 y 100. Bastaría seguir el algoritmo de Euclides hacia atrás.

$$25 = 1 \cdot 525 + (-5) \cdot 100$$

por tanto, los coeficientes buscados son $p = 1$ y $q = -5$ y según el citado teorema una solución para la ecuación sería

$$x_0 = \frac{cp}{d} \text{ e } y_0 = \frac{cq}{d}$$

donde c es el término independiente de la ecuación y d el máximo común divisor de los coeficientes de x e y. Consecuentemente,

$$x_0 = \frac{50 \cdot 1}{25} = 2$$

e

$$y_0 = \frac{50 \cdot (-5)}{25} = -10$$

■

15.2.2 Solución General

Sean a, b y c tres números enteros no nulos tales que el máximo común divisor de a y b divide a c. Entonces la solución general de la ecuación $ax + by = c$ es

$$x = x_0 + k \cdot \frac{b}{d}$$
$$y = y_0 - k \cdot \frac{a}{d}$$

donde x_0 e y_0 es una solución particular de la misma y k es cualquier número entero.

Demostración

Sea d el máximo común divisor de a y b. Por hipótesis d divide a c luego el teorema 15.2.1 asegura la existencia de una solución particular $x = x_0$ e $y = y_0$ para el sistema. Entonces,

$$ax_0 + by_0 = c$$

Dividiendo ahora ambos miembros de esta ecuación por el máximo común divisor de a y b, tendremos,

$$\frac{a}{d}x_0 + \frac{b}{d}y_0 = \frac{c}{d}$$

siendo $\frac{c}{d}$ entero y $\frac{a}{d}, \frac{b}{d}$ números enteros primos entre sí, luego el máximo común divisor de ambos es 1 y como 1 divide a $\frac{c}{d}$, el teorema 15.2.1 asegura la existencia de una solución particular x_1, y_1 para esta ecuación, luego

$$\frac{a}{d}x_1 + \frac{b}{d}y_1 = \frac{c}{d}$$

Pues bien,

$$\left.\begin{array}{l} \frac{a}{d}x_1 + \frac{b}{d}y_1 = \frac{c}{d} \\ \frac{a}{d}x_0 + \frac{b}{d}y_0 = \frac{c}{d} \end{array}\right\} \implies \frac{a}{d}(x_1 - x_0) + \frac{b}{d}(y_1 - y_0) = 0$$

$$\implies \frac{a}{d}(x_1 - x_0) = \frac{b}{d}(y_0 - y_1)$$

$$\iff \frac{b}{d} \left| \frac{a}{d}(x_1 - x_0) \right.$$

y al ser $\frac{b}{d}$ primo con $\frac{a}{d}$, dividirá a $x_1 - x_0$, luego

$$\frac{b}{d} | x_1 - x_0 \iff \exists k \in \mathbb{Z} : x_1 - x_0 = k \cdot \frac{b}{d} \implies x_1 = x_0 + k \cdot \frac{b}{d}$$

Sustituimos el valor de $x_1 - x_0$ en $\frac{a}{d}(x_1 - x_0) + \frac{b}{d}(y_1 - y_0) = 0$ y resulta

$$\frac{a}{d} \cdot k \cdot \frac{b}{d} + \frac{b}{d}(y_1 - y_0) = 0 \implies \frac{a}{d} \cdot k + y_1 - y_0 = 0 \implies y_1 = y_0 - k \cdot \frac{a}{d}$$

Veamos, finalmente, que x_1 e y_1 es solución de la ecuación $ax + by = c$.

En efecto,

$$\begin{aligned} ax_1 + by_1 &= a\left(x_0 + k \cdot \frac{b}{d}\right) + b\left(y_0 - k \cdot \frac{a}{d}\right) \\ &= ax_0 + a \cdot k \cdot \frac{b}{d} + by_0 - b \cdot k \cdot \frac{a}{d} \\ &= ax_0 + by_0 \\ &= c \end{aligned}$$

y tomando $x = x_1$ e $y = y_1$,

$$x = x_0 + k \cdot \frac{b}{d}$$

$$y = y_0 - k \cdot \frac{a}{d}$$

es solución de la ecuación $ax + by = c$ cualquiera que sea $k \in \mathbb{Z}$. La llamaremos *solución general* de dicha ecuación.

■

Nota 15.1 En el ejemplo anterior, teníamos que

$$x_0 = 2 \text{ e } y_0 = -10$$

era una solución particular para la ecuación

$$525x + 100y = 50$$

luego una solución general de la misma, será:

$$x = 2 + k \cdot \frac{100}{25} = 2 + 4k$$

$$y = -10 - k \cdot \frac{525}{25} = -10 - 21k$$

siendo k cualquier número entero.

■

Ejemplo 15.2

Calcular las soluciones enteras de la ecuación diofántica $66x + 550y = 88$

Solución

$$66x + 550y = 88$$

♢ Veamos si la ecuación admite solución entera.

Calculamos el máximo común divisor de 66 y 550 por el algoritmo de Euclides.

	8	3
550	66	22
22	0	

luego,

$$\text{m.c.d.}\,(66, 550) = 22$$

y como 22 divide a 88, término independiente de la ecuación, por el teorema 15.2.1 se sigue que la ecuación propuesta admite una solución particular $x = x_0$, $y = y_0$.

♢ Calculamos esta solución particular.

Volviendo hacia atrás en el algoritmo de Euclides, tendremos

$$22 = (-8) \cdot 66 + 1 \cdot 550$$

luego,

$$x_0 = \frac{88 \cdot (-8)}{22} = -32$$
$$y_0 = \frac{88 \cdot 1}{22} = 4$$

es una *solución particular* de la ecuación.

♢ Calculemos ahora la *solución general*.

Según lo visto en el teorema 15.2.2 si una solución particular de la misma es $x_0 = -32$ e $y_0 = 4$, entonces la solución general es:

$$x = -32 + k \cdot \frac{550}{22} = -32 + 25 \cdot k$$
$$y = 4 - k \cdot \frac{66}{22} = 4 - 3k$$

siendo k cualquier número entero.

■

Ejemplo 15.3

Una persona va a un supermercado y compra 12 *litros de leche, unos de leche entera y otros de desnatada, por* 1200 *ptas. Si la leche entera vale* 30 *ptas. más por litro que la desnatada, y ha comprado el mínimo posible de leche desnatada, ¿Cuántos litros habrá comprado de cada una?*

Solución

Si x el número de litros de leche entera, entonces $12 - x$ es el número de litros de leche desnatada y si y es el precio de la leche desnatada, entonces el precio de la leche entera será $y + 30$.

Como el precio total de la leche comprada es 1200, tendremos que

$$x(y + 30) + y(12 - x) = 1200$$

de aquí que

$$xy + 30x + 126 - xy = 1200$$

o sea,

$$30x + 12y = 1200$$

♢ Veamos si esta ecuación admite soluciones enteras. Hallamos el máximo común divisor de 30 y 12 por el algoritmo de Euclides.

	2	2
30	12	6
6	0	

luego,

$$\text{m.c.d.}\,(30, 12) = 6$$

y dado que 6 divide a 1200, la ecuación planteada admite soluciones enteras.

♢ Calculamos una *solución particular*.

Como m.c.d. $(30, 12) = 6$, existirán dos números enteros p y q tales que 6 pueda expresarse como combinación lineal de 30 y 12 con coeficientes enteros. Los hallaremos volviendo hacia atrás en el algoritmo de Euclides.

$$6 = 1 \cdot 30 + (-2) \cdot 12$$

luego entonces los coeficientes buscados son 1 y -2 y la *solución particular* de la ecuación es

$$x_0 = \frac{1200 \cdot 1}{6} = 200$$
$$y_0 = \frac{1200 \cdot (-2)}{6} = -400$$

♢ La *solución general* será:

$$x = 200 + k \cdot \frac{12}{6} = 200 + 2k$$
$$y = -400 - k \cdot \frac{30}{6} = -400 - 5k$$

siendo k cualquier número entero.

♢ Veamos, finalmente, cuantos litros se han comprado de cada tipo de leche.

Según lo visto hasta ahora, la cantidad de leche entera es

$$C_e = 200 + 2k : k \in \mathbb{Z}$$

y la cantidad de leche desnatada será, por tanto,

$$C_d = 12 - C_e = 12 - 200 - 2k = -188 - 2k : k \in \mathbb{Z}$$

Pues bien, suponiendo que se compra alguna cantidad de leche desnatada, tendremos que

$$\begin{aligned} C_d > 0 &\iff 12 - C_e > 0 \\ &\iff 0 < C_e < 12 \\ &\iff 0 < 200 + 2k < 12 \\ &\iff -200 < 2k < -188 \\ &\iff -100 < k < -94 \\ &\iff k \in \{-99, -98, -97, -96, -95\} \end{aligned}$$

y la cantidad mínima de leche desnatada se corresponderá con la máxima de leche entera y esta se da para el valor máximo que pueda tener k, es decir para $k = -95$. Por tanto,

$$\begin{aligned} C_e &= 200 + 2(-95) = 200 - 190 = 10 \\ C_d &= 12 - C_e = 2 \end{aligned}$$

o sea, se compraron 10 litros de leche entera y 2 litros de leche desnatada.

■

Ejemplo 15.4

Hallar los valores de $c \in \mathbb{Z}^+$, *con* $10 < c < 20$ *para los cuales no tiene solución la ecuación diofántica* $84x + 990y = c$. *Determinar la solución para los restantes valores de* c.

Solución

♢ La ecuación $84x + 990y = c$ admitirá solución entera si, y sólo si el máximo común divisor de 84 y 990 divide a c.

Hallamos dicho máximo común divisor por el algoritmo de Euclides.

	11	1	3	1	2
990	84	66	18	12	6
66	18	12	6	0	

luego

$$\text{m.c.d.}\,(84, 990) = 6$$

entonces,

$$84x + 990y = c \text{ tiene solución entera} \iff 6\,|c \iff \exists q \in \mathbb{Z} : c = 6 \cdot q$$

y como $10 < c < 20$, tendremos que las opciones posibles para las que la ecuación tiene solución son

$$c = 12 \text{ y } c = 18$$

por tanto los valores de c para los que la ecuación no admite solución entera serán:

$$11, 13, 14, 15, 16, 17 \text{ y } 19$$

♢ Calculamos una *solución particular* para la ecuación propuesta.

Volviendo hacia atrás el cálculo hecho en el algoritmo de Euclides, tendremos

$$\left.\begin{array}{l} 6 = 18 - 1 \cdot 12 \\ 12 = 66 - 3 \cdot 18 \end{array}\right\} \implies \begin{array}{rcl} 6 & = & 18 - 1(66 - 3 \cdot 18) \\ & = & -1 \cdot 66 + 4 \cdot 18 \end{array}$$

$$\left.\begin{array}{l} 6 = -1 \cdot 66 + 4 \cdot 18 \\ 18 = 84 - 1 \cdot 66 \end{array}\right\} \implies \begin{array}{rcl} 6 & = & -1 \cdot 66 + 4(84 - 1 \cdot 66) \\ & = & 4 \cdot 84 - 5 \cdot 66 \end{array}$$

$$\left.\begin{array}{l} 6 = 4 \cdot 84 - 5 \cdot 66 \\ 66 = 990 - 11 \cdot 84 \end{array}\right\} \implies \begin{array}{rcl} 6 & = & 4 \cdot 84 - 5(990 - 11 \cdot 84) \\ & = & -5 \cdot 990 + 59 \cdot 84 \end{array}$$

luego,

$$6 = 59 \cdot 84 + (-5) \cdot 990$$

♢ Solución para $c = 12$.

– Una *solución particular* es

$$x_0 = \frac{12 \cdot 59}{6} = 118$$
$$y_0 = \frac{12 \cdot (-5)}{6} = -10$$

– La *solución general* es

$$x = 118 + k \cdot \frac{990}{6} = 118 + 165k$$
$$y = -10 - k \cdot \frac{84}{6} = -10 - 14k$$

siendo k cualquier número entero.

♢ Solución para $c = 18$.

– Una *solución particular* es

$$x_0 = \frac{18 \cdot 59}{6} = 177$$
$$y_0 = \frac{18 \cdot (-5)}{6} = -15$$

– La *solución general* es

$$x = 177 + k \cdot \frac{990}{6} = 177 + 165k$$
$$y = -15 - k \cdot \frac{84}{6} = -15 - 14k$$

siendo k cualquier número entero.

■

Ejemplo 15.5

Hallar las soluciones enteras de la ecuación

$$\sqrt{(x+y)(x-y) + (2x+2y-3)y - 2(x-7)} = x + y + 3$$

Solución

Elevando al cuadrado ambos miembros

$$x^2 - y^2 + 2xy + 2y^2 - 3y - 2x + 14 = x^2 + y^2 + 2xy + 6x + 6y + 9$$

y simplificando, resulta

$$8x + 9y = 5$$

♢ Veamos si tiene soluciones enteras.

8 y 9 son primos entre sí, luego

$$\text{m.c.d.}\,(8, 9) = 1$$

y como 1 divide a 5, término independiente de la ecuación, esta tendrá soluciones enteras.

♢ Calculamos una *solución particular*

El máximo común divisor de 8 y 9 escrito en combinación lineal de ambos, es

$$1 = (-1) \cdot 8 + 1 \cdot 9$$

luego una solución particular es:

$$x_0 = \frac{5 \cdot (-1)}{1} = -5$$
$$y_0 = \frac{5 \cdot 1}{1} = 5$$

♢ La *solución general*, por tanto, será

$$x = -5 + 9k$$
$$y = 5 - 8k$$

siendo k cualquier número entero.

■

Ejemplo 15.6

Una mujer tiene un cesto de manzanas. Haciendo grupos de 3 *sobran* 2 *y haciendo grupos de* 4 *sobran* 3. *Hallar el número de manzanas que contiene el cesto sabiendo que están entre* 100 *y* 110.

Solución

Sean x e y los números de grupos de tres y cuatro manzanas, respectivamente. Si N es el número total de manzanas que contiene el cesto, tendremos

$$\left.\begin{array}{l} 3x+2=N \\ 4y+3=N \end{array}\right\}$$

y restando miembro a miembro, resulta

$$3x-4y=1$$

♢ Veamos si esta ecuación tiene soluciones enteras.

Como m.c.d. $(3,4)=1$ y 1 divide a 1, término independiente de la ecuación, resulta que la misma admite soluciones enteras.

♢♢ *Solución particular*

$$1=(-1)\cdot 3+(-1)(-4)$$

luego,

$$x_0=\frac{1\cdot(-1)}{1}=-1$$

$$y_0=\frac{1(-1)}{1}=-1$$

es una *solución particular* de la ecuación.

♢♢ *Solución general*

$$x=-1+\frac{-4}{1}\cdot k=-1-4k$$

$$y=1-\frac{3}{1}\cdot k=-1-3k$$

siendo k cualquier número entero.

♢ Calculemos, finalmente, cuantas manzanas hay en el cesto.

$$\left.\begin{array}{l} 3x+2=N \\ x=-1-4k \end{array}\right\}\Longrightarrow 3(-1-4k)+2=N\Longrightarrow N=-12k-1$$

y como N no puede ser 100 porque 100 es múltiplo de 4 y tampoco puede ser 110 porque da resto 2 al dividirlo entre 4,

$$100<N<110$$

tendremos

$$\begin{array}{rcl} 100<-12k-1<110 & \Longrightarrow & \dfrac{101}{12}<-k<\dfrac{111}{12} \\ & \Longrightarrow & \dfrac{-111}{12}<k<\dfrac{-101}{12} \\ & \Longrightarrow & -9.25<k<-8.42 \end{array}$$

y como k es un número entero, tendremos que

$$k=-9$$

Consecuentemente,

$$N = -12(-9) - 1 = 108 - 1 = 107$$

es decir el cesto contiene 107 manzanas.

■

Ejemplo 15.7

Hallar el menor número entero positivo de cuatro cifras que dividido por 4, 7 *y* 11 *da resto* 3, *y que dividido por* 13 *da resto* 1.

Solución

Sea n el número buscado, entonces por el algoritmo de la división existen q_1, q_2 y q_3 tales que

$$\left.\begin{array}{l} n = 4 \cdot q_1 + 3 \Longrightarrow n - 3 = 4 \cdot q_1 \\ n = 7 \cdot q_2 + 3 \Longrightarrow n - 3 = 7 \cdot q_2 \\ n = 11 \cdot q_3 + 3 \Longrightarrow n - 3 = 11 \cdot q_3 \end{array}\right\}$$

luego

$$4 \,|n-3\,,\ 7\,|n-3 \ \text{ y } 11\,|n-3$$

es decir, $n-3$ es un múltiplo común a 4, 7 y 11, por tanto ha de ser múltiplo de su mínimo común múltiplo y al ser

$$\text{m.c.m.}(4, 7, 11) = 4 \cdot 7 \cdot 11 = 308$$

será

$$308\,|n-3$$

luego existirá un entero x tal que

$$n - 3 = 308x$$

es decir,

$$n = 308x + 3$$

Por otro lado y también por el algoritmo de la división, existirá un entero y tal que

$$n = 13y + 1$$

por tanto,

$$\left.\begin{array}{l} n = 308x + 3 \\ n = 13y + 1 \end{array}\right\} \Longrightarrow 308x - 13y = -2$$

♢ Veamos si esta ecuación admite soluciones enteras.

Calculamos el máximo común divisor de 308 y 13 por el algoritmo de Euclides.

	23	1	2	4
308	13	9	4	1
9	4	1	0	

luego

$$\text{m.c.d.}\,(308, 13) = 1$$

y 1 divide a -2, término independiente de la ecuación, luego tiene soluciones enteras.

♢♢ *Solución particular*

Buscamos los coeficientes enteros de 1 expresado como combinación lineal de 308 y -13.

$$\left.\begin{array}{l} 1 = 9 - 2 \cdot 4 \\ 4 = 13 - 1 \cdot 9 \end{array}\right\} \implies \begin{array}{rcl} 1 & = & 9 - 2(13 - 1 \cdot 9) \\ & = & 2(-13) + 3 \cdot 9 \end{array}$$

$$\left.\begin{array}{l} 1 = 2(-13) + 3 \cdot 9 \\ 9 = 308 - 23 \cdot 13 \end{array}\right\} \implies \begin{array}{rcl} 1 & = & 2(-13) + 3 \cdot [308 + 23 \cdot (-13)] \\ & = & 3 \cdot 308 + 71 \cdot (-13) \end{array}$$

luego

$$1 = 3 \cdot 308 + 71 \cdot (-13)$$

y una *solución particular* es:

$$x_0 = \frac{(-2) \cdot 3}{1} = -6$$
$$y_0 = \frac{(-2) \cdot 71}{1} = -142$$

♢♢ *Solución general*

$$x = -6 + k \cdot \frac{-13}{1} = -6 - 13k$$
$$y = -142 - k \cdot \frac{308}{1} = -142 - 308k$$

donde k es cualquier número entero.

♢ Calculemos, finalmente, el número pedido.

$$\left.\begin{array}{l} n = 308x + 3 \\ x = -6 - 13k \end{array}\right\} \Longrightarrow n = 308(-6 - 13k) + 3 = -1845 - 4004k$$

y al ser $n > 0$, tendremos

$$-1845 - 4004k > 0 \Longrightarrow k < -\frac{1845}{4004} \Longrightarrow k < -0.46 \Longrightarrow k \leqslant -1$$

y el número más pequeño se producirá para el valor más alto de k.

Para $k = -1$,

$$n = -1845 - 4004(-1) = 2159$$

y es el menor número de cuatro cifras que cumple las condiciones del enunciado.

■

Ejemplo 15.8

Un granjero gastó 100.000 *pts. en* 100 *animales entre pollos, conejos y terneros. Si los pollos los compró a* 50 *pts, a* 1000 *pts. los conejos y a* 5000 *pts. los terneros y adquirió animales de las tres clases, ¿Cuántos animales compró de cada clase?*

Solución

Sean x, y y z el número de pollos, conejos y terneros, respectivamente. De acuerdo con el enunciado tendremos el siguiente sistema de ecuaciones:

$$\left.\begin{array}{l} x+y+z=100 \\ 50x+1000y+5000z=100000 \end{array}\right\} \implies \left\{\begin{array}{l} x+y+z=100 \\ x+20y+100z=2000 \end{array}\right.$$

$$\implies \left\{\begin{array}{l} x+y+z=100 \\ x+y+z+19y+99z=2000 \end{array}\right.$$

$$\implies 100+19y+99z=2000$$

♢ Veamos si la ecuación propuesta tiene soluciones enteras.

Calculamos el máximo común divisor de 19 y 99 por el algoritmo de Euclides.

	5	4	1	3
99	19	4	3	1
4	3	1	0	

luego,

$$\text{m.c.d.}\,(19,99)=1$$

y como 1 divide a 1990, término independiente de la ecuación, esta tiene soluciones enteras.

♢♢ Calculamos una *solución particular*

Expresamos 1 como combinación lineal de 19 y 99 volviendo hacia atrás los cálculos en el algoritmo de Euclides.

$$\left.\begin{array}{l} 1=4-1\cdot 3 \\ 3=19-4\cdot 4 \end{array}\right\} \implies \begin{array}{rcl} 1 & = & 4-1(19-4\cdot 4) \\ & = & -1\cdot 99+5\cdot 4 \end{array}$$

$$\left.\begin{array}{l} 1=-1\cdot 19+5\cdot 4 \\ 4=99-5\cdot 19 \end{array}\right\} \implies \begin{array}{rcl} 1 & = & -1\cdot 19+5(99-5\cdot 19) \\ & = & 5\cdot 99-26\cdot 19 \end{array}$$

luego,

$$1=(-26)\cdot 19+5\cdot 99$$

por tanto, una

$$y_0=\frac{1900\cdot(-26)}{1}=-49400$$

$$z_0=\frac{1900\cdot 5}{1}=9500$$

♢♢ La *solución general* será,

$$y = -49400 + k \cdot \frac{99}{1} = -49400 + 99k$$
$$z = 9500 - k \cdot \frac{19}{1} = 9500 - 19k$$

siendo k cualquier número entero.

♢ Veamos, finalmente, cuantos animales de cada clase compró.

Teniendo en cuenta que adquirió animales de las tres clases, tendremos

$$\left.\begin{array}{l} y > 0 \Longrightarrow -49400 + 99k > 0 \Longrightarrow 99k > 49400 \Longrightarrow k > 498.9 \\ z > 0 \Longrightarrow 9500 - 19k > 0 \Longrightarrow 19k < 9500 \Longrightarrow k < 500 \end{array}\right\} \Longrightarrow 498.9 < k < 500$$

y como k es un número entero, se sigue que $k = 499$.

Así pues,

$$y = -49400 + 99 \cdot 499 = 1$$
$$z = 9500 - 19 \cdot 499 = 19$$

y al ser

$$x + y + z = 100$$

será

$$x = 100 - 1 - 19 = 80$$

por tanto compró 80 pollos, 1 conejo y 19 terneros.

■

Lección 16

Aritmética en $\mathbb{Z}_m$

En su obra *Disquisitiones Arithmeticae*, publicada en 1801, Gauss introdujo en las Matemáticas el concepto de congruencia. Dada la analogía que existía entre ella y la igualdad algebraica, Gauss adopto el símbolo $\equiv$, notación que aún se utiliza para la congruencia.

la relación de congruencia ha proporcionado las herramientas con las cuales se han demostrado importantes hitos de la Teoría de Números, de hecho ha sido un instrumento de vital importancia para el estudio de la divisibilidad en $\mathbb{Z}$.

Muchos problemas de Cálculo con enteros muy grandes pueden reducirse a problemas equivalentes usando enteros pequeños mediante el uso de las congruencias.

16.1 Conceptos Básicos

Comenzamos definiendo el concepto central de la lección y analizando con detenimiento sus propiedades. Distintos ejemplos aclararán los conceptos que se definen y permitirán una aplicación directa de las propiedades.

16.1.1 Definición

Sea m un entero positivo y a, b dos números enteros. Diremos que a y b son congruentes módulo m si m divide a $a-b$. Utilizaremos la notación $a \equiv b(mód\ m)$, es decir,

$$a \equiv b(mód\ m) \Longleftrightarrow m|a-b$$

Ejemplo 16.1

$80 \equiv 20(mód\ 15)$, *ya que* $15|60$

$-8 \equiv 16(mód\ 4)$, *ya que* $4|-24$

$-5 \equiv -25(mód\ 10)$, *ya que* $10|20$

$12 \equiv -3(mód\ 5)$, *ya que* $5|15$

■

Ejemplo 16.2

Encontrar cinco número enteros distintos, cada uno los cuales sea congruente con 13 *módulo* 11.

Solución

Sea a cualquiera de los números buscados. Entonces,

$$\begin{aligned} a \equiv 13(\text{mód } 11) &\iff 11|a-13 \\ &\iff \exists q \in \mathbb{Z} : a-13 = 11q \\ &\iff \exists q \in \mathbb{Z} : a = 11q+13 \end{aligned}$$

Si ahora tomamos, por ejemplo, $q = -2,\ -1,\ 0,\ 1$ ó 2, tendremos los cinco números buscados:

$$\begin{aligned} a &= 11(-2)+13 = -9 \\ a &= 11(-1)+13 = 2 \\ a &= 11\cdot 0+13 = 13 \\ a &= 11\cdot 1+13 = 24 \\ a &= 11\cdot 2+13 = 35 \end{aligned}$$

■

16.1.2 Teorema

Sea m cualquier número entero positivo. Entonces,

(a) Cualquier número entero es congruente módulo m exactamente con uno de los enteros $0, 1, \ldots\ldots, m-1$.

(b) Dos números enteros son congruentes entre sí módulo m si, y sólo si ambos dan el mismo resto al dividirlos por m.

Demostración

(a) Probaremos que si a es un número entero cualquiera, entonces es congruente módulo m exactamente con uno de los enteros $0, 1, \ldots\ldots, m-1$.

En efecto,

$$\begin{aligned} a \in \mathbb{Z} \text{ y } m \in \mathbb{Z}^+ &\implies \text{Existen } q \text{ y } r, \text{ enteros y únicos} : a = mq+r, \text{ siendo } 0 \leqslant r < m \ \{(13.2.1)\} \\ &\iff \exists q, r \in \mathbb{Z} : a - r = mq, \text{ siendo } 0 \leqslant r < m \\ &\iff \exists r \in \mathbb{Z} : m|a-r, \text{ siendo } 0 \leqslant r < m \\ &\iff \exists r \in \mathbb{Z} : a \equiv r(\text{mód } m), \text{ siendo } 0 \leqslant r < m \\ &\iff \begin{cases} a \equiv 0(\text{mód } m) \\ \text{ó} \\ a \equiv 1(\text{mód } m) \\ \text{ó} \\ a \equiv 2(\text{mód } m) \\ \vdots \\ \text{ó} \\ a \equiv m-1(\text{mód } m) \end{cases} \end{aligned}$$

Al número r, único, lo llamaremos *menor residuo de a, módulo m.*

(b) En efecto, sean a y b dos enteros cualesquiera.

"Sólo si." En efecto, supongamos que $a \equiv b (\text{mód } m)$, entonces,

$$
\begin{aligned}
a \equiv b(\text{mód } m) &\iff m|a-b \\
&\iff \exists q \in \mathbb{Z} : a-b = mq \\
&\left\{ \begin{array}{l} \text{Por el teorema de existencia y unicidad de cociente y resto (13.2.1)} \\ \text{existirán } q_1, r_1, q_2, r_2, \text{ enteros y únicos, tales que} \\ \left. \begin{array}{l} a = mq_1 + r_1,\ 0 \leqslant r_1 < m \\ \text{y} \\ b = mq_2 + r_2,\ 0 \leqslant r_2 < m \end{array} \right\} \Longrightarrow a-b = m(q_1-q_2) + r_1 - r_2 \end{array} \right\} \\
&\Longrightarrow \left\{ \begin{array}{l} \exists q \in \mathbb{Z} : a-b = mq \\ \exists q_1, q_2, r_1, r_2 : a-b = m(q_1-q_2) + r_1 - r_2,\ 0 \leqslant r_1 < m,\ 0 \leqslant r_2 < m \end{array} \right. \\
&\left\{ \begin{array}{l} \left. \begin{array}{l} 0 \leqslant r_1 < m \\ \text{y} \\ 0 \leqslant r_2 < m \end{array} \right| \Longrightarrow -m < r_1 - r_2 < m \Longleftrightarrow 0 \leqslant |r_1 - r_2| < m \end{array} \right\} \\
&\Longrightarrow \left\{ \begin{array}{l} \exists q \in \mathbb{Z} : a-b = mq \\ \exists q_1, q_2, r_1, r_2 : a-b = m(q_1-q_2) + r_1 - r_2, \text{ siendo } 0 \leqslant |r_1 - r_2| < m \end{array} \right. \\
&\Longrightarrow |r_1 - r_2| = 0 \ \{\text{El resto de dividir } a-b \text{ entre } m \text{ ha de ser único}\} \\
&\Longleftrightarrow r_1 = r_2
\end{aligned}
$$

es decir, a y b dan, ambos, el mismo resto al dividirlos por m.

"Si." Recíprocamente, supongamos que a y b, dan, ambos, el mismo resto al dividirlos por m, es decir, existen q_1, q_2 y r, enteros, tales que

$$a = mq_1 + r \text{ y } b = mq_2 + r.$$

Entonces,

$$
\begin{aligned}
&\left. \begin{array}{l} a = mq_1 + r \\ \text{y} \\ a = mq_2 + r \end{array} \right\} \Longrightarrow a - b = m(q_1 - q_2) \\
&\Longrightarrow \exists q \in \mathbb{Z} : a-b = mq \ \{\text{Tomando } q = q_1 - q_2\} \\
&\Longleftrightarrow m|a-b \\
&\Longleftrightarrow a \equiv b\,(\text{mód } m)
\end{aligned}
$$

■

Ejemplo 16.3

Demuéstrese que todo número primo mayor o igual que 5 *es congruente con* 1 *ó con* 5, *módulo* 6.

Solución

Probaremos que

si p es primo y $p \geqslant 5$, entonces $p \equiv 1(\text{mód } 6)$ ó $p \equiv 5(\text{mód } 6)$.

En efecto, supongamos que la proposición es falsa, es decir,

p es primo y $p \geqslant 5$ y, sin embargo, $p \not\equiv 1(\text{mód } 6)$ y $p \not\equiv 5(\text{mód } 6)$.

Entonces, por (a) del teorema anterior, $p \equiv 0(\text{mód } 6)$ ó $p \equiv 2(\text{mód } 6)$ ó $p \equiv 3(\text{mód } 6)$ ó $p \equiv 4(\text{mód } 6)$. Pues bien,

- Si $p \equiv 0(\text{mód } 6)$, entonces $6|p$ lo cual es imposible ya que p es primo.
- Si $p \equiv 2(\text{mód } 6)$, entonces

$$\left.\begin{array}{l} 6|p-2 \\ \text{y} \\ 2|6 \end{array}\right\} \Longrightarrow \left.\begin{array}{l} 2|p-2 \\ \text{y} \\ 2|2 \end{array}\right\} \Longrightarrow 2|p-2+2 \Longrightarrow 2|p$$

  y esto contradice el que p sea primo.

- Si $p \equiv 3(\text{mód } 6)$, entonces

$$\left.\begin{array}{l} 6|p-3 \\ \text{y} \\ 3|6 \end{array}\right\} \Longrightarrow \left.\begin{array}{l} 3|p-3 \\ \text{y} \\ 3|3 \end{array}\right\} \Longrightarrow 3|p-3+3 \Longrightarrow 3|p$$

  y esto contradice el que p sea primo.

- Si $p \equiv 4(\text{mód } 6)$, entonces

$$\left.\begin{array}{l} 6|p-4 \\ \text{y} \\ 2|6 \end{array}\right\} \Longrightarrow \left.\begin{array}{l} 2|p-4 \\ \text{y} \\ 2|4 \end{array}\right\} \Longrightarrow 2|p-4+4 \Longrightarrow 2|p$$

  y esto contradice el que p sea primo.

Hemos llegado, por tanto, a una contradicción y la proposición propuesta es cierta, es decir, p ha de ser congruente módulo 6 con 1 ó con 5.

■

Ejemplo 16.4

Demuéstrese que si $d|m$ y $a \equiv b(\text{mód } m)$, entonces $a \equiv b(\text{mód } d)$.

Solución

Directamente de la transitividad de la relación de divisibilidad,

$$\left.\begin{array}{l} d|m \\ a \equiv b(\text{mód } m) \Longleftrightarrow m|a-b \end{array}\right\} \Longrightarrow d|a-b \Longleftrightarrow a \equiv b(\text{mód } d)$$

■

16.2 Propiedades

Veremos a continuación algunas propiedades de las congruencias que son, con frecuencia, bastante útiles

16.2.1 Teorema

Sean a, b, c y m son tres enteros con $m > 0$. Se verifica:

(a) $a \equiv a(\text{mód } m)$.

(b) Si $a \equiv b(\text{mód } m)$, *entonces* $b \equiv a(\text{mód } m)$

(c) Si $a \equiv b(\text{mód } m)$ *y* $b \equiv c(\text{mód } m)$, *entonces* $a \equiv c(\text{mód } m)$

Demostración

Utilizaremos las propiedades de la divisibilidad (13.1.2).

(a) $a \equiv a(\text{mód } m)$
Teniendo en cuenta que $m \neq 0$,

$$m|0 \iff m|a-a \iff a \equiv a(\text{mód } m)$$

(b) Si $a \equiv b(\text{mód } m)$, entonces $b \equiv a(\text{mód } m)$. En efecto,

$$a \equiv b(\text{mód } m) \iff m|a-b \iff m|(-1)(a-b) \implies m|b-a \iff b \equiv a(\text{mód } m)$$

(c) Si $a \equiv b(\text{mód } m)$ y $b \equiv c(\text{mód } m)$, entonces $a \equiv c(\text{mód } m)$. En efecto,

$$\left.\begin{array}{l} a \equiv b(\text{mód } m) \iff m|a-b \\ \text{y} \\ b \equiv c(\text{mód } m) \iff m|b-c \end{array}\right\} \implies m|(a-b)+(b-c) \implies m|a-c \implies a \equiv c(\text{mód } m)$$

■

16.2.2 Teorema

Sean a, b, c, d, p y m, enteros con $p \neq 0$ y $m > 0$. Se verifica:

(a) si $a \equiv b(\text{mód } m)$ *y* $c \equiv d(\text{mód } m)$, *entonces* $a+c \equiv b+d(\text{mód } m)$ *y* $ac \equiv bd(\text{mód } m)$.

(b) Si $a \equiv b(\text{mód } m)$, *entonces* $pa \equiv pb(\text{mód } m)$.

(c) Si $p|a$, $p|b$, $m.c.d.(p,m) = 1$ *y* $a \equiv b(\text{mód } m)$, *entonces* $\dfrac{a}{p} \equiv \dfrac{b}{p}(\text{mód } m)$.

Demostración

Utilizaremos, al igual que en el teorema anterior, las propiedades de la divisibilidad (13.1.2)

(a) si $a \equiv b(\text{mód } m)$ y $b \equiv c(\text{mód } m)$, entonces $a+c \equiv b+d(\text{mód } m)$ y $ac \equiv bd(\text{mód } m)$.

En efecto,

$$\left.\begin{array}{l} a \equiv b(\text{mód } m) \Longleftrightarrow m|a-b \\ \text{y} \\ c \equiv d(\text{mód } m) \Longleftrightarrow m|c-d \end{array}\right\} \Longrightarrow m|(a-b)+(c-d) \Longrightarrow m|(a+c)-(b+d)$$

luego,

$$a+c \equiv b+d(\text{módm}).$$

Análogamente,

$$\left.\begin{array}{l} a \equiv b(\text{mód } m) \Longleftrightarrow m|a-b \Longrightarrow m|ac-bc \\ \text{y} \\ c \equiv d(\text{mód } m) \Longleftrightarrow m|c-d \Longrightarrow m|bc-bd \end{array}\right\} \Longrightarrow m|(ac-bc)+(bc-bd) \Longrightarrow m|ac-bd$$

por lo tanto,

$$ac \equiv bd(\text{módm}).$$

(b) Si $a \equiv b(\text{mód } m)$, entonces $pa \equiv pb(\text{mód } m)$. En efecto,

$$a \equiv b(\text{mód } m) \Longleftrightarrow m|a-b \Longrightarrow m|p(a-b) \Longrightarrow m|pa-pb \Longleftrightarrow pa \equiv pb(\text{mód } m)$$

(c) Si $p|a$, $p|b$, m.c.d.$(p,m)=1$ y $a \equiv b(\text{mód } m)$, entonces $\dfrac{a}{p} \equiv \dfrac{b}{p}(\text{mód } m)$.

En efecto,

$$\left.\begin{array}{l} \left.\begin{array}{l} p|a \\ \text{y} \\ p|b \end{array}\right\} \Longrightarrow p|a-b \\ \text{y} \\ a \equiv b(\text{mód } m) \Longleftrightarrow m|a-b \Longleftrightarrow \exists q_1 \in \mathbb{Z} : a-b=mq_1 \end{array}\right\} \Longrightarrow p|mq_1$$

Pues bien, si $p|mq_1$, como m.c.d.$(p,m)=1$, tendremos que $p|q_1$, es decir, $q_1 = pq$ con q entero. Entonces,

$$\left.\begin{array}{l} a-b=mq_1 \\ q_1=pq \end{array}\right\} \Longrightarrow a-b=mpq \Longrightarrow \frac{a}{p}-\frac{b}{p}=mq \Longleftrightarrow m\left|\frac{a}{p}-\frac{b}{p}\right.$$

Consecuentemente,

$$\frac{a}{p} \equiv \frac{b}{p}(\text{mód } m)$$

■

Ejemplo 16.5

Demostrar que el cuadrado de cualquier número entero es divisible por 3 *o es congruente con* 1 *módulo* 3.

Solución

Sea a un número entero arbitrario. Por el teorema 16.1.2 a es congruente módulo 3 con 0, 1 ó 2. Pues bien,

$$\begin{aligned}
a \equiv 0(\text{mód } 3) &\implies a^2 \equiv 0(\text{mód } 3) \ \{(16.2.2\ (a))\} \\
&\iff 3|a^2 \\
&\iff a^2 \text{ es divisible por } 3
\end{aligned}$$

ó

$$\begin{aligned}
a \equiv 1(\text{mód } 3) &\implies a^2 \equiv 1(\text{mód } 3) \ \{(16.2.2\ (a))\}
\end{aligned}$$

ó

$$\begin{aligned}
a \equiv 2(\text{mód } 3) &\implies a^2 \equiv 4(\text{mód } 3) \ \{(16.2.2\ (a))\} \\
&\iff \begin{cases} a^2 \equiv 4(\text{mód } 3) \\ \text{y} \\ 4 \equiv 1(\text{mód } 3) \end{cases} \\
&\iff a^2 \equiv 1(\text{mód } 3) \ \{16.2.1(c)\}
\end{aligned}$$

luego a^2 es divisible por 3 o es congruente con 1 módulo 3.

■

Veamos ahora un corolario que generaliza algunos apartados del teorema anterior.

16.2.3 Corolario

Si $a_i \equiv b_i(\text{mód } m)$ para $1 \leqslant i \leqslant n$, entonces

(i) $\displaystyle\sum_{i=1}^{n} a_i \equiv \sum_{i=1}^{n} b_i(\text{mód } m)$

(ii) $\displaystyle\prod_{i=1}^{n} a_i \equiv \prod_{i=1}^{n} b_i(\text{mód } m)$

Demostración

Procederemos, en ambos casos, por inducción.

(i) $\displaystyle\sum_{i=1}^{n} a_i \equiv \sum_{i=1}^{n} b_i(\text{mód } m)$

Paso básico. Veamos que es cierto para $n = 2$. En efecto, por el teorema anterior,

$$\left.\begin{aligned} a_1 &\equiv b_1(\text{mód } m) \\ a_2 &\equiv b_2(\text{mód } m) \end{aligned}\right\} \implies a_1 + a_2 \equiv b_1 + b_2(\text{mód } m)$$

Paso inductivo. Supongamos que la proposición es cierta para $n = p$, es decir,

$$\text{si } a_i \equiv b_i(\text{mód } m),\ i = 1, 2, \ldots, p, \text{ entonces } \sum_{i=1}^{p} a_i \equiv \sum_{i=1}^{p} b_i(\text{mód } m)$$

Veamos que también se cumple para $n = p + 1$. En efecto, si

$$a_i \equiv b_i(\text{mód } m),\ i = 1, 2, \ldots, p, p+1$$

entonces por la hipótesis de inducción y por ser cierta la propiedad para $i = 2$, tendremos que

$$\left.\begin{array}{l} \sum_{i=1}^{p} a_i \equiv \sum_{i=1}^{p} b_i(\text{mód } m) \\ a_{p+1} \equiv b_{p+1}(\text{mód } m) \end{array}\right\} \Longrightarrow \sum_{i=1}^{p} a_i + a_{p+1} \equiv \sum_{i=1}^{p} b_i + b_{p+1}(\text{mód } m) \Longrightarrow \sum_{i=1}^{p+1} a_i \equiv \sum_{i=1}^{p+1} b_i(\text{mód } m)$$

y, consecuentemente, la proposición será cierta para todo n.

(ii) $\prod_{i=1}^{n} a_i \equiv \prod_{i=1}^{n} b_i(\text{mód } m)$

Basta aplicar el apartado (a) del teorema anterior y la igualdad

$$\prod_{i=1}^{p+1} a_i = \prod_{i=1}^{p} a_i \cdot a_{p+1}$$

para llegar, al igual que en el apartado anterior, al resultado.

■

Ejemplo 16.6

Demostrar que si el último dígito de un número n es t, entonces

$$n^2 \equiv t^2(\text{mód } 10)$$

Solución

En efecto, si

$$n = a_k 10^k + a_{k-1} 10^{k-1} + \cdots + a_1 10 + a_0$$

es la descomposición polinómica de n, entonces $a_0 = t$, luego

$$n = \sum_{i=1}^{k} a_i 10^i + t$$

de aquí que

$$n - t = \sum_{i=1}^{k} a_i 10^i$$

Ahora bien,

$$10 \equiv 0(\text{mód } 10)$$

luego

$$10^i \equiv 0(\text{mód } 10),\ 1 \leqslant i \leqslant k$$

y también

$$a_i 10^i \equiv 0(\text{mód } 10),\ 1 \leqslant i \leqslant k$$

de aquí que por el corolario anterior,

$$\sum_{i=1}^{k} a_i 10^i \equiv 0(\text{mód } 10).$$

Consecuentemente,

$$n - t \equiv 0(\text{mód } 10)$$

y, por lo tanto,

$$n \equiv t(\text{mód } 10)$$

de donde resulta que

$$n^2 \equiv t^2(\text{mód } 10)$$

■

Ejemplo 16.7

Demostrar que el resto de dividir 20^{4572} *entre* 7 *es* 1.

Solución

En efecto,

$$\left.\begin{array}{r} 21 \equiv 0(\text{mód } 7) \\ -1 \equiv -1(\text{mód } 7) \end{array}\right\} \Longrightarrow 20 \equiv -1(\text{mód } 7) \Longrightarrow 20^{4572} \equiv (-1)^{4572}(\text{mód } 7) \Longrightarrow 20^{4572} \equiv 1(\text{mód } 7)$$

es decir el resto es 1.

■

Ejemplo 16.8

Demostrar:

(a) Si $a \equiv b(\text{mód } m)$*, entonces m.c.d.*$(a, m) = m.c.d.(b, m)$.

(b) Si $a \equiv b(\text{mód } m)$*, entonces* $a^n \equiv b^n(\text{mód } m)$ *para cualquier entero positivo* n.

(c) Si $a + b \equiv c(\text{mód } m)$*, entonces* $a \equiv c - b(\text{mód } m)$.

(d) Si $a \equiv b(\text{mód } m)$ *y* $d|a$ *y* $d|m$*, entonces* $d|b$.

Solución

(a) Si $a \equiv b(\text{mód } m)$, entonces $\text{m.c.d.}(a, m) = \text{m.c.d.}(b, m)$. En efecto,

$$a \equiv b(\text{mód } m) \Longleftrightarrow m|a - b \Longleftrightarrow \exists q \in \mathbb{Z} : a - b = mq$$

Pues bien, sea $d_1 = \text{m.c.d}(a, m)$ y $d_2 = \text{m.c.d}(b, m)$. Entonces,

$$d_1 = \text{m.c.d}(a, m) \Longrightarrow \left\{\begin{array}{l} d_1|a \\ \text{y} \\ d_1|m \Longrightarrow d_1|mq \Longrightarrow d_1|a - b \end{array}\right\} \Longrightarrow d_1|a - (a - b) \Longrightarrow d_1|b$$

Es decir, d_1 divide a b y a m, por tanto dividirá al máximo común divisor de ambos, luego

$$d_1|d_2$$

Análogamente,

$$d_2 = \text{m.c.d}(b,m) \Longrightarrow \left\{ \begin{array}{l} d_2|b \\ \text{y} \\ d_2|m \Longrightarrow d_2|mq \Longrightarrow d_2|a-b \end{array} \right\} \Longrightarrow d_2|a-b+b \Longrightarrow d_2|a$$

O sea, d_2 divide a a y a m, luego dividirá al máximo común divisor de ambos, de aquí que

$$d_2|d_1$$

Finalmente, como d_1 y d_2 son enteros positivos, por la antisimetría de la relación de divisibilidad en $\mathbb{Z}^+$, d_1 será igual a d_2, es decir,

$$\text{m.c.d.}(a,m) = \text{m.c.d.}(b,m)$$

(b) Si $a \equiv b(\text{mód } m)$, entonces $a^n \equiv b^n(\text{mód } m)$ para cualquier entero positivo n.
Basta aplicar el apartado (ii) del corolario anterior para $a_i = a,\ 1 \leqslant i \leqslant n$ y $b_i = b,\ 1 \leqslant i \leqslant n$

(c) Si $a+b \equiv c(\text{mód } m)$, entonces $a \equiv c-b(\text{mód } m)$.
En efecto,

$$a+b \equiv c(\text{mód } m) \Longleftrightarrow m|a+b-c \Longleftrightarrow m|a-(c-b) \Longleftrightarrow a \equiv c-b(\text{mód } m)$$

(d) Si $a \equiv b(\text{mód } m)$ y $d|a$ y $d|m$, entonces $d|b$.
En efecto,

$$a \equiv b(\text{mód } m) \Longleftrightarrow m|a-b$$

y como $d|m$, por la transitividad de la relación de divisibilidad, $d|a-b$. Así pues,

$$\left. \begin{array}{l} d|a \\ d|a-b \end{array} \right\} \Longrightarrow d|a-(a-b) \Longrightarrow d|b$$

■

Ejemplo 16.9

Demostrar que para cualquier entero positivo n, el número $3 \cdot 5^{2n+1} + 2^{3n+1}$ es divisible por 17.

Solución

Observemos lo siguiente:

$$\left. \begin{array}{l} 3 \cdot 5^{2n+1} = 3 \cdot (5^2)^n \cdot 5 = 15 \cdot 25^n \\ 2^{3n+1} = (2^3)^n \cdot 2 = 2 \cdot 8^n \end{array} \right\} \Longrightarrow \quad 3 \cdot 5^{2n+1} + 2^{3n+1} = 15 \cdot 25^n + 2 \cdot 8^n$$

Por otra parte,

$$\left. \begin{array}{l} 15 \equiv -2(\text{mód } 17) \\ 25 \equiv 8(\text{mód } 17) \Longrightarrow 25^n \equiv 8^n(\text{mód } 17) \end{array} \right\} \Longrightarrow 15 \cdot 25^n \equiv -2 \cdot 8^n(\text{mód } 17)$$

luego,

$$15 \cdot 25^n + 2 \cdot 8^n \equiv 0(\text{mód } 17)$$

es decir,

$$3 \cdot 5^{2n+1} + 2^{3n+1} \equiv 0(\text{mód } 17)$$

por lo tanto, el número dado es divisible por 17.

■

Ejemplo 16.10

Demostrar por inducción que el número $7^{2n} - 48n - 1$ *es divisible por* 2304 *para cualquier entero positivo* n.

Solución

Probaremos que

$$7^{2n} - 48n - 1 \equiv 0(\text{mód } 2304)$$

o lo que es igual,

$$(7^2)^n \equiv 48n + 1(\text{mód } 2304)$$

es decir,

$$49^n \equiv 48n + 1(\text{mód } 2304)$$

o sea,

$$(48 + 1)^n \equiv 48n + 1(\text{mód } 2304)$$

Procederemos por inducción.

- Para $n = 1$ es cierto claramente.
- Veamos si es cierto para $n = 2$. En efecto,

$$\begin{aligned} (48+1)^2 = 48^2 + 2 \cdot 48 + 1 &\iff (48+1)^2 = 48 \cdot 2 + 1 + 2304 \\ &\iff (48+1)^2 - (48 \cdot 2 + 1) = 2304 \\ &\iff (48+1)^2 \equiv 48 \cdot 2 + 1(\text{mód } 2304) \end{aligned}$$

- Supongamos que es cierto para $n = p$, es decir,

$$(48 + 1)^p \equiv 48p + 1(\text{mód } 2304)$$

- Veamos que es cierto para $n = p + 1$. En efecto,

$$\begin{aligned} 48 + 1 &\equiv 48 + 1(\text{mód } 2304) \quad \{\text{Por ser cierto para } n = 1\} \\ (48 + 1)^p &\equiv 48p + 1(\text{mód } 2304) \quad \{\text{Por la hipótesis de inducción}\} \end{aligned}$$

  luego,

$$(48 + 1)^p(48 + 1) \equiv (48p + 1)(48 + 1)(\text{mód } 2304).$$

  Por otra parte,

$$(48p + 1)(48 + 1) = 2304p + 48 + 48p + 1$$

  es decir,

$$(48p + 1)(48 + 1) - [48(p + 1) + 1] = 2304p$$

  de aquí que

$$(48p + 1)(48 + 1) \equiv 48(p + 1) + 1(\text{mód } 2304).$$

  Finalmente, por la transitividad de la relación de congruencia, de

$$\begin{aligned} (48 + 1)^p(48 + 1) &\equiv (48p + 1)(48 + 1)(\text{mód } 2304) \\ (48p + 1)(48 + 1) &\equiv 48(p + 1) + 1(\text{mód } 2304) \end{aligned}$$

  se sigue que

$$(48 + 1)^{p+1} \equiv 48(p + 1) + 1(\text{mód } 2304).$$

  Consecuentemente, la congruencia es cierta para cada entero positivo n, o sea,

$$(48 + 1)^n \equiv 48n + 1(\text{mód } 2304)$$

  y, consecuentemente,

$$7^{2n} - 48n + 1$$

  es divisible por 2304 para cualquier entero positivo n.

■

Ejemplo 16.11

Calcular el resto de dividir $9^{6n+1} + 3^{2n+1} \cdot 487^{2n} - 10$ *por* 730.

Solución

Observemos lo siguiente:

$$\begin{aligned} 9^{6n+1} + 3^{2n+1} \cdot 487^{2n} - 10 &= (9^3)^{2n} \cdot 9 + (3 \cdot 487)^{2n} \cdot 3 - 10 \\ &= 729^{2n} \cdot 9 + 1461^{2n} \cdot 3 - 10 \end{aligned}$$

Pues bien,

$$\begin{aligned} 729 \equiv -1(\text{mód } 730) &\implies 729^{2n} \equiv (-1)^{2n}(\text{mód } 730) \\ &\implies 729^{2n} \equiv 1(\text{mód } 730) \\ &\implies 729^{2n} \cdot 9 \equiv 9(\text{mód } 730) \\ &\iff 9^{6n+1} \equiv 9(\text{mód } 730). \end{aligned}$$

Por otra parte,

$$\begin{aligned} 1461 \equiv 1(\text{mód } 730) &\implies 1461^{2n} \equiv 1^{2n}(\text{mód } 730) \\ &\implies 1461^{2n} \equiv 1(\text{mód } 730) \\ &\implies 1461^{2n} \cdot 3 \equiv 3(\text{mód } 730) \\ &\iff 3^{2n+1} \cdot 487^{2n} \equiv 3(\text{mód } 730) \end{aligned}$$

de aquí que

$$9^{6n+1} + 3^{2n+1} \cdot 487^{2n} \equiv 12(\text{mód } 730)$$

es decir,

$$9^{6n+1} + 3^{2n+1} \cdot 487^{2n} - 10 \equiv 2(\text{mód } 730)$$

y, consecuentemente, el resto de dividir el número dado entre 730 es 2.

■

Ejemplo 16.12

Demostrar que para cualquier entero positivo n*, el número* $10^n(9n-1)+1$ *es divisible por* 9.

Solución

En efecto,

$$10 \equiv 1(\text{mód } 9) \implies 10^n \equiv 1(\text{mód } 9)$$

y

$$9n \equiv 0(\text{mód } 9) \iff 9n \equiv 1 - 1(\text{mód } 9) \iff 9n - 1 \equiv -1(\text{mód } 9)$$

luego,

$$10^n(9n-1) \equiv -1(\text{mód } 9)$$

por lo tanto,

$$10^n(9n-1) + 1 \equiv 0(\text{mód } 9)$$

y, consecuentemente, el resto de dividir el número dado entre 9 es cero.

■

16.3 Conjunto de las clases de restos módulo m

En este apartado veremos que la relación de congruencia es de equivalencia y calcularemos el conjunto cociente, al cual llamaremos $\mathbb{Z}_m$. Este conjunto será $\{[0], [1], \ldots, [m-1]\}$, donde

$$\begin{aligned} [0] &= \{n : n = mq, q \in \mathbb{Z}\} \\ [1] &= \{n : n = mq + 1, q \in \mathbb{Z}\} \\ &\vdots \qquad\qquad\qquad \vdots \\ [m-1] &= \{n : n = mq + m - 1, q \in \mathbb{Z}\} \end{aligned}$$

Con esta interpretación, cada elemento de $\mathbb{Z}_m$ es considerado como el conjunto de todos los enteros congruentes con un entero r tal que $0 \leqslant r \leqslant m - 1$.

Esta es la razón de que la propiedad cíclica de las congruencias sea tan importante. Si contamos desde 0 a 10 en base decimal, originamos un ciclo desde 0 a 9 y volvemos al 0. Por ejemplo, el cuentakilómetros de un coche es una instrumentación física de esta propiedad. Los dígitos desde el 0 hasta el 9 se sitúan en un círculo, y cuando éste gira, tiene lugar la cuenta. Cuando un círculo pasa desde el 9 hasta el 0, el siguiente círculo a su izquierda se incrementa en 1. El cuentakilómetros vuelve a 0 de nuevo cuando el coche recorre 100.000 kms. Así pues, el cuentakilómetros es una instrumentación de $\mathbb{Z}_{100.000}$ y cada una de las ruedas de dígitos son instrumentaciones de $\mathbb{Z}_{10}$.

La informática también es bastante dependiente de esta propiedad. Por ejemplo, un byte es un número de ocho bits que varía desde 00000000 hasta 11111111; si añadimos 1 a 11111111 volvemos de nuevo a 00000000. Esta transición se registra normalmente como un desbordamiento. El hecho de contar en un ordenador, supone exactamente el mismo principio que el utilizado en el cuentakilómetros. Además, no importa lo potente que sea el mismo, siempre será una máquina finita. Así que cada esfuerzo para tratar con los números enteros es, básicamente, una aproximación de los enteros por $\mathbb{Z}_m$ para algún m lo suficientemente grande. Este hecho, combinado con la naturaleza cíclica de $\mathbb{Z}_m$, es la base para algoritmos utilizados en la generación de números aleatorios.

16.3.1 Relación de Equivalencia

Dado un entero $m > 0$, la relación de congruencia módulo m es una relación de equivalencia en el conjunto de los números enteros.

Demostración

Se sigue directamente del teorema 16.2.2.

■

16.3.2 Clases de Equivalencia

Dado un número entero cualquiera, a, su clase de equivalencia es el conjunto formado por todos los enteros que dan el mismo resto que a al dividirlos entre m.

Demostración

Sea, pues, a cualquier número entero. Hallaremos $[a]$.

Por el teorema de existencia y unicidad de cociente y resto, (13.2.1), existirán q_2 y r, enteros y únicos, tales que

$$a = mq_2 + r, \text{ siendo } 0 \leqslant r < m \tag{16.1}$$

Pues bien, si b es un entero elegido arbitrariamente, entonces,

$$\begin{aligned}
b \in [a] &\iff b \equiv a \,(\text{mód } m) \\
&\iff m|b-a \\
&\iff \exists q_1 \in \mathbb{Z} : b - a = mq_1 \\
&\iff \exists q_1 \in \mathbb{Z} : b = mq_1 + a \\
&\implies \exists q_1, q_2, r \in \mathbb{Z} : b = mq_1 + mq_2 + r, \text{ siendo } 0 \leqslant r < m \ \{(16.1)\} \\
&\iff \exists q_1, q_2, r \in \mathbb{Z} : b = m(q_1 + q_2) + r, \text{ siendo } 0 \leqslant r < m \\
&\implies \exists q, r \in \mathbb{Z} : b = mq + r, \text{ siendo } 0 \leqslant r < m \ \{\text{Tomando } q = q_1 + q_2\} \\
&\iff \exists q, r \in \mathbb{Z} : b - r = mq, \text{ siendo } 0 \leqslant r < m \\
&\iff \exists r \in \mathbb{Z} : m|b-r, \text{ siendo } 0 \leqslant r < m \\
&\iff \exists r \in \mathbb{Z} : b \equiv r \,(\text{mód } m)\,, \text{ siendo } 0 \leqslant r < m \\
&\iff \exists r \in \mathbb{Z} : b \in [r]\,, \text{ siendo } 0 \leqslant r < m
\end{aligned}$$

Como b era cualquier entero, hemos probado la veracidad de la proposición,

$$\forall n, (n \in [a] \longrightarrow \exists r \in \{0, 1, \ldots, m-1\} : n \in [r])$$

lo cual, por la definición de inclusión de conjuntos, equivale a decir que puede encontrarse, al menos, un r en $\{0, 1, \ldots, m-1\}$ tal que

$$[a] \subseteq [r]$$

Recíprocamente, supongamos que existe $r \in \{0, 1, \ldots, m-1\}$ tal que $b \in [r]$. Entonces,

$$\begin{aligned}
b \in [r] &\iff b \equiv r \,(\text{mód } m)\,, \text{ siendo } 0 \leqslant r < m \\
&\iff m|b-r, \text{ siendo } 0 \leqslant r < m \\
&\iff \exists q_1 \in \mathbb{Z} : b - r = mq_1, \text{ siendo } 0 \leqslant r < m \\
&\iff \exists q_1 \in \mathbb{Z} : b = mq_1 + r, \text{ siendo } 0 \leqslant r < m \\
&\implies \exists q_1, q_2 \in \mathbb{Z} : b = mq_1 + a - mq_2 \,\{(16.1)\} \\
&\iff \exists q_1, q_2 \in \mathbb{Z} : b = m(q_1 - q_2) + a \\
&\implies \exists q \in \mathbb{Z} : b = mq + a \ \{\text{Tomando } q = q_1 - q_2\} \\
&\iff \exists q \in \mathbb{Z} : b - a = mq \\
&\iff m|b-a \\
&\iff b \equiv a \,(\text{mód } m) \\
&\iff b \in [a]
\end{aligned}$$

De la arbitrariedad de b se sigue, nuevamente, la veracidad de la proposición,

$$\forall n, (n \in [r] \longrightarrow n \in [a])$$

para algún $r \in \{0, 1, \ldots, m-1\}$ luego por la definición de inclusión de conjuntos,

$$[r] \subseteq [a]$$

Finalmente, por la doble inclusión de conjuntos, hemos llegado a que si a es cualquier número entero, entonces,

$$\exists r \in \{0, 1, \ldots, m-1\} : [a] = [r]$$

o lo que es igual, la clase de equivalencia de a, $[a]$, es igual a la clase de su resto, r, al dividir por m, es decir,

$$\begin{array}{rcl} [a] & = & [0] \\ \text{o} & & \\ [a] & = & [1] \\ \text{o} & & \\ [a] & = & [2] \\ \text{o} & & \\ \vdots & & \vdots \\ \text{o} & & \\ [a] & = & [m-1] \end{array}$$

Solo nos falta hallar $[r]$, siendo $0 \leqslant r < m$. En efecto, si b es cualquier número entero, entonces,

$$\begin{array}{rcl} b \in [r] & \iff & b \equiv r (\text{mód } m) \\ & \iff & m | b - r \\ & \iff & \exists q \in \mathbb{Z} : b - r = mq \\ & \iff & \exists q \in \mathbb{Z} : b = mq + r \end{array}$$

y al ser b cualquiera, esto significa que la proposición

$$\forall n, (x \in [r] \longleftrightarrow x \in \{n : n = mq + r,\ 0 \leqslant r < m\})$$

es verdadera y, por lo tanto, el *axioma de extensión*, asegura que

$$[r] = \{n : n = mq + r,\ 0 \leqslant r < m\}$$

es decir, la clase de equivalencia de r, siendo $0 \leqslant r < m$ está integrada por todos los números que dan resto r al dividirlos por m. Luego,

$$\begin{array}{rcl} [0] & = & \{n : n = mq, q \in \mathbb{Z}\} \\ [1] & = & \{n : n = mq + 1, q \in \mathbb{Z}\} \\ [2] & = & \{n : n = mq + 2, q \in \mathbb{Z}\} \\ \vdots & & \vdots \\ [m-1] & = & \{n : n = mq + m - 1, q \in \mathbb{Z}\} \end{array}$$

■

16.3.3 Conjunto Cociente

Al conjunto formado por las clases de equivalencia, es decir al conjunto cociente, lo llamaremos conjunto de las clases de resto módulo m y lo notaremos por $\mathbb{Z}_m$

$$\mathbb{Z}_m = \{[0], [1], [2], \ldots, [m-1]\}$$

Demostración

Por definición de conjunto cociente,

$$\mathbb{Z}\Big/_{\equiv} = \{[n] : n \in \mathbb{Z}\}$$

Entonces, si N es cualquier subconjunto de números enteros,

$$\begin{aligned} N \in \mathbb{Z}\Big/_{\equiv} &\iff \exists a \in \mathbb{Z} : N = [a] \\ &\iff \exists r \in \{0, 1, 2, \ldots, m-1\} : N = [r] \text{ (16.3.2)} \\ &\iff N = [0] \ \vee \ N = [1] \ \vee \ N = [2] \ \vee \ \ldots \ \vee \ N = [m-1] \\ &\iff N = \{[0], [1], [2], \ldots, [m-1]\} \end{aligned}$$

Por lo tanto, el axioma de extensión asegura que el conjunto cociente, que a partir de ahora notaremos como $\mathbb{Z}_m$, será

$$\begin{aligned} \mathbb{Z}_m &= \{[0], [1], \ldots, [m-1]\} \\ &= \{\{n : n = mq, q \in \mathbb{Z}\}, \{n : n = mq+1, q \in \mathbb{Z}\}, \ldots, \{n : n = mq+m-1, q \in \mathbb{Z}\}\} \end{aligned}$$

y lo llamaremos *conjunto de las clases de restos módulo* m.

■

Ejemplo 16.13

En el conjunto de los números enteros se considera la relación de congruencia módulo 5. *Hallar las clases de equivalencia del* -22, -6, 0, 3, 5, 7, 18 *y* 20.

Solución

Sea a cualquier número entero. Según acabamos de ver,

$$[a] = [r], \text{ siendo } r \text{ el resto de dividir } a \text{ entre } 5.$$

Entonces,

- $-22 = 5(-5) + 3$, luego $[-22] = [3]$, es decir,
$$[-22] = \{n : n = 5q + 3, q \in \mathbb{Z}\}$$
- $-6 = 5(-2) + 4$, luego $[-6] = [4]$, es decir,
$$[-6] = \{n : n = 5q + 4, q \in \mathbb{Z}\}$$
- $0 = 5 \cdot 0 + 0$, luego
$$[0] = \{n : n = 5q, q \in \mathbb{Z}\}$$
- $3 = 5 \cdot 0 + 3$, luego
$$[3] = \{n : n = 5q + 3, q \in \mathbb{Z}\}$$
- $5 = 5 \cdot 1 + 0$, luego $[5] = [0]$, es decir,
$$[5] = \{n : n = 5q, q \in \mathbb{Z}\}$$

⁎ $7 = 5 \cdot 1 + 2$, luego $[7] = [2]$, es decir,

$$[7] = \{n : n = 5q + 2, q \in \mathbb{Z}\}$$

⁎ $18 = 5 \cdot 3 + 3$, luego $[18] = [3]$, es decir,

$$[18] = \{n : n = 5q + 3, q \in \mathbb{Z}\}$$

⁎ $20 = 5 \cdot 4 + 0$, luego $[20] = [0]$, es decir,

$$[20] = \{n : n = 5q, q \in \mathbb{Z}\}$$

■

16.4 Aritmética en $\mathbb{Z}_m$

16.4.1 Suma

Dados dos enteros cualesquiera a y b, definimos la suma en $\mathbb{Z}_m$ en la forma siguiente:

$$[a] + [b] = [a + b]$$

Ejemplo 16.14

Sumar en el conjunto de las clases de restos módulo 5, $\mathbb{Z}_5$, las clases $[31]$ y $[58]$.

Solución

Según la definición que acabamos de ver,

$$[31] + [58] = [31 + 58] = [89]$$

y como $89 = 5 \cdot 17 + 4$, entonces $[89] = [4]$ de aquí que $[31] + [58] = [4]$.

También podíamos haber hecho lo siguiente:

$$\left.\begin{array}{rcl} 31 = 5 \cdot 6 + 1 & \Longrightarrow & [31] = [1] \\ 58 = 5 \cdot 11 + 3 & \Longrightarrow & [58] = [3] \end{array}\right\} \Longrightarrow [31] + [58] = [1] + [3] = [1 + 3] = [4]$$

■

16.4.2 Bien Definida

La suma está bien definida, es decir, no depende de los representantes que se elijan en cada clase, en el sentido de que si $[a] = [a']$ *y* $[b] = [b']$*, entonces* $[a] + [b] = [a'] + [b']$*.*

Demostración

En efecto,

$$\left.\begin{array}{l} [a] = [a'] \Longleftrightarrow a \equiv a'(\text{mód } m) \\ \text{y} \\ [b] = [b'] \Longleftrightarrow b \equiv b'(\text{mód } m) \end{array}\right\} \Longrightarrow a + b \equiv a' + b'(\text{mód } m) \Longrightarrow [a + b] = [a' + b'] \Longleftrightarrow [a] + [b] = [a'] + [b']$$

■

La suma en $\mathbb{Z}_m$ es asociativa y conmutativa. Veamos, a continuación, cuál es su elemento neutro.

16.4.3 Elemento Neutro para la Suma

El elemento neutro para la suma en $\mathbb{Z}_m$ *es la clase* $[0]$*.*

Demostración

Sea $[a]$ cualquiera de $\mathbb{Z}_m$ y sea $[e]$ el neutro para la suma. Entonces,

$$\begin{aligned} [e] + [a] = [a] &\iff [e + a] = [a] \\ &\iff e + a \equiv a(\text{mód } m) \\ &\iff e \equiv a - a(\text{mód } m) \\ &\iff e \equiv 0(\text{mód } m) \\ &\iff [e] = [0] \end{aligned}$$

■

16.4.4 Elemento Opuesto

Si $[a]$ *es cualquiera de* $\mathbb{Z}_m$*, entonces su opuesto es* $[-a]$

Demostración

En efecto, sea $[a']$ el opuesto de $[a]$. Entonces,

$$\begin{aligned} [a] + [a'] = [0] &\iff [a + a'] = [0] \\ &\iff a + a' \equiv 0(\text{mód } m) \\ &\iff m | a + a' \\ &\iff \exists q \in \mathbb{Z} : a + a' = mq \\ &\iff \exists q \in \mathbb{Z} : a' = mq - a \\ &\iff [a'] = [mq - a] \end{aligned}$$

■

16.4.5 Producto

Dados dos enteros cualesquiera a y b, definimos el producto en $\mathbb{Z}_m$ en la forma siguiente:

$$[a] \cdot [b] = [a \cdot b]$$

■

16.4.6 Bien Definido

El producto está bien definido, es decir, no depende de los representantes que se elijan en cada clase, en el sentido de que si $[a] = [a']$ y $[b] = [b']$, entonces $[a] \cdot [b] = [a'] \cdot [b']$.

Demostración

En efecto,

$$\left.\begin{array}{l} [a] = [a'] \Longleftrightarrow a \equiv a'(\text{mód}m) \\ \text{y} \\ [b] = [b'] \Longleftrightarrow b \equiv b'(\text{mód}m) \end{array}\right\} \Longrightarrow a \cdot b \equiv a' \cdot b'(\text{mód}m) \Longrightarrow [a \cdot b] = [a' \cdot b'] \Longleftrightarrow [a] \cdot [b] = [a'] \cdot [b']$$

■

El producto en $\mathbb{Z}_m$ es asociativo y conmutativo.

16.4.7 Elemento Neutro para el Producto

El elemento neutro para la multiplicación en $\mathbb{Z}_m$ es la clase $[1]$.

Demostración

En efecto, para cada $[a]$ de $\mathbb{Z}_m$, se verifica que

$$[1] \cdot [a] = [1 \cdot a] = [a]$$

■

16.4.8 Elemento Inverso

Un elemento $[a]$ de $\mathbb{Z}_m$ es invertible (admite inverso) si, y sólo si, a y m son primos entre si.

Demostración

En efecto, sea $[a]$ cualquiera de $\mathbb{Z}_m$. Entonces,

$$\begin{aligned}
[a] \text{ es invertible en } \mathbb{Z}_m &\iff \exists [a'] \in \mathbb{Z}_m : [a][a'] = [1] \\
&\iff \exists [a'] \in \mathbb{Z}_m : [aa'] = [1] \\
&\iff \exists a' \in \mathbb{Z} : aa' \equiv 1 (\text{mód } m) \\
&\iff \exists a' \in \mathbb{Z} : m | aa' - 1 \\
&\iff \exists a', q \in \mathbb{Z} : aa' - 1 = mq \\
&\iff \exists a', q \in \mathbb{Z} : aa' - mq = 1 \\
&\iff \text{La ecuación diofántica } aa' - mq = 1 \text{ tiene solución} \\
&\iff \text{m.c.d.}(a, m) | 1 \\
&\iff \text{m.c.d.}(a, m) = 1 \\
&\iff a \text{ y } m \text{ son primos entre sí.}
\end{aligned}$$

Obsérvese que si a'_0 es una solución particular de la ecuación $aa' - mq = 1$, entonces la solución general será

$$a' = a'_0 - mk, \ k \in \mathbb{Z}$$

luego,

$$\begin{aligned}
a' = a'_0 - mk &\iff a' - a'_0 = m(-k), k \in \mathbb{Z} \\
&\iff m | a' - a'_0 \\
&\iff a' \equiv a'_0 (\text{mód } m) \\
&\iff [a'] = [a'_0]
\end{aligned}$$

es decir, $[a'] = [a'_0]$, donde a'_0 es una solución particular de la ecuación. El inverso de un elemento de $\mathbb{Z}_m$, caso de existir, es, por lo tanto, único.

■

Nota 16.1 Observemos lo siguiente:

$$[a] \in \mathbb{Z}_m \iff 0 \leqslant a \leqslant m - 1$$

por lo tanto,

- Si m es primo, entonces m.c.d.$(a, m) = 1$ para todo a distinto de cero, luego todos los elementos de $\mathbb{Z}_m$, excepto el cero, poseen inverso.

Podemos concluir, pues, que *una condición necesaria y suficiente para que todos los elementos de $\mathbb{Z}_m$ distintos de cero posean inverso es que m sea primo.*

■

Nota 16.2 De aquí en adelante, y siempre que no haya peligro de confusión, escribiremos a en vez de $[a]$ para notar la clase de equivalencia de a en el conjunto $\mathbb{Z}_m$.

■

Ejemplo 16.15

Hallar los inversos de

(a) 2 *en* $\mathbb{Z}_{11}$

(b) 7 *en* $\mathbb{Z}_{15}$

(c) 7 *en* $\mathbb{Z}_{16}$

(d) 5 *en* $\mathbb{Z}_{13}$

Solución

(a) Inverso de 2 en $\mathbb{Z}_{11}$.

Como 11 es primo, todos los elementos de $\mathbb{Z}_{11}$, excepto el cero, tienen inverso. Sea, pues, x el inverso de 2 en $\mathbb{Z}_{11}$. Entonces,

$$\begin{aligned} x \text{ es el inverso de 2 en } \mathbb{Z}_{11} &\iff 2x = 1 \text{ en } \mathbb{Z}_{11} \\ &\iff 2x \equiv 1 (\text{mód } 11) \text{ en } \mathbb{Z} \\ &\iff 11 | 2x - 1 \text{ en } \mathbb{Z} \\ &\iff \exists y \in \mathbb{Z} : 2x - 11y = 1 \end{aligned}$$

Tenemos una ecuación diofántica del tipo $ax + by = c$ donde $a = 2$, $b = -11$ y $c = 1$.

1 Solución particular. Utilizamos el algoritmo de Euclides para obtener el máximo común divisor de 2 y -11 y los coeficientes p y q necesarios para el cálculo.

		5	2
11	2	1	
1	0		

$$\implies d = \text{m.c.d.}(2, -11) = 1 \implies 1 = 11 - 5 \cdot 2 \implies 1 = -5 \cdot 2 + (-1)(-11)$$

De aquí que $p = -5$, $q = -1$ y la solución particular será, por tanto,

$$x_0 = \frac{cp}{d} \Longrightarrow x_0 = \frac{1(-5)}{1} \Longrightarrow x_0 = -5$$

2 Solución general.

$$x = x_0 + k\frac{b}{d}, k \in \mathbb{Z} \Longrightarrow x = -5 + k\frac{-11}{1} \Longrightarrow x = -5 - 11k, k \in \mathbb{Z}$$

3 Cálculo del inverso.

Buscamos soluciones para x que estén entre 0 y 11. Entonces,

$$\begin{aligned} 0 < x < 11 &\iff 0 < -5 - 11k < 11 \\ &\iff 5 < -11k < 16 \\ &\iff -16 < 11k < -5 \\ &\iff -\frac{16}{11} < k < -\frac{5}{11} \\ &\iff -1,455 < k < -0,455 \\ &\iff -1 \leqslant k \leqslant -1 \\ &\iff k = -1 \end{aligned}$$

Sustituyendo en la solución general,

$$\left.\begin{array}{l} x = -5 - 11k \\ \text{y} \\ k = -1 \end{array}\right\} \implies x = -5 - 11(-1) \text{ en } \mathbb{Z}$$

$$\begin{aligned} &\iff x = 6 \text{ en } \mathbb{Z} \\ &\implies x \equiv 6 \,(\text{mód } 11) \text{ en } \mathbb{Z} \\ &\iff [x] = [6] \\ &\iff x = 6 \text{ en } \mathbb{Z}_{11} \end{aligned}$$

luego el inverso de 2 en $\mathbb{Z}_{11}$ es 6.

(b) Inverso de 7 en $\mathbb{Z}_{15}$.

Como 7 y 15 son primos entre sí, 7 tendrá inverso en $\mathbb{Z}_{15}$. Pues bien,

$$\begin{aligned} x \text{ es el inverso de } 7 \text{ en } \mathbb{Z}_{15} &\iff 7x = 1 \text{ en } \mathbb{Z}_{15} \\ &\iff 7x \equiv 1 (\text{mód } 15) \text{ en } \mathbb{Z} \\ &\iff 15 | 7x - 1 \text{ en } \mathbb{Z} \\ &\iff \exists y \in \mathbb{Z} : 7x - 15y = 1 \end{aligned}$$

Ecuación diofántica de la forma $ax + by = c$, donde $a = 7$, $b = -15$ y $c = 1$.

1 Solución particular. Obtenemos el máximo común divisor de los coeficientes, 7 y -15, mediante el algoritmo de Euclides y lo volvemos atrás para obtener los coeficientes p y q necesarios para el cálculo.

		2	7
15	7	1	
1	0		

$$\implies d = \text{m.c.d.}(7, -15) = 1 \implies 1 = 15 - 2 \cdot 7 \implies 1 = -2 \cdot 7 + (-1)(-15)$$

Luego, $p = -2$, $q = -1$ y, por tanto, la solución particular de la ecuación es:

$$x_0 = \frac{cp}{d} \Longrightarrow x_0 = \frac{1(-2)}{1} \Longrightarrow x_0 = -2$$

2 Solución general.

$$x = x_0 + k\frac{b}{d}, k \in \mathbb{Z} \Longrightarrow x = -2 + k\frac{-15}{1} \Longrightarrow x = -2 - 15k, k \in \mathbb{Z}$$

3 Cálculo del inverso.

Buscamos soluciones para x que estén entre 0 y 15. Entonces,

$$\begin{aligned} 0 < x < 15 &\iff 0 < -2 - 15k < 15 \\ &\iff 2 < -15k < 17 \\ &\iff -17 < 15k < -2 \\ &\iff -\frac{17}{15} < k < -\frac{2}{15} \\ &\iff -1,133 < k < -0,133 \\ &\iff -1 \leqslant k \leqslant -1 \\ &\iff k = -1 \end{aligned}$$

Sustituyendo en la solución general,

$$\left.\begin{array}{l} x = -2 - 15k \\ \text{y} \\ k = -1 \end{array}\right\} \implies x = -2 - 15(-1) \text{ en } \mathbb{Z}$$

$$\begin{aligned} &\iff x = 13 \text{ en } \mathbb{Z} \\ &\implies x \equiv 13 \,(\text{mód } 15) \text{ en } \mathbb{Z} \\ &\iff [x] = [13] \\ &\iff x = 13 \text{ en } \mathbb{Z}_{15} \end{aligned}$$

luego el inverso de 7 en $\mathbb{Z}_{15}$ es 13.

(c) Inverso de 7 en $\mathbb{Z}_{16}$.

Como 7 y 16 son primos entre sí, 7 tendrá inverso en $\mathbb{Z}_{16}$. Pues bien,

$$\begin{aligned} x \text{ es el inverso de 7 en } \mathbb{Z}_{16} &\iff 7x = 1 \text{ en } \mathbb{Z}_{16} \\ &\iff 7x \equiv 1 (\text{mód } 16) \text{ en } \mathbb{Z} \\ &\iff 16 | 7x - 1 \text{ en } \mathbb{Z} \\ &\iff \exists x \in \mathbb{Z} : 7x - 16y = 1 \end{aligned}$$

Tenemos, pues, una ecuación diofántica del tipo $ax + by = c$ con $a = 7$, $b = -16$ y $c = 1$

1 Solución particular. Obtenemos el máximo común divisor de los coeficientes, 7 y -16, mediante el algoritmo de Euclides y lo volvemos atrás para obtener los coeficientes p y q necesarios para el cálculo.

		2	3	2
16	7	2	1	
2	1	0		

$$\implies d = \text{m.c.d.}(7, -16) = 1 \implies \begin{cases} 1 = 7 - 3 \cdot 2 \\ 2 = 16 - 2 \cdot 7 \end{cases}$$

$$\begin{aligned} &\implies 1 = 7 - 3(16 - 2 \cdot 7) \\ &\implies 1 = 7 \cdot 7 + 3(-16) \end{aligned}$$

Por lo tanto, $p = 7$, $q = 3$ y, consecuentemente,

$$x_0 = \frac{cp}{d} \implies x_0 = \frac{1 \cdot 7}{1} \implies x_0 = 7$$

2 Solución general.

$$x = x_0 + k\frac{b}{d} \Longrightarrow x = 7 + k\frac{-16}{1} \Longrightarrow x = 7 - 16k$$

3 Cálculo del inverso.

Buscamos soluciones para x que estén entre 0 y 16. Entonces,

$$\begin{aligned} 0 < x < 16 &\iff 0 < 7 - 16k < 16 \\ &\iff -7 < -16k < 9 \\ &\iff -9 < 16k < 7 \\ &\iff -\frac{9}{16} < k < \frac{7}{16} \\ &\iff -0,5625 < k < 0,4375 \\ &\iff 0 \leqslant k \leqslant 0 \\ &\iff k = 0 \end{aligned}$$

Sustituyendo en la solución general,

$$\left.\begin{array}{l} x = 7 - 16k \\ \text{y} \\ k = 0 \end{array}\right\} \Longrightarrow x = 7 - 16 \cdot 0 \text{ en } \mathbb{Z}$$

$$\begin{aligned} &\iff x = 7 \text{ en } \mathbb{Z} \\ &\Longrightarrow x \equiv 7 \,(\text{mód } 16) \text{ en } \mathbb{Z} \\ &\iff [x] = [7] \\ &\iff x = 7 \text{ en } \mathbb{Z}_{16} \end{aligned}$$

luego el inverso de 7 en $\mathbb{Z}_{16}$ es 7.

(d) Inverso de 5 en $\mathbb{Z}_{13}$.

Como 13 es primo, todos los elementos de $\mathbb{Z}_{13}$, excepto el cero, tienen inverso. Lo calcularemos utilizando un procedimiento análogo al utilizado en los apartados anteriores.

$$\begin{aligned} x \text{ es el inverso de 5 en } \mathbb{Z}_{13} &\iff 5x = 1 \text{ en } \mathbb{Z}_{13} \\ &\iff 5x \equiv 1 (\text{mód } 13) \text{ en } \mathbb{Z} \\ &\iff 13 | 5x - 1 \text{ en } \mathbb{Z} \\ &\iff \exists x \in \mathbb{Z} : 5x - 13y = 1 \end{aligned}$$

Ecuación diofántica del tipo $ax + by = c$, donde $a = 5$, $b = -13$ y $c = 1$.

1 Solución particular. Obtenemos el máximo común divisor de los coeficientes, 5 y -13, mediante el algoritmo de Euclides y lo volvemos atrás para obtener los coeficientes p y q necesarios para el cálculo.

		2	1	1	2
13	5	3	2	1	
3	2	1	0		

$$\Longrightarrow d = \text{m.c.d.}(5, -13) = 1$$

luego,

$$\left.\begin{array}{rcrcr} 1 & = & 3 & - & 1 \cdot 2 \\ 2 & = & 5 & - & 1 \cdot 3 \end{array}\right\} \Longrightarrow 1 = 3 - 1(5 - 1 \cdot 3) = (-1) \cdot 5 + 2 \cdot 3$$

$$\left.\begin{array}{rcrcr} 1 & = & (-1) \cdot 5 & + & 2 \cdot 3 \\ 3 & = & 13 & - & 2 \cdot 5 \end{array}\right\} \Longrightarrow 1 = (-1) \cdot 5 + 2(13 - 2 \cdot 5) = (-5) \cdot 5 + 2 \cdot 13$$

es decir,

$$1 = (-5)\cdot 5 + (-2)(-13) \implies p = -5 \text{ y } q = -2$$

Entonces,

$$x_0 = \frac{cp}{d} \Longrightarrow x_0 = \frac{1(-5)}{1} \Longrightarrow x_0 = -5$$

2 Solución general.

$$x = x_0 + k\frac{b}{d} \Longrightarrow x = -5 + k\frac{-13}{1} \Longrightarrow x = -5 - 13k$$

3 Cálculo del inverso.

Buscamos soluciones para x que estén entre 0 y 13. Entonces,

$$\begin{aligned} 0 < x < 16 &\iff 0 < -5 - 13k < 13 \\ &\iff 5 < -13k < 18 \\ &\iff -18 < 13k < -5 \\ &\iff -\frac{18}{13} < k < -\frac{5}{13} \\ &\iff -1,3846 < k < -0,3846 \\ &\iff -1 \leqslant k \leqslant -1 \\ &\iff k = -1 \end{aligned}$$

Sustituyendo en la solución general,

$$\left.\begin{array}{l} x = -5 - 13k \\ \text{y} \\ k = -1 \end{array}\right\} \implies x = -5 - 13(-1) \text{ en } \mathbb{Z}$$

$$\begin{aligned} &\iff x = 8 \text{ en } \mathbb{Z} \\ &\implies x \equiv 8\,(\text{mód } 13) \text{ en } \mathbb{Z} \\ &\iff [x] = [8] \\ &\iff x = 8 \text{ en } \mathbb{Z}_{13} \end{aligned}$$

luego el inverso de 5 en $\mathbb{Z}_{13}$ es 8.

■

Ejemplo 16.16

Obtener los opuestos, los inversos y escribir las tablas de sumar y multiplicar en $\mathbb{Z}_5$ y $\mathbb{Z}_6$.

Solución

$\mathbb{Z}_5 = \{[0], [1], [2], [3], [4]\}$

- Opuestos.
  - El opuesto de [0] es, obviamente, [0].
  - El opuesto de [1] es, $[5 - 1] = [4]$.

- El opuesto de $[2]$ es, $[5-2]=[3]$.
- El opuesto de $[3]$ es, $[5-3]=[2]$.
- El opuesto de $[4]$ es, $[5-4]=[1]$.

⁕ Inversos. Como el 5 es primo, todos los elementos de $\mathbb{Z}_5$, excepto el $[0]$ poseen inverso.

- El inverso de $[1]$ es $[1]$.
- El inverso de $[2]$ es $[3]$.
- El inverso de $[3]$ es $[2]$.
- El inverso de $[4]$ es $[4]$.

⁕ Tabla de sumar.

$+$	$[0]$	$[1]$	$[2]$	$[3]$	$[4]$
$[0]$	$[0]$	$[1]$	$[2]$	$[3]$	$[4]$
$[1]$	$[1]$	$[2]$	$[3]$	$[4]$	$[0]$
$[2]$	$[2]$	$[3]$	$[4]$	$[0]$	$[1]$
$[3]$	$[3]$	$[4]$	$[0]$	$[1]$	$[2]$
$[4]$	$[4]$	$[0]$	$[1]$	$[2]$	$[3]$

⁕ Tabla de multiplicar.

$\times$	$[0]$	$[1]$	$[2]$	$[3]$	$[4]$
$[0]$	$[0]$	$[0]$	$[0]$	$[0]$	$[0]$
$[1]$	$[0]$	$[1]$	$[2]$	$[3]$	$[4]$
$[2]$	$[0]$	$[2]$	$[4]$	$[1]$	$[3]$
$[3]$	$[0]$	$[3]$	$[1]$	$[4]$	$[2]$
$[4]$	$[0]$	$[4]$	$[3]$	$[2]$	$[1]$

$\mathbb{Z}_6=\{[0],[1],[2],[3],[4],[5]\}$

⁕ Opuestos.

- El opuesto de $[0]$ es $[0]$.
- El opuesto de $[1]$ es $[5]$.
- El opuesto de $[2]$ es $[4]$.
- El opuesto de $[3]$ es $[3]$.
- El opuesto de $[4]$ es $[2]$.
- El opuesto de $[5]$ es $[1]$.

⁕ Inversos. Como el $[6]$ no es primo, no todos los elementos de $\mathbb{Z}_6$ tienen inverso.

- m.c.d.$(1,6)=1$, luego $[1]$ tiene inverso, el $[1]$.
- m.c.d.$(2,6)=2$, luego $[2]$ no tiene inverso.
- m.c.d.$(3,6)=3$, luego $[3]$ no tiene inverso.
- m.c.d.$(4,6)=2$, luego $[4]$ no tiene inverso.
- m.c.d.$(5,6)=1$, luego $[5]$ tiene inverso, el $[5]$.

⁕ Tabla de sumar.

$+$	$[0]$	$[1]$	$[2]$	$[3]$	$[4]$	$[5]$
$[0]$	$[0]$	$[1]$	$[2]$	$[3]$	$[4]$	$[5]$
$[1]$	$[1]$	$[2]$	$[3]$	$[4]$	$[5]$	$[0]$
$[2]$	$[2]$	$[3]$	$[4]$	$[5]$	$[0]$	$[1]$
$[3]$	$[3]$	$[4]$	$[5]$	$[0]$	$[1]$	$[2]$
$[4]$	$[4]$	$[5]$	$[0]$	$[1]$	$[2]$	$[3]$
$[5]$	$[5]$	$[0]$	$[1]$	$[2]$	$[3]$	$[4]$

⁕ Tabla de multiplicar.

$\times$	$[0]$	$[1]$	$[2]$	$[3]$	$[4]$	$[5]$
$[0]$	$[0]$	$[0]$	$[0]$	$[0]$	$[0]$	$[0]$
$[1]$	$[0]$	$[1]$	$[2]$	$[3]$	$[4]$	$[5]$
$[2]$	$[0]$	$[2]$	$[4]$	$[0]$	$[2]$	$[4]$
$[3]$	$[0]$	$[3]$	$[0]$	$[3]$	$[0]$	$[3]$
$[4]$	$[0]$	$[4]$	$[2]$	$[0]$	$[1]$	$[2]$
$[5]$	$[0]$	$[5]$	$[4]$	$[3]$	$[2]$	$[1]$

■

Nota 16.3 En $\mathbb{Z}$ se verifica la ley de cancelación, es decir, si a, b y c son tres números enteros con $a \neq 0$, se verifica que

$$ab = ac \Longrightarrow b = c$$

En $\mathbb{Z}_m$ esta ley, en general, no se verifica, es decir pueden encontrarse $a \neq 0$, b y c tales que

$$ab = ac \text{ y, sin embargo, } b \neq c$$

Por ejemplo, en $\mathbb{Z}_4$

$$2 \cdot 1 = 2 \cdot 3 \text{ y, sin embargo, } 1 \neq 3$$

Obsérvese, también, que en $\mathbb{Z}$ no existen divisores de cero, es decir, para cualquier par de enteros a y b se verifica

$$ab = 0 \Longrightarrow a = 0 \text{ ó } b = 0$$

En $\mathbb{Z}_m$ si existen divisores de cero, es decir pueden encontrarse a y b tales que

$$ab = 0 \text{ y, sin embargo, } a \neq 0 \text{ y } b \neq 0$$

Por ejemplo en $\mathbb{Z}_6$ se tiene que

$$3 \cdot 2 = 0 \text{ y, sin embargo, } 3 \neq 0 \text{ y } 2 \neq 0$$

■

Ejemplo 16.17

Resolver el siguiente sistema de ecuaciones en $\mathbb{Z}_7$.

$$\left.\begin{array}{rcrcl} x & + & 2y & = & 4 \\ 4x & + & 3y & = & 4 \end{array}\right\}$$

Solución

Lo resolvemos por los tres métodos tradicionales de la matemática elemental.

⊛ Sustitución.

Despejamos x en la primera ecuación y sustituimos en la segunda.

$$x + 2y = 4 \Longrightarrow x + 2y + 5y = 4 + 5y \Longrightarrow x = 4 + 5y$$

Entonces,

$$\left.\begin{array}{rcrcrl} x & = & 4 & + & 5y & \\ 4x & + & 3y & = & 4 & \end{array}\right\} \implies 4\,(4+5y)+3y=4$$

$$\begin{aligned} &\implies 2+6y+3y=4\\ &\implies 2+2y=4\\ &\implies 2y=4+5\\ &\implies 2y=2 \end{aligned}$$

y como 7 es primo, todos los elementos de $\mathbb{Z}_7$ tienen inverso, luego multiplicando ambos miembros por el inverso de 2 se sigue que

$$y=1$$

Pues bien,

$$\left.\begin{array}{rcrcrl} x & = & 4 & + & 5y & \\ y & = & 1 & & & \end{array}\right\} \implies x=4+5\cdot 1 \implies x=2$$

⊛ Igualación.

Despejamos x en ambas ecuaciones.

$$\begin{aligned} x+2y=4 &\implies x+2y+5y=4+5y\\ &\implies x=4+5y \end{aligned}$$

$$\begin{aligned} 4x+3y=4 &\implies 2\cdot 4x+2\cdot 3y=2\cdot 4\\ &\implies x+6y=1\\ &\implies x+6y+1y=1+1y\\ &\implies x=1+1y \end{aligned}$$

Igualando ambos resultados,

$$1+1y=4+5y \implies 6+1+2y+1y=4+6+5y+2y \implies 3y=3 \implies y=1$$

Consecuentemente,

$$\left.\begin{array}{rcrcrl} x & = & 1 & + & 1y & \\ y & = & 1 & & & \end{array}\right\} \implies x=1+1\cdot 1 \implies x=2$$

⊛ Reducción.

Multiplicamos la primera ecuación por 3, la segunda por 1 y las sumamos.

$$\left.\begin{array}{rcrcrl} x & + & 2y & = & 4 & \\ 4x & + & 3y & = & 4 & \end{array}\right\} \implies \left.\begin{array}{rcrcrl} 3x & + & 6y & = & 5 & \\ 4x & + & 3y & = & 4 & \end{array}\right\} \implies 2y=2 \implies y=1$$

Análogamente, multiplicando la primera por 2, la segunda por 1 y sumándolas posteriormente,

$$\left.\begin{array}{rcrcrl} x & + & 2y & = & 4 & \\ 4x & + & 3y & = & 4 & \end{array}\right\} \implies \left.\begin{array}{rcrcrl} 2x & + & 4y & = & 1 & \\ 4x & + & 3y & = & 4 & \end{array}\right\}$$

$$\begin{aligned} &\implies 6y=5\\ &\implies 6\cdot 1x=6\cdot 5\\ &\implies x=2 \end{aligned}$$

■

Ejemplo 16.18

Resolver la ecuación $x^2 + 3x + 4 = 0$ *en* $\mathbb{Z}_{11}$.

Solución

$$\begin{aligned}
x &= \frac{-3 \pm \sqrt{(3)^2 - 4 \cdot 1 \cdot 4}}{2 \cdot 1} \\
&= \frac{-3 \pm \sqrt{3 \cdot 3 - 4 \cdot 4}}{2} \\
&= \frac{8 \pm \sqrt{9 - 16}}{2} \\
&= \frac{8 \pm \sqrt{-7}}{2} \\
&= \frac{8 \pm \sqrt{4}}{2} \\
&= \frac{8 \pm \sqrt{2^2}}{2} \\
&= \frac{8 \pm 2}{2} \\
&= \begin{cases} \dfrac{8+2}{2} \\ \dfrac{8-2}{2} \end{cases} \\
&\quad \{\text{El inverso de 2 es 6}\} \\
&= \begin{cases} 6 \cdot 10 \\ 6 \cdot 6 \end{cases} \\
&= \begin{cases} 60 \\ 36 \end{cases} \\
&= \begin{cases} 5 \\ 3 \end{cases}
\end{aligned}$$

■

Ejemplo 16.19

Demostrar que en $\mathbb{Z}_p$, *con* p *primo, se verifica la igualdad* $(x+y)^p = x^p + y^p$.

Solución

Por el Teorema del Binomio, tendremos

$$(x+y)^p = x^p + \sum_{k=1}^{p-1} \binom{p}{k} x^{p-k} y^k + y^p \tag{16.2}$$

Pues bien,

$$\left(\begin{array}{c} p \\ k \end{array}\right) = \frac{p!}{k!(p-k)!} \implies k!\left(\begin{array}{c} p \\ k \end{array}\right) = \frac{p!}{(p-k)!}$$

$$\implies k!\left(\begin{array}{c} p \\ k \end{array}\right) = p(p-1)\cdots(p-k+1)$$

$$\implies p \left| k!\left(\begin{array}{c} p \\ k \end{array}\right)\right.$$

Por otra parte, como p es primo, p y k serán primos entre sí para $1 < k < p$, es decir,

$$\text{m.c.d.}(p,k) = 1,\ 1 < k < p$$

y aplicando reiteradamente el ejemplo 13.**??**, tendremos que

$$\text{m.c.d.}\,(p,k!) = 1$$

Así pues,

$$p \left| k!\left(\begin{array}{c} p \\ k \end{array}\right)\right. \text{ y m.c.d.}\,(p,k!) = 1$$

luego por el Lema de Euclides,

$$p \left| \left(\begin{array}{c} p \\ k \end{array}\right)\right.$$

es decir,

$$\left(\begin{array}{c} p \\ k \end{array}\right) \equiv 0(\text{mód } p) \text{ para } 1 < k < p$$

o lo que es igual,

$$\left(\begin{array}{c} p \\ k \end{array}\right) = 0$$

para $1 < k < p$ en $\mathbb{Z}_p$. Por lo tanto,

$$\sum_{k=1}^{p-1}\left(\begin{array}{c} p \\ k \end{array}\right)x^{p-k}y^k = \sum_{k=1}^{p-1} 0x^{p-k}y^k = 0.$$

Sustituimos este resultado en (16.2) y

$$(x+y)^p = x^p + y^p$$

■

Ejemplo 16.20

Demostrar que para p, primo, $3^p + (-2)^p + (-1)^p$ es divisible por p.

Solución

Observemos lo siguiente: $3^p + (-2)^p + (-1)^p$ será divisible por p, si da resto cero al dividirlo por p, es decir, si

$$3^p + (-2)^p + (-1)^p \equiv 0(\text{mód } p) \text{ en } \mathbb{Z}$$

lo cual es lo mismo que decir que

$$3^p + (-2)^p + (-1)^p = 0 \text{ en } \mathbb{Z}_p.$$

Así pues, si probamos esto último, tendremos resuelta la demostración.

Pues bien,

$$\begin{aligned} 3^p + (-2)^p + (-1)^p &= (3 + (-2))^p + (-1)^p && \{\text{Ejemplo anterior}\} \\ &= 1^p + (-1)^p \\ &= (1 + (-1))^p && \{\text{Ejemplo anterior}\} \\ &= 0^p \\ &= 0 \end{aligned}$$

y, consecuentemente, el número propuesto es divisible por p.

■

Ejemplo 16.21

En el conjunto $\mathbb{Z}_5$ de las clases de restos módulo 5, se pide:

(a) Divisores de cero.

(b) Elementos invertibles.

(c) Resolver el siguiente sistema de ecuaciones.

$$\left.\begin{array}{rcrcl} 2x & + & y & = & 2 \\ 3x & + & 4y & = & 3 \end{array}\right\}$$

Solución

(a) Veamos si $\mathbb{Z}_5$ tiene divisores de cero.

Recordemos que

$$\mathbb{Z}_5 \text{ no tiene divisores de cero } \iff \forall a, b \in \mathbb{Z}_5 : ab = 0 \Longrightarrow a = 0 \text{ ó } b = 0$$

por lo tanto,

$$\mathbb{Z}_5 \text{ tiene divisores de cero } \iff \exists a, b \in \mathbb{Z}_5 : ab = 0 \text{ y } a \neq 0 \text{ y } b \neq 0$$

Pues bien, sean a y b cualesquiera de $\mathbb{Z}_5$. Entonces,

$$\begin{aligned} ab = 0 \text{ en } \mathbb{Z}_5 &\iff ab \equiv 0(\text{mód } 5) \text{ en } \mathbb{Z} \\ &\iff 5|ab \text{ en } \mathbb{Z} \\ &\iff 5|a \text{ ó } 5|b \text{ en } \mathbb{Z} \ \{\text{Corolario 14.3.2}\} \\ &\iff a \equiv 0(\text{mód } 5) \text{ ó } b \equiv 0(\text{mód } 5) \text{ en } \mathbb{Z} \\ &\iff a = 0 \text{ ó } b = 0 \text{ en } \mathbb{Z}_5 \end{aligned}$$

Por lo tanto, $\mathbb{Z}_5$ no tiene divisores de cero.

(b) Elementos invertibles. Como 5 es primo todos los elementos de $\mathbb{Z}_5$, excepto el 0, son invertibles.

(c) Resolvamos el sistema de ecuaciones propuesto.

$$\left.\begin{array}{rcrcl} 2x & + & y & = & 2 \\ 3x & + & 4y & = & 3 \end{array}\right\}$$

Obsérvese que la segunda ecuación es igual a la primera multiplicada por 4, luego ambas ecuaciones son equivalentes en $\mathbb{Z}_5$, entonces,

$$2x + y = 2 \Longleftrightarrow 3x + 2x + y = 2 + 3x \Longleftrightarrow y = 2 + 3x : x \in \mathbb{Z}_5$$

y las soluciones serían:

Para $x = 0,\ y = 2$

Para $x = 1,\ y = 0$

Para $x = 2,\ y = 3$

Para $x = 3,\ y = 1$

Para $x = 4,\ y = 4$

■

16.5 Ecuaciones Lineales en $\mathbb{Z}_m$

Planteamos, a continuación, ecuaciones del tipo $ax = b$ donde a y b son de $\mathbb{Z}_m$ y x es la indeterminada. Resolver esta ecuación significa obtener todos los números en $\mathbb{Z}_m$ que al ser escritos en lugar de la indeterminada, verifiquen la ecuación.

Veremos que la resolución de una ecuación de este tipo equivale a la de una ecuación diofántica.

16.5.1 Teorema

La ecuación $ax = b$ tiene solución en $\mathbb{Z}_m$ si, y sólo si el máximo común divisor de a y m divide a b

Demostración

En efecto, sean a y b cualesquiera de $\mathbb{Z}_m$. Entonces,

$$\begin{aligned} ax = b \text{ tiene solución en } \mathbb{Z}_m &\Longleftrightarrow \exists x \in \mathbb{Z}_m : ax = b \\ &\Longleftrightarrow \exists x \in \mathbb{Z} : ax \equiv b(\text{mód } m) \\ &\Longleftrightarrow \exists x \in \mathbb{Z} : m | ax - b \\ &\Longleftrightarrow \exists x, y \in \mathbb{Z} : ax - b = my \\ &\Longleftrightarrow \exists x, y \in \mathbb{Z} : ax - my = b \\ &\Longleftrightarrow \text{La ecuación diofántica } ax - my = b \text{ tiene solución en } \mathbb{Z} \\ &\Longleftrightarrow \text{m.c.d.}(a, -m) | b \ \{15.2.1\} \\ &\Longleftrightarrow \text{m.c.d.}(a, m) | b \end{aligned}$$

Ejemplo 16.22

Resolver las siguientes ecuaciones en los conjuntos de clases de restos que se indican.

(a) $5x = 8$ *en* $\mathbb{Z}_6$.

(b) $15x = 6$ *en* $\mathbb{Z}_{21}$

(c) $3x = 27$ *en* $\mathbb{Z}_6$.

(d) $3x = 8$ *en* $\mathbb{Z}_6$.

(e) $12x = 45$ *en* $\mathbb{Z}_3$.

Solución

(a) $5x = 8$ en $\mathbb{Z}_6$.

$$\begin{aligned} 5x = 8 \text{ tiene solución en } \mathbb{Z}_6 &\iff \exists x \in \mathbb{Z}_6 : 5x = 8 \\ &\iff \exists x \in \mathbb{Z} : 5x \equiv 8(\text{mód } 6) \\ &\iff \exists x \in \mathbb{Z} : 6 \,|\, 5x - 8 \\ &\iff \exists x, y \in \mathbb{Z} : 5x - 8 = 6y \\ &\iff \exists x, y \in \mathbb{Z} : 5x - 6y = 8 \end{aligned}$$

La ecuación anterior será, por tanto, una ecuación diofántica del tipo $ax + by = c$ con $a = 5$, $b = -6$ y $c = 8$.

1 Veamos si la ecuación diofántica $5x - 6y = 8$ tiene solución.

Obtenemos el máximo común divisor de 5 y -6 mediante el algoritmo de Euclides y lo volvemos atrás para obtener los coeficientes p y q necesarios para el cálculo.

		1	5
6	5	1	
1	0		

$$\Longrightarrow \quad d = \text{m.c.d.}(5, -6) = 1 \quad \Longrightarrow \quad 1 = 6 - 1 \cdot 5 \quad \Longrightarrow \quad 1 = -1 \cdot 5 + (-1)(-6)$$

Luego, $p = -1$ y $q = -1$.

Como 1, máximo común divisor de 5 y -6, divide a 8, según el teorema anterior, (16.5.1), la ecuación tiene solución.

2 Solución particular.

$$x_0 = \frac{cp}{d} \Longrightarrow x_0 = \frac{8(-1)}{1} \Longrightarrow x_0 = -8$$

3 Solución general.

$$x = x_0 + k\frac{b}{d}, k \in \mathbb{Z} \Longrightarrow x = -8 + k\frac{-6}{1}, k \in \mathbb{Z} \Longrightarrow x = -8 - 6k, k \in \mathbb{Z}$$

4 Solución de la ecuación propuesta.

Buscamos soluciones para x que estén entre 0 y 6. Entonces,

$$\begin{aligned} 0 < x < 6 &\iff 0 < -8 - 6k < 6 \\ &\iff 8 < -6k < 14 \\ &\iff -14 < 6k < -8 \\ &\iff -\frac{14}{6} < k < -\frac{8}{6} \\ &\iff -2,333 < k < -1,333 \\ &\iff -2 \leqslant k \leqslant -2 \\ &\iff k = -2 \end{aligned}$$

Sustituyendo en la solución general,

$$\left.\begin{array}{l} x = -8 - 6k \\ \text{y} \\ k = -2 \end{array}\right\} \implies x = -8 - 6(-2) \text{ en } \mathbb{Z}$$

$$\begin{aligned} &\iff x = 4 \text{ en } \mathbb{Z} \\ &\implies x \equiv 4 \,(\text{mód } 6) \text{ en } \mathbb{Z} \\ &\iff [x] = [6] \\ &\iff x = 4 \text{ en } \mathbb{Z}_6 \end{aligned}$$

(b) $15x = 6$ en $\mathbb{Z}_{21}$.

$$\begin{aligned} 15x = 6 \text{ tiene solución en } \mathbb{Z}_{21} &\iff \exists x \in \mathbb{Z}_{21} : 15x = 6 \\ &\iff \exists x \in \mathbb{Z} : 15x \equiv 6 (\text{mód } 21) \\ &\iff \exists x \in \mathbb{Z} : 21 \,|15x - 6 \\ &\iff \exists x, y \in \mathbb{Z} : 15x - 6 = 21y \\ &\iff \exists x, y \in \mathbb{Z} : 15x - 21y = 6 \end{aligned}$$

Ecuación diofántica del tipo $ax + by = c$ con $a = 15$, $b = -21$ y $c = 6$.

1 Veamos, primero, si la ecuación diofántica $15x - 21y = 6$ tiene solución.
Obtenemos el máximo común divisor de 15 y -21 mediante el algoritmo de Euclides y lo volvemos atrás para obtener los coeficientes p y q necesarios para el cálculo.

	1	2	2
21	15	6	3
6	3	0	

$$\implies d = \text{m.c.d.}(15, -21) = 3 \implies \left\{\begin{array}{l} 3 = 15 - 2 \cdot 6 \\ 6 = 21 - 1 \cdot 15 \end{array}\right.$$

$$\begin{aligned} &\implies 3 = 15 - 2(21 - 1 \cdot 15) \\ &\implies 3 = 3 \cdot 15 + 2(-21) \\ &\implies p = 3 \text{ y } q = 2 \end{aligned}$$

Como 3, máximo común divisor de 15 y -21, divide a 6, según el teorema anterior, (16.5.1), la ecuación tiene solución.

2 Solución particular.

$$x_0 = \frac{cp}{d} \implies x_0 = \frac{6 \cdot 3}{3} \implies x_0 = 6$$

3 Solución general.

$$x = x_0 + k_1\frac{b}{d}, k_1 \in \mathbb{Z} \Longrightarrow x = 6 + k_1\frac{-21}{3}, k_1 \in \mathbb{Z} \Longrightarrow x = 6 - 7k_1, k_1 \in \mathbb{Z}$$

4 Solución de la ecuación propuesta.

Buscamos soluciones para x que estén entre 0 y 21. Entonces,

$$\begin{aligned}
0 < x < 6 &\iff 0 < 6 - 7k < 21 \\
&\iff -6 < -7k < 15 \\
&\iff -15 < 7k < 6 \\
&\iff -\frac{15}{7} < k < \frac{6}{7} \\
&\iff -2,143 < k < 0,857 \\
&\iff -2 \leqslant k \leqslant 0 \\
&\iff k = -2 \text{ o } k = -1 \text{ o } k = 0
\end{aligned}$$

Sustituyendo en la solución general,

⁕ Para $k = 0$,

$$\begin{aligned}
x = 6 - 7 \cdot 0 \text{ en } \mathbb{Z} &\iff x = 6 \text{ en } \mathbb{Z} \\
&\Longrightarrow x \equiv 6 \,(\text{mód } 21) \text{ en } \mathbb{Z} \\
&\iff [x] = [6] \\
&\iff x = 6 \text{ en } \mathbb{Z}_{21}
\end{aligned}$$

⁕ Para $k = -1$,

$$\begin{aligned}
x = 6 - 7(-1) \text{ en } \mathbb{Z} &\iff x = 13 \text{ en } \mathbb{Z} \\
&\Longrightarrow x \equiv 13 \,(\text{mód } 21) \text{ en } \mathbb{Z} \\
&\iff [x] = [13] \\
&\iff x = 13 \text{ en } \mathbb{Z}_{21}
\end{aligned}$$

⁕ Para $k = -2$,

$$\begin{aligned}
x = 6 - 7(-2) \text{ en } \mathbb{Z} &\iff x = 20 \text{ en } \mathbb{Z} \\
&\Longrightarrow x \equiv 20 \,(\text{mód } 21) \text{ en } \mathbb{Z} \\
&\iff [x] = [20] \\
&\iff x = 20 \text{ en } \mathbb{Z}_{21}
\end{aligned}$$

(c) $3x = 27$ en $\mathbb{Z}_6$.

$$
\begin{aligned}
3x = 27 \text{ tiene solución en } \mathbb{Z}_6 &\iff \exists x \in \mathbb{Z}_6 : 3x = 27 \\
&\iff \exists x \in \mathbb{Z} : 3x \equiv 27(\text{mód } 6) \\
&\iff \begin{cases} 3x \equiv 27(\text{mód } 6) \text{ en } \mathbb{Z} \\ \text{y} \\ 27 \equiv 3(\text{mód } 6) \text{ en } \mathbb{Z} \end{cases} \\
&\iff \exists x \in \mathbb{Z} : 3x \equiv 3(\text{mód } 6) \\
&\iff \exists x \in \mathbb{Z} : 6 | 3x - 3 \text{ en } \mathbb{Z} \\
&\iff \exists x, y \in \mathbb{Z} : 3x - 6y = 3 \\
&\iff \exists x, y \in \mathbb{Z} : x = \frac{3 + 6y}{3} \\
&\iff \exists x, y \in \mathbb{Z} : x = 2y + 1 \\
&\iff \exists x, q, r \in \mathbb{Z} : x = 2(3q + r) + 1, \text{ siendo } 0 \leqslant r < 3 \text{ (13.2.1)} \\
&\iff \begin{cases} x = 6q + 1, \ q \in \mathbb{Z} \\ \text{o} \\ x = 6q + 3, \ q \in \mathbb{Z} \\ \text{o} \\ x = 6q + 5, \ q \in \mathbb{Z} \end{cases} \\
&\iff \begin{cases} x \equiv 1(\text{mód } 6) \\ \text{o} \\ x \equiv 3(\text{mód } 6) \\ \text{o} \\ x \equiv 5(\text{mód } 6) \end{cases} \\
&\iff \begin{cases} x = 1, \text{ en } \mathbb{Z}_6 \\ \text{ó} \\ x = 3, \text{ en } \mathbb{Z}_6 \\ \text{ó} \\ x = 5, \text{ en } \mathbb{Z}_6 \end{cases}
\end{aligned}
$$

(d) $3x = 8$ en $\mathbb{Z}_6$.

$$
\begin{aligned}
3x = 8 \text{ tiene solución en } \mathbb{Z}_6 &\iff \exists x \in \mathbb{Z}_6 : 3x = 8 \\
&\iff \exists x \in \mathbb{Z} : 3x \equiv 8(\text{mód } 6) \\
&\iff \exists x \in \mathbb{Z} : 6 | 3x - 8 \text{ en } \mathbb{Z} \\
&\iff \exists x, y \in \mathbb{Z} : 3x - 6y = 8 \\
&\iff \text{m.c.d.}(3, -6) \, | 8 \\
&\iff 3 \, | 8
\end{aligned}
$$

Como 3 no divide a 8, la ecuación diofántica, $3x - 6y = 8$ no tiene solución en $\mathbb{Z}$ y, consecuentemente, la ecuación propuesta tampoco la tiene en $\mathbb{Z}_6$.

(e) $12x = 45$ en $\mathbb{Z}_3$.

Obsérvese que

$$12 = 0 \text{ en } \mathbb{Z}_3 \text{ y } 45 = 0 \text{ en } \mathbb{Z}_3$$

luego,

$$\begin{aligned} 12x = 45 \text{ en } \mathbb{Z}_3 &\iff 0 \cdot x = 0 \text{ en } \mathbb{Z}_3 \\ &\iff x \text{ es cualquiera de } \mathbb{Z}_3 \\ &\iff \begin{cases} x = 0 \text{ en } \mathbb{Z}_3 \\ \text{ó} \\ x = 1 \text{ en } \mathbb{Z}_3 \\ \text{ó} \\ x = 2 \text{ en } \mathbb{Z}_3 \end{cases} \end{aligned}$$

■

En el siguiente apartado, estableceremos el *Teorema Chino del resto*, resultado que aparece en los más importantes manuscritos chinos de la antigüedad, como en los trabajos de Sun Tsu en el siglo I. También, y en esa misma época, es conocido por el neopitagórico Nicómaco.[1]

16.5.2 Teorema Chino del Resto

Si $m_1, m_2, \cdots, m_k$ son enteros positivos primos entre sí dos a dos, entonces el sistema de ecuaciones,

$$\begin{aligned} x &= a_1 \ \textit{en}\ \mathbb{Z}_{m_1} \\ x &= a_2 \ \textit{en}\ \mathbb{Z}_{m_2} \\ &\cdots\cdots\cdots\cdots \\ x &= a_k \ \textit{en}\ \mathbb{Z}_{m_k} \end{aligned}$$

tiene solución única en $\mathbb{Z}_{m_1 \cdot m_2 \cdots m_k}$.

Demostración

Primero obtendremos una solución, probando así su existencia, y luego demostraremos que es única.

En efecto, sea x una combinación lineal con coeficientes enteros de las soluciones a_i en $\mathbb{Z}_{m_i}$ para cada $i = 1, 2, \cdots, k$, es decir,

$$x = c_1 a_1 + c_2 a_2 + \cdots + c_k a_k \tag{16.3}$$

Si ahora elegimos los coeficientes c_i $(1 \leqslant i \leqslant k)$ de tal manera que

$$\begin{aligned} &c_i = 1 \text{ en } \mathbb{Z}_{m_i} \\ &\text{y} \\ &c_i = 0 \text{ en } \mathbb{Z}_{m_j}, \text{ para } j \neq i \end{aligned}$$

[1] Vivió cerca de Jerusalén alrededor del año 100. Parece ser que tenía ascendencia siria, pero lo cierto es que en su obra predominan las tendencias filosóficas griegas. Es autor de la *Introductio Aritmeticae* de la que nos han llegado sólo dos libros, pero es posible que ésta sea solamente una versión abreviada de un tratado originalmente más extenso. Esta obra comienza con la ya veterana clasificación pitagórica de los números pares e impares, siguen las definiciones de los números primos, compuestos y perfectos, incluyendo una descripción de la criba de Eratóstenes y una lista de los cuatro primeros números perfectos (6,28, 496 y 8128). La obra incluye también una clasificación de las razones y de las combinaciones de razones (puesto que las razones entre enteros son esenciales para la teoría pitagórica de los intervalos musicales), un amplio tratamiento del tema favorito de la aritmética pitagórica, los números figurados en dos y tres dimensiones, y una exposición exhaustiva de los diversos tipos de medias (de nuevo un tema favorito de la matemática y de la filosofía pitagóricas). Como tantos otros escritores, Nicómaco considera al 3 como el primer número en el estricto sentido de la palabra, ya que 1 y 2 no eran en realidad números, sino sólo los generadores de la sucesión numérica, y además, para Nicómaco los números estaban dotados de cualidades tales como mejor o peor, más joven o más viejo, etc..., y podían transmitir estos caracteres, como los padres a sus hijos. La *Introductio* no tenía la intención de ser un tratado de cálculo ni de álgebra, sino un manual conteniendo aquellos elementos de la matemática que resultaban esenciales para entender la filosofía pitagórica y platónica, y en este sentido sirvió como modelo para muchos imitadores y comentadores posteriores.

tendremos que

$$\left.\begin{array}{l} c_1 = 1 \text{ en } \mathbb{Z}_{m_1} \\ \text{y} \\ c_1 = 0 \text{ en } \mathbb{Z}_{m_j}, \text{ para } j \neq 1 \end{array}\right\} \implies x = a_1 \text{ en } \mathbb{Z}_{m_1}$$

$$\left.\begin{array}{l} c_2 = 1 \text{ en } \mathbb{Z}_{m_2} \\ \text{y} \\ c_2 = 0 \text{ en } \mathbb{Z}_{m_j}, \text{ para } j \neq 2 \end{array}\right\} \implies x = a_2 \text{ en } \mathbb{Z}_{m_2}$$

$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \quad \ldots\ldots \quad \ldots\ldots\ldots\ldots$$

$$\left.\begin{array}{l} c_k = 1 \text{ en } \mathbb{Z}_{m_k} \\ \text{y} \\ c_k = 0 \text{ en } \mathbb{Z}_{m_j}, \text{ para } j \neq k \end{array}\right\} \implies x = a_k \text{ en } \mathbb{Z}_{m_k}$$

luego la x dada por la expresión (16.3) sería solución simultánea de todas las ecuaciones propuestas. Centremos, pues, nuestra atención en obtener estos coeficientes.

Empecemos por c_1. Por hipótesis los m_i son primos entre sí dos a dos, es decir,

$$\text{m.c.d.}(m_i, m_j) = 1, \ \forall i \neq j, \ 1 \leqslant i, j \leqslant k$$

Entonces, aplicando reiteradamente el ejercicio 13.24

$$\left.\begin{array}{r} \text{m.c.d.}(m_2, m_1) = 1 \\ \text{m.c.d.}(m_3, m_1) = 1 \end{array}\right\} \implies \text{m.c.d.}(m_2 m_3, m_1) = 1$$

y

$$\left.\begin{array}{r} \text{m.c.d.}(m_2 m_3, m_1) = 1 \\ \text{m.c.d.}(m_4, m_1) = 1 \end{array}\right\} \implies \text{m.c.d.}(m_2 m_3 m_4, m_1) = 1$$

y así sucesivamente, llegaríamos a que

$$\text{m.c.d.}(m_2 m_3 \cdots m_k, m_1) = 1$$

y haciendo $m_2 m_3 \cdots m_k = t_1$,

$$\text{m.c.d.}(t_1, m_1) = 1$$

luego t_1 es invertible en $\mathbb{Z}_{m_1}$, es decir existe $y_1 \in \mathbb{Z}_{m_1}$ tal que

$$t_1 y_1 = 1 \text{ en } \mathbb{Z}_{m_1}.$$

Además, $t_1 y_1$ es múltiplo de todos los m_j para $j \neq 1$ luego

$$t_1 = 0 \text{ en } \mathbb{Z}_{m_j} \text{ para } j \neq 1, \ (2 \leqslant j \leqslant k).$$

Si procedemos de forma idéntica para $c_j, \ j = 2, 3, \cdots, k$, tendremos que

$$t_j y_j = 1 \text{ en } \mathbb{Z}_{m_j}, \text{ para } j = 2, 3, \cdots, k$$

y

$$t_j = 0 \text{ en } \mathbb{Z}_{m_i}, \text{ para } i \neq j$$

Así pues, si tomamos

$$c_i = t_i y_i, \ 1 \leqslant i \leqslant k$$

y sustituimos en (16.3), nos queda

$$x = t_1 y_1 a_1 + t_2 y_2 a_2 + \cdots + t_k y_k a_k$$

que es una solución de todas las ecuaciones propuestas.

Veamos ahora que esta solución es única en $\mathbb{Z}_{m_1 m_2 \cdots m_k}$. En efecto, supongamos que no lo es, es decir que existe otra solución x', distinta de la x, en $\mathbb{Z}_{m_1 m_2 \cdots m_k}$ del sistema de ecuaciones propuesto. Entonces, como x es única en $\mathbb{Z}_{m_i}$, tendremos

$$x = x' \text{ en } \mathbb{Z}_{m_i},\ i = 1, 2, \cdots, k$$

o sea,

$$m_i | x - x',\ i = 1, 2, \cdots, k.$$

Pues bien,

$$\left.\begin{array}{c} m_1 | x - x' \\ \text{y} \\ m_2 | x - x' \end{array}\right\} \Longrightarrow \text{m.c.m.}(m_1, m_2) | x - x' \overset{\text{m.c.d.}_{(m_1,m_2)=1}}{\Longrightarrow} m_1 m_2 | x - x'$$

y

$$\left.\begin{array}{c} m_1 m_2 | x - x' \\ \text{y} \\ m_3 | x - x' \end{array}\right\} \Longrightarrow \text{m.c.m.}(m_1 m_2, m_3) | x - x' \overset{\text{m.c.d.}_{(m_1 m_2, m_3)=1}}{\Longrightarrow} m_1 m_2 m_3 | x - x'$$

y

$$\left.\begin{array}{c} m_1 m_2 m_3 | x - x' \\ \text{y} \\ m_4 | x - x' \end{array}\right\} \Longrightarrow \text{m.c.m.}(m_1 m_2 m_3, m_4) | x - x' \overset{\text{m.c.d.}_{(m_1 m_2 m_3, m_4)=1}}{\Longrightarrow} m_1 m_2 m_3 m_4 | x - x'$$

y así sucesivamente, llegaríamos a que

$$m_1 m_2 \cdots m_k | x - x'$$

es decir,

$$x = x' \text{ en } \mathbb{Z}_{m_1 m_2 \cdots m_k}$$

y la solución que hemos construido es, por tanto, única.

■

El siguiente ejemplo se debe a Sun Tsu.

Ejemplo 16.23

Encontrar el menor número entero positivo que dividido por 3 *da como resto* 2*, dividido por* 5 *da resto* 3 *y dividido por* 7 *da resto* 2*.*

Solución

Sea x el número buscado. Por el teorema de existencia y unicidad de cociente y resto, existirán q_1, q_2 y q_3, enteros, tales que $x = 3q_1 + 2$ y $x = 5q_2 + 3$ y $x = 7q_3 + 2$. Entonces,

$$\left.\begin{array}{l} x = 3q_1 + 2 \\ \text{y} \\ x = 5q_2 + 3 \\ \text{y} \\ x = 7q_3 + 2 \end{array}\right\} \iff \left\{\begin{array}{l} x - 2 = 3q_1 \\ \text{y} \\ x - 3 = 5q_2 \\ \text{y} \\ x - 2 = 7q_3 \end{array}\right.$$

$$\iff \left\{\begin{array}{l} 3 \,|\, x - 2 \\ \text{y} \\ 5 \,|\, x - 3 \\ \text{y} \\ 7 \,|\, x - 2 \end{array}\right.$$

$$\iff \left\{\begin{array}{l} x \equiv 2 \,(\text{mód } 3) \\ \text{y} \\ x \equiv 3 \,(\text{mód } 5) \\ \text{y} \\ x \equiv 2 \,(\text{mód } 7) \end{array}\right.$$

$$\iff \left\{\begin{array}{l} x = 2 \text{ en } \mathbb{Z}_3 \\ \text{y} \\ x = 3 \text{ en } \mathbb{Z}_5 \\ \text{y} \\ x = 2 \text{ en } \mathbb{Z}_7 \end{array}\right.$$

Tendremos que encontrar, pues, un número que satisfaga este sistema de ecuaciones.

Los números 3, 5 y 7 son primos entre sí dos a dos, luego podremos aplicar el *teorema chino del resto*, (16.5.2), y encontrar una única solución en $\mathbb{Z}_{3\cdot 5\cdot 7} = \mathbb{Z}_{105}$. En efecto,

$$\left.\begin{array}{l} \text{m.c.d.}(5,3) = 1 \\ \text{y} \\ \text{m.c.d.}(7,3) = 1 \end{array}\right\} \implies \text{m.c.d.}(5 \cdot 7, 3) = 1 \text{ (13.24)}$$

$$\implies \text{m.c.d.}(35, 3) = 1$$

$$\iff 35 \text{ es invertible en } \mathbb{Z}_3 \text{ (16.4.8)}$$

$$\iff \exists y_1 \in \mathbb{Z}_3 : 35y_1 = 1$$

siendo,

$$\begin{array}{l} 35 \text{ es múltiplo de } 5 \implies 35 = 0 \text{ en } \mathbb{Z}_5 \\ \text{y} \\ 35 \text{ es múltiplo de } 7 \implies 35 = 0 \text{ en } \mathbb{Z}_7 \end{array}$$

Análogamente,

$$\left.\begin{array}{l} \text{m.c.d.}(3,5) = 1 \\ \text{y} \\ \text{m.c.d.}(7,5) = 1 \end{array}\right\} \implies \text{m.c.d.}(3 \cdot 7, 5) = 1 \text{ (13.24)}$$

$$\implies \text{m.c.d.}(21, 5) = 1$$

$$\iff 21 \text{ es invertible en } \mathbb{Z}_5 \text{ (16.4.8)}$$

$$\iff \exists y_2 \in \mathbb{Z}_5 : 21y_2 = 1$$

siendo,

$$\begin{array}{l} 21 \text{ es múltiplo de } 3 \implies 21 = 0 \text{ en } \mathbb{Z}_3 \\ \text{y} \\ 21 \text{ es múltiplo de } 7 \implies 21 = 0 \text{ en } \mathbb{Z}_7 \end{array}$$

y

$$\left.\begin{array}{l}\text{m.c.d.}(3,7)=1\\ \text{y}\\ \text{m.c.d.}(5,7)=1\end{array}\right\} \begin{array}{ll}\Longrightarrow & \text{m.c.d.}(3\cdot 5,7)=1 \text{ (13.24)}\\ \Longrightarrow & \text{m.c.d.}(15,7)=1\\ \Longleftrightarrow & 15 \text{ es invertible en } \mathbb{Z}_7 \text{ (16.4.8)}\\ \Longleftrightarrow & \exists y_3\in\mathbb{Z}_7 : 15y_3=1\end{array}$$

siendo,

$$\begin{array}{l}15 \text{ es múltiplo de } 3 \implies 15=0 \text{ en } \mathbb{Z}_3\\ \text{y}\\ 15 \text{ es múltiplo de } 5 \implies 15=0 \text{ en } \mathbb{Z}_5\end{array}$$

luego,

$$x=35y_1\cdot 2+21y_2\cdot 3+15y_3\cdot 2 \implies \left\{\begin{array}{l}x=2 \text{ en } \mathbb{Z}_3\\ \text{y}\\ x=3 \text{ en } \mathbb{Z}_5\\ \text{y}\\ x=2 \text{ en } \mathbb{Z}_7\end{array}\right.$$

Aplicamos el teorema anterior y,

$$x=35y_1\cdot 2+21y_2\cdot 3+15y_3\cdot 2=70y_1+63y_2+30y_3$$

es la solución única del sistema propuesto en $\mathbb{Z}_{3\cdot 5\cdot 7}=\mathbb{Z}_{105}$, siendo y_1, y_2 e y_3 los inversos de 35, 21 y 15 en $\mathbb{Z}_3$, $\mathbb{Z}_5$ y $\mathbb{Z}_7$, respectivamente. Calculémoslos,

- Inverso de 35 en $\mathbb{Z}_3$.

$$\left.\begin{array}{l}y_1 \text{ es el inverso de } 35 \text{ en } \mathbb{Z}_3\\ \text{y}\\ 35\equiv 2(\text{mód } 3)\Longleftrightarrow 35=2 \text{ en } \mathbb{Z}_3\end{array}\right\} \begin{array}{ll}\Longrightarrow & y_1 \text{ es el inverso de } 2 \text{ en } \mathbb{Z}_3\\ \Longleftrightarrow & 2y_1=1 \text{ en } \mathbb{Z}_3\\ \Longrightarrow & y_1=2 \text{ en } \mathbb{Z}_3\end{array}$$

- Inverso de 21 en $\mathbb{Z}_5$.

$$\left.\begin{array}{l}y_2 \text{ es el inverso de } 21 \text{ en } \mathbb{Z}_5\\ \text{y}\\ 21\equiv 1(\text{mód } 5)\Longleftrightarrow 21=1 \text{ en } \mathbb{Z}_5\end{array}\right\} \Longrightarrow y_2 \text{ es el inverso de } 1 \text{ en } \mathbb{Z}_5 \Longleftrightarrow y_2=1 \text{ en } \mathbb{Z}_5$$

- Inverso de 15 en $\mathbb{Z}_7$.

$$\left.\begin{array}{l}y_3 \text{ es el inverso de } 15 \text{ en } \mathbb{Z}_7\\ \text{y}\\ 15\equiv 1(\text{mód } 7)\Longleftrightarrow 15=1 \text{ en } \mathbb{Z}_7\end{array}\right\} \Longrightarrow y_3 \text{ es el inverso de } 1 \text{ en } \mathbb{Z}_7 \Longleftrightarrow y_3=1 \text{ en } \mathbb{Z}_7$$

Por lo tanto, la solución es:

$$x=70\cdot 2+63\cdot 1+30\cdot 1=233 \text{ en } \mathbb{Z}_{105}.$$

Entonces,

$$\begin{array}{lll}x=233 \text{ en } \mathbb{Z}_5 & \Longleftrightarrow & x\equiv 233(\text{mód } 105) \text{ en } \mathbb{Z}\\ & \Longleftrightarrow & 105\,|x-233 \text{ en } \mathbb{Z}\\ & \Longleftrightarrow & \exists q\in\mathbb{Z} : x-233=105q\\ & \Longleftrightarrow & \exists q\in\mathbb{Z} : x=105q+233.\end{array}$$

Ahora bien, como $x > 0$, tendremos

$$x > 0 \Longrightarrow 105q + 233 > 0 \Longrightarrow q > \frac{-233}{105} \Longrightarrow q > -2,22 \Longrightarrow q \geqslant -2$$

y, por lo tanto, el menor entero positivo se obtendrá para $q = -2$, es decir,

$$\left.\begin{array}{l} x = 105q + 233 \\ \text{y} \\ q = -2 \end{array}\right\} \implies x = 105(-2) + 233 \implies x = 23$$

o lo que es igual "el menor número entero positivo que dividido por 3 da como resto 2, dividido por 5 da resto 3 y dividido por 7 da resto 2 es el 23".

■

Ejemplo 16.24

Encontrar el menor entero positivo cuyos restos al dividirlo por 3, 4, 5 *y* 6 *sean, respectivamente,* 2, 3, 4 *y* 5. *(Brahmagupta*[2]*).*

Solución

Sea x el número buscado. Por el teorema de existencia y unicidad de cociente y resto, existirán q_1, q_2, q_3 y

[2]Matemático hindú del siglo VII. Es autor del *Brahma-Sphuta-Siddanta*, obra de astronomía. Los siete capítulos del XII al XVIII, tratan de matemáticas. Aparentemente, fue el primero que dio una solución general de la ecuación diofántica lineal $ax + by = c$, con a, b y c enteros. Para que esta ecuación tenga soluciones enteras, el máximo común divisor de a y b debe dividir a c, y Brahmagupta sabía que si a y b son primos entre sí, entonces todas las soluciones de la ecuación vienen dadas por las fórmulas $x = p + mb$, $y = q - ma$, donde m es un entero arbitrario. Brahmagupta estudió también la ecuación diofántica cuatrática $x^2 + 1 + py^2$, que recibe erróneamente el nombre de John Pell (1611-1685) y que apareció por primera vez en el problema de los bueyes de Arquímedes. Esta ecuación de Pell fue resuelta en algunos casos particulares por el matemático Bhaskara (1114-1185), hindú como Brahmagupta. Es muy notable el mérito de Brahmagupta al dar todas las soluciones enteras de la ecuación diofántica lineal, mientras que Diofanto se había contentado con dar una única solución particular de una ecuación indeterminada. Dado que Brahmagupta utiliza en algunos casos los mismos ejemplos que Diofanto, podemos ver de nuevo reforzada la evidencia de una influencia griega en la India, o bien la posibilidad de que ambos hicieran uso de una fuente común, verosímilmente de la antigua Babilonia.

q_4, enteros, tales que $x = 3q_1 + 2$ y $x = 4q_2 + 3$ y $x = 5q_3 + 4$ y $x = 6q_4 + 5$. Entonces,

$$\left.\begin{array}{l} x = 3q_1 + 2 \\ \text{y} \\ x = 4q_2 + 3 \\ \text{y} \\ x = 5q_3 + 4 \\ \text{y} \\ x = 6q_4 + 5 \end{array}\right\} \iff \left\{\begin{array}{l} x - 2 = 3q_1 \\ \text{y} \\ x - 3 = 4q_2 \\ \text{y} \\ x - 4 = 5q_3 \\ \text{y} \\ x - 5 = 6q_4 \end{array}\right.$$

$$\iff \left\{\begin{array}{l} 3 \,|\, x - 2 \\ \text{y} \\ 4 \,|\, x - 3 \\ \text{y} \\ 5 \,|\, x - 4 \\ \text{y} \\ 6 \,|\, x - 5 \end{array}\right.$$

$$\iff \left\{\begin{array}{l} x \equiv 2 \,(\text{mód } 3) \\ \text{y} \\ x \equiv 3 \,(\text{mód } 4) \\ \text{y} \\ x \equiv 4 \,(\text{mód } 5) \\ \text{y} \\ x \equiv 5 \,(\text{mód } 6) \end{array}\right.$$

$$\iff \left\{\begin{array}{l} x = 2 \text{ en } \mathbb{Z}_3 \\ \text{y} \\ x = 3 \text{ en } \mathbb{Z}_4 \\ \text{y} \\ x = 4 \text{ en } \mathbb{Z}_5 \\ \text{y} \\ x = 5 \text{ en } \mathbb{Z}_6 \end{array}\right.$$

Buscaremos, pues, x, que satisfaga este sistema de ecuaciones.

Obsérvese que 3 es primo con 4 y con 5 pero no con 6 y lo mismo le sucede al 4, además 5 es primo con 6, luego podemos aplicar el *teorema Chino del resto* (16.5.2) a las tres primeras ecuaciones y calcular una solución única en $\mathbb{Z}_{3\cdot 4\cdot 5} = \mathbb{Z}_{60}$. En efecto,

$$\left.\begin{array}{l} \text{m.c.d.}(4,3) = 1 \\ \text{y} \\ \text{m.c.d.}(5,3) = 1 \end{array}\right\} \implies \text{m.c.d.}(4 \cdot 5, 3) = 1 \text{ (13.24)}$$

$$\implies \text{m.c.d.}(20, 3) = 1$$

$$\iff 20 \text{ es invertible en } \mathbb{Z}_3 \text{ (16.4.8)}$$

$$\iff \exists y_1 \in \mathbb{Z}_3 : 20y_1 = 1$$

siendo,

$$\begin{array}{l} 20 \text{ es múltiplo de } 4 \implies 20 = 0 \text{ en } \mathbb{Z}_4 \\ \text{y} \\ 20 \text{ es múltiplo de } 5 \implies 20 = 0 \text{ en } \mathbb{Z}_5. \end{array}$$

Análogamente,

$$\left.\begin{array}{l}\text{m.c.d.}(3,4)=1\\ \text{y}\\ \text{m.c.d.}(5,4)=1\end{array}\right\} \Longrightarrow \text{m.c.d.}(3\cdot 5,4)=1 \text{ (13.24)}$$
$$\Longrightarrow \text{m.c.d.}(15,4)=1$$
$$\Longleftrightarrow 15 \text{ es invertible en } \mathbb{Z}_4 \text{ (16.4.8)}$$
$$\Longleftrightarrow \exists y_2\in\mathbb{Z}_4 : 15y_2=1$$

siendo,

$$\begin{array}{l}15 \text{ es múltiplo de } 3 \Longrightarrow 15=0 \text{ en } \mathbb{Z}_3\\ \text{y}\\ 15 \text{ es múltiplo de } 5 \Longrightarrow 15=0 \text{ en } \mathbb{Z}_5\end{array}$$

y también,

$$\left.\begin{array}{l}\text{m.c.d.}(3,5)=1\\ \text{y}\\ \text{m.c.d.}(4,5)=1\end{array}\right\} \Longrightarrow \text{m.c.d.}(3\cdot 4,5)=1 \text{ (13.24)}$$
$$\Longrightarrow \text{m.c.d.}(12,5)=1$$
$$\Longleftrightarrow 12 \text{ es invertible en } \mathbb{Z}_5 \text{ (16.4.8)}$$
$$\Longleftrightarrow \exists y_3\in\mathbb{Z}_5 : 12y_3=1$$

siendo,

$$\begin{array}{l}12 \text{ es múltiplo de } 3 \Longrightarrow 12=0 \text{ en } \mathbb{Z}_3\\ \text{y}\\ 12 \text{ es múltiplo de } 4 \Longrightarrow 12=0 \text{ en } \mathbb{Z}_4.\end{array}$$

Entonces, si

$$x=20y_1\cdot 2+15y_2\cdot 3+12y_3\cdot 4 \text{ en } \mathbb{Z}_{60}$$

tendremos que

$$\begin{array}{l}x=2 \text{ en } \mathbb{Z}_3\\ \text{y}\\ x=3 \text{ en } \mathbb{Z}_4\\ \text{y}\\ x=4 \text{ en } \mathbb{Z}_5\end{array}$$

es decir, es solución de las tres primeras ecuaciones y solo nos faltará calcular y_1, y_2 e y_3. Pues bien,

- Inverso de 20 en $\mathbb{Z}_3$.

$$\left.\begin{array}{l}y_1 \text{ es el inverso de } 20 \text{ en } \mathbb{Z}_3\\ \text{y}\\ 20\equiv 2(\text{mód } 3)\Longleftrightarrow 20=2 \text{ en } \mathbb{Z}_3\end{array}\right\} \Longrightarrow y_1 \text{ es el inverso de } 2 \text{ en } \mathbb{Z}_3$$
$$\Longleftrightarrow 2y_1=1 \text{ en } \mathbb{Z}_3$$
$$\Longrightarrow y_1=2 \text{ en } \mathbb{Z}_3$$

- Inverso de 15 en $\mathbb{Z}_4$.

$$\left.\begin{array}{l}y_2 \text{ es el inverso de } 15 \text{ en } \mathbb{Z}_4\\ \text{y}\\ 15\equiv 3(\text{mód } 4)\Longleftrightarrow 15=3 \text{ en } \mathbb{Z}_4\end{array}\right\} \Longrightarrow y_2 \text{ es el inverso de } 3 \text{ en } \mathbb{Z}_4$$
$$\Longleftrightarrow 3y_2=1 \text{ en } \mathbb{Z}_4$$
$$\Longrightarrow y_2=3 \text{ en } \mathbb{Z}_4$$

⁕ Inverso de 12 en $\mathbb{Z}_5$.

$$\left.\begin{array}{l} y_3 \text{ es el inverso de } 12 \text{ en } \mathbb{Z}_5 \\ \text{y} \\ 12 \equiv 2(\text{mód } 5) \Longleftrightarrow 12 = 2 \text{ en } \mathbb{Z}_5 \end{array}\right\} \begin{array}{rl} \Longrightarrow & y_3 \text{ es el inverso de } 2 \text{ en } \mathbb{Z}_5 \\ \Longleftrightarrow & 2y_3 = 1 \text{ en } \mathbb{Z}_5 \\ \Longrightarrow & y_3 = 3 \text{ en } \mathbb{Z}_5 \end{array}$$

La solución es, por tanto,

$$\begin{array}{rcl} x & = & 20y_1 \cdot 2 + 15y_2 \cdot 3 + 12y_3 \cdot 4 \text{ en } \mathbb{Z}_{60} \\ & = & 20 \cdot 2 \cdot 2 + 15 \cdot 3 \cdot 3 + 12 \cdot 3 \cdot 4 \text{ en } \mathbb{Z}_{60} \\ & = & 359 \text{ en } \mathbb{Z}_{60}. \end{array}$$

Entonces,

$$\begin{array}{rcl} x = 359 \text{ en } \mathbb{Z}_{60} & \Longleftrightarrow & x \equiv 359(\text{mód } 60) \text{ en } \mathbb{Z} \\ & \Longleftrightarrow & 60 \,|\, x - 359 \text{ en } \mathbb{Z} \\ & \Longleftrightarrow & \exists q \in \mathbb{Z} : x - 359 = 60q \\ & \Longleftrightarrow & \exists q \in \mathbb{Z} : x = 60q + 359 \end{array}$$

$$\left\{\begin{array}{l} \text{Obsérvese que} \\ x = 60q + 359 \Longleftrightarrow x = 6(10q + 59) + 5 \\ \qquad\qquad\quad \Longleftrightarrow 6 \,|\, x - 5 \\ \qquad\qquad\quad \Longleftrightarrow x \equiv 5(\text{mód } 6) \\ \qquad\qquad\quad \Longleftrightarrow x = 5 \text{ en } \mathbb{Z}_6 \end{array}\right\}$$

El menor entero positivo que cumple las condiciones del enunciado se dará cuando $0 < x < 60$, entonces

$$\begin{array}{rcl} 0 < x < 60 & \Longleftrightarrow & 0 < 60q + 359 < 60 \\ & \Longleftrightarrow & 0 < 60q + 359 < 60 \\ & \Longleftrightarrow & \dfrac{-359}{60} < q < \dfrac{-299}{60} \\ & \Longleftrightarrow & -5,9 < q < -4,9 \\ & \Longleftrightarrow & -5 \leqslant q \leqslant -5 \\ & \Longleftrightarrow & q = -5 \end{array}$$

luego,

$$\left.\begin{array}{l} x = 60q + 359 \\ \text{y} \\ q = -5 \end{array}\right\} \Longrightarrow x = 60(-5) + 359 \Longrightarrow x = 59$$

es decir, 59 es el menor entero positivo cuyos restos al dividirlo por 3, 4, 5 y 6 son, respectivamente, 2, 3, 4 y 5.

■

16.6 Euler, Fermat y Wilson

Estudiaremos en este apartado tres importantes teoremas sobres congruencias. Introduremos previamente la función de Euler[3] que nos permitirá demostrar con facilidad tales teoremas.

[3]Leonhard Euler (Basilea 1707-San Petesburgo 1783), aprendió matemáticas de su padre que había estudiado con Jacques I Bernouilli. Fue enviado a estudiar teología a Basilea, donde siguió el curso de Jacques I Bernouilli, con cuyos hijos le unió una

16.6.1 Función ϕ de Euler

Dado un número entero positivo m, definimos la función $\phi(m)$ como el número de enteros positivos primos con m y que sean menores o iguales que m. Su expresión es

$$\phi(m) = \sum_{0<r\leqslant m} 1$$

siendo $m.c.d.(r, m) = 1$. A $\phi(m)$ la llamaremos función de Euler del número m.

Ejemplo 16.25

Por ejemplo,

$\phi(1) = 1$

$\phi(2) = 1$

$\phi(3) = 2$

$\phi(4) = 2$

$\phi(5) = 4$

$\phi(6) = 2$

$\phi(7) = 6$

$\phi(8) = 4$

■

Nota 16.4 Obsérvese que si p es un número primo, entonces todos los enteros positivos menores que p son primos con p, luego

$$\phi(p) = p - 1$$

■

gran amistad. Cuando éstos fueron llamados a San Petesburgo por Catalina I, Euler los siguió en 1732, y allí sucedió a Daniel Bernouilli en la cátedra de matemáticas. Desgraciadamente, en 1735, una congestión cerebral le hizo perder el ojo derecho, y una ceguera progresiva le afligió durante buena parte de su existencia. En 1736 publicó un tratado completo de mecánica, en el cual aplicó el análisis matemático a la ciencia del movimiento. En 1741 fue invitado a Berlín por Federico II, que en 1744 le nombró director de la clase de matemáticas de la Academia de Berlín. En esta época construyó su *Teoría de los isoperímetros*, que permite determinar las curvas o las superficies para las cuales ciertas funciones indefinidas son mayores o menores que para todas las otras. Este problema sólo había recibido antes soluciones parciales. Euler desarrolló el método contenido en estas soluciones parciales y lo definió en fórmula general. También publicó *Teoría del movimiento de los planetas y de los cometas y Teoría de la imantación*, y resolvió para el rey de Prusia los principales problemas de balística. Con todo, sus dos grandes obras de análisis son *Introducción al análisis de los infinitésimos (1748)* e *Instituciones del cálculo diferencial (1755)*, que han sido clásicas durante mucho tiempo. Regresó a San Petesburgo en 1766, perdió el ojo que le quedaba, a pesar de lo cual siguió trabajando. De 1768 a 1770 aparecieron sus *Instituciones del cálculo integral*. Aunque una operación de cataratas le devolvió parcialmente al vista, su curación no fue completa. Murió de un ataque de apoplejía.

16.6.2 Teorema de Euler

Si a es invertible en $\mathbb{Z}_m$, entonces $a^{\phi(m)} = 1$ en $\mathbb{Z}_m$.

Demostración

Supongamos que en $\mathbb{Z}_m$ hay k elementos invertibles $r_1, r_2, \cdots, r_k$. Entonces, m.c.d.$(r_i, m) = 1,\ 1 \leqslant i \leqslant k$ luego $\phi(m) = k$.

Veremos que $ar_1, ar_2, \cdots, ar_k$ son también k elementos invertibles en $\mathbb{Z}_m$. En efecto,

- ar_i es invertible en $\mathbb{Z}_m$ para $1 \leqslant i \leqslant k$ (supondremos $a \neq 1$ en $\mathbb{Z}_m$ para evitar el caso trivial).
  En efecto,

$$\left.\begin{array}{l} a \text{ es invertible en } \mathbb{Z}_m \Longrightarrow \text{m.c.d.}(a, m) = 1 \\ r_i \text{ es invertible en } \mathbb{Z}_m \Longrightarrow \text{m.c.d.}(r_i, m) = 1 \end{array}\right\} \overset{(13.24)}{\Longrightarrow} \text{m.c.d.}(ar_i, m) = 1 \Longrightarrow ar_i \text{ es invertible en } \mathbb{Z}_m$$

- Probaremos ahora que los $ar_i,\ 1 \leqslant i \leqslant k$ son distintos dos a dos, es decir también hay k elementos invertibles de la forma ar_i.
  En efecto, si $i \neq j$ y, sin embargo, $ar_i = ar_j$, entonces si a^{-1} es el inverso de a, tendremos

$$ar_i = ar_j \Longrightarrow a^{-1}ar_i = a^{-1}ar_j \Longrightarrow r_i = r_j$$

  lo cual es imposible ya que $r_i \neq r_j$.

Veamos ahora que $ar_i = r_j$ con $i \neq j$ en $\mathbb{Z}_m$. En efecto, por el teorema de existencia y unicidad del cociente y resto, existen enteros q_i y r, únicos, tales que

$$ar_i = mq_i + r :\ 0 < r < m.$$

Pues bien, sea $d = \text{m.c.d.}(m, r)$. Entonces

$$\left.\begin{array}{l} d|r \\ \text{y} \\ d\,|m \Longrightarrow d\,|mq_i \end{array}\right\} \Longrightarrow d\,|mq_i m + r \Longrightarrow d\,|ar_i$$

luego

$$\begin{array}{rcl} \left.\begin{array}{l} d|m \\ \text{y} \\ d|ar_i \end{array}\right\} & \Longrightarrow & d|\text{m.c.d.}(m, ar_i) \\ & \Longrightarrow & d|1 \\ & \Longrightarrow & d = 1 \\ & \Longrightarrow & \text{m.c.d.}(m, r) = 1 \\ & \Longrightarrow & r \text{ es invertible en } \mathbb{Z}_m \\ & \Longrightarrow & r = r_j,\ \text{con } j \neq i \end{array}$$

Si ahora multiplicamos miembro a miembro $ar_i = r_k,\ 1 \leqslant i, j \leqslant k$ y reordenamos,

$$ar_1 \cdot ar_2 \cdots ar_k = r_1 \cdot r_2 \cdots r_k \text{ en } \mathbb{Z}_m$$

o sea,

$$a^k r_1 \cdot r_2 \cdots r_k = r_1 \cdot r_2 \cdots r_k \text{ en } \mathbb{Z}_m$$

y como

$$\text{m.c.d.}(r_1 \cdot r_2 \cdots r_k, m) = 1 \text{ (13.24)}$$

resulta que $r_1 \cdot r_2 \cdots r_k$ es invertible. Bastaría multiplicar ambos miembros por su inverso para obtener

$$a^k = 1 \text{ en } \mathbb{Z}_m$$

es decir,

$$a^{\phi(m)} = 1 \text{ en } \mathbb{Z}_m$$

■

El segundo de los teoremas es, en realidad, un corolario al teorema de Euler y se debe a Fermat[4]

16.6.3 Corolario (Fermat)

Si a es invertible en $\mathbb{Z}_p$ con p primo, entonces

$$a^{p-1} = 1 \text{ en } \mathbb{Z}_p$$

Demostración

En efecto, al ser p primo, será $\phi(p) = p - 1$. Aplicamos el teorema de Euler para $m = p$, y

$$a^{p-1} = 1 \text{ en } \mathbb{Z}_p$$

■

Ejemplo 16.26

Encontrar el resto que se obtiene al dividir 23^{2587} entre 7.

Solución

Por el teorema de existencia y unicidad de cociente y resto, existirán q y r, enteros y únicos tales que

$$23^{2587} = 7q + r, \ 0 \leqslant r < 7$$

luego,

$$23^{2587} = r \text{ en } \mathbb{Z}_7.$$

[4]Pierre de Fermat, matemático francés (Beaumont-de-Lomagne 1601-Castres 1665). Fue consejero del parlamento de Tolouse (1631). Pascal le llamó el "primer hombre del mundo" y on siempre pudo seguirle en sus investigaciones. Fermat que rara vez publicaba sus descubrimientos, e incluso olvidaba anotar las demostraciones matemáticas que iba encontrando, por lo que gran número de sus trabajos se han perdido. D'Alambert, Lagrange y Laplace le concedieron el honor de haber tenido la primera idea sobre el cálculo diferencial. Desde 1636, las cartas de Fermat prueban que ya representaba las curvas mediante ecuaciones, antes de la publicación de la geometría de Descartes. Asimismo, es opinión de Laplace que Fermat debía compartir con Pascal el honor de haber inventado el cálculo de probabilidades. Sus principales escritos fueron publicados por su hijo Samuel (1679), con el título de *Varia opera mathematica*. En ellos se encuentran enunciados varios principios y teoremas que en la actualidad son conocidos y estudiados.

Bastará, pues, con resolver esta ecuación.

Como m.c.d.$(23, 7) = 1$, 23 es invertible en $\mathbb{Z}_7$, además 7 es primo luego por el teorema de Fermat,

$$23^6 = 1 \text{ en } \mathbb{Z}_7.$$

Por otra parte,

$$2587 = 6 \cdot 431 + 1$$

luego,

$$23^{2587} = \left(23^6\right)^{431} \cdot 23.$$

Entonces,

$$\left.\begin{array}{l} 23^6 = 1 \text{ en } \mathbb{Z}_7 \Longrightarrow \left(23^6\right)^{431} = 1 \text{ en } \mathbb{Z}_7 \\ 23 = 2 \text{ en } \mathbb{Z}_7 \end{array}\right\} \Longrightarrow \left(23^6\right)^{431} \cdot 23 = 2 \text{ en } \mathbb{Z}_7 \Longrightarrow 23^{2587} = 2 \text{ en } \mathbb{Z}_7$$

es decir el resto buscado es 2.

■

Ejemplo 16.27

Calcular el resto de dividir 3^{47} *entre* 23.

Solución

Al igual que en el ejercicio anterior, el teorema de existencia y unicidad de cociente y resto asegura la existencia de dos enteros, q y r, únicos tales que

$$3^{47} = 23q + r,\ 0 \leqslant r < 23$$

y esto es lo mismo que decir que

$$3^{47} = r \text{ en } \mathbb{Z}_{23}.$$

Pues bien, como 3 y 23 son primos entre sí, 3 es invertible y además 23 es primo, luego por el teorema de Fermat,

$$3^{22} = 1 \text{ en } \mathbb{Z}_{23}.$$

Por otra parte,

$$47 = 22 \cdot 2 + 3$$

luego

$$3^{47} = \left(3^{22}\right) \cdot 3^3$$

y

$$\left.\begin{array}{l} 3^{22} = 1 \text{ en } \mathbb{Z}_{23} \Longrightarrow \left(3^{22}\right)^2 = 1 \text{ en } \mathbb{Z}_{23} \\ 3^3 = 4 \text{ en } \mathbb{Z}_{23} \end{array}\right\} \Longrightarrow \left(3^{22}\right)^2 \cdot 3^3 = 1 \cdot 4 \text{ en } \mathbb{Z}_{23} \Longrightarrow 3^{47} = 4 \text{ en } \mathbb{Z}_{23}$$

y, consecuentemente, el resto pedido es 4

■

Ejemplo 16.28

Demostrar que el número $\left(27^4\right)^9 - \left(25^3\right)^6$ *es divisible por* 37.

Solución

Probaremos que

$$\left(27^4\right)^9 - \left(25^3\right)^6 = 0 \text{ en } \mathbb{Z}_{37}$$

En efecto,

$$\left(27^4\right)^9 - \left(25^3\right)^6 = 27^{36} - 5^{36}$$

y al ser 37 un número primo, 27 y 5 serán primos con él, luego ambos son invertibles en $\mathbb{Z}_{37}$. Aplicando el teorema de Fermat,

$$\left.\begin{array}{l} 27^{36} = 1 \text{ en } \mathbb{Z}_{37} \\ 5^{36} = 1 \text{ en } \mathbb{Z}_{37} \end{array}\right\} \Longrightarrow 27^{36} - 5^{36} = 0 \text{ en } \mathbb{Z}_{37} \Longrightarrow \left(27^4\right)^9 - \left(25^3\right)^6 = 0 \text{ en } \mathbb{Z}_{37}$$

es decir el número propuesto es divisible por 37

■

Ejemplo 16.29

Demostrar:

(a) Si $a = b$ *en* $\mathbb{Z}_{m_i}$ $1 \leqslant i \leqslant k$, *entonces* $a = b$ *en* $\mathbb{Z}_{m.c.m.(m_1, m_2, \ldots, m_k)}$

(b) $2^{132} - 1$ *es divisible por* $3 \cdot 13 \cdot 23$

Solución

(a) Si $a = b$ en $\mathbb{Z}_{m_i}$ $1 \leqslant i \leqslant k$, entonces $a = b$ en $\mathbb{Z}_{\text{m.c.m.}(m_1, m_2, \ldots, m_k)}$
En efecto,

$$\begin{array}{rcl} a = b \text{ en } \mathbb{Z}_{m_i},\ i = 1, 2, \ldots, k & \Longleftrightarrow & a - b = 0 \text{ en } \mathbb{Z}_{m_i},\ i = 1, 2, \ldots, k \\ & \Longleftrightarrow & m_i \,|a - b\ ,\ i = 1, 2, \ldots, k \\ & \Longrightarrow & \text{m.c.m.}\,(m_1, m_2, \ldots, m_k)\,|a - b \\ & \Longleftrightarrow & a - b = 0 \text{ en } \mathbb{Z}_{\text{m.c.m.}(m_1, m_2, \ldots, m_k)} \\ & \Longleftrightarrow & a = b \text{ en } \mathbb{Z}_{\text{m.c.m.}(m_1, m_2, \ldots, m_k)} \end{array}$$

(b) $2^{132} - 1$ es divisible por $3 \cdot 13 \cdot 23$
Probaremos que

$$2^{132} - 1 = 0 \text{ en } \mathbb{Z}_{3 \cdot 13 \cdot 23}$$

En efecto, como 3, 13 y 23 son primos, 2 es invertible en $\mathbb{Z}_3$, $\mathbb{Z}_{13}$ y $\mathbb{Z}_{23}$, luego por el teorema de Fermat,

$$2^2 = 1 \text{ en } \mathbb{Z}_3$$

$$2^{12} = 1 \text{ en } \mathbb{Z}_{13}$$

$$2^{22} = 1 \text{ en } \mathbb{Z}_{23}$$

y

$$2^2 = 1 \text{ en } \mathbb{Z}_3 \implies \left(2^2\right)^{66} = 1 \text{ en } \mathbb{Z}_3 \implies 2^{132} = 1 \text{ en } \mathbb{Z}_3$$
$$2^{12} = 1 \text{ en } \mathbb{Z}_{13} \implies \left(2^{12}\right)^{11} = 1 \text{ en } \mathbb{Z}_{13} \implies 2^{132} = 1 \text{ en } \mathbb{Z}_{13}$$
$$2^{22} = 1 \text{ en } \mathbb{Z}_{23} \implies \left(2^{22}\right)^{6} = 1 \text{ en } \mathbb{Z}_{23} \implies 2^{132} = 1 \text{ en } \mathbb{Z}_{23}$$

Aplicando el apartado (a)

$$2^{132} = 1 \text{ en } \mathbb{Z}_{\text{m.c.m.}(3,13,23)}$$

y como m.c.m. $(3, 13, 23) = 3 \cdot 13 \cdot 23$, resulta

$$2^{132} = 1 \text{ en } \mathbb{Z}_{3\cdot 13\cdot 23}$$

es decir,

$$2^{132} - 1 = 0 \text{ en } \mathbb{Z}_{3\cdot 13\cdot 23}$$

y, consecuentemente, $2^{132} - 1$ es divisible por $3 \cdot 13 \cdot 23$.

■

Ejemplo 16.30

Demostrar que para cualquier entero positivo n, siempre se verifica que $n^{37} - n$ es divisible por 383838. *(Sugerencia:* $383838 = 37 \cdot 19 \cdot 13 \cdot 7 \cdot 3 \cdot 2$*).*

Solución

Sea n cualquiera de $\mathbb{Z}^+$. Por el teorema de existencia y unicidad del cociente y resto, existirán q_1, q_2, q_3, q_4, q_5, q_6 y r_1, r_2, r_3, r_4, r_5, r_6, enteros y únicos tales que

$$n = 37q_1 + r_1,\ 0 \leqslant r_1 < 37$$
$$n = 19q_2 + r_2,\ 0 \leqslant r_2 < 19$$
$$n = 13q_3 + r_3,\ 0 \leqslant r_3 < 13$$
$$n = 7q_4 + r_4,\ 0 \leqslant r_4 < 7$$
$$n = 3q_5 + r_5,\ 0 \leqslant r_5 < 3$$
$$n = 2q_1 + r_6,\ 0 \leqslant r_6 < 2$$

es decir, tales que

$$n = r_1 \text{ en } \mathbb{Z}_{37}$$
$$n = r_2 \text{ en } \mathbb{Z}_{19}$$
$$n = r_3 \text{ en } \mathbb{Z}_{13}$$
$$n = r_4 \text{ en } \mathbb{Z}_{7}$$
$$n = r_5 \text{ en } \mathbb{Z}_{3}$$
$$n = r_6 \text{ en } \mathbb{Z}_{2}$$

Ahora bien, 37, 19, 13, 7, 3 y 2 son primos, luego

$$\text{m.c.d.}(r_1, 37) = 1$$
$$\text{m.c.d.}(r_2, 19) = 1$$
$$\text{m.c.d.}(r_3, 13) = 1$$
$$\text{m.c.d.}(r_4, 7) = 1$$
$$\text{m.c.d.}(r_5, 3) = 1$$
$$\text{m.c.d.}(r_6, 2) = 1$$

es decir, r_1, r_2, r_3, r_4, r_5 y r_6 son invertibles en $\mathbb{Z}_{37}$, $\mathbb{Z}_{19}$, $\mathbb{Z}_{13}$, $\mathbb{Z}_7$, $\mathbb{Z}_3$ y $\mathbb{Z}_2$, respectivamente. Aplicamos el teorema de Fermat, y

$$\begin{aligned}
& r_1^{36} = 1 \text{ en } \mathbb{Z}_{37} \\
r_2^{18} = 1 \text{ en } \mathbb{Z}_{19} \quad &\Longrightarrow \quad r_2^{36} = 1 \text{ en } \mathbb{Z}_{19} \\
r_3^{12} = 1 \text{ en } \mathbb{Z}_{13} \quad &\Longrightarrow \quad r_3^{36} = 1 \text{ en } \mathbb{Z}_{13} \\
r_4^{6} = 1 \text{ en } \mathbb{Z}_{7} \quad &\Longrightarrow \quad r_4^{36} = 1 \text{ en } \mathbb{Z}_{7} \\
r_5^{2} = 1 \text{ en } \mathbb{Z}_{3} \quad &\Longrightarrow \quad r_5^{36} = 1 \text{ en } \mathbb{Z}_{3} \\
r_6 = 1 \text{ en } \mathbb{Z}_{2} \quad &\Longrightarrow \quad r_6^{36} = 1 \text{ en } \mathbb{Z}_{2}
\end{aligned}$$

y

$$\begin{aligned}
n = r_1 \text{ en } \mathbb{Z}_{37} \quad &\Longrightarrow \quad n = r_1 \text{ en } \mathbb{Z}_{37} \\
n = r_2 \text{ en } \mathbb{Z}_{19} \quad &\Longrightarrow \quad n^{36} = r_2^{36} \text{ en } \mathbb{Z}_{19} \\
n = r_3 \text{ en } \mathbb{Z}_{13} \quad &\Longrightarrow \quad n^{36} = r_3^{36} \text{ en } \mathbb{Z}_{13} \\
n = r_4 \text{ en } \mathbb{Z}_{7} \quad &\Longrightarrow \quad n^{36} = r_4^{36} \text{ en } \mathbb{Z}_{7} \\
n = r_5 \text{ en } \mathbb{Z}_{3} \quad &\Longrightarrow \quad n^{36} = r_5^{36} \text{ en } \mathbb{Z}_{3} \\
n = r_6 \text{ en } \mathbb{Z}_{2} \quad &\Longrightarrow \quad n^{36} = r_6^{36} \text{ en } \mathbb{Z}_{2}
\end{aligned}$$

por lo tanto,

$$n^{36} = 1 \text{ en } \mathbb{Z}_{37}$$
$$n^{36} = 1 \text{ en } \mathbb{Z}_{19}$$
$$n^{36} = 1 \text{ en } \mathbb{Z}_{13}$$
$$n^{36} = 1 \text{ en } \mathbb{Z}_{7}$$
$$n^{36} = 1 \text{ en } \mathbb{Z}_{3}$$
$$n^{36} = 1 \text{ en } \mathbb{Z}_{2}$$

de aquí que por el ejercicio anterior,

$$n^{36} = 1 \text{ en } \mathbb{Z}_{\text{m.c.m.}(37,19,13,7,3,2)}$$

es decir,

$$n^{36} = 1 \text{ en } \mathbb{Z}_{37 \cdot 19 \cdot 13 \cdot 7 \cdot 3 \cdot 2}$$

o sea,

$$n^{36} = 1 \text{ en } \mathbb{Z}_{383838}$$

y como

$$n = n \text{ en } \mathbb{Z}_{383838}$$

tendremos que

$$n^{37} = n \text{ en } \mathbb{Z}_{383838}$$

y, consecuentemente,

$$n^{37} - n = 0 \text{ en } \mathbb{Z}_{383838}$$

o lo que es igual

$$n^{37} - n \text{ es divisible por } 383838$$

■

En 1770, el matemático inglés Edward Waring publicó en Meditationes Algebraicae varios teoremas nuevos. Uno de ellos refleja una importante propiedad de los números primos. Lleva el nombre de John Wilson, alumno de Waring.

16.6.4 Teorema de Wilson

Si p es un número primo, entonces $(p-1)! = -1$ en $\mathbb{Z}_p$.

Demostración

Como p es primo, todos los elementos de $\mathbb{Z}_p$, excepto el 0, son invertibles. Además, los únicos elementos de $\mathbb{Z}_p$ que coinciden con sus inversos son 1 y $p-1$. En efecto, sea r cualquiera de $\mathbb{Z}_p$ y sea x su inverso. Entonces,

$$\begin{aligned}
x = r &\iff r \cdot r = 1 \text{ en } \mathbb{Z}_p \\
&\iff r^2 - 1 = 0 \text{ en } \mathbb{Z}_p \\
&\iff (r+1)(r-1) = 0 \text{ en } \mathbb{Z}_p \\
&\iff p|(r+1)(r-1) \\
&\iff p|r+1 \text{ ó } p|r-1 \ \{p \text{ es primo}\} \\
&\iff r+1 = 0 \text{ ó } r-1 = 0 \text{ en } \mathbb{Z}_p \\
&\iff r = -1 \text{ ó } r = 1 \text{ en } \mathbb{Z}_p \\
&\iff r = p-1 \text{ ó } r = 1 \text{ en } \mathbb{Z}_p
\end{aligned}$$

por lo tanto,

$$x \neq r \iff r \neq 1 \text{ y } r \neq p-1 \text{ en } \mathbb{Z}_p$$

es decir,

$$r \in \{2, 3, \ldots, p-2\} \iff x \in \{2, 3, \ldots, p-2\}$$

luego el producto de todos ellos es 1 en $\mathbb{Z}_p$, o sea,

$$2 \cdot 3 \cdots (p-2) = 1 \text{ en } \mathbb{Z}_p$$

y como

$$p - 1 = -1 \text{ en } \mathbb{Z}_p$$

multiplicando ambas igualdades miembro a miembro,

$$2 \cdot 3 \cdots (p-2)(p-1) = 1(-1) \text{ en } \mathbb{Z}_p$$

y, consecuentemente,

$$(p-1)! = -1 \text{ en } \mathbb{Z}_p$$

■

Ejemplo 16.31

Demostrar que $138! + 197^{138}$ *es divisible por* 139.

Solución

Probaremos que $138! + 197^{138} = 0$ en $\mathbb{Z}_{139}$. En efecto, 139 es primo, luego por el teorema de Wilson,

$$(139 - 1)! = -1 \text{ en } \mathbb{Z}_{139}$$

es decir,

$$138! = -1 \text{ en } \mathbb{Z}_{139}$$

Por otra parte, 139 y 197 son primos entre sí, luego por el teorema de Fermat,

$$197^{139-1} = 1 \text{ en } \mathbb{Z}_{139}$$

o sea,

$$197^{138} \text{ en } \mathbb{Z}_{139}$$

y sumando ambos resultados,

$$138! + 197^{138} = 0 \text{ en } \mathbb{Z}_{139}$$

Consecuentemente, $138! + 197^{138}$ es divisible por 139.

■