Apuntes de Matemática Discreta

Francisco José González Gutiérrez

27 de Diciembre de 2019

Contenido

Unidad Temática I

Lógica Matemática y Teoría de Conjuntos

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 enunciado que sea verdadero o falso, 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 gran cantidad de dinero.

♦

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.

♦

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.

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].

♦

1.1.6 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, al menos, 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] *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).

1.2 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 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

♦

1.2.4 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 $p \wedge \neg p$.

♦

1.2.5 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 1.3 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.

♦

1.2.6 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"*.

♦

1.2.7 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.

♦

1.2.8 Proposición bicondicional

Dadas dos proposiciones p y q, a la proposición compuesta

$$\text{“}p \text{ si y sólo si } q\text{”}$$

se le llama “proposición bicondicional” y se nota por

$$p \longleftrightarrow q$$

La interpretación del enunciado es:

$$p \text{ sólo si } q \text{ y } p \text{ si } q$$

o lo que es igual

$$\text{si } p, \text{ entonces } q \text{ y si } q, \text{ entonces } p$$

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 1.4 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 1.5 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, (1.2.5), $p \longrightarrow q$ 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 la proposición condicional "si P, entonces Q", $P \longrightarrow Q$, es una tautología.

♦

Ejemplo 1.15

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

Solución.

Probaremos, de acuerdo con la definición dada en el punto anterior, que el condicional $[p \wedge (p \longrightarrow q)] \longrightarrow q$ es una tautología. Como ya sabemos, una proposición condicional únicamente es falsa cuando la hipótesis sea verdadera y la conclusión falsa. Veamos que esto no puede ocurrir.

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, (1.2.5), q tenga que ser verdadera luego

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

es una tautología 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 $\neg(p \vee q) \longrightarrow \neg p$ es una tautología.

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 luego $\neg(p \vee q) \longrightarrow \neg p$ es una tautología y por la definición (1.3.1) hay implicación lógica, es decir,

$$\neg(p \vee q) \Longrightarrow \neg p$$

y la demostración termina.

♦

Nota 1.6 Ahora podremos entender algo mejor lo que comentábamos en 1. de la nota 1.3. 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"*.

♦

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

1.3.2 Implicaciones lógicas más comunes

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,

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

es una tautología y en consecuencia,

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

verificándose 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, (1.2.5), 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, (1.2.5), R ha de ser verdadera y la conclusión $P \longrightarrow R$, será verdadera independientemente del valor de verdad que tenga P.

En cualquier caso, el condicional,

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

será una tautología 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.

Por lo tanto, el condicional

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

es una tautología y en consecuencia,

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

♦

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 siendo verdadera la hipótesis,

(a) Q sea verdadera.

(b) Q sea falsa.

Solución.

Como la hipótesis es verdadera, por el valor de verdad de la conjunción, $P \longrightarrow Q$ y $Q \longrightarrow R$ han de ser, ambas, verdaderas.

Por otra parte, al ser el condicional $(P \longrightarrow Q) \wedge (Q \longrightarrow R) \longrightarrow (P \longrightarrow R)$ una tautología siendo verdadera la hipótesis, la conclusión, $P \longrightarrow R$ también ha de serlo.

(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, el condicional,

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

es una tautología 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 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 $P \iff Q$.

Entonces, $P \Longrightarrow Q$ y $Q \Longrightarrow P$ y por 1.3.1, tendremos que $P \longrightarrow Q$ y $Q \longrightarrow P$ son, ambas, tautologías y, consecuentemente, $P \longleftrightarrow Q$ también lo será.

♦

1.4.3 Equivalencias lógicas más comunes

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

♦

Ejemplo 1.21

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. $\neg(P \vee Q) \Longrightarrow (\neg P \wedge \neg Q)$.
   En efecto, si $\neg(P \vee Q)$ es verdad, entonces por 1.2.3, $P \vee Q$ es falso, luego por 1.2.2, P y Q serán, ambas, falsas, de aquí que, de nuevo por 1.2.3, $\neg P$ y $\neg Q$ sean, las dos, verdaderas y, consecuentemente, $\neg P \wedge \neg Q$ es verdad (por 1.2.1).
   Por tanto,
   $$\neg(P \vee Q) \longrightarrow (\neg P \wedge \neg Q)$$
   es una tautología y, consecuentemente,
   $$\neg(P \vee Q) \Longrightarrow (\neg P \wedge \neg Q)$$
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 verdaderas luego, por 1.2.3, P y Q tienen de ser, ambas, falsas y por 1.2.2 $P \vee Q$ es falsa de aquí que $\neg(P \vee Q)$ sea verdad.
   Hemos probado que el condicional
   $$(\neg P \wedge \neg Q) \longrightarrow \neg(P \vee Q)$$
   es una tautología y, de nuevo por 1.3.1,
   $$(\neg P \wedge \neg Q) \Longrightarrow \neg(P \vee Q)$$

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, para lo cual probaremos que ambas proposiciones tienen los mismos valores de verdad.

1. 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.
2. 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 y su negación, $\neg(P \vee Q)$, falsa.

Ahora bastaría tener en cuenta 1., 2. y lo dicho en 1.4.2 para concluir que
$$\neg(P \vee Q) \iff (\neg P \wedge \neg Q)$$

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

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

1. Veamos que $\neg(P \wedge Q) \Longrightarrow (\neg P \vee \neg Q)$.
   En efecto, si $\neg(P \wedge Q)$ es verdad, entonces por 1.2.3, $P \wedge Q$ 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 1.2.3, 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).
   Por lo tanto, el condicional,
   $$\neg(P \wedge Q) \longrightarrow (\neg P \vee \neg Q)$$
   es una tautología, y en consecuencia,
   $$\neg(P \wedge Q) \Longrightarrow (\neg P \vee \neg Q)$$
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 al menos una de las dos proposiciones, $\neg P$ o $\neg Q$, han de ser verdad luego, por 1.2.3, 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.
   Hemos probado, nuevamente, que el condicional
   $$(\neg P \vee \neg Q) \longrightarrow \neg(P \wedge Q)$$
   es tautología y, por tanto,
   $$(\neg P \vee \neg Q) \Longrightarrow \neg(P \wedge Q)$$

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. Probaremos que ambas proposiciones tienen los mismos valores de verdad.

1. 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.
2. 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 1.4.2 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 1.4.2 para concluir que
$$\neg(P \wedge Q) \Longleftrightarrow (\neg P \vee \neg Q)$$

♦

Ejemplo 1.22

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 siempre, comprobaremos que el condicional $(P \longrightarrow Q) \longrightarrow (\neg Q \longrightarrow \neg P)$ es una tautología.

  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, $\neg Q \longrightarrow \neg P$ es verdadera,

  o

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

  Por lo tanto el condicional es una tautología y

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

  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

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

  En efecto, si $\neg Q \longrightarrow \neg P$ es verdad, 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,

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

  También podemos comprobar que el condicional es una tautología haciendo 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 1.23

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

Solución.

En efecto,

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

♦

Ejemplo 1.24

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

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

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

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

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

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

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

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

♦♦♦

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 cuando sea una tautología.

♦

Nota 1.7 Obsérvese que esto 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.

Obsérvese, también, que de acuerdo con la definición de implicación lógica, 1.3.1, un razonamiento será válido cuando

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

lo cual significaría, a su vez, que la veracidad de la conclusión, q, se sigue de la veracidad de la hipótesis, $p_1 \wedge p_2 \wedge \cdots \wedge p_n$.

♦

Ejemplo 1.25

Estudiar la validez del siguiente razonamiento:

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

Solución.

Lo haremos de varias formas.

1 Veremos que es una tautología, comprobando que si la hipótesis es verdad, entonces la conclusión también ha de serlo.

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 Comprobaremos, ahora, que el condicional

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

es una tautología mediante una tabla de verdad *abreviada*.

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.

$$\begin{aligned} p \wedge ((p \wedge q) \longrightarrow r) &\iff p \wedge [p \longrightarrow (q \longrightarrow r)] && \{\text{Exportación}\} \\ &\implies q \longrightarrow r && \{\text{Modus Ponendo Ponens}\} \end{aligned}$$

♦

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" (1.4.3),

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

Demostración.

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 1.4.3, es equivalente al primero.

♦

Ejemplo 1.26

Estudiar la validez del razonamiento:

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

por contradicción.

Solución.

Probaremos que es una tautología.

En efecto, supongamos que el condicional,

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

es falso. Entonces, la hipótesis, $p \wedge ((p \wedge q) \longrightarrow r)$, sería verdad y la conclusión $q \longrightarrow r$ falsa, lo cual por los valores de verdad de la conjunción y del condicional significa que

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

Pues bien, como $(p \wedge q) \longrightarrow r$ es verdad, siendo r falsa, por el valor de verdad del condicional, $p \wedge q$ ha de ser falsa, y como q es verdad, el valor de verdad de la conjunción asegura que p ha de ser falsa.

Tenemos, por tanto, que p es verdadera y también falsa lo cual, obviamente, es una contradicción de aquí que sea falsa la suposición inicial de que el condicional era falso, por tanto será verdadero y, consecuentemente, el razonamiento 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" (1.4.3),

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

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 1.27

Estudiar la validez del razonamiento:

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

por la contrarrecíproca.

Solución.

Probaremos que el condicional,

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

es una tautología.

Aplicando las equivalencias lógicas correspondientes,

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

y

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

Probaremos, por tanto, que el condicional

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

es tautología.

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 1.4.3, 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.

♦

Ejemplo 1.28

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:

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

Solución.

Tenemos que comprobar que el condicional,

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

es una tautología.

Lo haremos de varias formas.

1 Comprobando que si la hipótesis es verdadera, entonces la conclusión también ha de serlo.

En efecto, si $(p \longrightarrow q) \wedge (q \longrightarrow \neg r)$ es verdad, entonces $p \longrightarrow q$ ha de ser verdad y $q \longrightarrow \neg r$ 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. En este caso, la conclusión $p \longrightarrow \neg r$ es verdadera, independientemente del valor de verdad que tenga r.
- q es verdadera. En tal caso, como $q \longrightarrow \neg r$ es verdad, $\neg r$ 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

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

es una tautología y el razonamiento es válido.

2 Probemos, ahora, que el razonamiento es válido utilizando una *tabla de verdad abreviada*.

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

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

En efecto, supongamos que

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

es falso.

Entonces, la hipótesis, $(p \longrightarrow q) \wedge (q \longrightarrow \neg r)$, es verdadera y la conclusión, $p \longrightarrow \neg r$, falsa. Por los valores de verdad de la conjunción y el condicional, tendríamos,

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

Pues bien, como $\neg r$ es falsa y $q \longrightarrow \neg r$ es verdad, el valor de verdad del condicional, (1.2.5), asegura que q ha de ser falsa y al ser p verdad, por el mismo motivo tendremos que $p \longrightarrow q$ es falso.

Concluimos, por tanto, que $p \longrightarrow q$ es verdadera y falsa al mismo tiempo lo que, obviamente, es una contradicción. Quiere esto decir que la suposición que hicimos al principio sobre la falsedad del condicional es falsa lo cual equivale a decir que es verdadero y, consecuentemente, el razonamiento sería válido.

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

Veamos que

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

es tautología.

Utilizando las equivalencias lógicas correspondientes,

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

y

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

Probaremos, pues, que

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

es tautología.

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, $(p \wedge \neg q) \vee (q \wedge r)$, 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, $(p \wedge \neg q) \vee (q \wedge r)$, será verdadera.

Como la veracidad de la conclusión se sigue de la veracidad de la hipótesis hemos comprobado que el condicional,

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

es decir,

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

es una tautología. Utilizando la equivalencia lógica "*contrarrecíproca*", 1.4.3,

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

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.

Si Florinda se tira al tren, entonces Torcuato no se hace cura.

Por lo tanto,

si Torcuato se casa, entonces no se hace cura.

♦

Ejemplo 1.29

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 este condicional es una tautología.

1 Comprobando que si la hipótesis es verdadera, entonces la conclusión también ha de serlo.

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 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.

3 Demostración por contradicción.

En efecto, supongamos que el condicional,

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

es falso. Entonces, la hipótesis, $(p \longrightarrow q) \wedge (\neg r \longrightarrow p) \wedge \neg q$, será verdadera y la conclusión, r, falsa. Por el valor de verdad de la conjunción, (1.2.1), tendremos que

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

Pus bien, si r es falsa, entonces su negación, $\neg r$, será verdadera y, al ser $\neg r \longrightarrow p$ verdadera, el valor de verdad del condicional, (1.2.5), asegura que p es verdadera. Por otra parte, $\neg q$ es verdad luego q es falsa lo cual, nuevamente por el valor de verdad del condicional, significa que la proposición $p \longrightarrow q$ es falsa.

Tendremos, por tanto, que $p \longrightarrow q$ es verdadera y, al mismo tiempo, falsa, lo cual es una contradicción. La suposición inicial de que el condicional era falso es falsa y, consecuentemente, dicho condicional es verdadero y el razonamiento sería válido.

4 Demostración por la contrarrecíproca.

Probaremos que

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

es una tautología.

Utilizando las equivalencias lógicas correspondientes,

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

Probaremos, pues, que

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

es una tautología.

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 el condicional,

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

es una tautología, luego

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

también lo será y en virtud de la equivalencia entre un condicional y su contrarrecíproco, (1.4.3),

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

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

♦

Ejemplo 1.30

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 deberá ser 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 1.31

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 1.32

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 una determinada propiedad p o que, al menos, 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 o enunciado 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 $p(x,y)$, $q(x,y)$, $r(x,y,z)$. En todos los casos, x, y o z son los objetos o variables referidos por el predicado.

♦

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 "$q(x, y)$: 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 como 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.

♦

2.1.4 Variables Libres y Ligadas

Una variable estará libre cuando pueda tomar cualquier valor en el Universo del Discurso y estará ligada cuando haya tomado un valor concreto en dicho Universo.

♦♦♦

2.2 Cuantificadores

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.

2.2.1 Introducción

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,

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

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.

♦

2.2.2 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", "para x arbitrario" o "elegido cualquier x".

♦

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,

$$\forall n_1, \forall n_2, (n_1 n_2 \neq 0 \longrightarrow n_1 \neq 0 \ \wedge \ n_2 \neq 0)$$

la cual, utilizando los predicados del enunciado, se escribiría

$$\forall n_1, \forall n_2, [\neg p(n_1, n_2, 0) \longrightarrow (\neg p(n_1, 0) \wedge \neg q(n_2, 0))]$$

(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:

$$\forall n_1, \forall n_2, (n_1 n_2 = 0 \longrightarrow n_1 = 0 \ \vee \ n_2 = 0)$$

y utilizando los predicados,

$$\forall n_1, \forall n_2, [p(n_1, n_2, 0) \longrightarrow (q(n_1, 0) \vee q(n_2, 0))]$$

(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:

$$\forall n_1, \forall n_2, (n_1 \leqslant n_2 \ \wedge \ n_2 \leqslant n_1 \longrightarrow n_1 = n_2)$$

y con los predicados,

$$\forall n_1, \forall n_2, [(\neg r(n_1, n_2) \wedge \neg r(n_2, n_1)) \longrightarrow q(n_1, n_2)]$$

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

Utilizando el cuantificador universal,

$$\forall n_1, \forall n_2, \forall n_3 \, (n_1 < n_2 \ \wedge \ n_3 < 0 \longrightarrow n_1 n_3 > n_2 n_3)$$

Para escribir la proposición con los predicados propuestos utilizaremos las variables auxiliares, n_4 y n_5. En efecto,

$$\forall n_1, \forall n_2, \forall n_3 \, [(r(n_2, n_1) \wedge r(0, n_3)) \longrightarrow \forall n_4, \forall n_5 \, ((p(n_1, n_3, n_4) \wedge p(n_2, n_3, n_5)) \longrightarrow r(n_4, n_5))]$$

♦

2.2.3 Valor de Verdad de una Proposición Cuantificada Universalmente

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

- ⁕ *La proposición $\forall x, p(x)$ es verdad si el predicado $p(x)$ se transforma en una proposición verdadera para todos los valores de x en el universo $\mathscr{U}$.*
- ⁕ *La proposición $\forall x, p(x)$ 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.

Tendremos que analizar el valor de verdad de la proposición universalmente cuantificada $\forall n, (n < n + 1)$ en el universo $\mathbb{Z}$ de los números enteros.

Por otra parte, dados dos enteros cualesquiera b y c, el primero será menor que el segundo si la diferencia entre el segundo y el primero es positiva, es decir,

$$c < d \iff d - c \in \mathbb{Z}^+$$

Pues bien, si a es cualquier número entero, se verifica que

$$a + 1 - a = 1 \in \mathbb{Z}^+$$

lo cual equivale, según acabamos de decir, a que

$$a < a + 1$$

Hemos probado, por tanto, que el predicado $n < n + 1$ se transforma en una proposición verdadera para todos y cada uno de los elementos del universo, luego por 2.2.3,

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

es una proposición verdadera.

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

La proposición $\forall n, (n = 5)$ será verdadera si el predicado $n = 5$ se transforma en una proposición verdadera para cada n en $\mathbb{Z}$ y será falsa si hay, al menos, un valor de n en $\mathbb{Z}$ que transforme el predicado $n = 5$ en una proposición falsa.

Cualquier entero a, tal que $a \neq 5$ transformaría el predicado $n = 5$ en una proposición falsa, es decir hay infinitos ejemplos.

Aplicando de nuevo, 2.2.3, la proposición

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

es falsa.

♦

2.2.4 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 palabra “existe” 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 “algún $x, p(x)$” o “existe, al menos, un x, tal que $p(x)$”.

♦

Ejemplo 2.7

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

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

(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) $\forall x, p(a, x)$
La forma equivalente pedida es
$$p(a, a) \wedge p(a, b)$$

(b) La proposición cuantificada $\forall x, (\forall y, (p(x, y)))$ se expande en la forma:
$$(\forall y, p(a, y)) \wedge (\forall y, p(b, y))$$
que, a su vez, equivale a
$$(p(a, a) \wedge p(a, b)) \wedge (p(b, a) \wedge p(b, b))$$
que por la asociatividad de $\wedge$ es equivalente a
$$p(a, a) \wedge p(a, b) \wedge p(b, a) \wedge p(b, b)$$

(c) Expandimos la proposición $\forall x, (\exists y : p(x, y))$ a
$$(\exists y : p(a, y)) \wedge (\exists y : p(b, y))$$
la cual equivale a
$$(p(a, a) \vee p(a, b)) \wedge (p(b, a) \vee p(b, b))$$
y aplicando la distributividad de $\wedge$ respecto de $\vee$,
$$((p(a, a) \vee p(a, b)) \wedge p(b, a)) \vee ((p(a, a) \vee p(a, b)) \wedge p(b, b))$$
es decir,
$$(p(a, a) \wedge p(b, a)) \vee (p(a, b) \wedge p(b, a)) \vee (p(a, a) \wedge p(b, b)) \vee (p(a, b) \wedge p(b, b))$$

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

$$(\forall y, p(a, y)) \vee (\forall y, p(b, y))$$

la cual equivale a la proposición

$$(p(a, a) \wedge p(a, b)) \vee (p(b, a) \wedge p(b, b))$$

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

$$((p(a, a) \wedge p(a, b)) \vee p(b, a)) \wedge ((p(a, a) \wedge p(a, b)) \vee p(b, b))$$

es decir,

$$(p(a, a) \vee p(a, b)) \wedge (p(a, b) \vee p(b, a)) \wedge (p(a, a) \vee p(b, b)) \wedge (p(a, b) \vee p(b, b))$$

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

$$(\exists x : p(x, a)) \vee (\exists x : p(x, b))$$

que es equivalente a la proposición,

$$p(a, a) \vee p(b, a) \vee p(a, b) \vee p(b, b)$$

♦

2.2.5 Valor de Verdad de una Proposición Cuantificada Existencialmente

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

- ⁕ *La proposición $\exists x : p(x)$ es verdadera, si el predicado $p(x)$ se transforma en una proposición verdadera para, al menos, uno de los valores de x en $\mathscr{U}$.*
- ⁕ *La proposición $\exists x : p(x)$ 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 universo 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 2.2.5, 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 2.2.5,

$$\exists n : n + 1$$

es una proposición falsa.

♦

2.2.6 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 enteros 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 enteros 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, la proposición $\forall n_2, (a \cdot n_2 = 1)$ será falsa si podemos encontrar, al menos, un valor de n_2 en $\mathbb{Z}$ para el cual 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 $a \cdot n_2 \neq 1$, luego la proposición $\forall n_2, (a \cdot n_2 = 1)$ es 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, al menos, 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,

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

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

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 $q(x)$ como $r(x)$ serían falsas para ese x.

Por ejemplo, si x es igual a 1, tendremos que $q(1)$ 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 $q(x) \vee r(x)$ en una proposición falsa y, consecuentemente, la proposición $\forall x, [q(x) \vee r(x)]$ es falsa.

♦♦♦

2.3 Cálculo con Predicados

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:

1. $\neg\forall x, p(x) \iff \exists x : \neg p(x)$
2. $\neg\exists x : p(x) \iff \forall x, \neg p(x)$

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 que los correspondientes condicionales son tautologías. Partiremos de la veracidad de la hipótesis y comprobaremos que la conclusión también es verdadera.

1. $\neg\forall x, p(x) \iff \exists x : \neg p(x)$

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

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.

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

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

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.

♦

Ejemplo 2.12

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

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

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

Solución.

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

Según la primera de las Leyes de De Morgan,

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

y negando ambos miembros, en virtud de la equivalencia entre una proposición y su contrarrecíproca, tendremos

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

de donde, por doble negación, resulta,

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

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

Por la segunda Ley de De Morgan,

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

y negando ambos miembros, en virtud de la equivalencia entre una proposición y su contrarrecíproca, tendremos

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

de donde, por doble negación, obtenemos el resultado,

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

♦

De todo lo dicho anteriormente 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.

♦

Ejemplo 2.13

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

$p(n)$: El número n es par.

$q(n)$: El número n es impar.

$r(n)$: El número n es no negativo.

$s(n)$: El número n es primo.

(a) Escribir en notación lógica la afirmación "algún número es par".

(b) Escribir en notación lógica la afirmación "ningún número es par".

(c) Considerando que si un número no es par, entonces ha de ser impar, escribir la afirmación "ningún número es par".

(d) Escribir en notación lógica "todo número entero es par o impar".

(e) Escribir en notación lógica "todos los números primos son no negativos".

(f) Escribir en notación lógica "el único número primo par es el 2".

(g) Escribir la negación de la afirmación "todos los números son pares".

Solución.

(a) Escribir en notación lógica la afirmación "algún número es par".

$$\exists n : p(n)$$

(b) Escribir en notación lógica la afirmación "ningún número es par".

Observemos lo siguiente:

$$\text{Ningún número es par} \iff \neg\,(\text{Algún número es par})$$

y según el apartado anterior,

$$\text{Algún número es par} \iff \exists n : p(n)$$

luego,

$$\begin{aligned} \text{Ningún número es par} &\iff \neg\,(\text{Algún número es par}) \\ &\iff \neg\exists n : p(n) \\ &\iff \forall n : \neg p(n) \qquad \{\text{Segunda Ley de De Morgan}\} \end{aligned}$$

(c) Considerando que si un número no es par, entonces ha de ser impar, escribir la afirmación "ningún número es par".

Según el apartado anterior,

$$\begin{aligned} \text{Ningún número es par} &\iff \forall n : \neg p(n) \\ &\iff \text{Todos los números son impares} \end{aligned}$$

(d) Escribir en notación lógica "todo número entero es par o impar".

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

(e) Escribir en notación lógica "todos los números primos son no negativos".

$$\forall n, (s(n) \longrightarrow r(n))$$

(f) Escribir en notación lógica "el único número primo par es el 2".

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

(g) Escribir la negación de la afirmación "todos los números son pares".

$$\text{Todos los números son pares} \iff \forall n, p(n)$$

luego,

$$\begin{aligned} \neg\,(\text{Todos los números son pares}) &\iff \neg\forall n, p(n) \\ &\iff \exists n : \neg p(n)\ \{\text{Primera Ley de De Morgan}\} \\ &\iff \text{Hay, al menos, un número que no es par} \\ &\iff \text{Algún número no es par} \\ &\iff \text{Algún número es impar} \end{aligned}$$

♦

2.3.3 Asociatividad

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

Demostración.

Sea $\mathscr{U}$ un universo del discurso cualquiera y $p(x), q(x)$ dos predicados arbitrarios, y x cualquier elemento de $\mathscr{U}$. Probaremos que los condicionales correspondientes son tautologías partiendo de la veracidad de la hipótesis.

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. $\exists x : [p(x) \vee q(x)] \Longleftrightarrow [\exists x : p(x)] \vee [\exists x : q(x)]$.

   $\Rightarrow$) $\exists x : [p(x) \vee q(x)] \Longrightarrow [\exists x : p(x)] \vee [\exists x : q(x)]$
   En efecto, si la proposición $\exists x : [p(x) \vee q(x)]$ es verdad, entonces el predicado a su alcance, $p(x) \vee q(x)$, se transforma en una proposición verdadera para, al menos, un valor de x en $\mathscr{U}$. Por el valor de la verdad de la disyunción esto significa que hemos encontrado, al menos, un valor de x que transforma $p(x)$ en proposición verdadera, con lo cual $\exists x : p(x)$ es verdad o a $q(x)$ en proposición verdadera, es decir, $\exists x : q(x)$ es verdad. Al ser verdadera, al menos, una de las dos proposiciones, tendremos que la disyunción de ambas, $[\exists x : p(x)] \vee [\exists x : q(x)]$, es verdad.

   $\Leftarrow$) $[\exists x : p(x)] \vee [\exists x : q(x)] \Longrightarrow \exists x : [p(x) \vee q(x)]$.
   Recíprocamente, si $[\exists x : p(x)] \vee [\exists x : q(x)]$ es verdad, entonces por el valor de verdad de la disyunción, tendremos dos opciones:
   - $\exists x : p(x)$ es verdad. En este caso, habrá, al menos, un valor de x en $\mathscr{U}$ que transforma $p(x)$ en proposición verdadera con lo cual el predicado $p(x) \vee q(x)$ se transformará en proposición verdadera para, al menos, ese valor de x independientemente de lo que ocurra con $q(x)$ y, consecuentemente, $\exists x : [p(x) \vee q(x)]$ será verdad.
   - $\exists x : q(x)$ es verdad. En tal caso, habría, al menos, un valor de x en $\mathscr{U}$ que transformaría $q(x)$ en proposición verdadera y bastaría razonar igual que en el caso anterior par concluir que $\exists x : [p(x) \vee q(x)]$ es verdad.

   La equivalencia demostrada suele enunciarse informalmente diciendo que "*el cuantificador existencial es asociativo respecto del conectivo lógico disyunción*"

♦

2.3.4 Distributividad

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

Demostración.

Sea $\mathscr{U}$ un universo del discurso cualquiera y $p(x), q(x)$ dos predicados arbitrarios, y x cualquier elemento de $\mathscr{U}$. Comprobaremos que los condicionales correspondientes son tautologías partiendo de la veracidad de la hipótesis.

1. $\exists x : [p(x) \wedge q(x)] \Longrightarrow [\exists x : p(x)] \wedge [\exists x : q(x)]$

   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.

2. $[\forall x, p(x)] \vee [\forall x, q(x)] \Longrightarrow \forall x, [p(x) \vee q(x)]$

   En efecto, si la hipótesis, $[\forall x, p(x)] \vee [\forall x, q(x)]$, es verdad, entonces por el valor de verdad de la disyunción habrá dos opciones:

   - $\forall x, p(x)$ es verdad. En este caso, y por el valor de verdad del cuantificador existencial, el predicado $p(x)$ se transformará en proposición verdadera para todos y cada uno de los valores de x en $\mathscr{U}$ luego el valor de verdad de la disyunción asegura que el predicado $p(x) \vee q(x)$ se transformará en proposición verdadera para cada x de $\mathscr{U}$ independientemente de lo que ocurra con $q(x)$ y, por lo tanto, $\forall x, [p(x) \vee q(x)]$ es verdad.
   - $\forall x, q(x)$ es verdad. En tal caso es el predicado $q(x)$ el que se transforma en proposición verdadera para cada x de $\mathscr{U}$ y el mismo razonamiento del caso anterior nos llevaría a la veracidad de $\forall x, [p(x) \vee q(x)]$.

♦

Ejemplo 2.14

Probar que la implicación recíproca de $\exists x : [p(x) \wedge q(x)] \Longrightarrow [\exists x : p(x)] \wedge [\exists x : q(x)]$ no se verifica.

Solución.

Para probar que

$$[\exists x : p(x)] \wedge [\exists x : q(x)] \not\Longrightarrow \exists x : [p(x) \wedge q(x)]$$

tendremos que probar que, en general, el condicional,

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

no es una tautología. Bastará, pues, que encontremos, al menos, un caso en el que la hipótesis sea verdadera y la conclusión falsa.

Consideremos un universo del discurso arbitrario, $\mathscr{U}$, un predicado cualquiera, $p(x)$, siendo x cualquiera de $\mathscr{U}$. Supongamos, también, que $q(x) = \neg p(x)$.

Pues bien, sean a y b dos elementos de $\mathscr{U}$ tales que $p(a)$ sea una proposición verdadera y $\neg p(b)$ también lo sea. Entonces, las proposiciones $\exists x : p(x)$ y $\exists x : \neg p(x)$ serán, ambas, verdaderas y, consecuentemente, su conjunción

$$[\exists x : p(x)] \wedge [\exists x : \neg p(x)]$$

también lo será.

Por otra parte, el predicado $p(x) \wedge \neg p(x)$ se transforma en una proposición falsa para cada x de $\mathscr{U}$ ya que $p(x)$ y $\neg p(x)$ se transforman en proposiciones con distintos valores de verdad y, por lo tanto,

$$\exists x : [p(x) \wedge \neg p(x)]$$

es una proposición falsa.

♦

Ejemplo 2.15

Probar que la implicación recíproca de $[\forall x, p(x)] \vee [\forall x, q(x)] \Longrightarrow \forall x, [p(x) \vee q(x)]$ no se verifica.

Solución.

Al igual que en el ejemplo anterior, para probar que

$$\forall x, [p(x) \vee q(x)] \not\Longrightarrow [\forall x, p(x)] \vee [\forall x, q(x)]$$

tendremos que probar que, en general, el condicional,

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

no es una tautología, es decir tendremos que encontrar, al menos, un caso en el que la hipótesis sea verdadera y la conclusión falsa. Utilizaremos un razonamiento similar al ejercicio anterior, pero en este caso con un universo del discurso específico y dos predicados concretos en el mismo.

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

$p(x) : x$ *es un número par*

$q(x) : x$ *es un número impar*

El predicado $p(x) \vee q(x)$ se transforma en proposición verdadera para cada x de $\mathscr{U}$ ya que los predicados $p(x)$ y $q(x)$ se transformarían en proposiciones verdaderas con distintos valores de verdad, luego la proposición,

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

es verdadera.

Por otra parte, si tomamos $x = 1$, tendremos que $p(1)$ es falsa y tomando $x = 2$, $q(2)$ también lo es y por lo tanto, habremos encontrado, al menos, un valor de x en $\mathscr{U}$ que transforma $p(x)$ en proposición falsa y lo mismo ocurre con $q(x)$. Esto significa que tanto $\forall x, p(x)$ como $\forall x, q(x)$ son falsas y, consecuentemente,

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

es una proposición falsa.

♦

Ejemplo 2.16

Probar, utilizando el universo del discurso $\mathscr{U} = \{a, b\}$,

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

(b) $[\exists x : p(x)] \wedge [\exists x : q(x)] \not\Longrightarrow \exists x : [p(x) \wedge q(x)]$

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

(d) $\forall x, [p(x) \vee q(x)] \not\Longrightarrow [\forall x, p(x)] \vee [\forall x, q(x)]$

Solución.

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

Expandiendo las proposiciones en el universo $\mathscr{U} = \{a, b\}$,

$$\begin{aligned} \exists x : (p(x) \wedge q(x)) &\iff (p(a) \wedge q(a)) \vee (p(b) \wedge q(b)) \\ &\iff [(p(a) \wedge q(a)) \vee p(b)] \wedge [(p(a) \wedge q(a)) \vee q(b)] \\ &\iff (p(a) \vee p(b)) \wedge (p(b) \vee q(a)) \wedge (p(a) \vee q(b)) \wedge (q(a) \vee q(b)) \end{aligned}$$

$$(\exists x : p(x)) \wedge (\exists x : q(x)) \iff (p(a) \vee p(b)) \wedge (q(a) \vee q(b))$$

Entonces, la implicación propuesta será equivalente a

$$(p(a) \vee p(b)) \wedge (p(b) \vee q(a)) \wedge (p(a) \vee q(b)) \wedge (q(a) \vee q(b)) \Longrightarrow (p(a) \vee p(b)) \wedge (q(a) \vee q(b))$$

y si la hipótesis es verdad, entonces todas las proposiciones unidas por la conjunción que la integran son verdaderas. En concreto, $p(a) \vee p(b)$ y $q(a) \vee q(b)$ serán verdaderas y también la conclusión al ser la conjunción de ambas.

(b) $[\exists x : p(x)] \wedge [\exists x : q(x)] \not\Longrightarrow \exists x : [p(x) \wedge q(x)]$

El recíproco sería equivalente a

$$(p(a) \vee p(b)) \wedge (q(a) \vee q(b)) \Longrightarrow (p(a) \vee p(b)) \wedge (p(b) \vee q(a)) \wedge (p(a) \vee q(b)) \wedge (q(a) \vee q(b))$$

y si suponemos, por ejemplo, que

$p(a)$ es verdadera.
$p(b)$ es falsa.
$q(a)$ es falsa.
$q(b)$ es verdadera.

tendremos que la hipótesis,

$$(p(a) \vee p(b)) \wedge (q(a) \vee q(b))$$

sería verdadera, en tanto que la conclusión

$$(p(a) \vee p(b)) \wedge (p(b) \vee q(a)) \wedge (p(a) \vee q(b)) \wedge (q(a) \vee q(b))$$

sería falsa ya que la proposición $p(b) \vee q(a)$ lo es.

Hemos encontrado, pues, al menos un caso en el que la hipótesis se transforma en una proposición verdadera y la conclusión en proposición falsa, luego

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

no es una tautología y, consecuentemente,

$$[\exists x : p(x)] \wedge [\exists x : q(x)] \not\Longrightarrow \exists x : [p(x) \wedge q(x)]$$

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

Expandiendo, al igual que en el primer apartado, las proposiciones en el universo propuesto,

$$(\forall x, p(x)) \vee (\forall x, q(x)) \iff (p(a) \wedge p(b)) \vee (q(a) \wedge q(b))$$

y

$$\begin{aligned} \forall x, (p(x) \vee q(x)) &\iff (p(a) \vee q(a)) \wedge (p(b) \vee q(b)) \\ &\iff [(p(a) \vee q(a)) \wedge p(b)] \vee [(p(a) \vee q(a)) \wedge q(b)] \\ &\iff (p(a) \wedge p(b)) \vee (p(b) \wedge q(a)) \vee (p(a) \wedge q(b)) \vee (q(a) \wedge q(b)) \end{aligned}$$

Entonces, la implicación propuesta será equivalente a

$$(p(a) \wedge p(b)) \vee (q(a) \wedge q(b)) \Longrightarrow (p(a) \wedge p(b)) \vee (p(b) \wedge q(a)) \vee (p(a) \wedge q(b)) \vee (q(a) \wedge q(b))$$

y si la hipótesis es verdad, entonces, al menos una de las dos proposiciones que la integran ha de ser verdad lo cual significa que una, al menos, de las cuatro proposiciones que integran la conclusión es verdadera y, consecuentemente, esta también lo será.

(d) $\forall x, [p(x) \vee q(x)] \not\Longrightarrow [\forall x, p(x)] \vee [\forall x, q(x)]$

El recíproco será equivalente a

$$(p(a) \wedge p(b)) \vee (p(b) \wedge q(a)) \vee (p(a) \wedge q(b)) \vee (q(a) \wedge q(b)) \Longrightarrow (p(a) \wedge p(b)) \vee (q(a) \wedge q(b))$$

y suponiendo, por ejemplo, que

- $p(a)$ es verdadera.
- $p(b)$ es falsa.
- $q(a)$ es falsa.
- $q(b)$ es verdadera.

tendremos que la hipótesis,

$$(p(a) \wedge p(b)) \vee (p(b) \wedge q(a)) \vee (p(a) \wedge q(b)) \vee (q(a) \wedge q(b))$$

sería verdadera, ya que la proposición $p(a) \wedge q(b)$ es verdadera. Sin embargo la conclusión

$$(p(a) \wedge p(b)) \vee (q(a) \wedge q(b))$$

sería falsa ya que ambas proposiciones $(p(a) \wedge p(b))$ y $(q(a) \wedge q(b))$ lo son.

Hemos encontrado, pues, al menos un caso en el que la hipótesis se transforma en una proposición verdadera y la conclusión en proposición falsa, luego

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

no es una tautología y, consecuentemente,

$$\forall x, [p(x) \vee q(x)] \not\Longrightarrow [\forall x, p(x)] \vee [\forall x, q(x)]$$

♦

Ejemplo 2.17

Si $p(x)$ y $q(x)$ son dos predicados arbitrarios, siendo x cualquiera de un universo $\mathscr{U}$, probar que

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

Solución.

$\Longrightarrow$) Veamos que el condicional,

$$\forall x, (p(x) \longrightarrow q(x)) \longrightarrow \neg\exists x : (p(x) \wedge \neg q(x))$$

es una tautología para lo cual partiremos de la verdad de la hipótesis para llegar a la veracidad de la conclusión.

En efecto, si

$$\forall x, (p(x) \longrightarrow q(x))$$

es verdad, entonces, por el valor de verdad de una proposición universalmente cuantificada, (2.2.3), el predicado al alcance del cuantificador,

$$p(x) \longrightarrow q(x)$$

ha de transformarse en una proposición verdadera para cada x en $\mathscr{U}$. Nos apoyaremos en las distintas opciones que puede haber para el predicado $p(x)$.

- $p(x)$ se transforma en proposición verdadera para cada x de $\mathscr{U}$. En tal caso, $q(x)$ ha de transformarse, también, en proposición verdadera y $\neg q(x)$ en falsa para todos y cada uno de los x en $\mathscr{U}$ luego el predicado $p(x) \wedge \neg q(x)$ se transformará, a su vez, en proposición falsa para cada x y, consecuentemente, el valor de verdad de una proposición cuantificada existencialmente asegura que

  $$\exists x : (p(x) \wedge \neg q(x))$$

  es falsa y, por lo tanto,

  $$\neg\exists x : (p(x) \wedge \neg q(x))$$

  es verdadera.
- $p(x)$ se transforma en proposición falsa para cada x de $\mathscr{U}$. En este caso e independientemente de lo que ocurra con $\neg q(x)$, el predicado $p(x) \wedge \neg q(x)$ se transformará en proposición falsa para cada x de $\mathscr{U}$ y, al igual que en el caso anterior,

  $$\exists x : (p(x) \wedge \neg q(x))$$

  será falsa y, por lo tanto,

  $$\neg\exists x : (p(x) \wedge \neg q(x))$$

  es verdadera.
- $p(x)$ se transforma en proposición verdadera para determinados valores de x en $\mathscr{U}$ y en proposición falsa para el resto. En tal caso, para los valores de x que transformen $p(x)$ en proposición verdadera, el predicado $q(x)$ también ha de transformase en proposición verdadera, $\neg q(x)$ en proposición falsa y, consecuentemente, $p(x) \wedge \neg q(x)$ se trasformará en proposición falsa. Para el resto de valores de x, $p(x)$ se transformará en proposición falsa luego $p(x) \wedge \neg q(x)$ también, independientemente de lo que pueda ocurrir con $q(x)$.

  Por lo tanto, el predicado $p(x) \wedge \neg q(x)$ se transformará en proposición falsa para cada x de $\mathscr{U}$ y, al igual que en los casos anteriores,

  $$\exists x : (p(x) \wedge \neg q(x))$$

  será falsa y, consecuentemente,

  $$\neg\exists x : (p(x) \wedge \neg q(x))$$

  será verdadera.

$\Longleftarrow$) Veamos ahora que el condicional,

$$\neg\exists x : (p(x) \wedge \neg q(x)) \longrightarrow \forall x, (p(x) \longrightarrow q(x))$$

es una tautología para lo cual partiendo de la veracidad de la hipótesis llegaremos a la veracidad de la conclusión.

En efecto, si

$$\neg\exists x : (p(x) \wedge \neg q(x))$$

es verdad, entonces,

$$\exists x : (p(x) \wedge \neg q(x))$$

es falsa y por el valor de verdad de una proposición existencialmente cuantificada, (2.2.5), el predicado al alcance del cuantificador,

$$p(x) \wedge \neg q(x)$$

ha de transformarse en una proposición falsa para cada x en $\mathscr{U}$.

Al igual que en la prueba de la implicación anterior, nos apoyaremos en las distintas opciones que puede haber para el predicado $p(x)$.

- $p(x)$ se transforma en proposición verdadera para cada x de $\mathscr{U}$. En este caso, el predicado $\neg q(x)$ ha de transformarse en proposición falsa y $q(x)$ en verdadera para cada x de $\mathscr{U}$ luego el predicado $p(x) \longrightarrow q(x)$ se transformara en proposición verdadera, también para cada x en $\mathscr{U}$ y, consecuentemente, el valor de verdad de una proposición universalmente cuantificada, (2.2.3), asegura que la proposición

  $$\forall x, (p(x) \longrightarrow q(x))$$

  es verdadera.
- $p(x)$ se transforma en proposición falsa para cada x de $\mathscr{U}$. En tal caso, el predicado $p(x) \longrightarrow q(x)$ se transformara en proposición verdadera para cada x en $\mathscr{U}$ independientemente de lo que ocurra con $q(x)$ y, al igual que en el caso anterior, esto significa que la proposición

  $$\forall x, (p(x) \longrightarrow q(x))$$

  es verdadera.
- $p(x)$ se transforma en proposición verdadera para determinados valores de x en $\mathscr{U}$ y en proposición falsa para el resto. En tal caso, para los valores de x que transformen $p(x)$ en verdadera, $\neg q(x)$ ha de transformarse en proposición falsa y $q(x)$ en verdadera, luego para estos valores el predicado $p(x) \longrightarrow q(x)$ se transformará en una proposición verdadera. Para el resto de valores de x, $p(x)$ se transformará en proposición falsa y, por lo tanto, el predicado $p(x) \longrightarrow q(x)$ se transformará proposición verdadera independientemente de lo que ocurra con $q(x)$. Consecuentemente, y en cualquier caso, el predicado $p(x) \longrightarrow q(x)$ se transformará en una proposición verdadera para cada x de $\mathscr{U}$ y, al igual que en los casos anteriores, la proposición

  $$\forall x, (p(x) \longrightarrow q(x))$$

  será verdadera.

♦

Ejemplo 2.18

Considerando como Universo del Discurso el conjunto $\mathbb{Z}$ de los números enteros, escribir en notación lógica la afirmación "ningún número par es impar".

Solución.

Sea n cualquier número entero y sean los predicados,

$p(n)$: El número n es par.

$q(n)$: El número n es impar.

Utilizaremos, para obtener el resultado, el hecho de que "ningún" es la negación de "algún".

$$\begin{aligned} \text{Ningún número par es impar} &\iff \neg\,(\text{Algún número par es impar}) \\ &\iff \neg\exists n : (p(n) \wedge q(n)) \\ &\iff \forall n, (p(n) \longrightarrow \neg q(n)) \qquad \{\text{Ejemplo 2.17}\} \end{aligned}$$

♦

Ejemplo 2.19

Probar, en el universo de los números enteros, que la negación de la afirmación *"ningún múltiplo de* 3 *da resto* 1 *ni* 2 *al dividirlo entre* 3*"* es equivalente a *"algún múltiplo de* 3 *da resto* 1 *o* 2 *al dividirlo por* 3*"*.

Solución.

Sea n cualquier número entero y consideremos los predicados,

$p(n)$: El número n es múltiplo de 3.

$q(n)$: El número n da resto 1 al dividirlo entre 3.

$r(n)$: El número n da resto 2 al dividirlo entre 3.

Probaremos que

$$\neg\forall n, (p(n) \longrightarrow (\neg q(n) \wedge \neg r(n))) \iff \exists n : (p(n) \wedge (q(n) \vee r(n)))$$

$\Longrightarrow$) Veamos que el condicional

$$\neg\forall n, (p(n) \longrightarrow (\neg q(n) \wedge \neg r(n))) \longrightarrow \exists n : (p(n) \wedge (q(n) \vee r(n)))$$

es una tautología comprobando que la conclusión es verdad si la hipótesis lo es.

En efecto, si

$$\neg\forall n, (p(n) \longrightarrow (\neg q(n) \wedge \neg r(n)))$$

es verdad, entonces la proposición

$$\forall n, (p(n) \longrightarrow (\neg q(n) \wedge \neg r(n)))$$

es falsa. Esto significa, por el valor de verdad de una proposición cuantificada universalmente, (2.2.3), que podemos encontrar un valor de n en el universo que transforma el predicado

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

en una proposición falsa. Si a este valor concreto lo llamamos a, tendremos que la proposición

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

es falsa lo que, a su vez, equivale a decir, por el valor de verdad del condicional que $p(a)$ es una proposición verdadera y $\neg q(a) \wedge \neg r(a)$, falsa.

Aplicando las *Leyes de De Morgan*, (1.4.3), entre proposiciones,

$$\neg q(a) \wedge \neg r(a) \Longleftrightarrow \neg\left(q(a) \vee r(a)\right)$$

luego $\neg\left(q(a) \vee r(a)\right)$ es falsa y, consecuentemente, $q(a) \vee r(a)$ es verdadera. Como $p(a)$ era verdadera, el valor de verdad de la conjunción asegura que la proposición

$$p(a) \wedge \left(q(a) \vee r(a)\right)$$

es verdadera y habremos encontrado, al menos, un valor de verdad en el Universo que transforma el predicado

$$p(n) \wedge \left(q(n) \vee r(n)\right)$$

en una proposición verdadera lo que, por el valor de verdad de una proposición cuantificada existencialmente, (2.2.5), significa que

$$\exists n : \left(p(n) \wedge \left(q(n) \vee r(n)\right)\right)$$

es verdadera y, consecuentemente, el condicional

$$\neg\forall n, \left(p(n) \longrightarrow \left(\neg q(n) \wedge \neg r(n)\right)\right) \longrightarrow \exists n : \left(p(n) \wedge \left(q(n) \vee r(n)\right)\right)$$

es tautología y

$$\neg\forall n, \left(p(n) \longrightarrow \left(\neg q(n) \wedge \neg r(n)\right)\right) \Longrightarrow \exists n : \left(p(n) \wedge \left(q(n) \vee r(n)\right)\right)$$

$\Longleftarrow$) Probaremos, ahora, que el condicional

$$\exists n : \left(p(n) \wedge \left(q(n) \vee r(n)\right)\right) \longrightarrow \neg\forall n, \left(p(n) \longrightarrow \left(\neg q(n) \wedge \neg r(n)\right)\right)$$

es una tautología comprobando, también, que la conclusión es verdad si la hipótesis lo es.

En efecto, si la proposición

$$\exists n : \left(p(n) \wedge \left(q(n) \vee r(n)\right)\right)$$

es verdadera, entonces el valor de verdad de una proposición existencialmente cuantificada, (2.2.5), asegura que ha de existir, al menos, un valor de n en el Universo que transforme el predicado

$$p(n) \wedge \left(q(n) \vee r(n)\right)$$

en una proposición verdadera. Si a este valor concreto de n lo llamamos a, tendremos que la proposición

$$p(a) \wedge \left(q(a) \vee r(a)\right)$$

es verdadera. Esto significa, por el valor de verdad de la conjunción, que tanto $p(a)$ como $q(a) \vee r(a)$ han de ser verdaderas.

Pues bien, si $q(a) \vee r(a)$ es verdad, entonces, por el valor de verdad de la disyunción, una de las dos proposiciones $q(a)$ o $r(a)$, al menos, ha de ser verdadera y su negación, $\neg q(a)$ o $\neg r(a)$, falsa luego la conjunción $\neg q(a) \wedge \neg r(a)$ será, en cualquier caso, falsa. Como $p(a)$ era verdadera, tendremos que el condicional,

$$p(a) \longrightarrow \left(\neg q(a) \wedge \neg r(a)\right)$$

es falso y habremos encontrado, al menos, un valor de n en $\mathscr{U}$ que transforma el predicado

$$p(n) \longrightarrow \left(\neg q(n) \wedge \neg r(n)\right)$$

en una proposición falsa lo cual por el valor de verdad de una proposición universalmente cuantificada, (2.2.3), significa que

$$\forall n, \left(p(n) \longrightarrow \left(\neg q(n) \wedge \neg r(n)\right)\right)$$

es falsa y, consecuentemente,

$$\neg\forall n, \left(p(n) \longrightarrow \left(\neg q(n) \wedge \neg r(n)\right)\right)$$

será verdadera. El condicional

$$\exists n : \left(p(n) \wedge \left(q(n) \vee r(n)\right)\right) \longrightarrow \neg\forall n, \left(p(n) \longrightarrow \left(\neg q(n) \wedge \neg r(n)\right)\right)$$

es una tautología y, por tanto,

$$\exists n : \left(p(n) \wedge \left(q(n) \vee r(n)\right)\right) \Longrightarrow \neg\forall n, \left(p(n) \longrightarrow \left(\neg q(n) \wedge \neg r(n)\right)\right)$$

completando la equivalencia.

♦

2.4 Razonamientos y Cuantificadores

En este apartado veremos algunos ejemplos de razonamientos con proposiciones cuantificadas. Los métodos de demostración serán los que ya hemos estudiado en la lección anterior (1.5).

Ejemplo 2.20

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

$p(x)$: El alumno x es de Informática.

$q(x)$: El alumno 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 Partiremos de la veracidad de la hipótesis para llegar a la veracidad de la conclusión.

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.

El condicional,

$$[\forall x, (p(x) \longrightarrow q(x)) \wedge p(f)] \longrightarrow q(f)$$

será, por tanto, una tautología y, consecuentemente, el razonamiento es válido.

2 Utilizando el método de demostración por reducción al absurdo o contradicción (1.5.3).

En efecto, supongamos que el condicional

$$[\forall x, (p(x) \longrightarrow q(x)) \wedge p(f)] \longrightarrow q(f)$$

es falso.

Entonces, la hipótesis, $\forall x, (p(x) \longrightarrow q(x)) \wedge p(f)$, será verdadera y la conclusión, $q(f)$, falsa. Por el valor de verdad de la conjunción, tendríamos

- $\forall x, (p(x) \longrightarrow q(x))$ es verdad.
- $p(f)$ es verdad.
- $q(f)$ es falsa.

Pues bien, si $\forall x, (p(x) \longrightarrow q(x))$ es verdad, el predicado $p(x) \longrightarrow q(x)$ se transformará en una proposición verdadera para cada x de $\mathscr{U}$, en particular para Florinda ($x = f$), es decir $p(f) \longrightarrow q(f)$ es verdadera.

Tendremos, pues, que $p(f) \longrightarrow q(f)$ es verdad y $q(f)$ es falsa. El valor de verdad del condicional asegura, entonces, que $p(f)$ ha de ser falsa.

Por lo tanto, $p(f)$ es una proposición verdadera y falsa al mismo tiempo lo cual, obviamente, es una contradicción y la suposición inicial de que el condicional era falso es falsa y, consecuentemente, será una tautología y el razonamiento válido.

Veamos otra forma de hacerlo. Como $p(f)$ es verdad y $q(f)$ falsa, el condicional $p(f) \longrightarrow q(f)$ será falso y habremos encontrado, al menos, un valor de x en $\mathscr{U}$ que transforma el predicado $p(x) \longrightarrow q(x)$ en una proposición falsa, lo cual por el valor de verdad de una proposición cuantificada universalmente (2.2.3), significa que $\forall x\,(p(x) \longrightarrow q(x))$ es falsa. Tendremos pues que la proposición $\forall x\,(p(x) \longrightarrow q(x))$ es verdadera y falsa al mismo tiempo, es decir tendremos una contradicción.

3 Utilizando el método de demostración por la contrarrecíproca (1.5.4).

$$\begin{aligned}
[(\forall x, (p(x) \longrightarrow q(x))) \wedge p(f)] \longrightarrow q(f) &\iff \neg q(f) \longrightarrow \neg\,[(\forall x, (p(x) \longrightarrow q(x))) \wedge p(f)] \\
&\iff \neg q(f) \longrightarrow \neg \forall x, (p(x) \longrightarrow q(x)) \vee \neg p(f) \qquad (1.4.3) \\
&\iff \neg q(f) \longrightarrow (\exists x, (p(x) \wedge \neg q(x))) \vee \neg p(f) \qquad (2.17)
\end{aligned}$$

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 la proposición $p(f)$ y habrá, por tanto, dos opciones:

- $p(f)$ es verdad. En este caso, $p(f) \wedge \neg q(f)$ será una proposición verdadera y habremos encontrado, al menos, un valor de x en $\mathscr{U}$ que transforma el predicado $p(x) \wedge \neg q(x)$ en una proposición verdadera. El valor de verdad de una proposición existencialmente cuantificada, (2.2.5), asegura que $\exists x : (p(x) \wedge \neg q(x))$ es una proposición verdadera.
- $p(f)$ es falsa. En tal caso, $\neg p(f)$ es verdad.

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 2.21

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

$p(x)$: El número x es par.

$q(x)$: El número x es divisible por 2.

$r(x)$: El número 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 De acuerdo con la definición de razonamiento válido, comprobaremos que el condicional es una tautología.

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*, (2.2.3), 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*, (2.2.3), 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*, (1.2.5), $q(a)$ 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 el condicional es una tautología y, consecuentemente, el razonamiento válido.

2 Utilizando el método de demostración por reducción al absurdo o contradicción, (1.5.3).

En efecto, supongamos que el condicional,

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

es falso.

Entonces, la hipótesis, $\neg r(a) \wedge (\forall x, (p(x) \longrightarrow q(x))) \wedge (\forall x, (q(x) \longrightarrow r(x)))$ sería verdadera y la conclusión, $\neg p(a)$, falsa.

Entonces, por el valor de verdad de la conjunción,

- $\neg r(a)$ es verdad, es decir, $r(a)$ es falsa.
- $\forall x, (p(x) \longrightarrow q(x))$ es verdad.
- $\forall x, (q(x) \longrightarrow r(x))$ es verdad.
- $\neg p(a)$ es falsa, o sea, $p(a)$ es verdad.

Si $\forall x, (p(x) \longrightarrow q(x))$ es verdadera entonces, por el valor de verdad de una proposición universalmente cuantificada, (2.2.3), el predicado $p(x) \longrightarrow q(x)$ se transforma en proposición verdadera para cualquier elemento del universo. Al ser a uno de ellos, tendremos que la proposición $p(a) \longrightarrow q(a)$ es verdadera y al ser $p(a)$ verdadera, el valor de verdad del condicional asegura que $q(a)$ también ha de serlo.

Pues bien, como $q(a)$ es verdad y $r(a)$ es falsa, el condicional $q(a) \longrightarrow r(a)$ será falso y habremos encontrado, al menos, un valor de x en $\mathscr{U}$ que transforma el predicado $q(x) \longrightarrow r(x)$ en una proposición falsa. Por el valor de verdad de una proposición cuantificada universalmente, (2.2.3), esto significa que la proposición $\forall x, (q(x) \longrightarrow r(x))$ es falsa.

Tenemos, pues, que la proposición $\forall x, (q(x) \longrightarrow r(x))$ es verdadera y también falsa lo cual es una contradicción. La suposición inicial de que el condicional era falso es, por tanto, falsa y este será verdadero y, consecuentemente, el razonamiento será válido.

3 Utilizando el método de demostración por la contrarrecíproca (1.5.4).

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

$$\Longleftrightarrow \{\text{Contrarrecíproca}\}$$

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

$$\Longleftrightarrow \{\text{De Morgan}\}$$
$$p(a) \longrightarrow r(a) \vee (\neg\forall x, (p(x) \longrightarrow q(x))) \vee (\neg\forall x, (q(x) \longrightarrow r(x)))$$

$$\Longleftrightarrow \{\text{Ejemplo 2.17}\}$$

$$p(a) \longrightarrow r(a) \vee (\exists x : (p(x) \wedge \neg q(x))) \vee (\exists x : (q(x) \wedge \neg r(x)))$$

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 $q(x)$ cuando $x = a$.
  - ◎◎ $q(a)$ es verdad. En este caso, $q(a) \wedge \neg r(a)$ será verdadera y habremos 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 que, por el valor de verdad de una proposición existencialmente cuantificada, significa que $\exists x : (q(x) \wedge \neg r(x))$ es verdad.
  - ◎◎ $q(a)$ es falsa. En tal caso, como $p(a)$ es verdad, $p(a) \wedge \neg q(a)$ también lo será y, nuevamente, habríamos encontrado, al menos, un valor de x en $\mathscr{U}$ que transforma el predicado $p(x) \wedge \neg q(x)$ en una proposición verdadera y, por tanto, la proposición $\exists x : (p(x) \wedge \neg q(x))$ será verdadera.

Por lo tanto, y en cualquier caso, el valor de verdad de la disyunción asegura que 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 2.2 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 2.22

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 Matemática, 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,

$p(x)$: El alumno x es de Informática.

$q(x)$: El alumno x estudia Lógica Matemática.

$r(x)$: El alumno 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 Veamos, primero, que el condicional es una tautología partiendo de la veracidad de la hipótesis y comprobando que, en tal caso, la conclusión ha de ser verdadera.

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. Esto significa que los predicados $p(x) \longrightarrow q(x)$ y $q(x) \longrightarrow r(x)$ se transformarán, ambos, en proposiciones verdaderas para cada valor de x en $\mathscr{U}$.

Obtendremos el valor de verdad de la conclusión, $\forall x, (p(x) \longrightarrow r(x))$ analizando las distintas opciones que puedan presentarse para el predicado $q(x)$.

- $q(x)$ se transforma en proposición verdadera para cada x de $\mathscr{U}$. En este caso, $r(x)$ se transformará en proposición verdadera para cada x de $\mathscr{U}$ y, por tanto, el predicado $p(x) \longrightarrow r(x)$ también y, consecuentemente, la conclusión, $\forall x, (q(x) \longrightarrow r(x))$, será verdadera.
- $q(x)$ se transforma en proposición falsa para cada x de $\mathscr{U}$. En tal caso, $p(x)$ deberá transformarse en proposición falsa para cada x de $\mathscr{U}$ y, por tanto, el predicado $p(x) \longrightarrow r(x)$ también se transformará en proposición verdadera y, consecuentemente, la conclusión, $\forall x, (q(x) \longrightarrow r(x))$, será verdadera.

- ✳ $q(x)$ se transforma en proposición verdadera para determinados valores de x en $\mathscr{U}$ y en proposición falsa para el resto. En este caso y para los valores de x que transformen $q(x)$ en proposición verdadera, el predicado $r(x)$ ha de transformarse en proposición verdadera y, consecuentemente, $p(x) \longrightarrow r(x)$ también. Para los restantes valores de x, $q(x)$ se transformará en proposición falsa y esto obliga a que para estos valores el predicado $p(x)$ se transforme en proposición falsa y, por lo tanto, también lo hará el predicado $p(x) \longrightarrow r(x)$.
  Tendremos, pues, que el predicado $p(x) \longrightarrow r(x)$ se transforma en proposición verdadera para cada x de $\mathscr{U}$ y, consecuentemente, la proposición $\forall x, (p(x) \longrightarrow r(x))$ será verdadera.

En cualquier caso, 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 Utilizando el método de demostración por reducción al absurdo o contradicción (1.5.3).

Supongamos que 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 falso. Entonces, la hipótesis, $(\forall x, (p(x) \longrightarrow q(x))) \wedge (\forall x, (q(x) \longrightarrow r(x)))$ sería verdad y la conclusión, $\forall x, (p(x) \longrightarrow r(x))$, falsa y por el valor de verdad de la conjunción esto significa que

- $\forall x, (p(x) \longrightarrow q(x))$ es verdad.
- $\forall x, (q(x) \longrightarrow r(x))$ es verdad.
- $\forall x, (p(x) \longrightarrow r(x))$ es falsa.

Pues bien, si $\forall x, (p(x) \longrightarrow r(x))$ es falsa, 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, como las proposiciones $\forall x, (p(x) \longrightarrow q(x))$ y $\forall x, (q(x) \longrightarrow r(x))$ son, ambas, verdaderas, el valor de verdad del cuantificador universal asegura que 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 lo cual, obviamente, es una contradicción. Esto significa que es falsa la suposición inicial de que el condicional era falso y, por lo tanto, el condicional es verdadero y, consecuentemente, el razonamiento es válido.

3 Utilizando el método de demostración por la contrarrecíproca (1.5.4).

Probaremos que

$$\neg\forall x, (p(x) \longrightarrow r(x)) \longrightarrow \neg\left[(\forall x, (p(x) \longrightarrow q(x))) \wedge (\forall x, (q(x) \longrightarrow r(x)))\right]$$

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 2.17, 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 opciones que pueda presentar el predicado $q(x)$ para $x = a$.

- $q(a)$ es verdad. En este caso, $q(a) \wedge \neg r(a)$ sería verdadera y habríamos encontrado, al menos, un valor de x en $\mathscr{U}$ que transforma el predicado $q(x) \wedge \neg r(x)$ en una proposición verdadera, es decir, $\exists x : (q(x) \wedge \neg r(x))$ es verdad.
- $q(a)$ es falsa. En tal caso $\neg q(a)$ sería verdadera y la proposición $p(a) \wedge \neg q(a)$ también. Hemos encontrado, pues, un valor de x en $\mathscr{U}$ que transforma el predicado $p(x) \wedge \neg q(x)$ en una proposición verdadera, es decir, $\exists x : (p(x) \wedge \neg q(x))$ es verdad.

Por lo tanto, al menos una de las dos proposiciones, $\exists x : (p(x) \wedge \neg q(x))$ o $\exists x : (q(x) \wedge \neg r(x))$ son, siempre, 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.

♦

Ejemplo 2.23

Analizar, en el universo de los estudiantes de la ESI, la validez del siguiente razonamiento:

Ningún alumno de este grupo suspendió la primera Unidad Temática.

Algún alumno suspendió la primera Unidad Temática.

Por lo tanto,

Hay, al menos, un alumno que no es de este grupo.

Solución.

Si llamamos x a un elemento genérico de $\mathscr{U}$, es decir a cualquier alumno de la ESI y consideramos los predicados,

$p(x)$: El alumno x es de este grupo.

$q(x)$: El alumno x suspendió la primera Unidad Temática.

el razonamiento propuesto escrito en lenguaje simbólico sería:

$$\forall x, (p(x) \longrightarrow \neg q(x)) \wedge \exists x : q(x) \longrightarrow \exists x : \neg p(x)$$

Como en los ejemplos anteriores, comprobaremos su validez por varios métodos.

1 Veremos, de acuerdo con la definición de razonamiento válido, que la veracidad de la conclusión se sigue de la veracidad de la hipótesis.

En efecto, si la hipótesis es verdad, entonces por el valor de verdad de la conjunción, las dos proposiciones que la conforman han de ser verdaderas, es decir,

$\forall x, (p(x) \longrightarrow \neg q(x))$ es verdad.

$\exists x : q(x)$ es verdad.

Pues bien, $\exists x : q(x)$ es verdad, entonces por el valor de verdad del cuantificador existencial, habrá, al menos, un valor de x en $\mathscr{U}$ que transforma el predicado $q(x)$ en una proposición verdadera. Si a este valor de x le llamamos a, tendremos que $q(a)$ será verdadera y $\neg q(a)$ falsa.

Por otra parte, la veracidad de la proposición $\forall x, (p(x) \longrightarrow \neg q(x))$ equivale a decir que el predicado $p(x) \longrightarrow \neg q(x)$ se transforma en una proposición verdadera para cada x de $\mathscr{U}$. En particular, esto se verificará para a, es decir la proposición $p(a) \longrightarrow \neg q(a)$ será verdadera.

Tenemos, pues, que $p(a) \longrightarrow \neg q(a)$ es verdad y $\neg q(a)$ falsa, luego por el valor de verdad del condicional, la proposición $p(a)$ ha de ser falsa y su negación, $\neg p(a)$, verdadera.

Por lo tanto, hemos encontrado, al menos, un elemento en $\mathscr{U}$ que transforma el predicado $\neg p(x)$ en una proposición verdadera, es decir, la conclusión, $\exists x : \neg p(x)$, es verdad y, consecuentemente, el razonamiento propuesto es válido.

2 Comprobamos, ahora, la validez del razonamiento utilizando el método de demostración por contradicción.

Supongamos que el condicional,

$$[\forall x, (p(x) \longrightarrow \neg q(x)) \wedge \exists x : q(x)] \longrightarrow \exists x : \neg p(x)$$

es falso. Entonces la hipótesis, $\forall x, (p(x) \longrightarrow \neg q(x)) \wedge \exists x : q(x)$, deberá ser verdadera y la conclusión, $\exists x : \neg p(x)$, falsa luego,

- $\forall x, (p(x) \longrightarrow \neg q(x))$ es verdad.
- $\exists x : q(x)$ es verdad.
- $\exists x : \neg p(x)$ es falsa.

Pues bien, si $\exists x : q(x)$ es verdadera, entonces habrá, al menos, un valor de x en $\mathscr{U}$ que transforme el predicado $q(x)$ en proposición verdadera. Si a este valor concreto de x lo llamamos a, esto significará que $q(a)$ es verdad y $\neg q(a)$ falsa.

Por otra parte, la falsedad de la proposición $\exists x : \neg p(x)$ equivale a decir que el predicado $\neg p(x)$ se transforma en proposición falsa y $p(x)$ en verdadera para cada x de $\mathscr{U}$. En particular $p(a)$ será verdadera.

Tendremos, pues, que $p(a)$ es verdad y $\neg q(a)$ es falsa y, por tanto, el condicional $p(a) \longrightarrow \neg q(a)$ será falso. Hemos encontrado un valor de x en $\mathscr{U}$ que transforma el predicado $p(x) \longrightarrow \neg q(x)$ en una proposición falsa lo cual, por el valor de verdad de una proposición universalmente cuantificada, (2.2.3), significa que $\forall x, (p(x) \longrightarrow \neg q(x))$ es falsa contradiciendo la hipótesis. La suposición hecha al principio de que el condicional era falso es falsa y, consecuentemente, dicho condicional es verdadero y el razonamiento válido.

3 Comprobamos, de nuevo, la validez del razonamiento utilizando el método de demostración por la proposición contrarrecíproca, (1.5.4).

Probaremos que

$$\neg\exists x : \neg p(x) \longrightarrow \neg\left[(\forall x, (p(x) \longrightarrow \neg q(x))) \wedge \exists x : q(x)\right]$$

es una tautología, lo cual, utilizando las leyes de De Morgan, equivale a probar que

$$\neg\exists x : \neg p(x) \longrightarrow \neg\left(\forall x, (p(x) \longrightarrow \neg q(x))\right) \vee \neg\exists x : q(x)$$

también lo es y que, a su vez, utilizando el resultado del ejemplo 2.17 y las *Leyes de DeMorgan generalizadas* equivale a probar que

$$\forall x, p(x) \longrightarrow \exists x : (p(x) \wedge q(x)) \vee \forall x, \neg q(x)$$

es una tautología.

Si $\forall x, p(x)$ es verdad, entonces $p(x)$ se transformará en una proposición verdadera para cada x de $\mathscr{U}$. Veamos que, en tal caso, la conclusión no puede ser falsa para lo cual comprobaremos que las dos proposiciones que la componen no pueden ser falsas al mismo tiempo. En efecto,

- si $\exists x : (p(x) \wedge q(x))$ fuera falsa, entonces $p(x) \wedge q(x)$ se habría de transformar en proposición falsa para cada x de $\mathscr{U}$ lo cual, por la veracidad de $\forall x, p(x)$, obligaría a que $q(x)$ se transformase en proposición falsa y $\neg q(x)$ en verdadera, también para cada x y por tanto, $\forall x, \neg q(x)$ sería verdadera.
- Si $\forall x, \neg q(x)$ fuera falsa, entonces existiría, al menos, un valor de x en $\mathscr{U}$ que transformaría el predicado $\neg q(x)$ en una proposición falsa y $q(x)$ en proposición verdadera. Para ese valor concreto de x, el predicado $p(x) \wedge q(x)$ se transformaría en proposición verdadera y, consecuentemente, la proposición $\exists x : (p(x) \wedge q(x))$ sería verdadera.

Por lo tanto, la conclusión

$$\neg \left(\forall x, (p(x) \longrightarrow \neg q(x))\right) \vee \neg \exists x : q(x)$$

será verdadera, el condicional

$$\neg \exists x : \neg p(x) \longrightarrow \neg \left(\forall x, (p(x) \longrightarrow \neg q(x))\right) \vee \neg \exists x : q(x)$$

también lo será y, como consecuencia, el razonamiento es válido.

♦♦♦

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)

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.

3.1 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.

3.1.1 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

$$a \in A$$

[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*.

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 los elementos a, b, c y d.

♦

3.1.2 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.

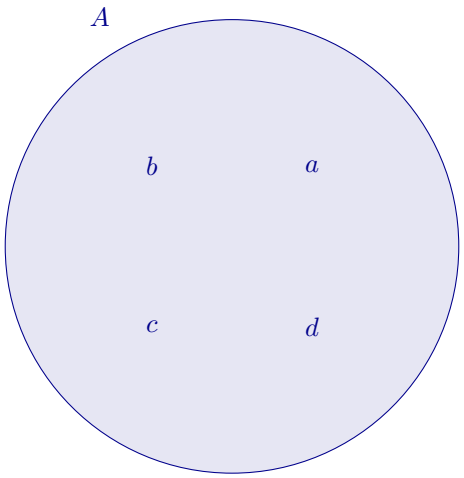


Diagrama de Venn del Conjunto $A = \{a, b, c, d\}$

♦

3.1.3 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) $A = \{n : n \in \mathbb{Z} \text{ y } 3 < n < 12\}$

(b) $B = \{n : n \text{ es un número de un dígito}\}$

(c) $B = \{n : n = 2 \text{ ó } n = 5\}$

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.

♦

3.1.4 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

Determinar 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 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.

♦

3.1.5 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 $C = \{n : n = 10q,\ q \in \mathbb{Z}\}$

♦

3.1.6 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 $\{\}$.

♦

3.1.7 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.

$A = \{n : n \text{ es par y } n^2 \text{ es impar}\}$

$B = \emptyset$

$C = \{1, 2, 3\}$

$D = \{3, 3, 2, 1, 2\}$

$E = \{n : n^3 - 6n^2 - 7n - 6 = 0\}$

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,

$$\begin{aligned}
\exists a : a \in A &\iff \begin{cases} a \text{ es par} \\ \wedge \\ a^2 \text{ es impar} \end{cases} \\
&\iff \begin{cases} a = 2q_1, \text{ con } q_1 \in \mathbb{Z} \\ \wedge \\ a^2 = 2q_2 + 1 \text{ con } q_2 \in \mathbb{Z} \end{cases} \\
&\iff \begin{cases} a^2 = 4{q_1}^2, \text{ con } q_1 \in \mathbb{Z} \\ \wedge \\ a^2 = 2q_2 + 1 \text{ con } q_2 \in \mathbb{Z} \end{cases} \\
&\implies 4{q_1}^2 = 2q_2 + 1 \\
&\iff 1 = 2\left(2{q_1}^2 - q_2\right), \text{ con } 2{q_1}^2 - q_2 \in \mathbb{Z} \\
&\implies 1 \text{ es par}
\end{aligned}$$

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 $A = B$.

⁕ $C = \{1, 2, 3\}$. Sea a cualquier número entero. Entonces,

$$\begin{aligned}
a \in C &\iff \begin{cases} a = 1 \\ \vee \\ a = 2 \\ \vee \\ a = 3 \end{cases} \\
&\iff a \in D
\end{aligned}$$

Por lo tanto,

$$\forall n, (n \in C \longleftrightarrow n \in D)$$

y por el *Axioma de Extensión*, (3.1.7), $C = D$.

⁕ $E = \{n : n^3 - 6n^2 - 7n - 6 = 0\}$. Ninguno de los divisores del término independiente, -6, satisface la ecuación, por lo tanto ningún número entero verifica la ecuación y, consecuentemente, el conjunto E es vacío, es decir, $E = B$.

♦

Ejemplo 3.8

En el conjunto de los números enteros, determinar por comprensión el conjunto formado por todos los números que den resto 5 al dividirlos entre 6 y cuyo valor absoluto sea menor 20.

Solución.

Sea A el conjunto a determinar y sea a cualquier número entero. Entonces,

$$\begin{aligned}
a \in A &\iff \exists q \in \mathbb{Z} : a = 6q+5 \text{ y } |a| < 20 \\
&\iff \exists q \in \mathbb{Z} : a = 6q+5 \text{ y } |6q+5| < 20 \\
&\left[\begin{array}{lll}
|6q+5| \leqslant 20 \iff -20 < 6q+5 < 20 & & \\
\iff 6(-4)+4 < 6q+5 < 6\cdot 3+2 & & \\
\iff 6(-4)-1 < 6q < 6\cdot 3-3 & & \\
\iff 6(-4) \leqslant 6q \leqslant 6\cdot 2 & & \\
\iff -4 \leqslant q \leqslant 2 & & \{q \in \mathbb{Z}\}
\end{array}\right] \\
&\iff a = 6q+5, \text{ con } -4 \leqslant q \leqslant 2 \\
&\iff a \in \{n : n = 6q+5,\ -4 \leqslant q \leqslant 2\}
\end{aligned}$$

Como a estaba elegido arbitrariamente en $\mathbb{Z}$, hemos probado que la proposición,

$$\forall x, (x \in A \longleftrightarrow x \in \{n : n = 6q+5,\ -4 \leqslant q \leqslant 2\})$$

es verdad, luego por el *Axioma de Extensión*, (3.1.7),

$$A = \{n : n = 6q+5,\ -4 \leqslant q \leqslant 2\}$$

♦

Ejemplo 3.9

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*, (3.1.7),

$$A = B \iff [\forall x, (x \in A \longrightarrow x \in B) \wedge \forall x, (x \in B \longrightarrow x \in A)]$$

y, negando ambos miembros,

$$\neg(A = B) \iff \neg\,[\forall x, (x \in A \longrightarrow x \in B) \wedge \forall x, (x \in B \longrightarrow x \in A)]$$

por lo tanto,

$$\begin{aligned}
A \neq B &\iff (\neg\forall x, (x \in A \longrightarrow x \in B)) \vee (\neg\forall x, (x \in B \longrightarrow x \in A)) && \{\text{DeMorgan, (1.4.3)}\} \\
&\iff (\exists x : (x \in A \wedge x \notin B)) \vee (\exists x : (x \in B \wedge x \notin A)) && \{\text{Ejemplo 2.17}\}
\end{aligned}$$

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.

♦♦♦

3.2 Inclusión de Conjuntos

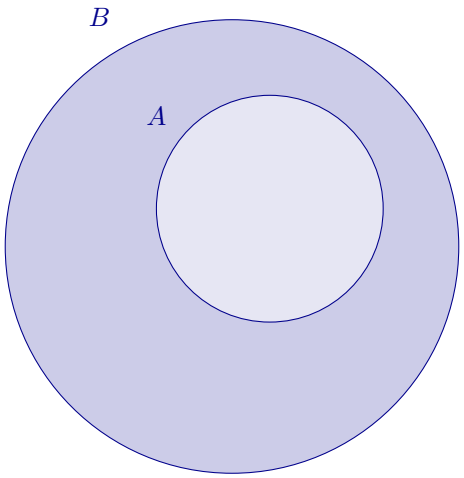
3.2.1 Subconjuntos

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 3.10

Probar que el conjunto $A = \left\{x \in \mathbb{R} : x^2 - 3x + 2 = 0\right\}$ es subconjunto de $B = \{1, 2, 3\}$

Solución.

En efecto, sea a cualquier número real. Entonces,

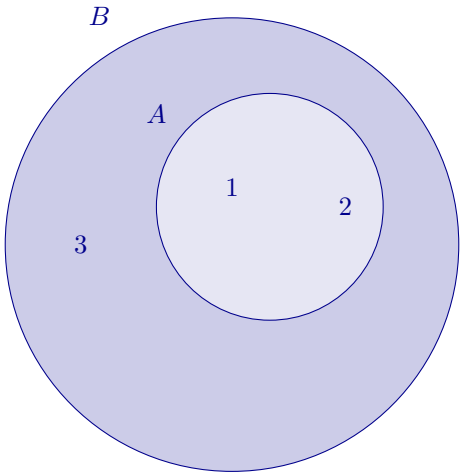
$$\begin{aligned} a \in A &\implies a^2 - 3a + 2 = 0 \\ &\implies a = \frac{3 \pm \sqrt{9 - 4 \cdot 1 \cdot 2}}{2} \\ &\implies a = \frac{3 \pm 1}{2} \\ &\implies \begin{cases} a = 1 \\ \text{ó} \\ a = 2 \end{cases} \\ &\implies a \in B \end{aligned}$$

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, (3.2.1), 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 3.11

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 3.9

$$\begin{aligned} A \nsubseteq B &\iff \neg\,(A \subseteq B) \\ &\iff \neg\,[\forall x, (x \in A \longrightarrow x \in B)] \\ &\iff \exists x : (x \in A \wedge x \notin B) \end{aligned}$$

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 3.12

¿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, $B \nsubseteq A$.

♦

3.2.2 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 3.13

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,

$$\begin{aligned} a \in A &\Longleftrightarrow a = 3q_1 + 3, \ q_1 \in \mathbb{Z}^+ \\ &\Longleftrightarrow a = 3(q_1 + 1), \ q_1 \in \mathbb{Z}^+ \\ &\Longrightarrow a = 3q, \ q \in \mathbb{Z}^+ \qquad \{\text{Tomando } q = q_1 + 1\} \\ &\Longleftrightarrow a \in B \end{aligned}$$

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, (3.2.1), 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 (3.2.2), equivale a decir que

$$A \subset B$$

o sea, A está incluido estrictamente en B.

♦

Ejemplo 3.14

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 3.9, 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 estrictamente contenido en otro es que exista inclusión y que ambos 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 3.15

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 (3.1.6).
- $\{\emptyset\}$. Conjunto con un único elemento que es el $\emptyset$.
- $\{\emptyset, \{\emptyset\}\}$. Conjunto con dos elementos, el $\emptyset$ y el $\{\emptyset\}$.

⧫

3.2.3 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, (3.1.5), 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,

$$A \subseteq \mathscr{U}$$

⧫

3.2.4 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, (3.1.6), 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 3.16

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 3.2.4 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, (3.2.1), $\{a\}$, $\{b\}$ 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 $a \nsubseteq \{a, b\}$ 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 3.17

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, 3.2.1,

$$A \subseteq B \Longleftrightarrow \forall x, (x \in A \longrightarrow x \in B)$$

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

$\emptyset \subseteq \{1,2,3\}$ (3.2.4).
$1 \in \{1,2,3\}$, 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,

$$\emptyset \text{ (3.2.4) y } \{\emptyset\} \text{ (3.2.1)}$$

(e) $\{\emptyset,\{\emptyset\}\}$. Este conjunto tiene dos elementos, $\emptyset$ y $\{\emptyset\}$, por lo tanto sus subconjuntos son

$$\emptyset \text{ (3.2.4) y } \{\emptyset\}, \{\{\emptyset\}\} \text{ y } \{\emptyset,\{\emptyset\}\} \text{ (3.2.1)}$$

(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

$$\emptyset, \{\{\emptyset,2\}\}, \{\{2\}\} \text{ y } \{\{\emptyset,2\},\{2\}\}$$

♦

3.2.5 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, (3.1.7), cada elemento de A es un elemento de B luego por definición de subconjunto, (3.2.1), $A \subseteq B$. 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, (3.1.7),

$$A = B$$

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 $B \subseteq A$.

♦

3.2.6 Corolario

De la caracterización anterior se sigue que para cualquier conjunto A, se verifica que $A \subseteq A$.

♦

3.2.7 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 3.18

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 3.9 $A \neq B$.

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, (3.1.7) 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, (3.1.7) 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.

♦♦♦

3.3 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 3.19

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:
$$\{a, b, c\}, \{a, b, d\}, \{a, b, e\}, \{a, c, d\}, \{a, c, e\}, \{a, d, e\}, \{b, c, d\}, \{b, c, e\} \text{ y } \{c, d, e\}$$

♦

3.3.1 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 3.20

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 3.21

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

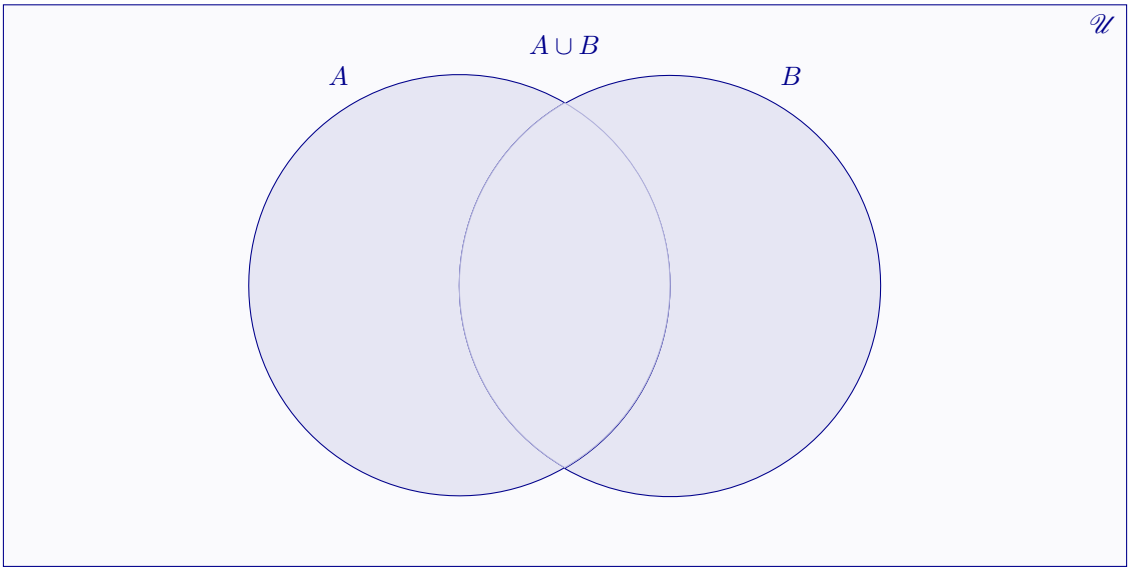
Introduciremos las operaciones con conjuntos que nos van a permitir obtener nuevos conjuntos, partiendo de conjuntos ya conocidos. A y B serán dos conjuntos cualesquiera de un universal arbitrario $\mathscr{U}$.

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,

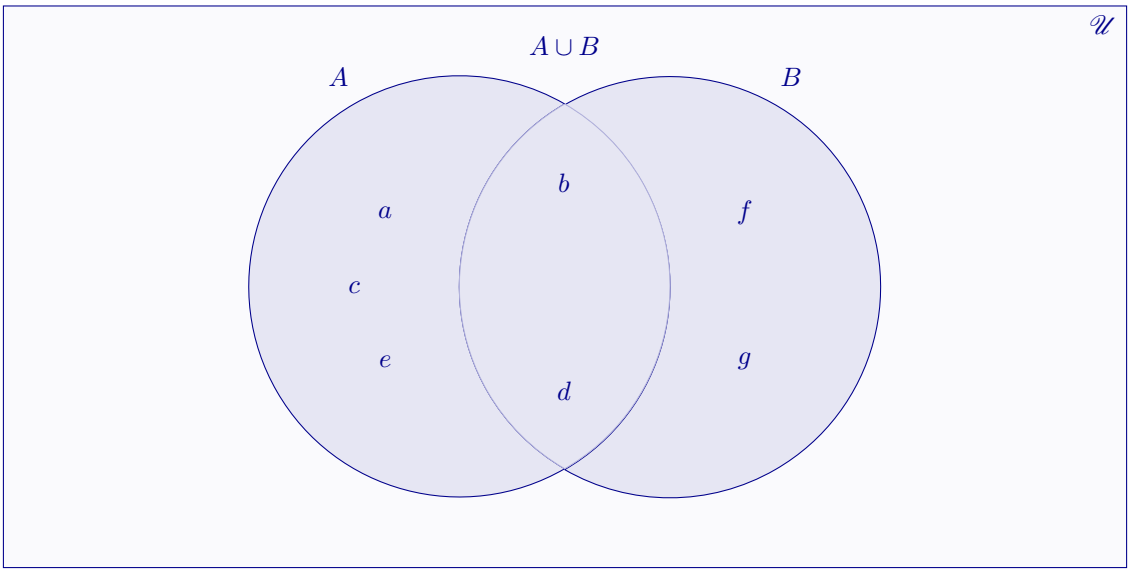
$$\begin{aligned} n \in A \cup B &\iff n \in A \text{ ó } n \in B \\ &\iff (n = a \text{ ó } n = b \text{ ó } n = c \text{ ó } n = d \text{ ó } n = e) \text{ ó } (n = b \text{ ó } n = d \text{ ó } n = f \text{ ó } n = g) \\ &\iff n = a \text{ ó } n = b \text{ ó } n = c \text{ ó } n = d \text{ ó } n = e \text{ ó } n = f \text{ ó } n = g \\ &\iff n \in \{a, b, c, d, e, f, g\} \end{aligned}$$

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, (3.1.7),

$$A \cup B = \{a, b, c, d, e, f, g\}$$



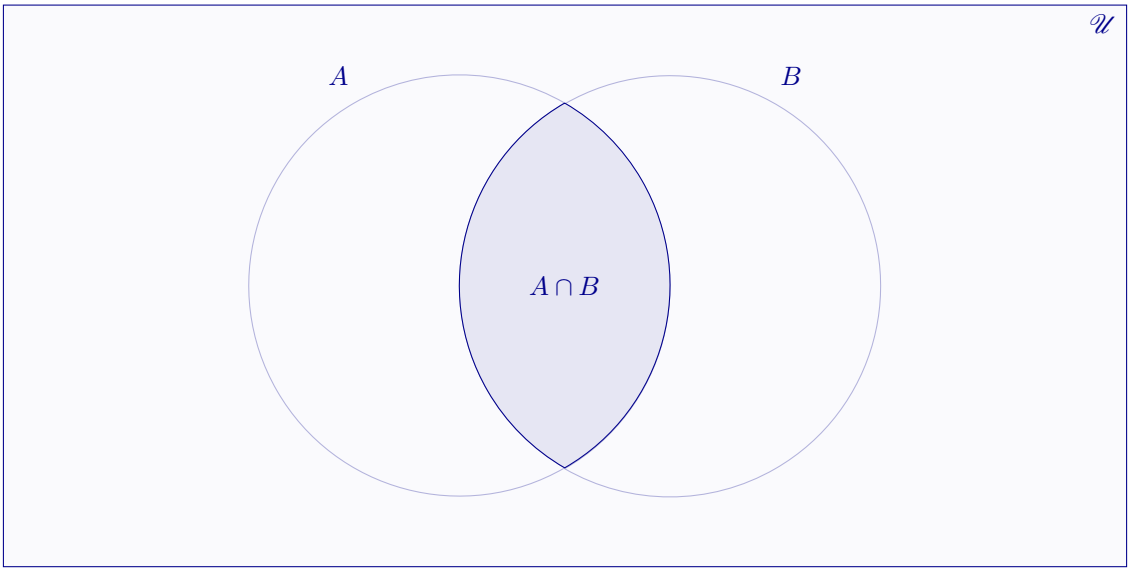
♦

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,

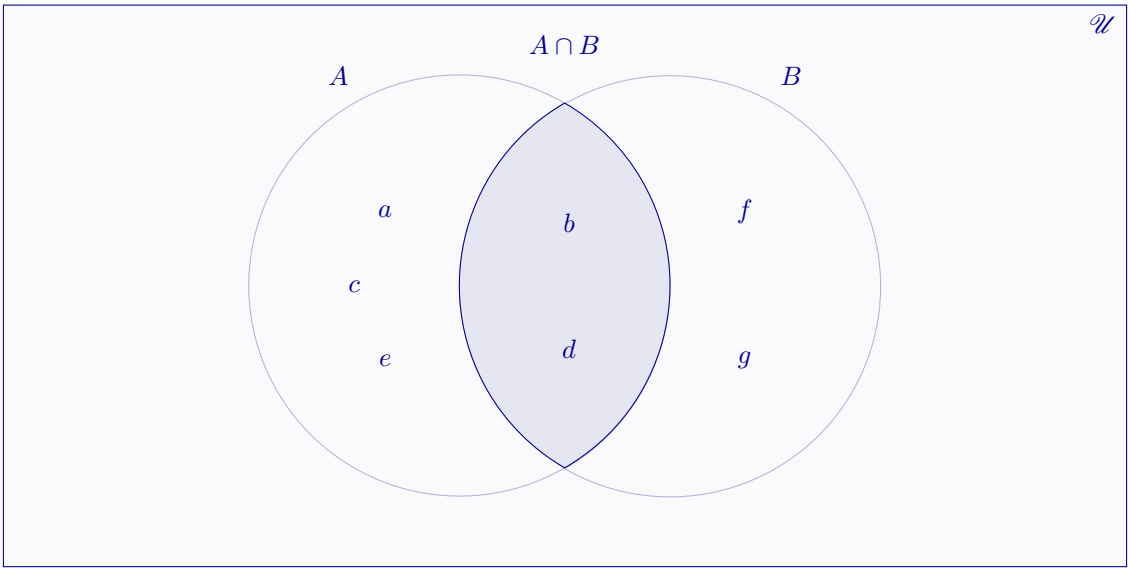
$$\begin{aligned} n \in A \cap B &\iff n \in A \text{ y } n \in B \\ &\iff n \in \{a, b, c, d, e\} \text{ y } n \in \{b, d, f, g\} \\ &\iff n = b \text{ ó } n = d \\ &\iff n \in \{b, d\} \end{aligned}$$

Como n es cualquiera del universal,

$$\forall x, (x \in A \cap B \longleftrightarrow x \in \{b, d, \})$$

y por el axioma de extensión, (3.1.7),

$$A \cap B = \{b, d\}$$



♦

4.1.3 Diferencia

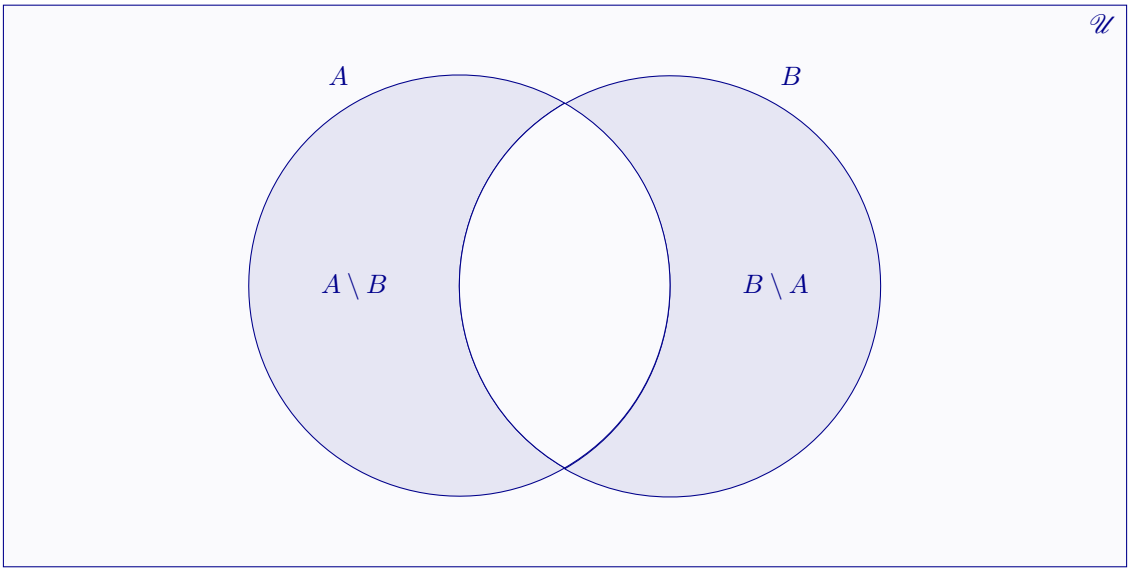
La diferencia entre dos conjuntos A y B es el conjunto formado por todos los elementos que pertenecen a A y no pertenecen a B. Se nota por $A \setminus B$.

$$A \setminus B = \{x : x \in A \text{ y } x \notin B\}$$

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, (3.1.7),

$$A \setminus B = \{a, c, e\}$$

Análogamente, sea t un elemento arbitrario del universal que contiene ambos conjuntos. Por la definición de diferencia,

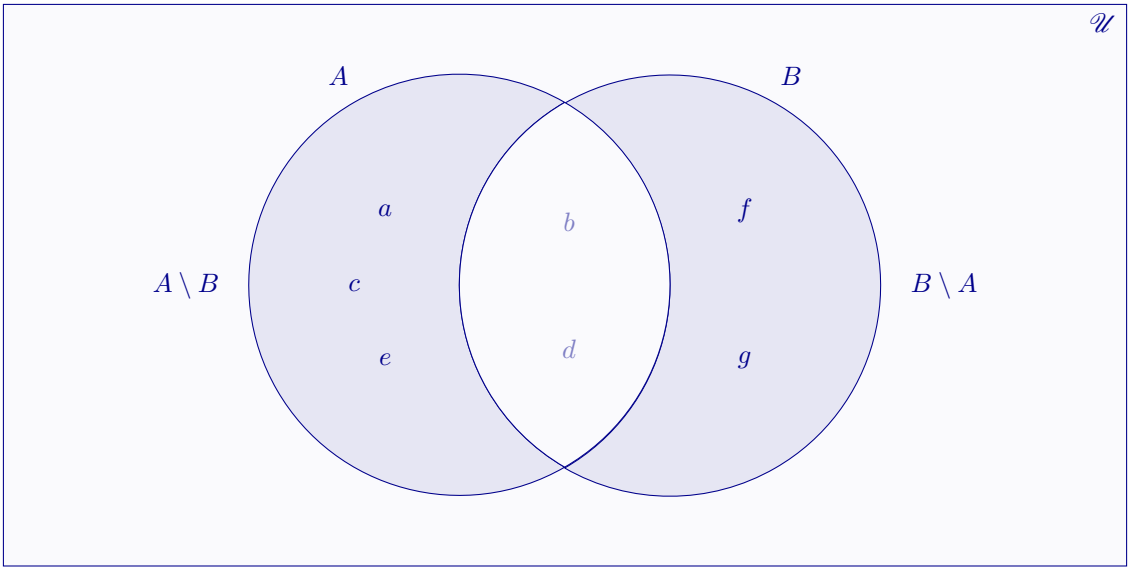
$$\begin{aligned} t \in B \setminus A &\iff t \in B \text{ y } x \notin A \\ &\iff t \in \{b, d, f, g\} \text{ y } t \notin \{a, b, c, d, e\} \\ &\iff t = f \text{ ó } t = g \\ &\iff t \in \{f, g\} \end{aligned}$$

Por lo tanto,

$$\forall x, (x \in B \setminus A \longleftrightarrow x \in \{f, g\})$$

y por el axioma de extensión, (3.1.7),

$$B \setminus A = \{f, g\}$$



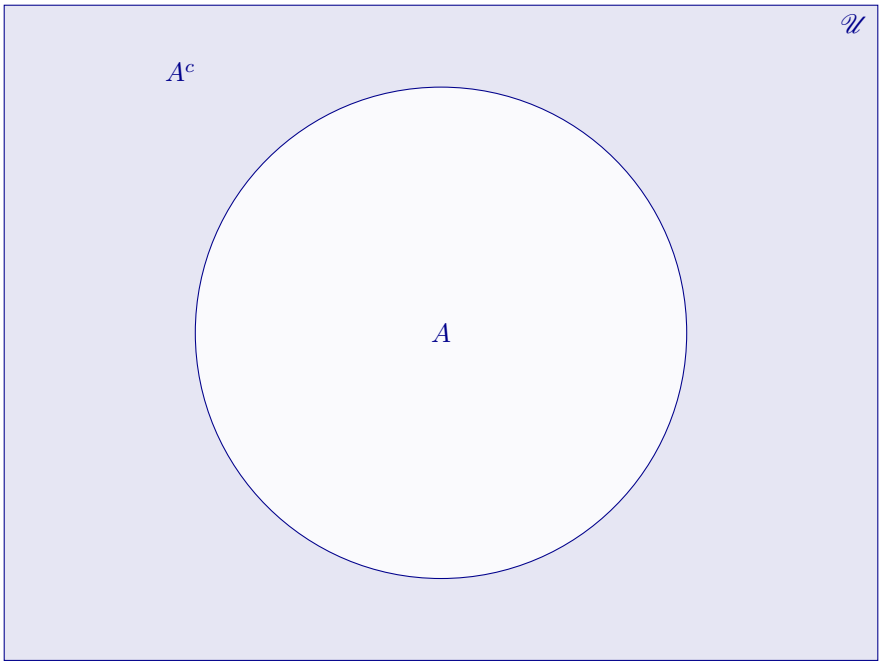
♦

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,

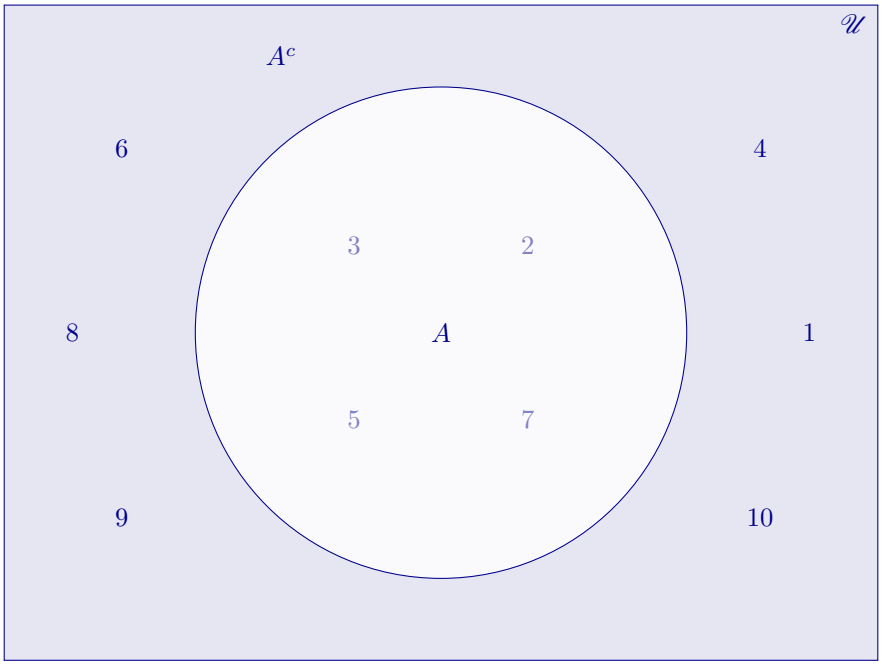
$$\begin{aligned}
a \in A^c &\iff a \in \mathscr{U} \text{ y } a \notin A \\
&\iff a \leqslant 10 \text{ y } a \text{ no es primo} \\
&\iff a \leqslant 10 \text{ y } a \neq 2 \text{ y } a \neq 3 \text{ y } a \neq 5 \text{ y } a \neq 7 \\
&\iff a = 1 \text{ ó } a = 4 \text{ ó } a = 6 \text{ ó } a = 8 \text{ ó } a = 9 \text{ ó } a = 10 \\
&\iff a \in \{1, 4, 6, 8, 9, 10\}
\end{aligned}$$

Por lo tanto,

$$\forall n, (n \in A^c \longleftrightarrow n \in \{1, 4, 6, 8, 9, 10\})$$

y por el axioma de extensión, (3.1.7),

$$A^c = \{1, 4, 6, 8, 9, 10\}$$



♦

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 $A \triangle B$.

$$A \triangle B = \{x : x \in (A \cup B) \ \wedge \ x \notin (A \cap B)\}$$

♦

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:

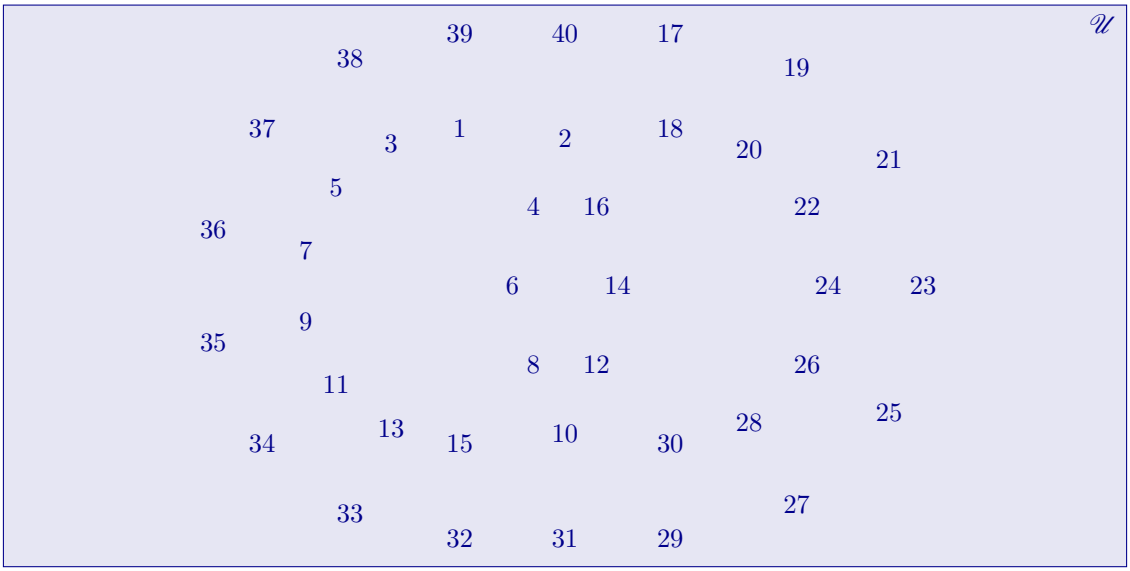
A: Conjunto formado por todos los números menores o iguales que 16.

B: Conjunto formado por todos los números pares menores o iguales que 30.

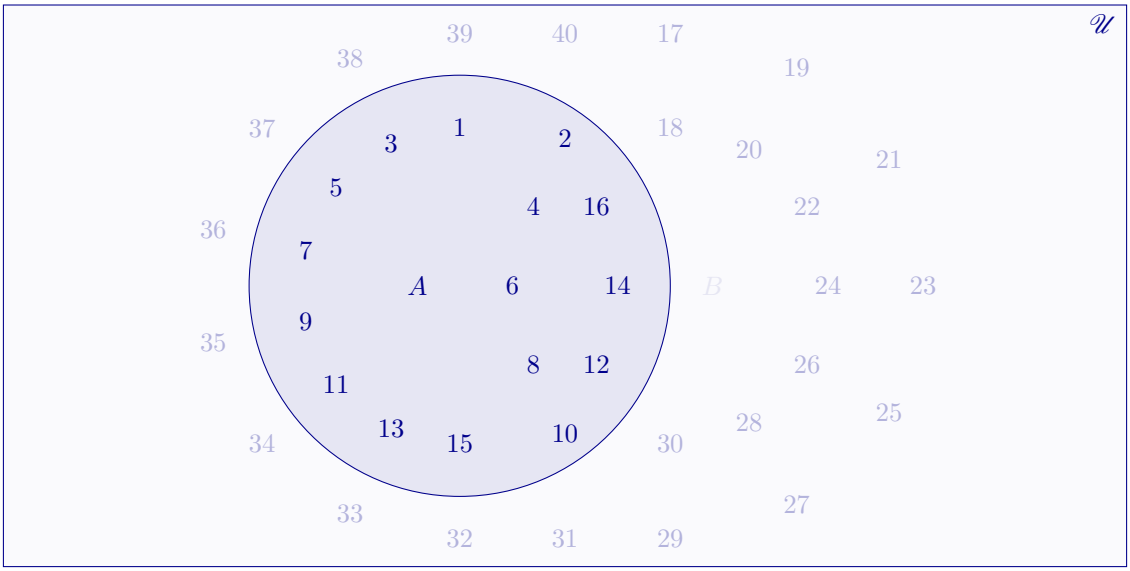
Representar gráficamente, $\mathscr{U}$, A y B y calcular $A \cup B$, $A \cap B$, $A \setminus B$, $B \setminus A$, A^c, B^c dibujando, además, sus correspondientes representaciones gráficas.

Solución.

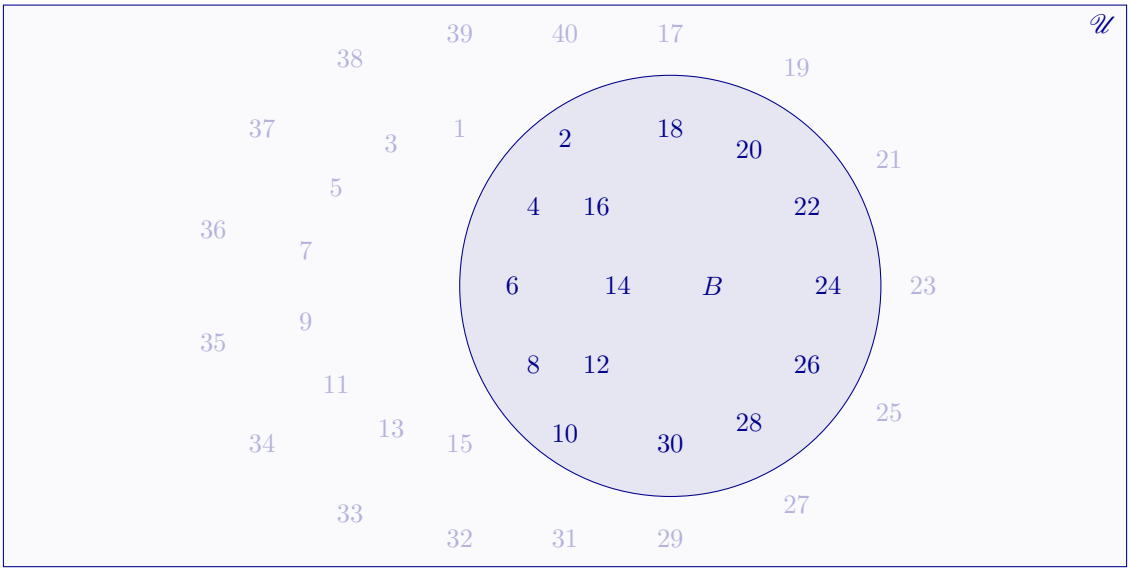
$\mathscr{U} = \{n \in \mathbb{Z}^+ : n \leqslant 40\}$



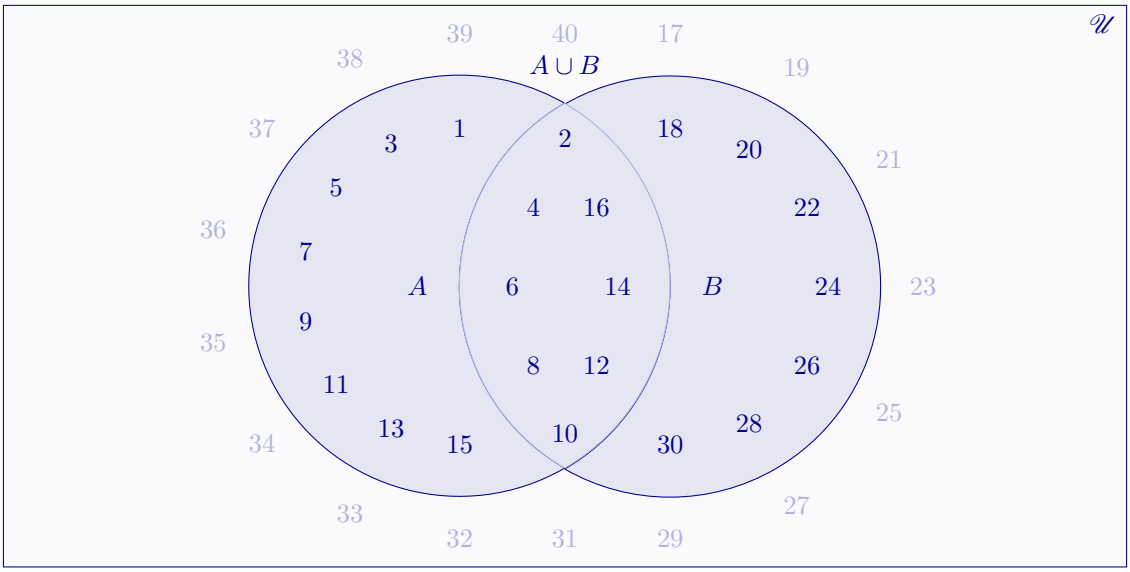
$A = \{n : n \leqslant 16\} = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16\}$



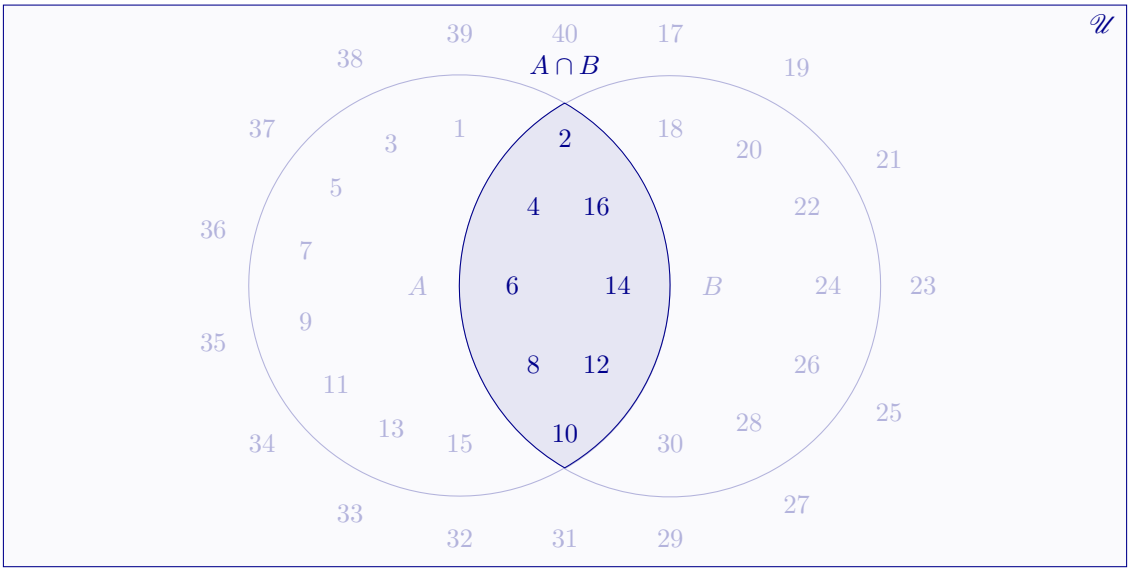
$B = \{n : n = 2q \text{ y } q \leqslant 15\} = \{2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30\}$



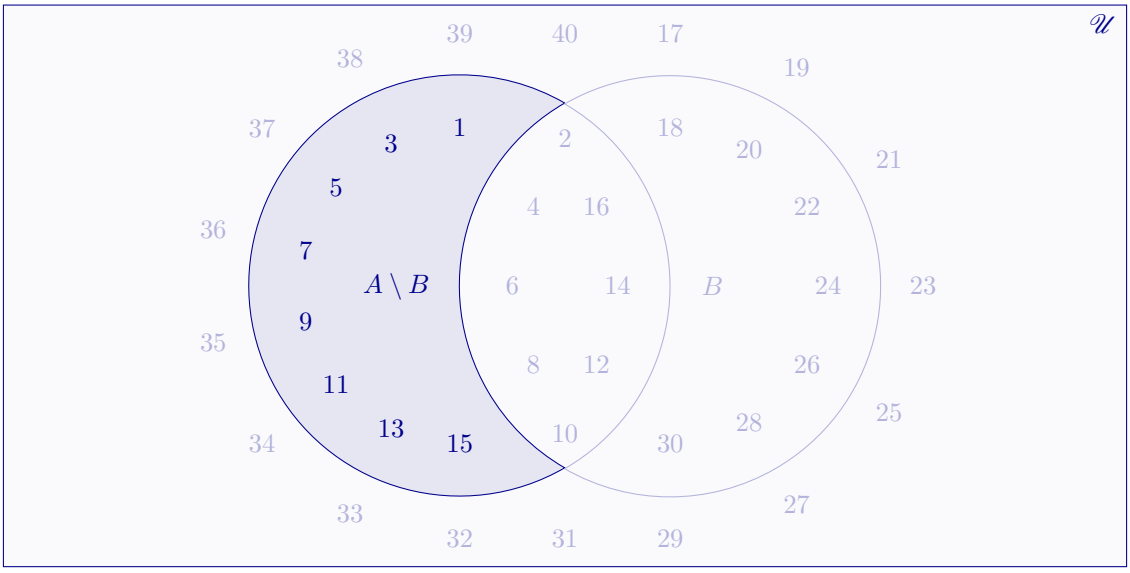
$$\begin{aligned} A \cup B &= \{n : n \leqslant 16\} \cup \{n : n = 2q \text{ y } q \leqslant 15\} \\ &= \{1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16\} \cup \{2,4,6,8,10,12,14,16,18,20,22,24,26,28,30\} \\ &= \{1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,18,20,22,24,26,28,30\} \end{aligned}$$



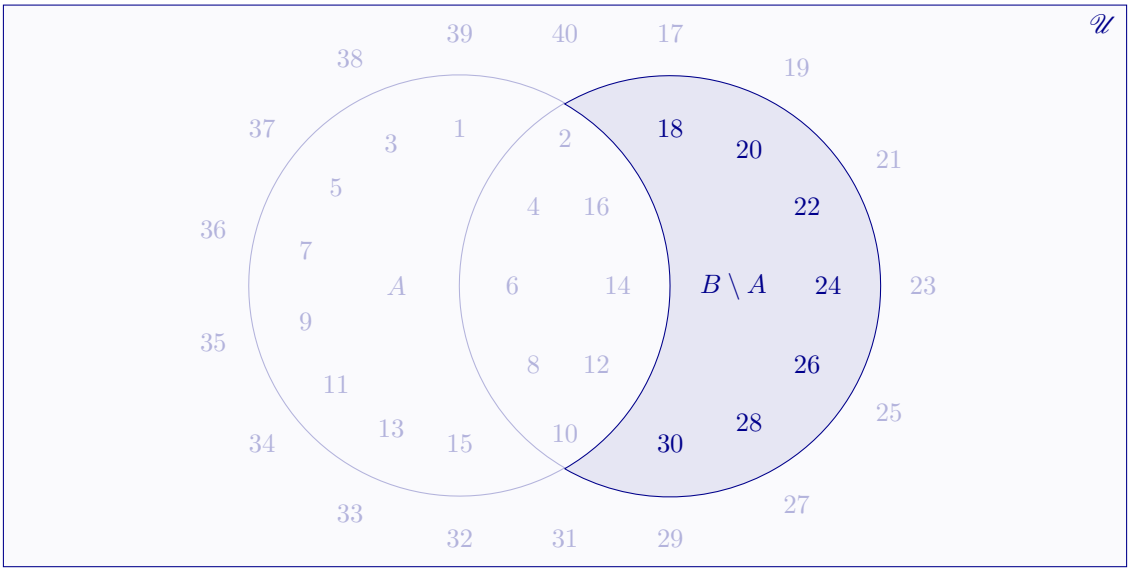
$$\begin{aligned} A \cap B &= \{n : n \leqslant 16\} \cap \{n : n = 2q \text{ y } n \leqslant 15\} \\ &= \{1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16\} \cap \{2,4,6,8,10,12,14,16,18,20,22,24,26,28,30\} \\ &= \{2,4,6,8,10,12,14,16\} \end{aligned}$$



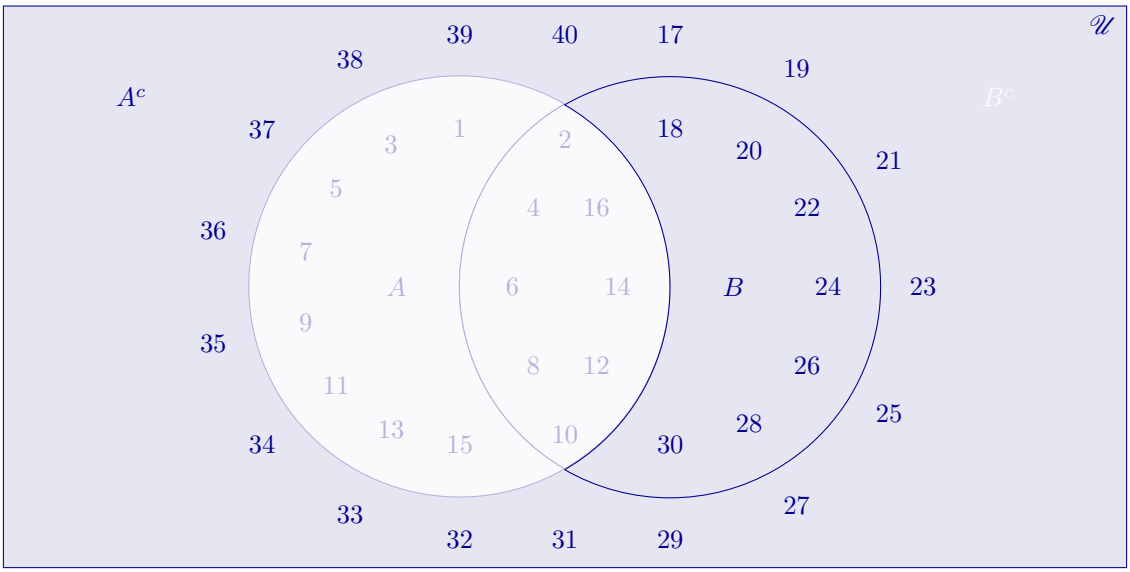
$$
\begin{aligned}
A \setminus B &= \{n : n \in A \text{ y } n \notin B\} \\
&= \{n : n \leqslant 16 \text{ y } (n = 2q+1 \text{ o } n > 30)\} \\
&= \{n : (n \leqslant 16 \text{ y } n = 2q+1) \text{ ó } (n \leqslant 16 \text{ y } n > 30)\} \\
&= \{n : n \leqslant 16 \text{ y } n = 2q+1\} \\
&= \{n : n = 2q+1 \text{ y } q \leqslant 7\} \\
&= \{1, 3, 5, 7, 9, 11, 13, 15\}
\end{aligned}
$$



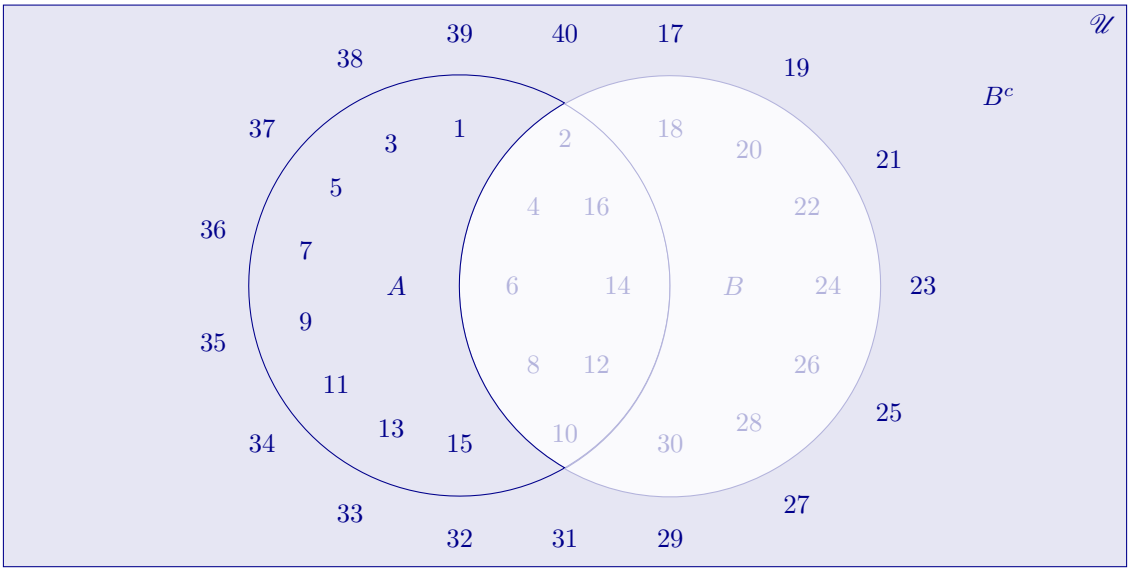
$$
\begin{aligned}
B \setminus A &= \{n : n \in B \text{ y } n \notin A\} \\
&= \{n : n = 2q \text{ y } n \leqslant 30 \text{ y } n > 16\} \\
&= \{n : n = 2q \text{ y } 16 < n \leqslant 30\} \\
&= \{n : n = 2q \text{ y } 16 < 2q \leqslant 30\} \\
&= \{n : n = 2q \text{ y } 8 < q \leqslant 15\} \\
&= \{18, 20, 22, 24, 26, 28, 30\}
\end{aligned}
$$



$$
\begin{aligned}
A^c &= \{n : n \notin A\} \\
&= \{n : n > 16\} \\
&= \{17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40\}
\end{aligned}
$$



$$
\begin{aligned}
B^c &= \{n : n \notin B\} \\
&= \{n : \neg\,(n \text{ es par y } n \leqslant 30)\} \\
&= \{n : \neg\,(n \text{ es par}) \text{ ó } \neg\,(n \leqslant 30)\} \\
&= \{n : n \text{ no es par ó } n > 30\} \\
&= \{n : n \text{ es impar ó } n > 30\} \\
&= \{1, 3, 5, 7, 9, 11, 13, 15, 17, 19, 21, 23, 25, 27, 29, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40\}
\end{aligned}
$$



♦♦♦

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, (3.1.7),

   $$A \cup A = A$$

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, (3.1.7), 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, (3.1.7), 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.

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, (3.1.7),

$$A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$$

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,

$$\begin{aligned}
a \in (A \cup \mathscr{U}) &\iff a \in A \text{ ó } a \in \mathscr{U} && \{\text{Definición de unión}\}\\
&\iff a \in \mathscr{U} \text{ ó } a \in \mathscr{U} && \{A \subseteq \mathscr{U} \text{ (3.2.3)}\}\\
&\iff a \in \mathscr{U} && \{\text{Idempotencia de la unión, (4.2.1)}\}
\end{aligned}$$

   luego,

$$\forall x, [x \in (A \cup \mathscr{U}) \longleftrightarrow x \in \mathscr{U}]$$

   de aquí que por el axioma de extensión, (3.1.7),

$$A \cup \mathscr{U} = \mathscr{U}$$

2. $A \cap \emptyset = \emptyset$. En efecto, sea a cualquiera de $\mathscr{U}$. Entonces,

$$\begin{aligned} a \in (A \cap \emptyset) &\iff a \in A \text{ y } a \in \emptyset && \{\text{Definición de intersección}\} \\ &\iff a \in \emptyset && \{a \in \emptyset \text{ es falso siempre. (1.4.3)}\} \end{aligned}$$

luego,

$$\forall x, [x \in (A \cap \emptyset) \longleftrightarrow x \in \emptyset]$$

de aquí que por el axioma de extensión, (3.1.7),

$$A \cap \emptyset = \emptyset$$

♦

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,

$$\begin{aligned} a \in (A \cup \emptyset) &\iff a \in A \text{ ó } a \in \emptyset && \{\text{Definición de unión}\} \\ &\iff a \in A \text{ ó } a \in A && \{\emptyset \subseteq A \text{ (3.2.4)}\} \\ &\iff a \in A \cup A && \{\text{Definición de unión}\} \\ &\iff a \in A && \{\text{Idempotencia de la unión, (4.2.1)}\} \end{aligned}$$

luego,

$$\forall x, [x \in (A \cup \emptyset) \longleftrightarrow x \in A]$$

de aquí que por el axioma de extensión, (3.1.7),

$$A \cup \emptyset = A$$

2. $A \cap \mathscr{U} = A$. En efecto, sea a cualquiera de $\mathscr{U}$. Entonces,

$$\begin{aligned} a \in (A \cap \mathscr{U}) &\iff a \in A \text{ y } a \in \mathscr{U} && \{\text{Definición de intersección}\} \\ &\iff a \in A && \{a \in \mathscr{U} \text{ es verdad siempre. (1.4.3)}\} \end{aligned}$$

luego,

$$\forall x, [x \in (A \cap \mathscr{U}) \longleftrightarrow x \in A]$$

de aquí que por el axioma de extensión, (3.1.7),

$$A \cap \mathscr{U} = A$$

♦

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,

$$\begin{array}{rcll} a \in (A^c)^c & \iff & a \notin A^c & \{\text{Definición de complementario}\} \\ & \iff & \neg\,(a \in A^c) & \{\text{Negación}\} \\ & \iff & \neg\,(a \notin A) & \{\text{Definición de complementario}\} \\ & \iff & \neg\neg\,(a \in A) & \{\text{Negación}\} \\ & \iff & a \in A & \{\text{Doble negación (1.4.3)}\} \end{array}$$

luego,

$$\forall x, [x \in (A^c)^c \longleftrightarrow x \in A]$$

de aquí que por el axioma de extensión, (3.1.7),

$$(A^c)^c = A$$

♦

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,

$$\begin{array}{rcll} a \in (A \cup A^c) & \iff & a \in A \text{ ó } a \in A^c & \{\text{Definición de unión}\} \\ & \iff & a \in A \text{ ó } a \notin A & \{\text{Complementario}\} \\ & \iff & a \in A \text{ ó } \neg\,(a \in A) & \{\text{Negación (1.2.3)}\} \\ & \iff & a \in \mathscr{U} & \{\text{Tautología (1.2.4)}\} \end{array}$$

   luego,

$$\forall x, [x \in (A \cup A^c) \longleftrightarrow x \in \mathscr{U}]$$

   de aquí que por el axioma de extensión, (3.1.7),

$$A \cup A^c = \mathscr{U}$$

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,
$$\begin{aligned} a \in (A \cup B)^c &\iff a \notin (A \cup B) && \{\text{Definición de complementario}\} \\ &\iff \neg\,[a \in (A \cup B)] && \{\text{Negación (1.2.3)}\} \\ &\iff \neg\,(a \in A \text{ ó } a \in B) && \{\text{Definición de unión}\} \\ &\iff \neg\,(a \in A) \text{ y } \neg\,(a \in B) && \{\text{De Morgan (1.4.3)}\} \\ &\iff a \notin A \text{ y } a \notin B && \{\text{Negación (1.2.3)}\} \\ &\iff a \in A^c \text{ y } a \in B^c && \{\text{Definición de complementario}\} \\ &\iff a \in (A^c \cap B^c) && \{\text{Definición de intersección}\} \end{aligned}$$
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, (3.1.7),
$$(A \cup B)^c = A^c \cap B^c$$

2. $(A \cap B)^c = A^c \cup B^c$. En efecto, sea a un elemento arbitrario del conjunto universal $\mathscr{U}$. Entonces,
$$\begin{aligned} a \in (A \cap B)^c &\iff a \notin (A \cap B) && \{\text{Definición de complementario}\} \\ &\iff \neg\,[a \in (A \cap B)] && \{\text{Negación (1.2.3)}\} \\ &\iff \neg\,(a \in A \text{ y } a \in B) && \{\text{Definición de intersección}\} \\ &\iff \neg\,(a \in A) \text{ ó } \neg\,(a \in B) && \{\text{De Morgan (1.4.3)}\} \\ &\iff a \notin A \text{ ó } a \notin B && \{\text{Negación (1.2.3)}\} \\ &\iff a \in A^c \text{ ó } a \in B^c && \{\text{Definición de complementario}\} \\ &\iff a \in (A^c \cup B^c) && \{\text{Definición de unión}\} \end{aligned}$$

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, (3.1.7),

$$(A \cap B)^c = A^c \cup B^c$$

♦

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 $\mathscr{U}$,

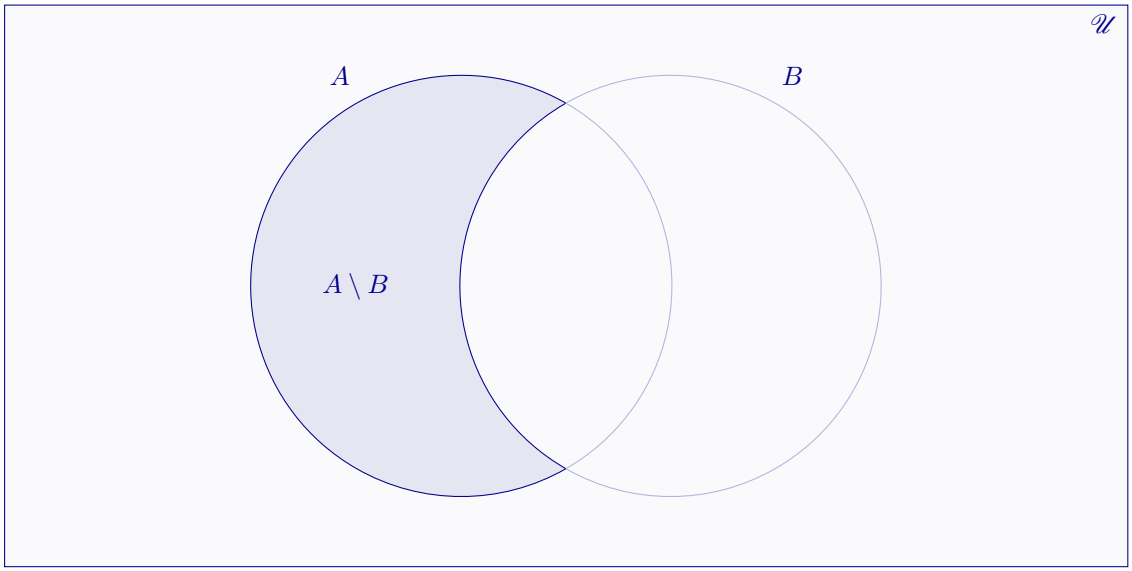
$$\begin{aligned} a \in A \setminus B &\iff a \in A \text{ y } a \notin B \quad \{\text{Definición de diferencia}\} \\ &\implies a \in A \end{aligned}$$

luego,

$$\forall x, [x \in A \setminus B \longrightarrow x \in A]$$

consecuentemente, y por definición de subconjunto (3.2.1),

$$A \setminus B \subseteq A$$



(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

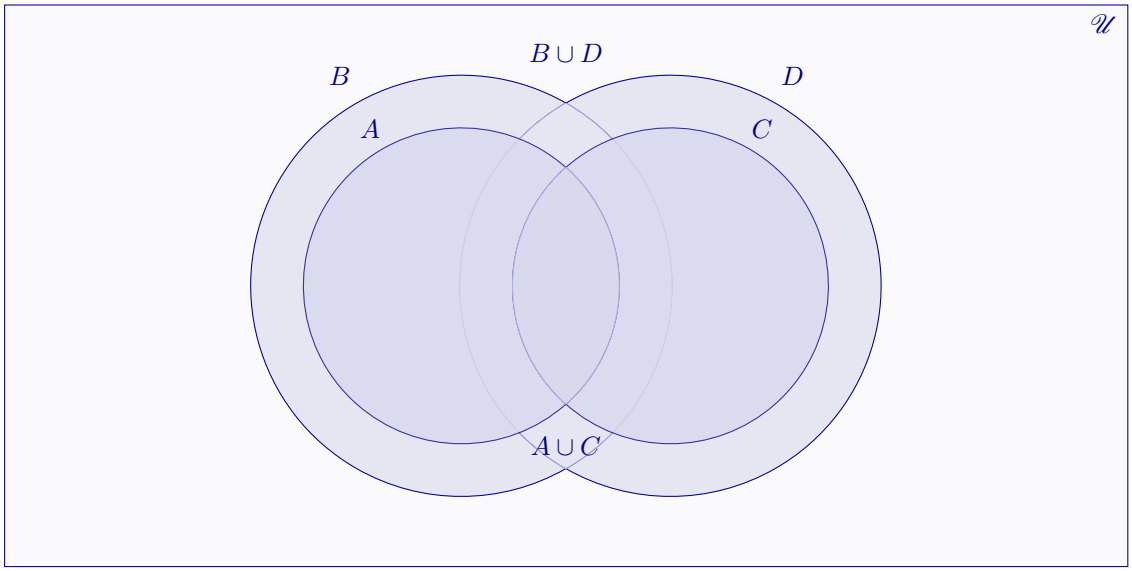
$$\begin{aligned} a \in A \cup C &\iff a \in A \text{ ó } a \in C && \{\text{Definición de unión}\} \\ &\implies a \in B \text{ ó } a \in D && \{\text{Hipótesis } A \subseteq B,\ C \subseteq D\} \\ &\iff a \in (B \cup D) && \{\text{Definición de unión}\} \end{aligned}$$

luego,

$$\forall x, [x \in (A \cup C) \longrightarrow x \in (B \cup D)]$$

por lo tanto, la definición de subconjunto, (3.2.1), 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

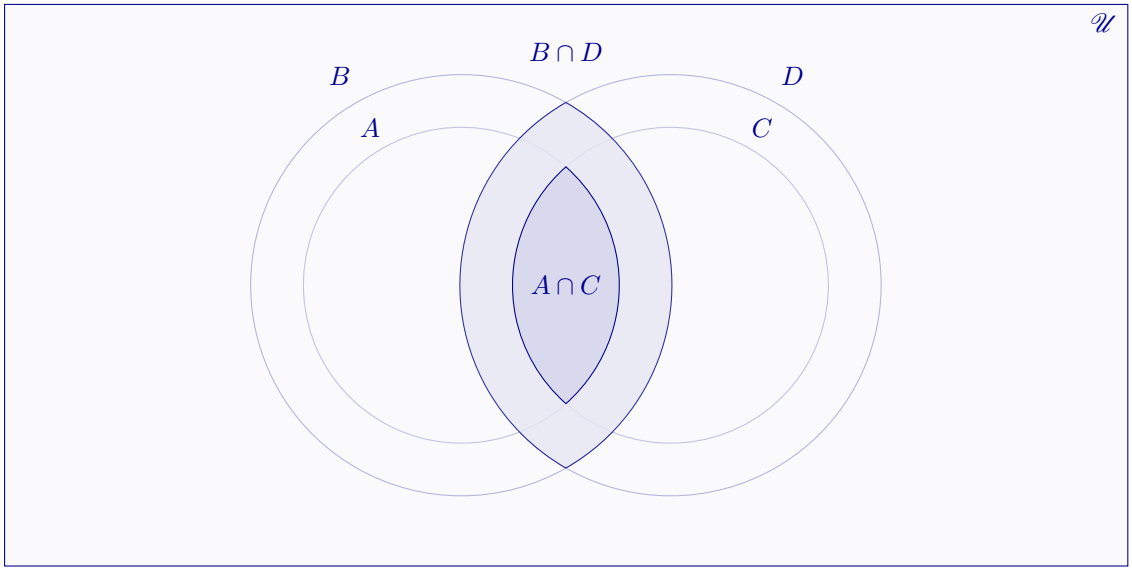
$$\begin{aligned} a \in A \cap C &\iff a \in A \text{ y } a \in C && \{\text{Definición de intersección}\} \\ &\implies a \in B \text{ y } a \in D && \{\text{Hipótesis } A \subseteq B,\ C \subseteq D\} \\ &\iff a \in (B \cap D) && \{\text{Definición de intersección}\} \end{aligned}$$

luego,

$$\forall x, [x \in (A \cap C) \longrightarrow x \in (B \cap D)]$$

por lo tanto, la definición de subconjunto, (3.2.1), 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,

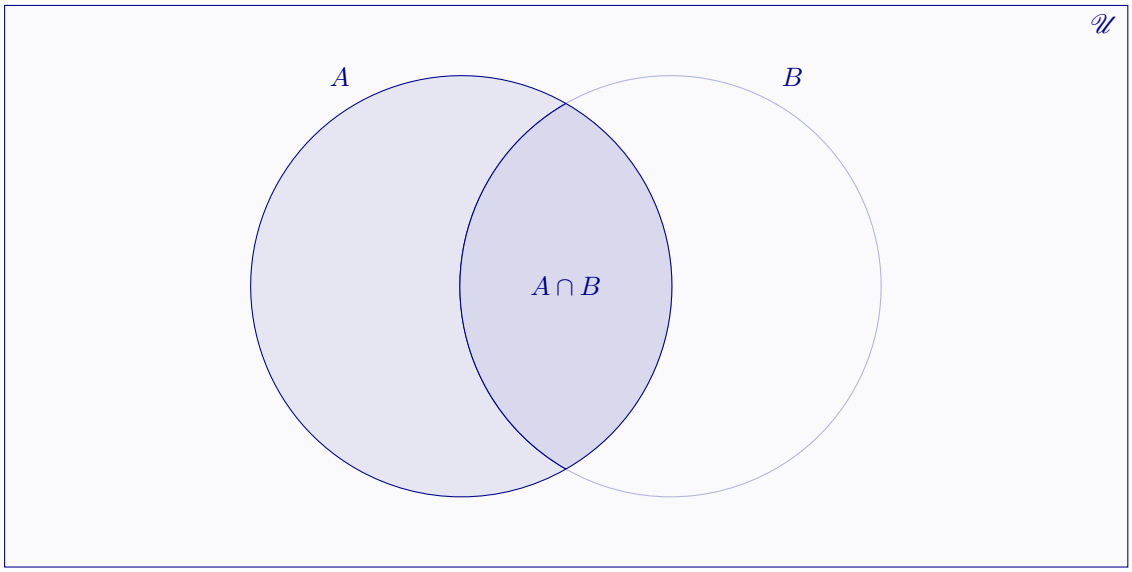
$$\begin{aligned} a \in A \cap B &\iff a \in A \text{ y } a \in B \quad \{\text{Definición de intersección}\} \\ &\implies a \in A \end{aligned}$$

luego por definición de subconjunto, (3.2.1),

$$\forall x, [x \in (A \cap B) \longrightarrow x \in A]$$

de donde se sigue

$$A \cap B \subseteq A$$



(e) $A \setminus \emptyset = A$

Sea a cualquiera de $\mathscr{U}$. Entonces,

$$\begin{aligned} a \in A \setminus \emptyset &\iff a \in A \text{ y } a \notin \emptyset && \{\text{Definición de diferencia}\} \\ &\iff a \in A && \{a \notin \emptyset \text{ es verdad siempre}\} \end{aligned}$$

luego,

$$\forall x, [x \in A \setminus \emptyset \longleftrightarrow x \in A]$$

de aquí que por el axioma de extensión, (3.1.7),

$$A \setminus \emptyset = A$$

(f) $A \setminus B = A \cap B^c$

En efecto, sea a cualquiera del conjunto universal $\mathscr{U}$. Entonces,

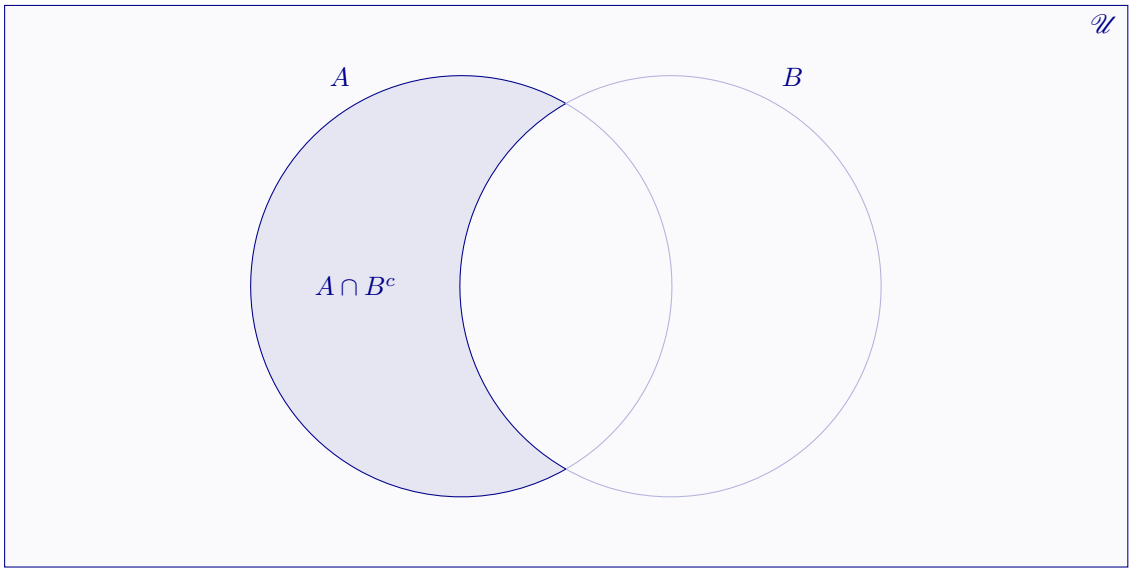
$$\begin{aligned} a \in A \setminus B &\iff a \in A \text{ y } a \notin B && \{\text{Definición de diferencia}\} \\ &\iff a \in A \text{ y } a \in B^c && \{\text{Definición de complementario}\} \\ &\iff a \in (A \cap B^c) && \{\text{Definición de intersección}\} \end{aligned}$$

luego,

$$\forall x, [x \in A \setminus B \iff x \in (A \cap B^c)]$$

de aquí que por el axioma de extensión, (3.1.7),

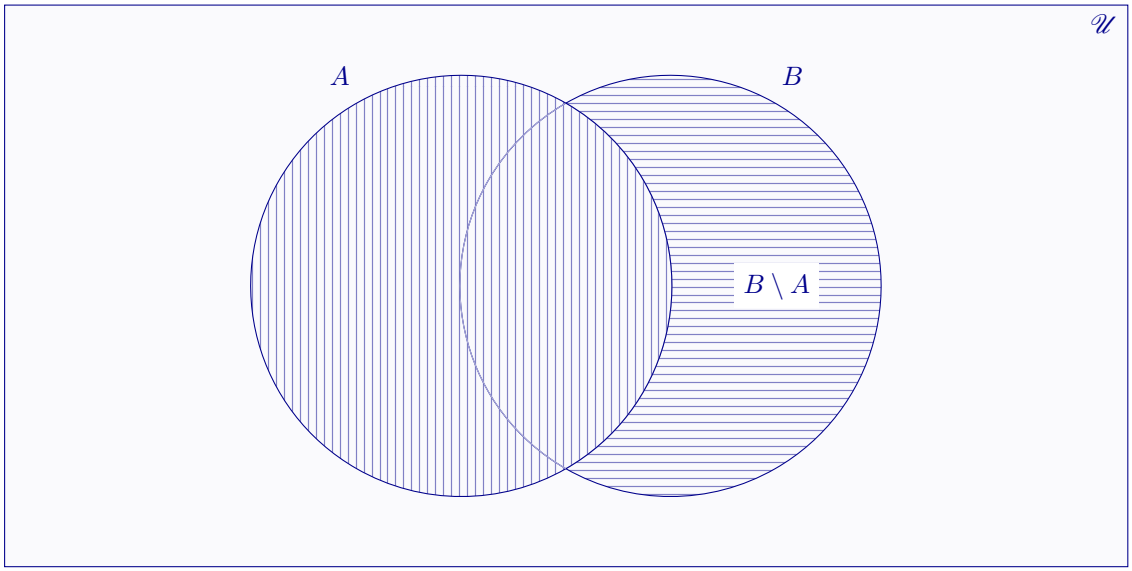
$$A \setminus B = A \cap B^c$$



(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) $(A \setminus B) \cup (A \cap B) \cup (B \setminus A) = A \cup B$

$$\begin{aligned} (A \setminus B) \cup (A \cap B) \cup (B \setminus A) &= (A \cap B^c) \cup (A \cap B) \cup (B \cap A^c) && \{\text{Diferencia (4.1.3)}\} \\ &= [A \cap (B^c \cup B)] \cup (B \cap A^c) && \{\text{Leyes distributivas (4.2.4)}\} \\ &= (A \cap \mathscr{U}) \cup (B \cap A^c) && \{\text{Leyes complementario (4.2.8)}\} \\ &= A \cup (B \cap A^c) && \{\text{Leyes de identidad (4.2.6)}\} \\ &= (A \cup B) \cap (A \cup A^c) && \{\text{Leyes distributivas (4.2.4)}\} \\ &= (A \cup B) \cap \mathscr{U} && \{\text{Leyes complementario (4.2.8)}\} \\ &= A \cup B && \{\text{Leyes de identidad (4.2.6)}\} \end{aligned}$$

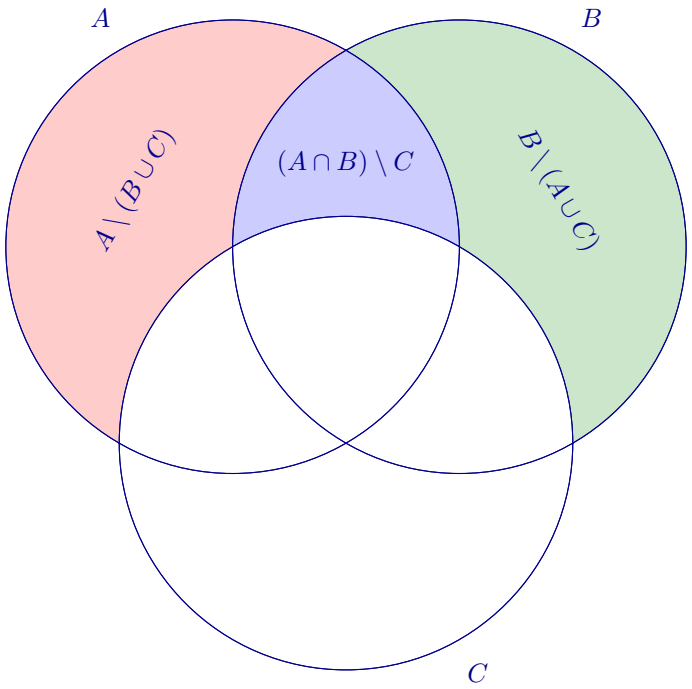
♦

Ejemplo 4.7

Probar que

$$[A \setminus (B \cup C)] \cup [(A \cap B) \setminus C] \cup [B \setminus (A \cup C)] = (A \cup B) \setminus C$$

Solución.



En efecto, utilizando las leyes del Álgebra de conjuntos,

$$
\begin{aligned}
&[A \setminus (B \cup C)] \cup [(A \cap B) \setminus C] \cup [B \setminus (A \cup C)] \\
&= \\
&[A \cap (B \cup C)^c] \cup (A \cap B \cap C^c) \cup [B \cap (A \cup C)^c] && \{\text{Diferencia (4.1.3)}\} \\
&= \\
&(A \cap B^c \cap C^c) \cup (A \cap B \cap C^c) \cup (B \cap A^c \cap C^c) && \{\text{Leyes de De Morgan (4.2.9}\} \\
&= \\
&[(A \cap C^c) \cap (B^c \cup B)] \cup (B \cap A^c \cap C^c) && \{\text{Leyes distributivas (4.2.4)}\} \\
&= \\
&(A \cap C^c \cap \mathscr{U}) \cup (B \cap A^c \cap C^c) && \{\text{Leyes del complementario (4.2.8)}\} \\
&= \\
&(A \cap C^c) \cup (B \cap A^c \cap C^c) && \{\text{Leyes de identidad (4.2.6)}\} \\
&= \\
&C^c \cap [A \cup (A^c \cap B)] && \{\text{Leyes distributivas (4.2.4)}\} \\
&= \\
&C^c \cap [(A \cup A^c) \cap (A \cup B)] && \{\text{Leyes del distributivas (4.2.4)}\} \\
&= \\
&C^c \cap [\mathscr{U} \cap (A \cup B)] && \{\text{Leyes complementario (4.2.8)}\} \\
&= \\
&C^c \cap (A \cup B) && \{\text{Leyes de identidad (4.2.6)}\} \\
&= \\
&(A \cup B) \setminus C && \{\text{Diferencia (4.1.3)}\}
\end{aligned}
$$

♦♦♦

4.3 Partición de un conjunto

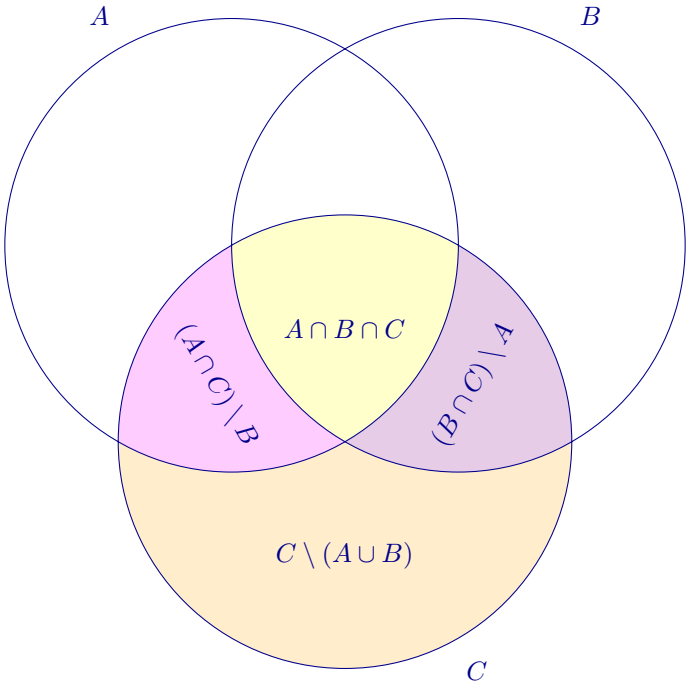
4.3.1 Definición

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 4.8

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 4.9

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 distinto de 3 al dividirlo entre 6.

Solución.

$A=\{n : n=2q,\ q\in\mathbb{Z}\}$ y $B=\{n : n=3q,\ q\in\mathbb{Z}\}$

a) $A \cap B$

Sea a cualquier número entero. Entonces,

$$\begin{aligned}
a \in (A \cap B) &\iff a \in A \wedge a \in B \quad \{\text{Definición de intersección. (4.1.2)}\} \\
&\iff \begin{cases} \exists q_1 \in \mathbb{Z} : a = 2q_1 & \{\text{Definición de } A\} \\ \wedge & \\ \exists q_2 \in \mathbb{Z} : a = 3q_2 & \{\text{Definición de } B\} \end{cases} \\
&\iff \exists q \in \mathbb{Z} : a = \text{m.c.m.}(2,3) \cdot q \quad \{\text{Definición de m.c.m.}\} \\
&\iff a = 6q,\ q \in \mathbb{Z} \\
&\iff a \in \{n : n = 6q,\ q \in \mathbb{Z}\}
\end{aligned}$$

Como a era un número entero elegido de forma arbitraria, hemos probado que la proposición,

$$\forall x, (x \in (A \cap B) \longleftrightarrow x \in \{n : n = 6q,\ q \in \mathbb{Z}\})$$

es verdadera y, consecuentemente, por el axioma de extensión, (3.1.7),

$$A \cap B = \{n : n = 6q,\ q \in \mathbb{Z}\}$$

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,

$$\begin{aligned}
a \in A \setminus B &\iff \begin{cases} a \in A \\ \wedge \qquad \{\text{Definición de Diferencia. (4.1.3)}\} \\ a \notin B \end{cases} \\
&\iff \begin{cases} \exists q_1 \in \mathbb{Z} : a = 2q_1 \\ \wedge \\ \exists q_2, r_2 \in \mathbb{Z} : a = 3q_2 + r_2,\ r_2 \neq 0 \quad \{\text{T.E.U.C.R. (5.2.1)}\} \end{cases} \\
&\left\{ \begin{array}{l} \text{Dividiendo } q_1 \text{ por 3, } q_1 = 3q_3 + r_3, \text{ con } q_3, r_3 \in \mathbb{Z}, \text{ y } r_3 \in \{0,1,2\} \\ \text{Dividiendo } q_2 \text{ por 2, } q_2 = 2q_4 + r_4, \text{ con } q_4, r_4 \in \mathbb{Z}, \text{ y } r_4 \in \{0,1\} \end{array} \right\} \\
&\implies \begin{cases} a = 2(3q_3 + r_3), \text{ con } q_3, r_3 \in \mathbb{Z}, \text{ y } r_3 \in \{0,1,2\} \\ \wedge \\ a = 3(2q_4 + r_4) + r_2, \text{ con } q_4, r_4, r_2 \in \mathbb{Z}, \text{ y } r_4 \in \{0,1\} \text{ y } r_2 \in \{1,2\} \end{cases} \\
&\iff \begin{cases} a = 6q_3 + 2r_3, \text{ con } q_3, r_3 \in \mathbb{Z}, \text{ y } 2r_3 \in \{0,2,4\} \\ \wedge \\ a = 6q_4 + 3r_4 + r_2, \text{ con } q_4, r_4, r_2 \in \mathbb{Z}, \text{ y } 3r_4 + r_2 \in \{1,2,4,5\} \end{cases} \\
&\quad \{\text{Unicidad de cociente y resto (5.2.1)} \quad q_3 = q_4 \text{ y } 2r_3 = 3r_4 + r_2\} \\
&\implies \exists q, r \in \mathbb{Z} : a = 6q + r, \text{ con } r \in \{0,2,4\} \cap \{1,2,4,5\} \quad \left\{ \begin{array}{l} q = q_3 = q_4 \\ \text{y} \\ r = 2r_3 = 3r_4 + r_2 \end{array} \right\} \\
&\iff \exists q, r \in \mathbb{Z} : a = 6q + r, \text{ con } r \in \{2,4\} \\
&\iff a \in \{n : n = 6q + 2 \ \vee \ n = 6q + 4,\ q \in \mathbb{Z}\}
\end{aligned}$$

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, (3.2.1),

$$(A \setminus B) \subseteq \{n : n = 6q + 2 \ \vee \ n = 6q + 4, \ q \in \mathbb{Z}\}$$

Recíprocamente,

$$\begin{aligned}
a \in \{n : n = 6q + 2 \ \vee \ n = 6q + 4, \ q \in \mathbb{Z}\} &\iff \begin{cases} \exists q_1 \in \mathbb{Z} : a = 6q_1 + 2 \\ \vee \\ \exists q_2 \in \mathbb{Z} : a = 6q_2 + 4 \end{cases} \\
&\iff \begin{cases} \exists q_1 \in \mathbb{Z} : a = 2(3q_1 + 1) \ \wedge \ a = 3(2q_1) + 2 \\ \vee \\ \exists q_2 \in \mathbb{Z} : a = 2(3q_2 + 2) \ \wedge \ a = 3(2q_2 + 1) + 1 \end{cases} \\
&\quad \begin{cases} a \text{ da resto 0 al dividir por 2} \\ \wedge \\ a \text{ da resto 1 o 2 al dividir por 3} \end{cases} \\
&\implies \begin{cases} \exists q_3 \in \mathbb{Z} : a = 2q_3 \\ \wedge \\ \exists q_4, r \in \mathbb{Z} : a = 3q_4 + r, \ \text{con } r \neq 0 \end{cases} \\
&\iff \begin{cases} a \in A \\ \wedge \\ a \notin B \end{cases} \\
&\iff a \in (A \setminus B)
\end{aligned}$$

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, (3.2.1),

$$\{n : n = 6q + 2 \ \vee \ n = 6q + 4, \ q \in \mathbb{Z}\} \subseteq (A \setminus B)$$

Finalmente, por la doble inclusión, tendremos, (3.2.5), 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 distinto de cero al dividirlos por 6.

c) $B \setminus A$

Sea a cualquier número entero. Entonces,

$$
\begin{aligned}
a \in B \setminus A &\iff \left\{ \begin{array}{l} a \in B \\ \wedge \\ a \notin A \end{array} \right. \\
&\iff \left\{ \begin{array}{l} \exists q_1 \in \mathbb{Z} : a = 3q_1 \\ \wedge \\ \exists q_2 \in \mathbb{Z} : a = 2q_2 + 1 \end{array} \right. \\
&\quad \left\{ \begin{array}{l} \text{Dividiendo } q_1 \text{ por 2, } q_1 = 2q_3 + r_3, \text{ con } q_3, r_3 \in \mathbb{Z} \text{ y } r_3 \in \{0,1\} \\ \text{Dividiendo } q_2 \text{ por 3, } q_2 = 3q_4 + r_4, \text{ con } q_4, r_4 \in \mathbb{Z} \text{ y } r_4 = \{0,1,2\} \end{array} \right\} \\
&\implies \left\{ \begin{array}{l} \exists q_3, r_3 \in \mathbb{Z} : a = 3(2q_3 + r_3), \text{ con } r_3 \in \{0,1\} \\ \wedge \\ \exists q_4, r_4 \in \mathbb{Z} : a = 2(3q_4 + r_4) + 1, \text{ con } r_4 = \{0,1,2\} \end{array} \right. \\
&\iff \left\{ \begin{array}{l} \exists q_3, r_3 \in \mathbb{Z} : a = 6q_3 + 3r_3, \text{ con } 3r_3 \in \{0,3\} \\ \wedge \\ \exists q_4, r_4 \in \mathbb{Z} : a = 6q_4 + 2r_4 + 1, \text{ con } 2r_4 + 1 = \{1,3,5\} \end{array} \right. \\
&\quad \{\text{Unicidad de cociente y resto (5.2.1)} \quad q_3 = q_4 \text{ y } 3r_3 = 2r_4 + 1\} \\
&\implies \exists q, r \in \mathbb{Z} : a = 6q + r, \text{ con } r \in \{0,3\} \cap \{1,3,5\} \quad \left\{ \begin{array}{l} q = q_3 = q_4 \\ \text{y} \\ r = 3r_3 = 2r_4 + 1 \end{array} \right\} \\
&\implies \exists q \in \mathbb{Z} : a = 6q + 3 \\
&\iff a \in \{n : n = 6q + 3, \ q \in \mathbb{Z}\}
\end{aligned}
$$

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, (3.2.1),

$$(B \setminus A) \subseteq \{n : n = 6q + 3, \ q \in \mathbb{Z}\}$$

Recíprocamente,

$$
\begin{aligned}
a \in \{n : n = 6q + 3, \ q \in \mathbb{Z}\} &\iff \exists q_1 \in \mathbb{Z} : a = 6q_1 + 3 \\
&\iff \left\{ \begin{array}{l} \exists q_1 \in \mathbb{Z} : a = 3(2q_1 + 1) \\ \wedge \\ \exists q_1 \in \mathbb{Z} : a = 2(3q_1 + 1) + 1 \end{array} \right. \\
&\implies \left\{ \begin{array}{ll} \exists q_2 \in \mathbb{Z} : a = 3q_2 & \{\text{Tomando } q_2 = 2q_1 + 1\} \\ \wedge & \\ \exists q_3 \in \mathbb{Z} : a = 2q_3 + 1 & \{\text{Tomando } q_3 = 3q_1 + 1\} \end{array} \right. \\
&\iff \left\{ \begin{array}{l} a \in B \\ \wedge \\ a \notin A \end{array} \right. \\
&\iff a \in (B \setminus A)
\end{aligned}
$$

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, (3.2.1),

$$\{n : n = 6q + 3,\ q \in \mathbb{Z}\} \subseteq (B \setminus A)$$

Finalmente, por la doble inclusión, tendremos, (3.2.5), 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,

$$\begin{aligned}
a \in (A^c \cap B^c) &\iff \begin{cases} a \in A^c \\ \wedge \\ a \in B^c \end{cases} \\
&\iff \begin{cases} a \notin A \\ \wedge \\ a \notin B \end{cases} \\
&\iff \begin{cases} \exists q_1 \in \mathbb{Z} : a = 2q_1 + 1 \\ \wedge \\ \exists q_2, r_2 \in \mathbb{Z} : a = 3q_2 + r_2,\ \text{con } r_2 \in \{1, 2\} \end{cases} \\
&\quad \left\{ \begin{array}{l} \text{Dividiendo } q_1 \text{ por } 3,\ q_1 = 3q_3 + r_3,\ \text{con } q_3, r_3 \in \mathbb{Z} \text{ y } r_3 \in \{0, 1, 2\} \\ \text{Dividiendo } q_2 \text{ por } 2,\ q_2 = 2q_4 + r_4,\ \text{con } q_4, r_4 \in \mathbb{Z} \text{ y } r_4 \in \{0, 1\} \end{array} \right\} \\
&\implies \begin{cases} \exists q_3, r_3 \in \mathbb{Z} : a = 2(3q_3 + r_3) + 1,\ \text{con } r_3 \in \{0, 1, 2\} \\ \wedge \\ \exists q_4, r_4 \in \mathbb{Z} : a = 3(2q_4 + r_4) + r_2,\ \text{con } r_2 \in \{1, 2\}\ \text{ y } r_4 \in \{0, 1\} \end{cases} \\
&\iff \begin{cases} \exists q_3, r_3 \in \mathbb{Z} : a = 6q_3 + 2r_3 + 1,\ \text{con } 2r_3 + 1 \in \{1, 3, 5\} \\ \wedge \\ \exists q_4, r_4 \in \mathbb{Z} : a = 6q_4 + 3r_4 + r_2,\ \text{con } 3r_4 + r_2 \in \{1, 2, 4, 5\} \end{cases} \\
&\quad \{\text{Unicidad de cociente y resto (5.2.1)} \quad q_3 = q_4 \text{ y } 2r_3 + 1 = 3r_4 + r_2\} \\
&\implies \exists q, r \in \mathbb{Z} : a = 6q + r,\ \text{con } r \in \{1, 3, 5\} \cap \{1, 2, 4, 5\} \quad \left\{ \begin{array}{l} q = q_3 = q_4 \\ \text{y} \\ r = 2r_3 + 1 = 3r_4 + r_2 \end{array} \right\} \\
&\iff \exists q, r \in \mathbb{Z} : a = 6q + r,\ \text{con } r \in \{1, 5\} \\
&\iff a \in \{n : n = 6q + 1\ \vee\ n = 6q + 5,\ q \in \mathbb{Z}\}
\end{aligned}$$

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, (3.2.1),

$$A^c \cap B^c \subseteq \{n : n = 6q + 1\ \vee\ n = 6q + 5,\ q \in \mathbb{Z}\}$$

Recíprocamente,

$$
\begin{aligned}
a \in \{n : n = 6q+1 \ \vee \ n = 6q+5,\ q \in \mathbb{Z}\} \iff & \left\{ \begin{array}{l} \exists q_1 \in \mathbb{Z} : a = 6q_1 + 1 \\ \vee \\ \exists q_2 \in \mathbb{Z} : a = 6q_2 + 5 \end{array} \right. \\
\iff & \left\{ \begin{array}{l} \exists q_1 \in \mathbb{Z} : a = 2(3q_1) + 1 \ \wedge \ a = 3(2q_1) + 1 \\ \vee \\ \exists q_2 \in \mathbb{Z} : a = 2(3q_2 + 2) + 1 \ \wedge \ a = 3(2q_2 + 1) + 2 \end{array} \right. \\
& \left\{ \begin{array}{l} a \text{ da resto 1 al dividir por 2} \\ \wedge \\ a \text{ da resto 1 o 2 al dividir por 3} \end{array} \right\} \\
\implies & \left\{ \begin{array}{l} \exists q_3 \in \mathbb{Z} : a = 2q_3 + 1 \\ \wedge \\ \exists q_4, r \in \mathbb{Z} : a = 3q_4 + r, \text{ con } r \neq 0 \end{array} \right. \\
\iff & \left\{ \begin{array}{l} a \notin A \\ \wedge \\ a \notin B \end{array} \right. \\
\iff & \left\{ \begin{array}{l} a \in A^c \\ \wedge \\ a \in B^c \end{array} \right. \\
\iff & a \in (A^c \cap B^c)
\end{aligned}
$$

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, (3.2.1),

$$\{n : n = 6q+1 \ \vee \ n = 6q+5,\ q \in \mathbb{Z}\} \subseteq A^c \cap B^c$$

Finalmente, por la doble inclusión, tendremos, (3.2.5), 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, si tomamos, por ejemplo, el 6, tendremos

$$
\left. \begin{array}{lll} 6 = 2 \cdot 3 & \implies & 6 \in A \\ \text{y} & & \wedge \\ 6 = 3 \cdot 2 & \implies & 6 \in B \end{array} \right\} \implies 6 \in (A \cap B) \iff A \cap B \neq \emptyset
$$

⁎ $A \setminus B \neq \emptyset$

En efecto, tomando, por ejemplo, el 2, tendremos

$$\left.\begin{array}{lcl} 2 = 2\cdot 1 & \Longrightarrow & 2 \in A \\ \wedge & & \wedge \\ 2 = 3\cdot 0 + 2 & \Longrightarrow & 2 \text{ da resto distinto de cero al dividir por } 3 \end{array} \right\} \Longrightarrow \quad 2 \notin B$$

luego, $2 \in (A \setminus B)$ y, consecuentemente, $A \setminus B \neq \emptyset$.

$\divideontimes$ $B \setminus A \neq \emptyset$

En efecto, tomando, por ejemplo, el 3, tendremos

$$\left.\begin{array}{lcl} 3 = 3\cdot 1 & \Longrightarrow & 3 \in B \\ \wedge & & \wedge \\ 3 = 2\cdot 1 + 1 & \Longrightarrow & 3 \text{ da resto distinto de cero al dividir por } 2 \end{array} \right\} \Longrightarrow \quad 3 \notin A$$

luego, $3 \in (B \setminus A)$ y, consecuentemente, $B \setminus A \neq \emptyset$.

$\divideontimes$ $A^c \cap B^c \neq \emptyset$

En efecto, tomando, por ejemplo, el 5, tendremos

$$\left.\begin{array}{l} 5 = 2\cdot 2 + 1 \Longrightarrow 5 \text{ da resto distinto de cero al dividir por } 2 \Longrightarrow 5 \notin A \Longrightarrow 5 \in A^c \\ \wedge \\ 5 = 3\cdot 1 + 2 \Longrightarrow 5 \text{ da resto distinto de cero al dividir por } 3 \Longrightarrow 5 \notin B \Longrightarrow 5 \in B^c \end{array} \right\}$$

luego, $5 \in (A^c \cap B^c)$ y, consecuentemente, $(A^c \cap B^c) \neq \emptyset$.

2 Los conjuntos que conforman $\mathscr{P}$ son dos a dos disjuntos.

En efecto,

$$\begin{array}{rcll}
(A \cap B) \cap (A \setminus B) & = & A \cap B \cap A \cap B^c & \{\text{Diferencia de conjuntos. (4.1.3)}\} \\
& = & A \cap A \cap B \cap B^c & \{\text{Leyes conmutativas. (4.2.2)}\} \\
& = & A \cap B \cap B^c & \{\text{Leyes de idempotencia. (4.2.1)}\} \\
& = & A \cap \emptyset & \{\text{Leyes del complementario. (4.2.8)}\} \\
& = & \emptyset & \{\text{Leyes de dominación (4.2.5)}\} \\
(A \cap B) \cap (B \setminus A) & = & A \cap B \cap B \cap A^c & \{\text{Diferencia de conjuntos. (4.1.3)}\} \\
& = & A \cap A^c \cap B \cap B & \{\text{Leyes conmutativas. (4.2.2)}\} \\
& = & A \cap A^c \cap B & \{\text{Leyes de idempotencia. (4.2.1)}\} \\
& = & \emptyset \cap B & \{\text{Leyes del complementario. (4.2.8)}\} \\
& = & \emptyset & \{\text{Leyes de dominación (4.2.5)}\} \\
(A \cap B) \cap (A^c \cap B^c) & = & A \cap A^c \cap B \cap B^c & \{\text{Leyes conmutativas. (4.2.2)}\} \\
& = & \emptyset \cap \emptyset & \{\text{Leyes del complementario. (4.2.8)}\} \\
& = & \emptyset & \{\text{Leyes de idempotencia. (4.2.1)}\} \\
(A \setminus B) \cap (B \setminus A) & = & A \cap B^c \cap B \cap A^c & \{\text{Diferencia de conjuntos. (4.1.3)}\} \\
& = & A \cap A^c \cap B \cap B^c & \{\text{Leyes conmutativas. (4.2.2)}\} \\
& = & \emptyset \cap \emptyset & \{\text{Leyes del complementario. (4.2.8)}\} \\
& = & \emptyset & \{\text{Leyes de idempotencia. (4.2.1)}\} \\
(A \setminus B) \cap (A^c \cap B^c) & = & A \cap B^c \cap A^c \cap B^c & \{\text{Diferencia de conjuntos. (4.1.3)}\} \\
& = & A \cap A^c \cap B^c \cap B^c & \{\text{Leyes conmutativas. (4.2.2)}\} \\
& = & A \cap A^c \cap B^c & \{\text{Leyes de idempotencia. (4.2.1)}\} \\
& = & \emptyset \cap B^c & \{\text{Leyes del complementario. (4.2.8)}\} \\
& = & \emptyset & \{\text{Leyes de dominación (4.2.5)}\}
\end{array}$$

$$
\begin{array}{rcll}
(B \setminus A) \cap (A^c \cap B^c) & = & B \cap A^c \cap A^c \cap B^c & \{\text{Diferencia de conjuntos. (4.1.3)}\} \\
& = & A^c \cap A^c \cap B \cap B^c & \{\text{Leyes conmutativas. (4.2.2)}\} \\
& = & A^c \cap B \cap B^c & \{\text{Leyes de idempotencia. (4.2.1)}\} \\
& = & A^c \cap \emptyset & \{\text{Leyes del complementario. (4.2.8)}\} \\
& = & \emptyset & \{\text{Leyes de dominación (4.2.5)}\}
\end{array}
$$

3 El conjunto de los enteros es igual a la unión de todos los conjuntos que integran la partición.

En efecto,

$$
\begin{array}{ll}
(A \cap B) \cup (A \setminus B) \cup (B \setminus A) \cup (A^c \cap B^c) & \\
= & \\
(A \cap B) \cup (A \cap B^c) \cup (B \cap A^c) \cup (A^c \cap B^c) & \{\text{Diferencia de conjuntos. (4.1.3)}\} \\
= & \\
(A \cap B) \cup (A \cap B^c) \cup (A^c \cap B) \cup (A^c \cap B^c) & \{\text{Leyes conmutativas. (4.2.2)}\} \\
= & \\
[A \cap (B \cup B^c)] \cup [A^c \cap (B \cup B^c)] & \{\text{Leyes distributivas. (4.2.4)}\} \\
= & \\
(A \cup A^c) \cap (B \cup B^c) & \{\text{Leyes distributivas. (4.2.4)}\} \\
= & \\
\mathbb{Z} \cap \mathbb{Z} & \{\text{Leyes del complementario. (4.2.8)}\} \\
= & \\
\mathbb{Z} & \{\text{Leyes idempotentes. (4.2.1)}\}
\end{array}
$$

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,

$$
a \in \mathbb{Z} \iff \begin{cases} a \in (A \cap B) \\ \vee \\ a \in (A \setminus B) \\ \vee \\ a \in (B \setminus A) \\ \vee \\ a \in (A^c \cap B^c) \end{cases}
$$

$$
\iff \begin{cases} a \in \{n : n = 6q,\ q \in \mathbb{Z}\} \\ \vee \\ a \in \{n : n = 6q+2 \ \vee \ n = 6q+4,\ q \in \mathbb{Z}\} \\ \vee \\ a \in \{n : n = 6q+3,\ q \in \mathbb{Z}\} \\ \vee \\ a \in \{n : n = 6q+1 \ \vee \ n = 6q+5,\ q \in \mathbb{Z}\} \end{cases}
$$

$$
\iff \begin{cases} \exists q \in \mathbb{Z} : a = 6q \\ \vee \\ \exists q \in \mathbb{Z} : a = 6q+2 \ \vee \ a = 6q+4 \\ \vee \\ \exists q \in \mathbb{Z} : a = 6q+3 \\ \vee \\ \exists q \in \mathbb{Z} : a = 6q+1 \ \vee \ a = 6q+5 \end{cases}
$$

$$
\iff \begin{cases} a \text{ es múltiplo de } 6 \\ \vee \\ a \text{ da resto par al dividirlo por } 6 \\ \vee \\ a \text{ da resto } 3 \text{ al dividirlo por } 6 \\ \vee \\ a \text{ da resto impar distinto de } 3 \text{ al dividirlo por } 6 \end{cases}
$$

♦

Ejemplo 4.10

En el conjunto universal de los números enteros, se consideran los siguientes conjuntos:

A: conjunto formado por todos los números pares.

B: conjunto formado por todos los múltiplos de 4.

C: conjunto formado por todos los múltiplos de 3.

(a) Calcular $A \setminus B$.

(b) Calcular $A \setminus C$.

(c) Calcular $B \setminus C$.

(d) Calcular $(A \setminus B) \cap (A \setminus C)$.

(e) Calcular $(A \setminus C) \setminus (A \setminus B)$.

(f) Calcular $(A \setminus C) \setminus (B \setminus C)$.

(g) Calcular $(A \setminus C) \cap (B \setminus C)$.

(h) Calcular $A \cap B \cap C$.

(i) Calcular $(A \setminus B) \cup (A \setminus C)$.

(j) Calcular $A \cap C$.

(k) Calcular $(A \cap C) \setminus (B \cap C)$.

(l) Calcular $(A \setminus B) \cap C$.

(m) Calcular $C \setminus B$.

(n) Calcular $(C \setminus B) \cap A$.

(o) Calcular $(C \setminus B) \cap (A \setminus B)$.

(p) Calcular $C \setminus A$.

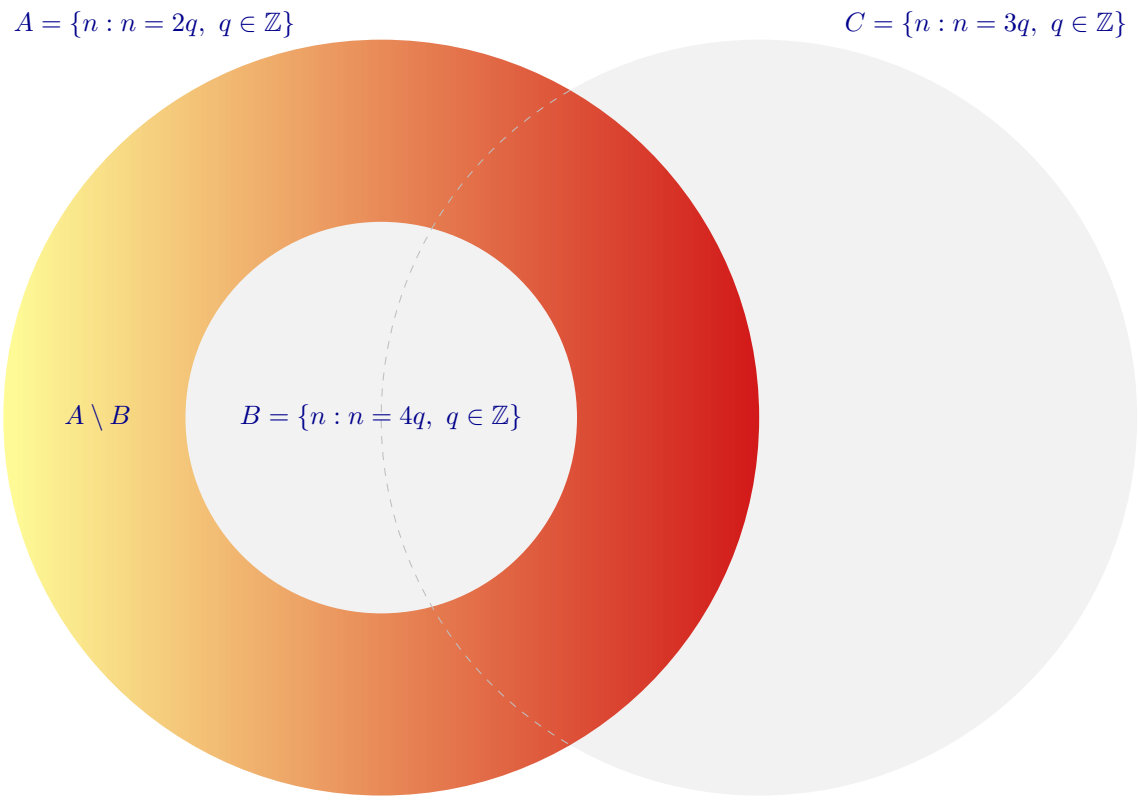
(q) Calcular $(C \setminus B) \setminus (A \setminus B)$.

(r) Calcular $(C \setminus B) \setminus (C \setminus A)$.

(s) Calcular $(C \setminus B) \cap (A \setminus B)$.

Solución.

(a) $A \setminus B$.



Sea a cualquier número entero. Entonces,

$$
\begin{aligned}
a \in A \setminus B \iff & \left\{ \begin{array}{l} a \in A \\ \wedge \\ a \notin B \end{array} \right. \\
\iff & \left\{ \begin{array}{l} \exists q_1 \in \mathbb{Z} : a = 2q_1 \\ \wedge \\ \exists q_2, r_2 \in \mathbb{Z} : a = 4q_2 + r_2,\ r_2 \neq 0 \end{array} \right. \\
& [\text{Dividiendo } q_1 \textit{ por } 2,\ q_1 = 2q_3 + r_3,\ q_3 \in \mathbb{Z},\ r_3 \in \{0,1\}] \\
\implies & \left\{ \begin{array}{l} \exists q_3, r_3 \in \mathbb{Z} : a = 2(2q_3 + r_3),\ r_3 \in \{0,1\} \\ \wedge \\ \exists q_2, r_2 \in \mathbb{Z} : a = 4q_2 + r_2,\ r_2 \in \{1,2,3\} \end{array} \right. \\
\iff & \left\{ \begin{array}{l} \exists q_3, r_3 \in \mathbb{Z} : a = 4q_3 + 2r_3,\ 2r_3 \in \{0,2\} \\ \wedge \\ \exists q_2, r_2 \in \mathbb{Z} : a = 4q_2 + r_2,\ r_2 \in \{1,2,3\} \end{array} \right. \\
& \left[\begin{array}{l} \text{Unicidad de cociente y resto (5.2.1)},\ q_3 = q_2 \text{ y } 2r_3 = r_2 \\ \text{Tomando } q = q_3 = q_2,\ r = 2r_3 = r_2 \end{array} \right] \\
\implies & \exists q, r \in \mathbb{Z} : a = 4q + r,\ r \in \{0,2\} \cap \{1,2,3\} \\
\iff & \exists q, r \in \mathbb{Z} : a = 4q + r,\ r \in \{2\} \\
\iff & a \in \{n : n = 4q + 2,\ q \in \mathbb{Z}\}
\end{aligned}
$$

De la arbitrariedad de a se sigue que la proposición,

$$\forall x, (x \in A \setminus B \longrightarrow x \in \{n : n = 4q + 2,\ q \in \mathbb{Z}\})$$

es verdadera y, por la definición de inclusión de conjuntos, (3.2.1),

$$A \setminus B \subseteq \{n : n = 4q + 2,\ q \in \mathbb{Z}\}$$

Recíprocamente,

$$
\begin{aligned}
a \in \{n : n = 4q + 2,\ q \in \mathbb{Z}\} \iff & \exists q \in \mathbb{Z} : a = 4q + 2 \\
\iff & \exists q \in \mathbb{Z} : \left\{ \begin{array}{l} a = 2(2q + 1) \\ \wedge \\ a = 4q + 2 \end{array} \right. \\
& \left[\begin{array}{l} a \text{ da resto 0 al dividir por 2} \\ \text{y} \\ a \text{ da resto distinto de 0 al dividir por 4} \end{array} \right] \\
\implies & \left\{ \begin{array}{l} \exists q_2 \in \mathbb{Z} : a = 2q_2 \\ \wedge \\ \exists q_3, r_3 \in \mathbb{Z} : a = 4q_3 + r_3,\ r_3 \neq 0 \end{array} \right. \\
\iff & \left\{ \begin{array}{l} a \in A \\ \wedge \\ a \notin B \end{array} \right. \\
\iff & a \in A \setminus B
\end{aligned}
$$

De la arbitrariedad de a se sigue que la proposición,

$$\forall x, (x \in \{n : n = 4q + 2,\ q \in \mathbb{Z}\} \longrightarrow x \in A \setminus B)$$

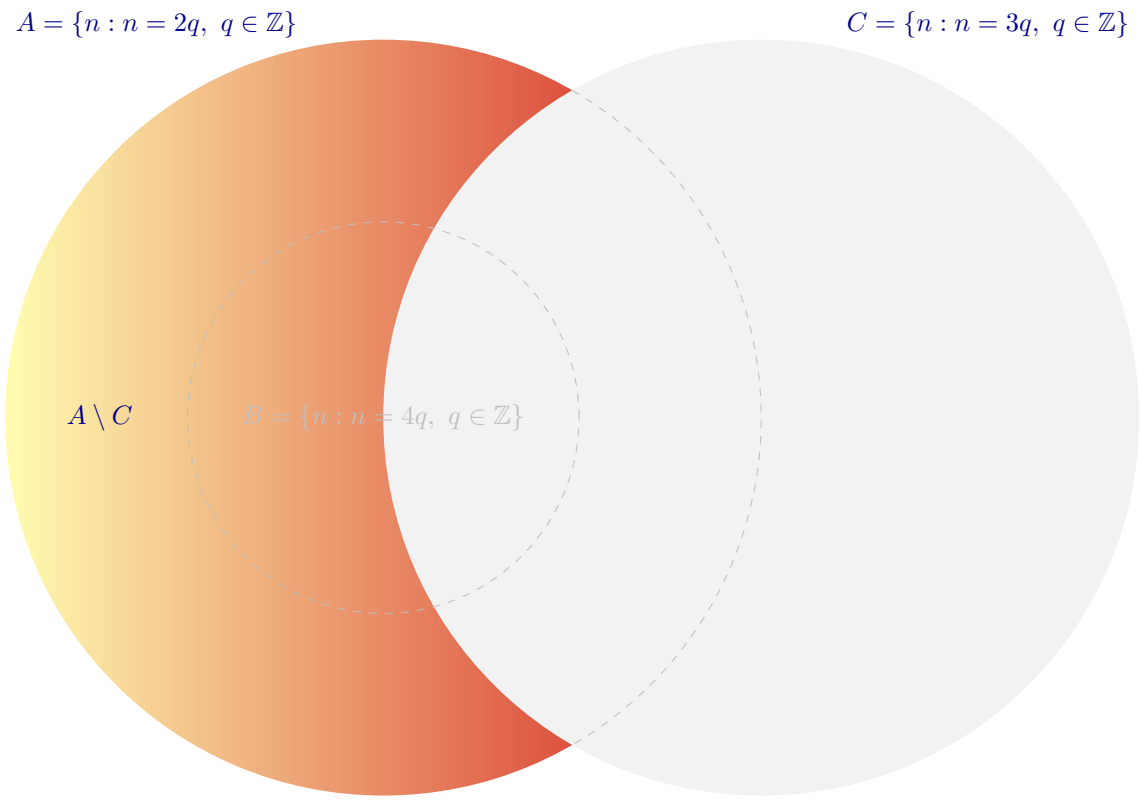
es verdadera y, por la definición de inclusión de conjuntos, (3.2.1),

$$\{n : n = 4q + 2,\ q \in \mathbb{Z}\} \subseteq A \setminus B$$

Finalmente, por la doble inclusión de conjuntos, (3.2.5), tendremos que

$$A \setminus B = \{n : n = 4q + 2,\ q \in \mathbb{Z}\}$$

(b) $A \setminus C$



Sea a cualquier número entero. Entonces,

$$
\begin{aligned}
a \in A \setminus C \iff & \left\{ \begin{array}{l} a \in A \\ \wedge \\ a \notin C \end{array} \right. \\
\iff & \left\{ \begin{array}{l} \exists q_1 \in \mathbb{Z} : a = 2q_1 \\ \wedge \\ \exists q_2, r_2 \in \mathbb{Z} : a = 3q_2 + r_2,\ r_2 \neq 0 \end{array} \right. \\
& \left[\begin{array}{l} \text{Dividiendo } q_1 \text{ por 3},\ q_1 = 3q_3 + r_3,\ q_3 \in \mathbb{Z},\ r_3 \in \{0,1,2\} \\ \text{y} \\ \text{Dividiendo } q_2 \text{ por 2},\ q_2 = 2q_4 + r_4,\ q_4 \in \mathbb{Z},\ r_4 \in \{0,1\} \end{array} \right] \\
\implies & \left\{ \begin{array}{l} \exists q_3, r_3 \in \mathbb{Z} : a = 2(3q_3 + r_3),\ r_3 \in \{0,1,2\} \\ \wedge \\ \exists q_4, r_4 \in \mathbb{Z} : a = 3(2q_4 + r_4) + r_2,\ r_2 \in \{1,2\},\ r_4 \in \{0,1\} \end{array} \right. \\
\iff & \left\{ \begin{array}{l} \exists q_3, r_3 \in \mathbb{Z} : a = 6q_3 + 2r_3,\ 2r_3 \in \{0,2,4\} \\ \wedge \\ \exists q_4, r_4 \in \mathbb{Z} : a = 6q_4 + 2r_4 + r_2,\ 2r_4 + r_2 \in \{1,2,3,4\} \end{array} \right. \\
& \left[\begin{array}{l} \text{Unicidad de cociente y resto, (5.2.1)},\ q_3 = q_4 \text{ y } 2r_3 = r_2 + 2r_4 \\ \\ \text{Tomando } q = q_3 = q_4,\ r = 2r_3 = r_2 + 2r_4 \end{array} \right] \\
\implies & \exists q, r \in \mathbb{Z} : a = 6q + r,\ r \in (\{0,2,4\} \cap \{1,2,3,4\}) \\
\iff & \exists q, r \in \mathbb{Z} : a = 6q + r,\ r \in \{2,4\} \\
\iff & a \in \{n : n = 6q + r,\ q \in \mathbb{Z},\ r \in \{2,4\}\}
\end{aligned}
$$

De la arbitrariedad de a se sigue que la proposición,

$$\forall x, (x \in (A \setminus C) \longrightarrow x \in \{n : n = 6q + r,\ q \in \mathbb{Z},\ r \in \{2,4\}\})$$

es verdadera y, por la definición de inclusión de conjuntos, (3.2.1),

$$A \setminus C \subseteq \{n : n = 6q + r,\ q \in \mathbb{Z},\ r \in \{2,4\}\}$$

Recíprocamente,

$$
\begin{aligned}
a \in \{n : n = 6q + r,\ q \in \mathbb{Z},\ r \in \{2,4\}\} \iff & \exists q \in \mathbb{Z} : a = 6q + 2 \ \vee \ a = 6q + 4 \\
\iff & \exists q \in \mathbb{Z} : \left\{ \begin{array}{l} a = 2(3q+1) \ \vee \ a = 2(3q+2) \\ \wedge \\ a = 3(2q) + 2 \ \vee \ a = 3(2q+1) + 1 \end{array} \right. \\
& \left[\begin{array}{l} a \text{ da resto 0 al dividir por 2} \\ \text{y} \\ a \text{ da resto distinto de 0 al dividir por 3} \end{array} \right] \\
\implies & \left\{ \begin{array}{l} \exists q_2 \in \mathbb{Z} : a = 2q_2 \\ \wedge \\ \exists q_3, r_3 \in \mathbb{Z} : a = 3q_3 + r_3,\ r_3 \neq 0 \end{array} \right. \\
\iff & \left\{ \begin{array}{l} a \in A \\ \wedge \\ a \notin C \end{array} \right. \\
\iff & a \in (A \setminus C)
\end{aligned}
$$

De la arbitrariedad de a se sigue que la proposición,

$$\forall x, (x \in \{n : n = 6q + r,\ q \in \mathbb{Z},\ r \in \{2,4\}\} \longrightarrow x \in (A \setminus C))$$

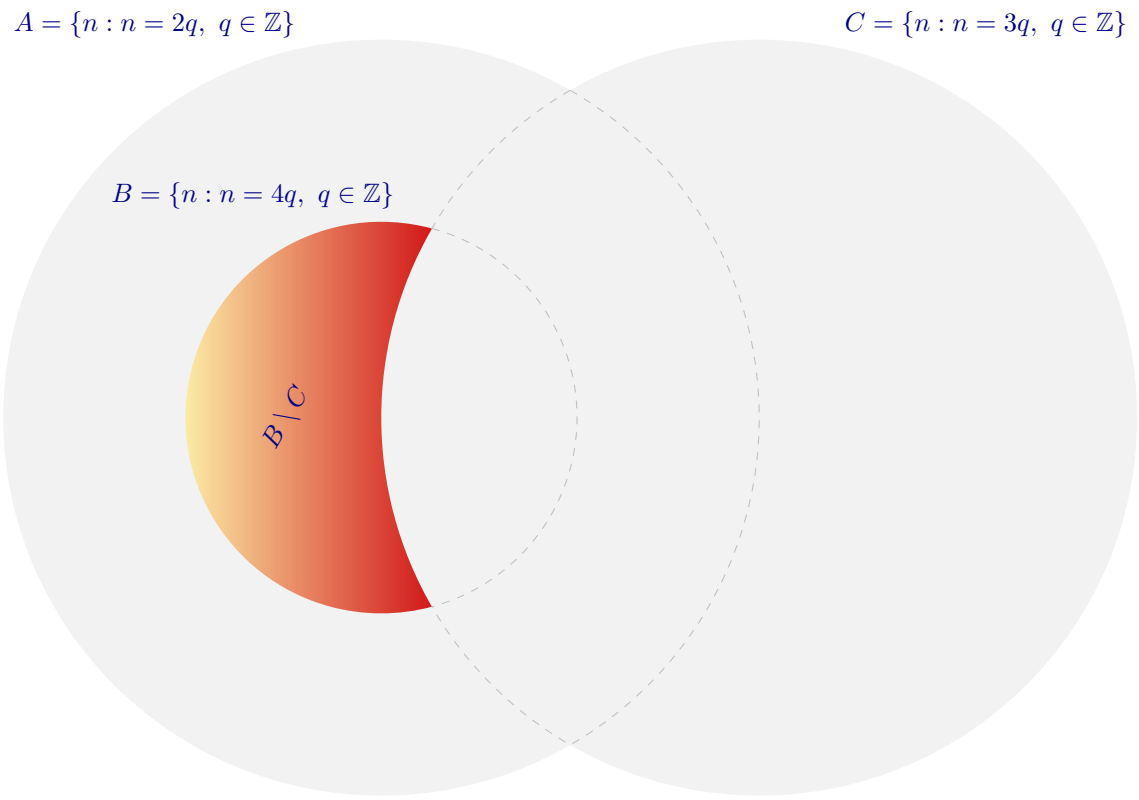
es verdadera y, por la definición de inclusión de conjuntos, (3.2.1),

$$\{n : n = 6q + r,\ q \in \mathbb{Z},\ r \in \{2, 4\}\} \subseteq A \setminus C$$

Finalmente, por la doble inclusión de conjuntos, (3.2.5), tendremos que

$$A \setminus C = \{n : n = 6q + r,\ q \in \mathbb{Z},\ r \in \{2, 4\}\}$$

(c) $B \setminus C$.



Sea a cualquier número entero. Entonces,

$$
\begin{aligned}
a \in B \setminus C \iff & \left\{ \begin{array}{l} a \in B \\ \wedge \\ a \notin C \end{array} \right. \\
\iff & \left\{ \begin{array}{l} \exists q_1 \in \mathbb{Z} : a = 4q_1 \\ \wedge \\ \exists q_2, r_2 \in \mathbb{Z} : a = 3q_2 + r_2,\ r_2 \neq 0 \end{array} \right. \\
& \left[\begin{array}{l} \text{Dividiendo } q_1 \text{ por } 3,\ q_1 = 3q_3 + r_3,\ q_3 \in \mathbb{Z},\ r_3 \in \{0,1,2\} \\ \text{y} \\ \text{Dividiendo } q_2 \text{ por } 4,\ q_2 = 4q_4 + r_4,\ q_4 \in \mathbb{Z},\ r_4 \in \{0,1,2,3\} \end{array} \right] \\
\Longrightarrow & \left\{ \begin{array}{l} \exists q_3, r_3 \in \mathbb{Z} : a = 4(3q_3 + r_3),\ r_3 \in \{0,1,2\} \\ \wedge \\ \exists q_4, r_4 \in \mathbb{Z} : a = 3(4q_4 + r_4) + r_2,\ r_2 \in \{1,2\},\ r_4 \in \{0,1,2,3\} \end{array} \right. \\
\iff & \left\{ \begin{array}{l} \exists q_3, r_3 \in \mathbb{Z} : a = 12q_3 + 4r_3,\ 4r_3 \in \{0,4,8\} \\ \wedge \\ \exists q_4, r_4 \in \mathbb{Z} : a = 12q_4 + 3r_4 + r_2,\ 3r_4 + r_2 \in \{1,2,4,5,7,8,10,11\} \end{array} \right. \\
& \left[\begin{array}{l} \text{Unicidad de cociente y resto (5.2.1)},\ q_3 = q_4 \text{ y } 4r_3 = r_2 + 3r_4 \\ \\ \text{Tomando } q = q_3 = q_4 \text{ y } r = 4r_3 = r_2 + 3r_4 \end{array} \right] \\
\Longrightarrow & \quad \exists q, r \in \mathbb{Z} : a = 12q + r,\ r \in \{0,4,8\} \cap \{1,2,4,5,7,8,10,11\} \\
\iff & \quad \exists q, r \in \mathbb{Z} : a = 12q + r,\ r \in \{4,8\} \\
\iff & \quad a \in \{n : n = 12q + r,\ q \in \mathbb{Z},\ r \in \{4,8\}\}
\end{aligned}
$$

De la arbitrariedad de a se sigue que la proposición,

$$\forall x, (x \in (B \setminus C) \longrightarrow x \in \{n : n = 12q + r,\ q \in \mathbb{Z},\ r \in \{4,8\}\})$$

es verdadera y, por la definición de inclusión de conjuntos, (3.2.1),

$$B \setminus C \subseteq \{n : n = 12q + r,\ q \in \mathbb{Z},\ r \in \{4,8\}\}$$

Recíprocamente,

$$
\begin{aligned}
a \in \{n : n = 12q + r,\ q \in \mathbb{Z},\ r \in \{4,8\}\} \iff & \quad \exists q \in \mathbb{Z} : a = 12q + 4 \ \vee \ a = 12q + 8 \\
\iff & \quad \exists q \in \mathbb{Z} : \left\{ \begin{array}{l} a = 4(3q+1) \ \vee \ a = 4(3q+2) \\ \wedge \\ a = 3(4q+1) + 1 \ \vee \ a = 3(4q+2) + 2 \end{array} \right. \\
& \left[\begin{array}{l} a \text{ da resto 0 al dividir por 4} \\ \text{y} \\ a \text{ da resto distinto de 0 al dividir por 3} \end{array} \right] \\
\Longrightarrow & \left\{ \begin{array}{l} \exists q_2 \in \mathbb{Z} : a = 4q_2 \\ \wedge \\ \exists q_3, r_3 \in \mathbb{Z} : a = 3q_3 + r_3,\ r_3 \neq 0 \end{array} \right. \\
\iff & \left\{ \begin{array}{l} a \in B \\ \wedge \\ a \notin C \end{array} \right. \\
\iff & \quad a \in (B \setminus C)
\end{aligned}
$$

De la arbitrariedad de a se sigue que la proposición,

$$\forall x, (x \in \{n : n = 12q + r,\ q \in \mathbb{Z},\ r \in \{4,8\}\} \longrightarrow x \in (B \setminus C))$$

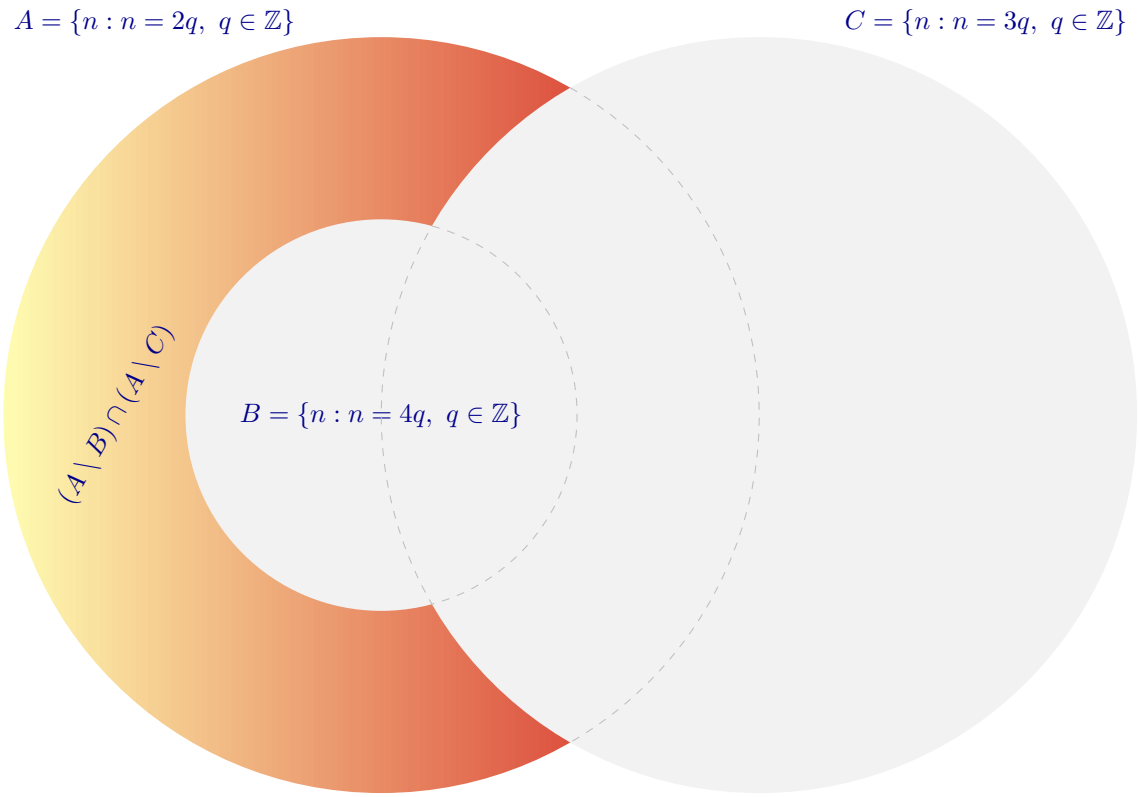
es verdadera y, por la definición de inclusión de conjuntos, (3.2.1),

$$\{n : n = 12q + r,\ q \in \mathbb{Z},\ r \in \{4, 8\}\} \subseteq B \setminus C$$

Finalmente, por la doble inclusión de conjuntos, (3.2.5), tendremos que

$$B \setminus C = \{n : n = 12q + r,\ q \in \mathbb{Z},\ r \in \{4, 8\}\}$$

(d) $(A \setminus B) \cap (A \setminus C)$



Según los resultados obtenidos en los apartados a) y b),

$$\begin{aligned} A \setminus B &= \{n : n = 4q + 2,\ q \in \mathbb{Z}\} \\ A \setminus C &= \{n : n = 6q + r,\ q \in \mathbb{Z},\ r \in \{2, 4\}\} \end{aligned}$$

Entonces, si a es cualquier entero,

$$
\begin{aligned}
a \in (A \setminus B) \cap (A \setminus C) &\iff \begin{cases} a \in A \setminus B \\ \wedge \\ a \in A \setminus C \end{cases} \\
&\iff \begin{cases} \exists q_1 \in \mathbb{Z} : a = 4q_1 + 2 \\ \wedge \\ \exists q_2 \in \mathbb{Z} : a = 6q_2 + r_2,\ r_2 \in \{2, 4\} \end{cases} \\
&\left[\begin{array}{l} \text{Dividiendo } q_1 \text{ por 3, } q_1 = 3q_3 + r_3,\ q_3 \in \mathbb{Z},\ r_3 \in \{0, 1, 2\} \\ \text{y} \\ \text{Dividiendo } q_2 \text{ por 2, } q_2 = 2q_4 + r_4,\ q_4 \in \mathbb{Z},\ r_4 \in \{0, 1\} \end{array} \right] \\
&\implies \begin{cases} \exists q_3, r_3 : a = 4(3q_3 + r_3) + 2,\ r_3 \in \{0, 1, 2\} \\ \wedge \\ \exists q_4, r_4 : a = 6(2q_4 + r_4) + r_2,\ r_2 \in \{2, 4\}\ \ r_4 \in \{0, 1\} \end{cases} \\
&\iff \begin{cases} \exists q_3, r_3 : a = 12q_3 + 4r_3 + 2,\ 4r_3 + 2 \in \{2, 6, 10\} \\ \wedge \\ \exists q_4, r_4 : a = 12q_4 + 6r_4 + r_2,\ 6r_4 + r_2 \in \{2, 4, 8, 10\} \end{cases} \\
&\left[\begin{array}{l} \text{Unicidad de cociente y resto, (5.2.1), } q_3 = q_4,\ 4r_3 + 2 = 6r_4 + r_2 \\ \text{Tomando } q = q_3 = q_4 \text{ y } r = 4r_3 + 2 = 6r_4 + r_2 \end{array} \right] \\
&\iff \exists q, r \in \mathbb{Z} : a = 12q + r,\ r \in (\{2, 6, 10\} \cap \{2, 4, 8, 10\}) \\
&\iff a \in \{n : n = 12q + r,\ q \in \mathbb{Z},\ r \in \{2, 10\}\}
\end{aligned}
$$

De la arbitrariedad de a se sigue que la proposición,

$$\forall x, (x \in (A \setminus B) \cap (A \setminus C) \longrightarrow x \in \{n : n = 12q + r,\ q \in \mathbb{Z},\ r \in \{2, 10\}\})$$

es verdadera y, por la definición de inclusión de conjuntos, (3.2.1),

$$(A \setminus B) \cap (A \setminus C) \subseteq \{n : n = 12q + r,\ q \in \mathbb{Z},\ r \in \{2, 10\}\}$$

Recíprocamente,

$$
\begin{aligned}
a \in \{n : n = 12q + r,\ q \in \mathbb{Z},\ r \in \{2, 10\}\} &\iff \exists q \in \mathbb{Z} : a = 12q + 2\ \vee\ a = 12q + 10 \\
&\iff \exists q \in \mathbb{Z} : \begin{cases} a = 4(3q) + 2\ \vee\ a = 4(3q + 2) + 2 \\ \wedge \\ a = 6(2q) + 2\ \vee\ a = 6(2q + 1) + 4 \end{cases} \\
&\left[\begin{array}{l} a \text{ da resto 2 al dividir por 4} \\ \text{y} \\ a \text{ da resto 2 o 4 al dividir por 6} \end{array} \right] \\
&\implies \begin{cases} \exists q_1 \in \mathbb{Z} : a = 4q_1 + 2 \\ \wedge \\ \exists q_2 \in \mathbb{Z} : a = 6q_2 + r,\ r \in \{2, 4\} \end{cases} \\
&\iff \begin{cases} a \in (A \setminus B) \\ \wedge \\ a \in (A \setminus C) \end{cases} \\
&\iff a \in (A \setminus B) \cap (A \setminus C)
\end{aligned}
$$

De la arbitrariedad de a se sigue que la proposición,

$$\forall x, (x \in \{n : n = 12q + r,\ q \in \mathbb{Z},\ r \in \{2, 10\}\} \longrightarrow x \in (A \setminus B) \cap (A \setminus C))$$

es verdadera y, por la definición de inclusión de conjuntos, (3.2.1),

$$\{n : n = 12q + r,\ q \in \mathbb{Z},\ r \in \{2, 10\}\} \subseteq (A \setminus B) \cap (A \setminus C)$$

Finalmente, por la doble inclusión de conjuntos, (3.2.5), tendremos que

$$(A \setminus B) \cap (A \setminus C) = \{n : n = 12q + r,\ q \in \mathbb{Z},\ r \in \{2, 10\}\}$$

Ahora lo haremos sin utilizar los resultados previos de $A \setminus B$ y $A \setminus C$. En efecto,

$$(A \setminus B) \cap (A \setminus C) = (A \cap B^c) \cap (A \cap C^c) = A \cap B^c \cap C^c$$

Entonces, si a es cualquier entero,

$$\begin{aligned}
a \in (A \setminus B) \cap (A \setminus C) &\iff a \in A \cap B^c \cap C^c \\
&\iff \left\{ \begin{array}{l} a \in A \\ \wedge \\ a \in B^c \\ \wedge \\ a \in C^c \end{array} \right. \\
&\iff \left\{ \begin{array}{l} a \in A \\ \wedge \\ a \notin B \\ \wedge \\ a \notin C \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 = 4q_2 + r_2,\ r_2 \neq 0 \\ \wedge \\ \exists q_3, r_3 \in \mathbb{Z} : a = 3q_3 + r_3,\ r_3 \neq 0 \end{array} \right. \\
&\left[\begin{array}{l} \text{m.c.m.}(2, 3, 4) = 12 \\ \text{Dividiendo } q_1 \text{ por } 6,\ q_1 = 6q_4 + r_4,\ \text{con } q_4 \in \mathbb{Z} \text{ y } r_4 \in \{0, 1, 2, 3, 4, 5\} \\ \text{Dividiendo } q_2 \text{ por } 3,\ q_2 = 3q_5 + r_5,\ \text{con } q_5 \in \mathbb{Z} \text{ y } r_5 \in \{0, 1, 2\} \\ \text{Dividiendo } q_3 \text{ por } 4,\ q_3 = 4q_6 + r_6,\ \text{con } q_6 \in \mathbb{Z} \text{ y } r_6 \in \{0, 1, 2, 3\} \end{array} \right] \\
&\implies \left\{ \begin{array}{l} \exists q_4, r_4 \in \mathbb{Z} : a = 2(6q_4 + r_4),\ r_4 \in \{0, 1, 2, 3, 4, 5\} \\ \wedge \\ \exists q_5, r_5 \in \mathbb{Z} : a = 4(3q_5 + r_5) + r_2,\ r_2 \in \{1, 2, 3\},\ r_5 \in \{0, 1, 2\} \\ \wedge \\ \exists q_3, r_3 \in \mathbb{Z} : a = 3(4q_6 + r_6) + r_3,\ r_3 \in \{1, 2\},\ r_6 \in \{0, 1, 2, 3\} \end{array} \right. \\
&\iff \left\{ \begin{array}{l} \exists q_4, r_4 \in \mathbb{Z} : a = 12q_4 + 2r_4,\ 2r_4 \in \{0, 2, 4, 6, 8, 10\} \\ \wedge \\ \exists q_5, r_5 \in \mathbb{Z} : a = 12q_5 + 4r_5 + r_2,\ 4r_5 + r_2 \in \{1, 2, 3, 5, 6, 7, 9, 10, 11\} \\ \wedge \\ \exists q_3, r_3 \in \mathbb{Z} : a = 12q_6 + 3r_6 + r_3,\ 3r_6 + r_3 \in \{1, 2, 4, 5, 7, 8, 10, 11\} \end{array} \right. \\
&\left[\begin{array}{l} \text{Unicidad de cociente y resto (5.2.1)} \left\{ \begin{array}{l} q_4 = q_5 = q_6 \\ 2r_4 = 4r_5 + r_2 = 3r_6 + r_3 \end{array} \right. \\ \text{Tomando } q = q_4 = q_5 = q_6 \text{ y } r = 2r_4 = 4r_5 + r_2 = 3r_6 + r_3 \end{array} \right] \\
&\implies \left\{ \begin{array}{l} \exists q, r \in \mathbb{Z} : a = 12q + r, \\ r \in \{0, 2, 4, 6, 8, 10\} \cap \{1, 2, 3, 5, 6, 7, 9, 10, 11\} \cap \{1, 2, 4, 5, 7, 8, 10, 11\} \end{array} \right. \\
&\iff \exists q, r \in \mathbb{Z} : a = 12q + r,\ r \in \{2, 10\} \\
&\iff a \in \{n : n = 12q + r,\ r \in \{2, 10\}\}
\end{aligned}$$

Razonando igual que antes, tendremos

$$(A \setminus B) \cap (A \setminus C) \subseteq \{n : n = 12q + r,\ q \in \mathbb{Z},\ r \in \{2, 10\}\}$$

Recíprocamente,

$$
\begin{aligned}
a \in \{n : n = 12q + r,\ q \in \mathbb{Z},\ r \in \{2, 10\}\} &\iff \exists q \in \mathbb{Z} : a = 12q + 2 \ \vee\ a = 12q + 10 \\
&\iff \exists q \in \mathbb{Z} : \left\{ \begin{array}{l} a = 2(6q+1) \ \vee\ a = 2(6q+5) \\ \wedge \\ a = 4(3q) + 2 \ \vee\ a = 4(3q+2) + 2 \\ \wedge \\ a = 3(4q) + 2 \ \vee\ a = 3(4q+3) + 1 \end{array} \right. \\
&\left[\begin{array}{l} a \text{ da resto cero al dividir por } 2 \\ \text{y} \\ a \text{ da resto distinto de cero al dividir por } 4 \\ \text{y} \\ a \text{ da resto distinto de cero al dividir por } 3 \end{array} \right] \\
&\implies \left\{ \begin{array}{l} \exists q_1 \in \mathbb{Z} : a = 2q_1 \\ \wedge \\ \exists q_2, r_2 \in \mathbb{Z} : a = 4q_2 + r_2,\ r_2 \neq 0 \\ \wedge \\ \exists q_3, r_3 \in \mathbb{Z} : a = 3q_3 + r_3,\ r_3 \neq 0 \end{array} \right. \\
&\iff \left\{ \begin{array}{l} a \in A \\ \wedge \\ a \notin B \\ \wedge \\ a \notin C \end{array} \right. \\
&\iff \left\{ \begin{array}{l} a \in A \\ \wedge \\ a \in B^c \\ \wedge \\ a \in C^c \end{array} \right. \\
&\iff a \in A \cap B^c \cap C^c \\
&\iff a \in (A \setminus B) \cap (A \setminus C)
\end{aligned}
$$

Razonando igual que anteriormente,

$$\{n : n = 12q + r,\ q \in \mathbb{Z},\ r \in \{2, 10\}\} \subseteq (A \setminus B) \cap (A \setminus C)$$

y, de nuevo, por la doble inclusión de conjuntos, (3.2.5), tendremos que

$$(A \setminus B) \cap (A \setminus C) = \{n : n = 12q + r,\ q \in \mathbb{Z},\ r \in \{2, 10\}\}$$

(e) $(A \setminus C) \setminus (A \setminus B)$.

Utilizando las leyes del Álgebra de conjuntos para simplificar la expresión,

$$
\begin{aligned}
(A \setminus C) \setminus (A \setminus B) &= (A \cap C^c) \cap (A \cap B^c)^c \\
&= (A \cap C^c) \cap (A^c \cup B) \\
&= (A \cap C^c \cap A^c) \cup (A \cap C^c \cap B) \\
&\quad [B \subseteq A \Longrightarrow A \cap B = B] \\
&= \emptyset \cup (B \cap C^c) \\
&= B \cap C^c \\
&= B \setminus C \\
&= \{n : n = 12q + r,\ q \in \mathbb{Z},\ r \in \{4, 8\}\}
\end{aligned}
$$

(f) $(A \setminus C) \setminus (B \setminus C)$.

Utilizando las leyes del Álgebra de conjuntos,

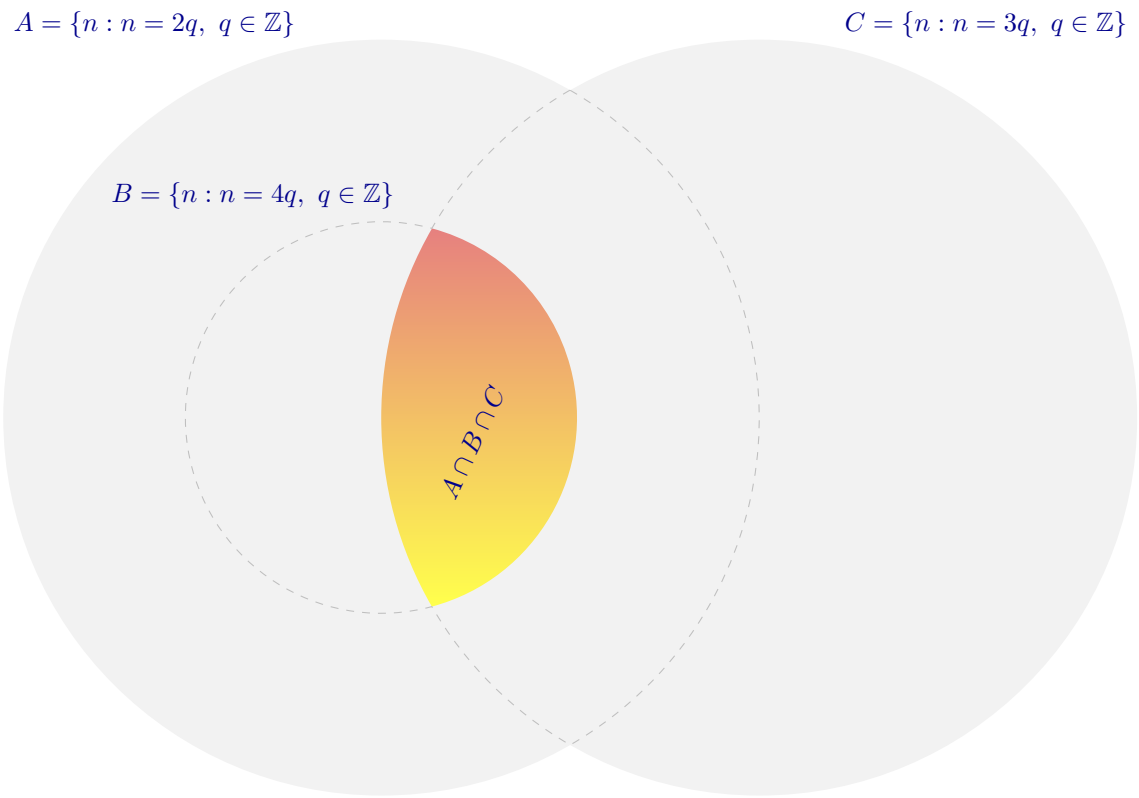
$$\begin{aligned}(A \setminus C) \setminus (B \setminus C) &= (A \cap C^c) \cap (B \cap C^c)^c \\ &= (A \cap C^c) \cap (B^c \cup C) \\ &= (A \cap C^c \cap B^c) \cup (A \cap C^c \cap C) \\ &= (A \cap C^c \cap B^c) \cup \emptyset \\ &= A \cap B^c \cap C^c \\ &= \{n : n = 12q + r,\ q \in \mathbb{Z},\ r \in \{2, 10\}\}\end{aligned}$$

(g) $(A \setminus C) \cap (B \setminus C)$.

Utilizando, de nuevo, las leyes del Álgebra de conjuntos,

$$\begin{aligned}(A \setminus C) \cap (B \setminus C) &= A \cap C^c \cap B \cap C^c \\ &[B \subseteq A \Longrightarrow A \cap B = B] \\ &= B \cap C^c \\ &= B \setminus C \\ &= \{n : n = 12q + r,\ q \in \mathbb{Z},\ r \in \{4, 8\}\}\end{aligned}$$

(h) $A \cap B \cap C$.



Sea a cualquier número entero. Entonces,

$$\begin{aligned} a \in (A \cap B \cap C) &\iff a \in (B \cap C) && \{B \subseteq A \Longrightarrow A \cap B = B\} \\ &\iff \begin{cases} a \in B \\ \text{y} \\ a \in C \end{cases} \\ &\iff \begin{cases} \exists q_1 \in \mathbb{Z} : a = 4q_1 \\ \text{y} \\ \exists q_2 \in \mathbb{Z} : a = 3q_2 \end{cases} \\ &\iff \exists q \in \mathbb{Z} : a = \text{m.c.m.}(3,4)q \\ &\iff \exists q \in \mathbb{Z} : a = 12q \\ &\iff a \in \{n : n = 12q,\ q \in \mathbb{Z}\} \end{aligned}$$

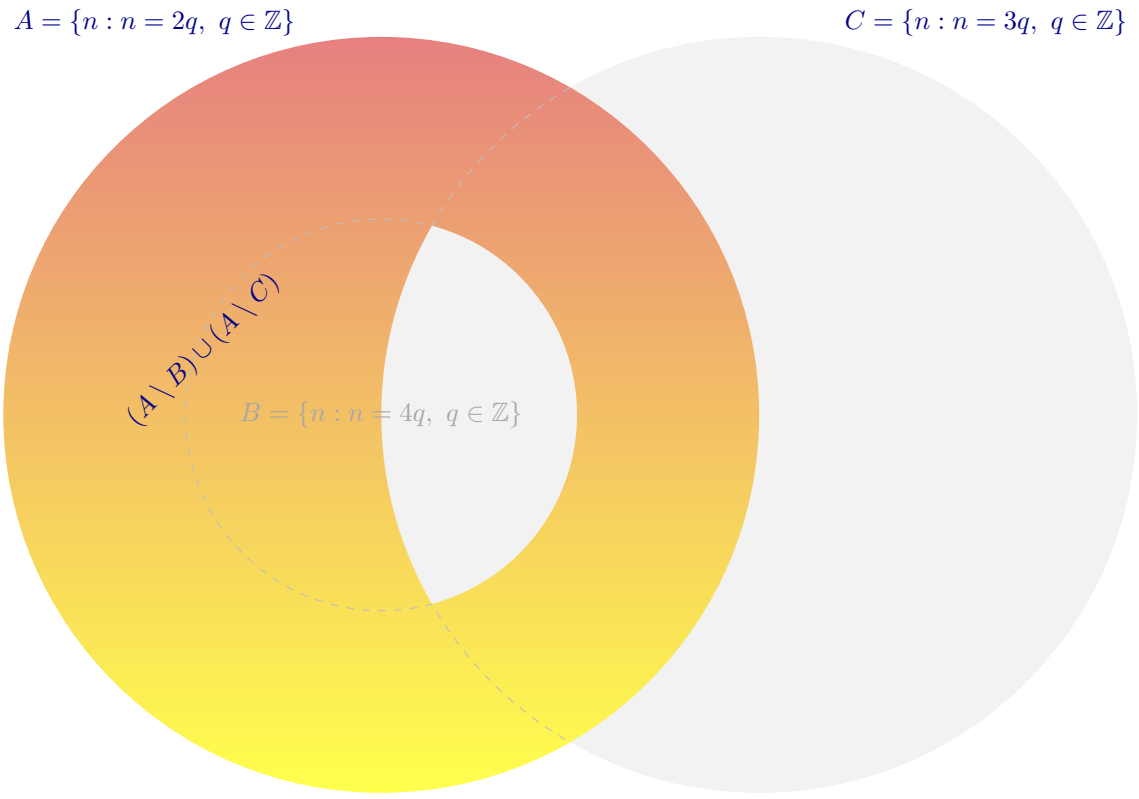
Como a era cualquiera, hemos probado que la proposición,

$$\forall x, (x \in (A \cap B \cap C) \longleftrightarrow x \in \{n : n = 12q,\ q \in \mathbb{Z}\})$$

lo cual, por el axioma de extensión, (3.1.7), significa que

$$A \cap B \cap C = \{n : n = 12q,\ q \in \mathbb{Z}\}$$

(i) Calcular $(A \setminus B) \cup (A \setminus C)$.



Utilizando las leyes del Álgebra de conjuntos para hacer operaciones,

$$\begin{aligned} (A \setminus B) \cup (A \setminus C) &= (A \cap B^c) \cup (A \cap C^c) \\ &= A \cap (B^c \cup C^c) \\ &= A \cap (B \cap C)^c \end{aligned}$$

Sea a cualquier número entero. Entonces,

$$
\begin{aligned}
a \in (A \setminus B) \cup (A \setminus C) &\iff a \in A \cap (B \cap C)^c \\
&\iff \left\{ \begin{array}{l} a \in A \\ \wedge \\ a \in (B \cap C)^c \end{array} \right. \\
&\iff \left\{ \begin{array}{l} a \in A \\ \wedge \\ a \notin (B \cap C) \end{array} \right. \\
&\iff \left\{ \begin{array}{l} \exists q_1 \in \mathbb{Z} : a = 2q_1 \\ \wedge \\ \exists q_2, r_2 \in \mathbb{Z} : a = 12q_2 + r_2,\ r_2 \neq 0 \end{array} \right. \\
&\text{[Dividiendo } q_1 \text{ por 6, } q_1 = 6q_3 + r_3, \text{ con } q_3 \in \mathbb{Z} \text{ y } r_3 \in \{0,1,2,3,4,5\}] \\
&\Longrightarrow \left\{ \begin{array}{l} \exists q_3, r_3 \in \mathbb{Z} : a = 2(6q_3 + r_3),\ r_3 \in \{0,1,2,3,4,5\} \\ \wedge \\ \exists q_2, r_2 \in \mathbb{Z} : a = 12q_2 + r_2,\ r_2 \neq 0 \end{array} \right. \\
&\iff \left\{ \begin{array}{l} \exists q_3, r_3 \in \mathbb{Z} : a = 12q_3 + 2r_3,\ 2r_3 \in \{0,2,4,6,8,10\} \\ \wedge \\ \exists q_2, r_2 \in \mathbb{Z} : a = 12q_2 + r_2,\ r_2 \in \{1,2,3,4,5,6,7,8,9,10,11\} \end{array} \right. \\
&\left[\begin{array}{l} \text{Unicidad de cociente y resto (5.2.1)} \left\{ \begin{array}{l} q_2 = q_3 \\ r_2 = 2r_3 \end{array} \right. \\ \text{Tomando } q = q_2 = q_3 \text{ y } r = r_2 = 2r_3 \end{array} \right] \\
&\Longrightarrow \left\{ \begin{array}{l} \exists q, r \in \mathbb{Z} : a = 12q + r, \\ r \in \{0,2,4,6,8,10\} \cap \{1,2,3,4,5,6,7,8,9,10,11\} \end{array} \right\} \\
&\iff \exists q, r \in \mathbb{Z} : a = 12q + r,\ r \in \{2,4,6,8,10\} \\
&\iff a \in \{n : n = 12q + r,\ r \in \{2,4,6,8,10\}\}
\end{aligned}
$$

De la arbitrariedad de a se sigue que la proposición,

$$\forall x, (x \in (A \setminus B) \cup (A \setminus C) \longrightarrow x \in \{n : n = 12q + r,\ q \in \mathbb{Z},\ r \in \{2,4,6,8,10\}\})$$

es verdadera y, por la definición de inclusión de conjuntos, (3.2.1),

$$(A \setminus B) \cup (A \setminus C) \subseteq \{n : n = 12q + r,\ q \in \mathbb{Z},\ r \in \{2,4,6,8,10\}\}$$

Recíprocamente,

$$
\begin{aligned}
a \in \{n : n = 12q + r,\ q \in \mathbb{Z},\ r \in \{2,4,6,8,10\}\} \iff & \exists q \in \mathbb{Z} : \left\{ \begin{array}{l} a = 12q + 2 \\ \vee \\ a = 12q + 4 \\ \vee \\ a = 12q + 6 \\ \vee \\ a = 12q + 8 \\ \vee \\ a = 12q + 10 \end{array} \right. \\
\iff & \exists q \in \mathbb{Z} : \left\{ \begin{array}{l} a = 2(6q+1) \ \wedge\ a = 12q + 2 \\ \vee \\ a = 2(6q+2) \ \wedge\ a = 12q + 4 \\ \vee \\ a = 2(6q+3) \ \wedge\ a = 12q + 6 \\ \vee \\ a = 2(6q+4) \ \wedge\ a = 12q + 8 \\ \vee \\ a = 2(6q+5) \ \wedge\ a = 12q + 10 \end{array} \right. \\
& \left[\begin{array}{l} a \text{ da resto cero al dividir por } 2 \\ \text{y} \\ a \text{ da resto distinto de cero al dividir por } 12 \end{array} \right] \\
\Longrightarrow & \left\{ \begin{array}{l} \exists q_1 \in \mathbb{Z} : a = 2q_1 \\ \wedge \\ \exists q_2, r_2 \in \mathbb{Z} : a = 12q_2 + r_2,\ r_2 \neq 0 \end{array} \right. \\
\iff & \left\{ \begin{array}{l} a \in A \\ \wedge \\ a \notin (B \cap C) \end{array} \right. \\
\iff & \left\{ \begin{array}{l} a \in A \\ \wedge \\ a \in (B \cap C)^c \end{array} \right. \\
\iff & a \in A \cap (B \cap C)^c \\
\iff & a \in (A \setminus B) \cup (A \setminus C)
\end{aligned}
$$

De la arbitrariedad de a se sigue que la proposición,

$$\forall x, (x \in \{n : n = 12q + r,\ q \in \mathbb{Z},\ r \in \{2,4,6,8,10\}\} \longrightarrow x \in (A \setminus B) \cup (A \setminus C))$$

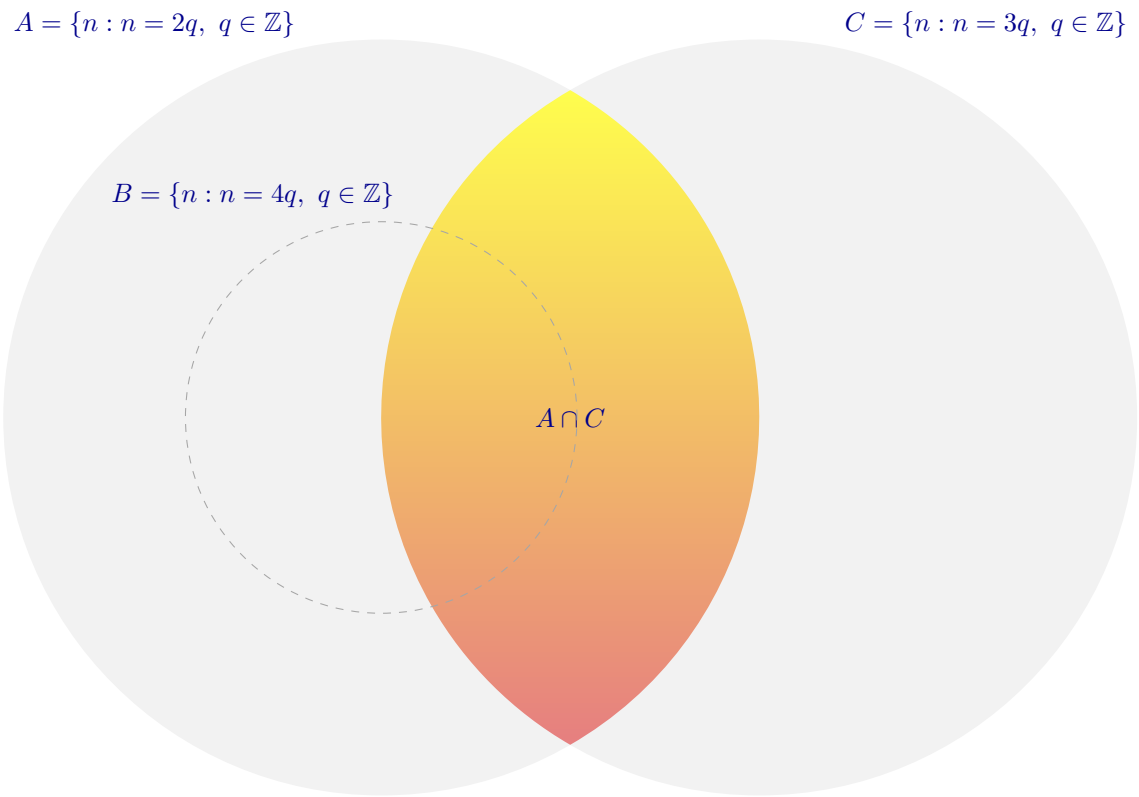
es verdadera y, por la definición de inclusión de conjuntos, (3.2.1),

$$\{n : n = 12q + r,\ q \in \mathbb{Z},\ r \in \{2,4,6,8,10\}\} \subseteq (A \setminus B) \cup (A \setminus C)$$

Finalmente, por la doble inclusión de conjuntos, (3.2.5), tendremos que

$$(A \setminus B) \cup (A \setminus C) = \{n : n = 12q + r,\ q \in \mathbb{Z},\ r \in \{2,4,6,8,10\}\}$$

(j) $A \cap C$.



Sea a cualquier número entero. Entonces,

$$
\begin{aligned}
a \in (A \cap C) &\iff \begin{cases} a \in A \\ \text{y} \\ a \in C \end{cases} \\
&\iff \begin{cases} \exists q_1 \in \mathbb{Z} : a = 2q_1 \\ \text{y} \\ \exists q_2 \in \mathbb{Z} : a = 3q_2 \end{cases} \\
&\iff \exists q \in \mathbb{Z} : a = \text{m.c.m.}(2,3)q \\
&\iff \exists q \in \mathbb{Z} : a = 6q \\
&\iff a \in \{n : n = 6q,\ q \in \mathbb{Z}\}
\end{aligned}
$$

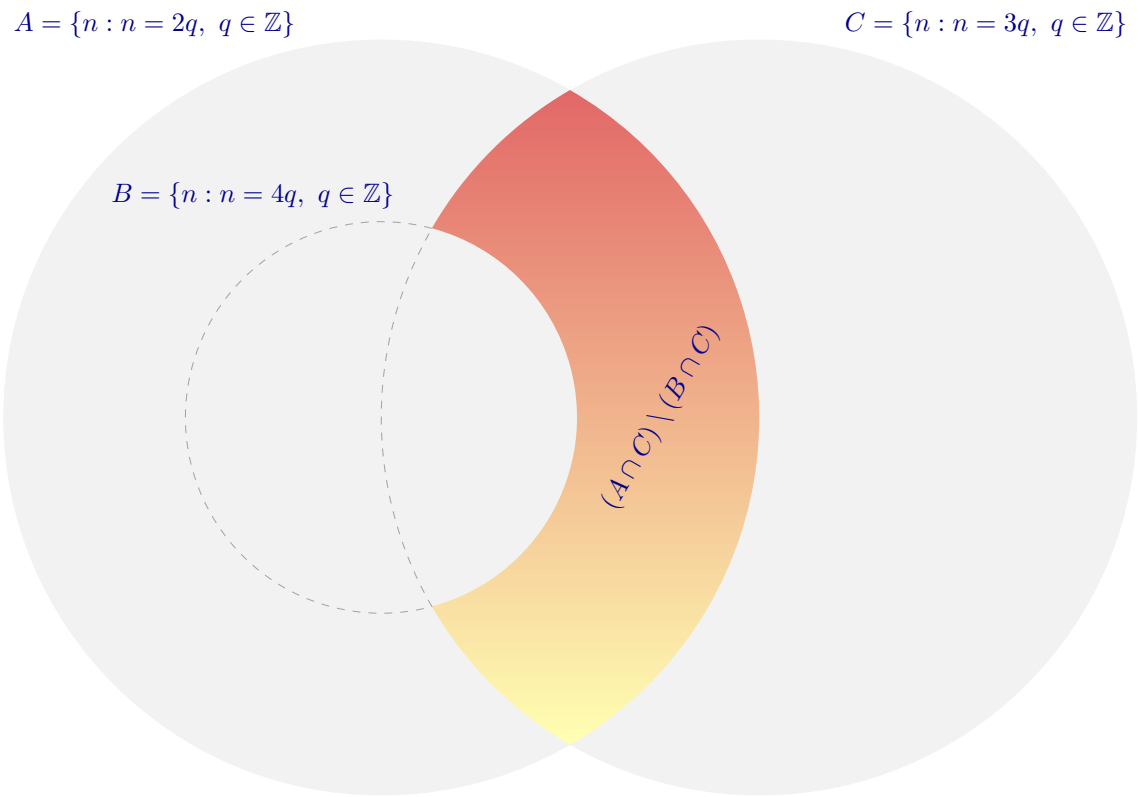
Como a era cualquiera, hemos probado que la proposición,

$$\forall x, (x \in (A \cap C) \longleftrightarrow x \in \{n : n = 6q,\ q \in \mathbb{Z}\})$$

lo cual, por el axioma de extensión, (3.1.7), significa que

$$A \cap C = \{n : n = 6q,\ q \in \mathbb{Z}\}$$

(k) $(A \cap C) \setminus (B \cap C)$.



Según resultados obtenidos en apartados anteriores,

$$\begin{aligned} A \cap C &= \{n : n = 6q,\ q \in \mathbb{Z}\} \\ B \cap C &= \{n : n = 12q,\ q \in \mathbb{Z}\} \end{aligned}$$

Pues bien, si a es cualquier entero, entonces,

$$\begin{aligned} a \in (A \cap C) \setminus (B \cap C) &\iff \begin{cases} a \in (A \cap C) \\ \wedge \\ a \notin (B \cap C) \end{cases} \\ &\iff \begin{cases} \exists q_1 \in \mathbb{Z} : a = 6q_1 \\ \wedge \\ \exists q_2, r_2 \in \mathbb{Z} : a = 12q_2 + r_2,\ r_2 \neq 0 \end{cases} \\ &\text{[Dividiendo } q_1 \text{ por 2, } q_1 = 2q_3 + r_3,\ q_3 \in \mathbb{Z},\ r_3 \in \{0,1\}] \\ &\implies \begin{cases} \exists q_3, r_3 \in \mathbb{Z} : a = 6(2q_3 + r_3),\ r_3 \in \{0,1\} \\ \wedge \\ \exists q_2, r_2 \in \mathbb{Z} : a = 12q_2 + r_2,\ r_2 \in \{1,2,3,4,5,6,7,8,9,10,11\} \end{cases} \\ &\iff \begin{cases} \exists q_3, r_3 \in \mathbb{Z} : a = 12q_3 + 6r_3,\ 6r_3 \in \{0,6\} \\ \wedge \\ \exists q_2, r_2 \in \mathbb{Z} : a = 12q_2 + r_2,\ r_2 \in \{1,2,3,4,5,6,7,8,9,10,11\} \end{cases} \\ &\left[\begin{array}{l} \text{Unicidad de cociente y resto (5.2.1)} \begin{cases} q_2 = q_3 \\ r_2 = 6r_3 \end{cases} \\ \text{Tomando } q = q_2 = q_3 \text{ y } r = r_2 = 6r_3 \end{array} \right] \\ &\implies \exists q, r \in \mathbb{Z} : a = 12q + r,\ r \in \{0,6\} \cap \{1,2,3,4,5,6,7,8,9,10,11\} \\ &\iff \exists q \in \mathbb{Z} : a = 12q + 6 \\ &\iff a \in \{n : n = 12q + 6,\ q \in \mathbb{Z}\} \end{aligned}$$

De la arbitrariedad de a se sigue que la proposición,

$$\forall x, (x \in (A \cap C) \setminus (B \cap C) \longrightarrow x \in \{n : n = 12q + 6,\ q \in \mathbb{Z}\})$$

es verdadera y, por la definición de inclusión de conjuntos, (3.2.1),

$$(A \cap C) \setminus (B \cap C) \subseteq \{n : n = 12q + 6,\ q \in \mathbb{Z}\}$$

Recíprocamente,

$$\begin{aligned}
a \in \{n : n = 12q + 6,\ q \in \mathbb{Z}\} &\iff \exists q \in \mathbb{Z} : a = 12q + 6 \\
&\iff \exists q \in \mathbb{Z} : \begin{cases} a = 6(2q + 1) \\ \wedge \\ a = 12q + 6 \end{cases} \\
&\left[\begin{array}{l} a \text{ da resto cero al dividir por } 6 \\ \text{y} \\ a \text{ da resto distinto de cero al dividir por } 12 \end{array}\right] \\
&\implies \begin{cases} \exists q_1 \in \mathbb{Z} : a = 6q_1 \\ \wedge \\ \exists q_2, r_2 \in \mathbb{Z} : a = 12q_2 + r_2,\ r_2 \neq 0 \end{cases} \\
&\iff \begin{cases} a \in (A \cap C) \\ \wedge \\ a \notin (B \cap C) \end{cases} \\
&\iff a \in (A \cap C) \setminus (B \cap C)
\end{aligned}$$

De la arbitrariedad de a se sigue que la proposición,

$$\forall x, (x \in \{n : n = 12q + 6,\ q \in \mathbb{Z}\} \longrightarrow x \in (A \cap C) \setminus (B \cap C))$$

es verdadera y, por la definición de inclusión de conjuntos, (3.2.1),

$$\{n : n = 12q + 6,\ q \in \mathbb{Z}\} \subseteq (A \cap C) \setminus (B \cap C)$$

Finalmente, por la doble inclusión de conjuntos, (3.2.5), tendremos que

$$(A \cap C) \setminus (B \cap C) = \{n : n = 12q + 6,\ q \in \mathbb{Z}\}$$

(l) $(A \setminus B) \cap C$.

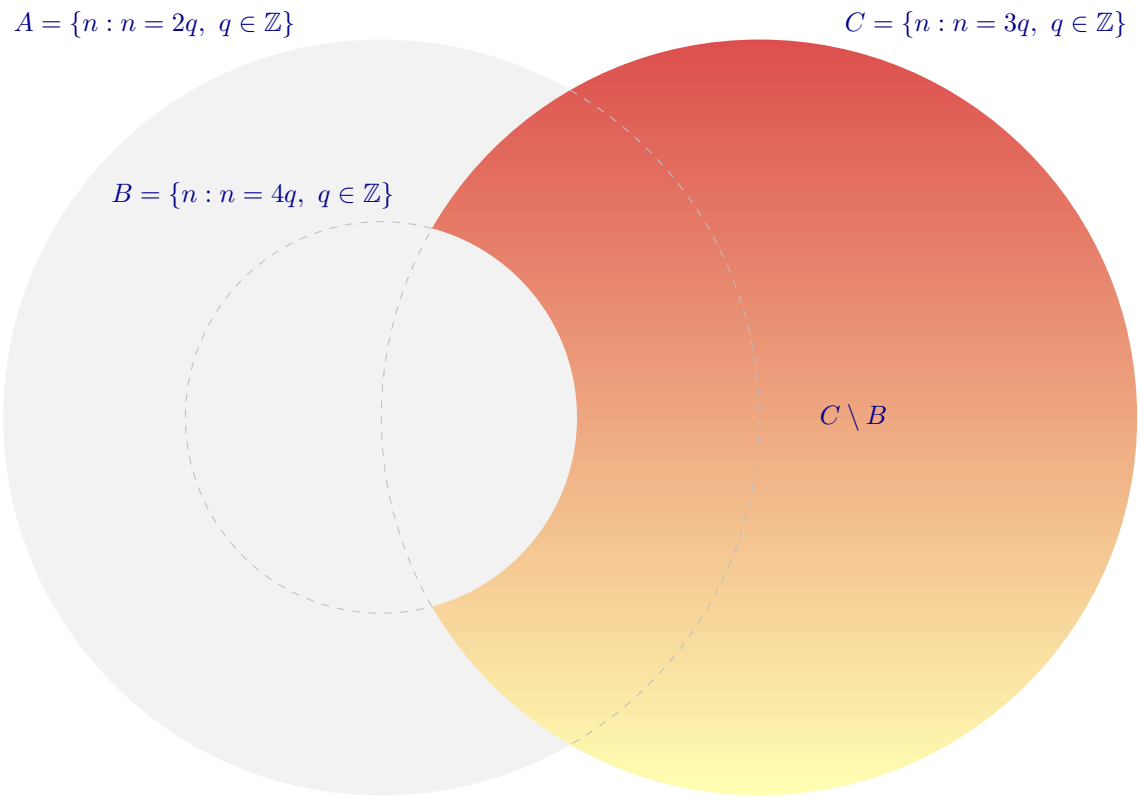
Es igual al anterior, ya que

$$\begin{aligned}
(A \cap C) \setminus (B \cap C) &= (A \cap C) \cap (B \cap C)^c \\
&= (A \cap C) \cap (B^c \cup C^c) \\
&= (A \cap C \cap B^c) \cup (A \cap C \cap C^c) \\
&= (A \cap C \cap B^c) \cup \emptyset \\
&= A \cap B^c \cap C \\
&= (A \setminus B) \cap C
\end{aligned}$$

luego,

$$(A \setminus B) \cap C = \{n : n = 12q + 6,\ q \in \mathbb{Z}\}$$

(m) $C \setminus B$.



Sea a un número arbitrariamente elegido en $\mathbb{Z}$. Entonces,

$$a \in C \setminus B \iff \begin{cases} a \in C \\ \wedge \\ a \notin B \end{cases}$$

$$\iff \begin{cases} \exists q_1 \in \mathbb{Z} : a = 3q_1 \\ \wedge \\ \exists q_2, r_2 \in \mathbb{Z} : a = 4q_2 + r_2,\ r_2 \neq 0 \end{cases}$$

$$\left[\begin{array}{l} \text{m.c.m.}(3,4) = 12 \\ \text{Dividiendo } q_1 \text{ por } 4,\ q_1 = 4q_3 + r_3,\ q_3 \in \mathbb{Z},\ r_3 \in \{0,1,2,3\} \\ \text{Dividiendo } q_2 \text{ por } 3,\ q_2 = 3q_4 + r_4,\ q_4 \in \mathbb{Z},\ r_4 \in \{0,1,2\} \end{array}\right]$$

$$\implies \begin{cases} \exists q_3, r_3 \in \mathbb{Z} : a = 3(4q_3 + r_3),\ r_3 \in \{0,1,2,3\} \\ \wedge \\ \exists q_4, r_4 \in \mathbb{Z} : a = 4(3q_4 + r_4) + r_2,\ r_2 \in \{1,2,3\},\ r_4 \in \{0,1,2\} \end{cases}$$

$$\implies \begin{cases} \exists q_3, r_3 \in \mathbb{Z} : a = 12q_3 + 3r_3,\ 3r_3 \in \{0,3,6,9\} \\ \wedge \\ \exists q_4, r_4 \in \mathbb{Z} a = 12q_4 + 4r_4 + r_2,\ 4r_4 + r_2 \in \{1,2,3,5,6,7,9,10,11\} \end{cases}$$

$$\left[\begin{array}{l} \text{Unicidad de cociente y resto (5.2.1)} \begin{cases} q_3 = q_4 \\ 3r_3 = r_2 + 4r_4 \end{cases} \\ \text{Tomando } q = q_3 = q_4 \text{ y } r = 3r_3 = r_2 + 4r_4 \end{array}\right]$$

$$\implies \exists q, r \in \mathbb{Z} : a = 12q + r,\ r \in (\{0,3,6,9\} \cap \{1,2,3,5,6,7,9,10,11\})$$

$$\iff \exists q, r \in \mathbb{Z} : a = 12q + r,\ r \in \{3,6,9\}$$

$$\iff a \in \{n : n = 12q + r,\ q \in \mathbb{Z},\ r \in \{3,6,9\}\}$$

De la arbitrariedad en la elección de a se sigue que la proposición,

$$\forall x, (x \in C \setminus B \longrightarrow x \in \{n : n = 12q + r,\ q \in \mathbb{Z},\ r \in \{3,6,9\}\})$$

es verdadera y, por la definición de inclusión de conjuntos, (3.2.1),

$$C \setminus B \subseteq \{n : n = 12q + r,\ q \in \mathbb{Z},\ r \in \{3, 6, 9\}\}$$

Recíprocamente,

$$\begin{aligned}
a \in \{n : n = 12q + r,\ q \in \mathbb{Z},\ r \in \{3, 6, 9\}\} &\iff \exists q \in \mathbb{Z} : \begin{cases} a = 12q + 3 \\ \vee \\ a = 12q + 6 \\ \vee \\ a = 12q + 9 \end{cases} \\
&\iff \exists q \in \mathbb{Z} : \begin{cases} a = 3(4q + 1) \ \wedge\ a = 4(3q) + 3 \\ \vee \\ a = 3(4q + 2) \ \wedge\ a = 4(3q + 1) + 2 \\ \vee \\ a = 3(4q + 3) \ \wedge\ a = 4(3q + 2) + 1 \end{cases} \\
&\left[\begin{array}{l} a \text{ da resto cero al dividir por } 3 \\ \text{y} \\ a \text{ da resto distinto de cero al dividir por } 4 \end{array}\right] \\
&\implies \begin{cases} \exists q_1 \in \mathbb{Z} : a = 3q_1 \\ \wedge \\ \exists q_2 \in \mathbb{Z} : a = 4q_2 + r_2,\ r_2 \neq 0 \end{cases} \\
&\iff \begin{cases} a \in C \\ \wedge \\ a \notin B \end{cases} \\
&\iff a \in C \setminus B
\end{aligned}$$

De la arbitrariedad de a se sigue que la proposición,

$$\forall x, (x \in \{n : n = 12q + r,\ q \in \mathbb{Z},\ r \in \{3, 6, 9\}\} \longrightarrow x \in (C \setminus B))$$

es verdadera y, por la definición de inclusión de conjuntos, (3.2.1),

$$\{n : n = 12q + r,\ q \in \mathbb{Z},\ r \in \{3, 6, 9\}\} \subseteq (C \setminus B)$$

Finalmente, por la doble inclusión de conjuntos, (3.2.5), tendremos que

$$C \setminus B = \{n : n = 12q + r,\ q \in \mathbb{Z},\ r \in \{3, 6, 9\}\}$$

(n) $(C \setminus B) \cap A$.

Utilizando las leyes del Álgebra de conjuntos,

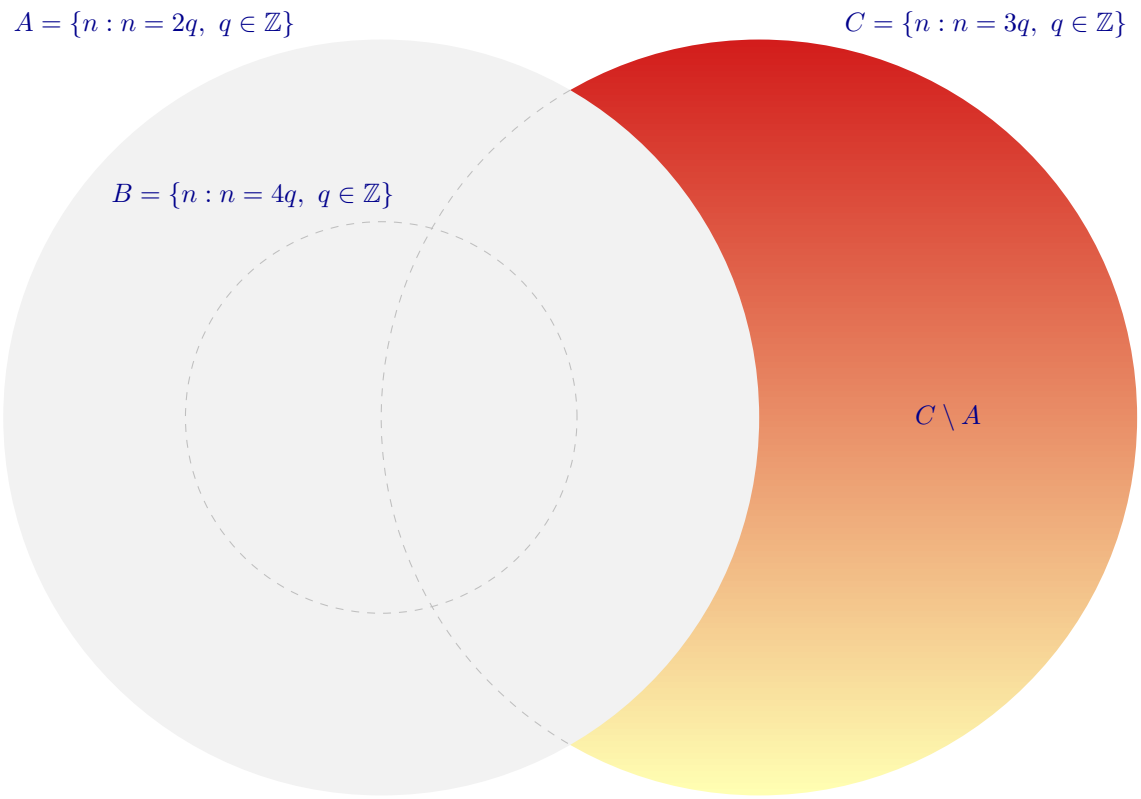
$$(C \setminus B) \cap A = C \cap B^c \cap A = A \cap B^c \cap C = \{n : n = 12q + 6,\ q \in \mathbb{Z}\}$$

(o) $(C \setminus B) \cap (A \setminus B)$.

Utilizando las leyes del Álgebra de conjuntos,

$$(C \setminus B) \cap (A \setminus B) = (C \cap B^c) \cap (A \cap B^c) = A \cap B^c \cap C = \{n : n = 12q + 6,\ q \in \mathbb{Z}\}$$

(p) $C \setminus A$.



Sea a cualquier número entero. Entonces,

$$
\begin{aligned}
a \in C \setminus A \iff & \begin{cases} a \in C \\ \wedge \\ a \notin A \end{cases} \\
\iff & \begin{cases} \exists q_1 \in \mathbb{Z} : a = 3q_1 \\ \wedge \\ \exists q_2 \in \mathbb{Z} : a = 2q_2 + 1 \end{cases} \\
& \left[\begin{array}{l} \text{m.c.m.}(2,3) = 6 \\ \text{Dividiendo } q_1 \text{ por } 2, q_1 = 2q_3 + r_3,\ q_3 \in \mathbb{Z}\ r_3 \in \{0,1\} \\ \text{Dividiendo } q_2 \text{ por } 3, q_2 = 3q_4 + r_4,\ q_4 \in \mathbb{Z}\ r_4 \in \{0,1,2\} \end{array} \right] \\
\implies & \begin{cases} \exists q_3, r_3 \in \mathbb{Z} : a = 3(2q_3 + r_3),\ r_3 \in \{0,1\} \\ \wedge \\ \exists q_4, r_4 \in \mathbb{Z} : a = 2(3q_4 + r_4) + 1, r_4 \in \{0,1,2\} \end{cases} \\
\implies & \begin{cases} \exists q_3, r_3 \in \mathbb{Z} : a = 6q_3 + 3r_3,\ 3r_3 \in \{0,3\} \\ \wedge \\ \exists q_4, r_4 \in \mathbb{Z} : a = 6q_4 + 2r_4 + 1,\ 2r_4 + 1 \in \{1,3,5\} \end{cases} \\
& \left[\begin{array}{l} \text{Unicidad de cociente y resto (5.2.1)} \begin{cases} q_3 = q_4 \\ 3r_3 = 2r_4 + 1 \end{cases} \\ \text{Tomando } q = q_3 = q_4,\ r = 3r_3 = 2r_4 + 1 \end{array} \right] \\
\implies & \exists q, r \in \mathbb{Z} : a = 6q + r,\ r \in (\{0,3\} \cap \{1,3,5\}) \\
\iff & \exists q, r \in \mathbb{Z} : a = 6q + r,\ r \in \{3\} \\
\iff & a \in \{n : n = 6q + 3,\ q \in \mathbb{Z}\}
\end{aligned}
$$

Como a era cualquiera, la proposición,

$$\forall x, (x \in (C \setminus A) \longrightarrow x \in \{n : n = 6q + 3,\ q \in \mathbb{Z}\})$$

es verdadera y, por la definición de inclusión de conjuntos, (3.2.1),

$$C \setminus A \subseteq \{n : n = 6q + 3,\ q \in \mathbb{Z}\}$$

Recíprocamente,

$$\begin{aligned}
a \in \{n : n = 6q + 3,\ q \in \mathbb{Z}\} &\iff \exists q \in \mathbb{Z} : a = 6q + 3 \\
&\iff \exists q \in \mathbb{Z} : \left\{ \begin{array}{l} a = 3(2q + 1) \\ \wedge \\ a = 2(3q + 1) + 1 \end{array} \right. \\
&\left[\begin{array}{l} a \text{ da resto cero al dividir por } 3 \\ \text{y} \\ a \text{ da resto distinto de cero al dividir por } 2 \end{array} \right] \\
&\implies \left\{ \begin{array}{l} \exists q_1 \in \mathbb{Z} : a = 3q_1 \\ \exists q_2 \in \mathbb{Z} : a = 2q_2 + 1 \end{array} \right. \\
&\iff \left\{ \begin{array}{l} a \in C \\ \wedge \\ a \notin A \end{array} \right. \\
&\iff a \in (C \setminus A)
\end{aligned}$$

Como a era cualquier entero, la proposición,

$$\forall x, (x \in \{n : n = 6q + 3,\ q \in \mathbb{Z}\} \longrightarrow x \in (C \setminus A))$$

es verdadera y, por la definición de inclusión de conjuntos, (3.2.1),

$$\{n : n = 6q + 3,\ q \in \mathbb{Z}\} \subseteq (C \setminus A)$$

Finalmente, por la doble inclusión de conjuntos, (3.2.5), tendremos que

$$C \setminus A = \{n : n = 6q + 3,\ q \in \mathbb{Z}\}$$

(q) $(C \setminus B) \setminus (A \setminus B)$.

Utilizando las leyes del Álgebra de conjuntos para simplificar,

$$\begin{aligned}
(C \setminus B) \setminus (A \setminus B) &= (C \cap B^c) \cap (A \cap B^c)^c \\
&= (C \cap B^c \cap A^c) \cup (C \cap B^c \cap B) \\
&\quad [B \subseteq A \Longrightarrow A^c \subseteq B^c \Longrightarrow A^c \cap B^c = A^c] \\
&= (C \cap A^c) \cup \emptyset \\
&= C \setminus A \\
&= \{n : n = 6q + 3,\ q \in \mathbb{Z}\}
\end{aligned}$$

(r) $(C \setminus B) \setminus (C \setminus A)$.

Utilizando las leyes del Álgebra de conjuntos para simplificar,

$$\begin{aligned}
(C \setminus B) \setminus (C \setminus A) &= (C \cap B^c) \cap (C \cap A^c)^c \\
&= (C \cap B^c) \cap (C^c \cup A) \\
&= (C \cap B^c \cap C^c) \cap (C \cap B^c \cap A) \\
&= \emptyset \cup (A \cap B^c \cap C) \\
&= A \cap B^c \cap C \\
&= \{n : n = 12q + 6,\ q \in \mathbb{Z}\}
\end{aligned}$$

(s) $(C \setminus B) \cap (C \setminus A)$.

Utilizando las leyes del Álgebra de conjuntos para simplificar,

$$B \subseteq A \Longrightarrow A^c \subseteq C^c \Longrightarrow (C \cap A^c) \subseteq (C \cap B^c) \Longrightarrow (C \setminus A) \subseteq (C \setminus B)$$

luego,

$$(C \setminus B) \cap (C \setminus A) = C \setminus A = \{n : n = 6q + 3,\ q \in \mathbb{Z}\}$$

♦♦♦

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 4.11

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 4.12

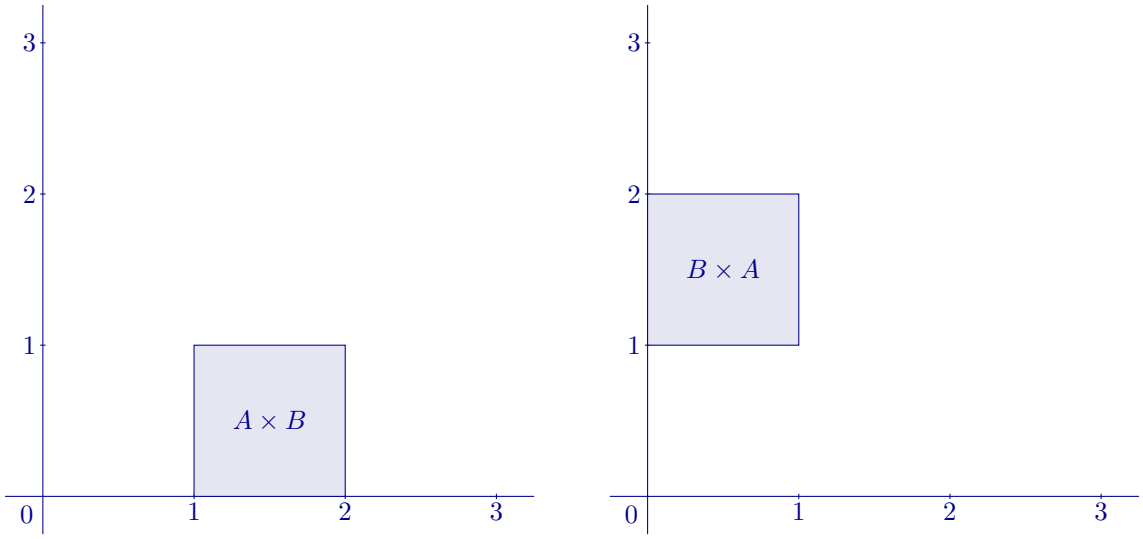
Sean $A = \{x \in \mathbb{R} : 1 \leqslant x \leqslant 2\}$ y $B = \{y \in \mathbb{R} : 0 \leqslant y \leqslant 1\}$. Representar gráficamente $A \times B$ y $B \times A$.

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 4.13

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 4.14

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,
$$A \times B \neq \emptyset \iff \exists (a,b) \in A \times B \iff \left\{\begin{array}{ccc} \exists a \in A & \iff & A \neq \emptyset \\ \text{y} & & \text{y} \\ \exists b \in B & \iff & B \neq \emptyset \end{array}\right.$$
es decir, hemos probado por la contrarrecíproca, (1.5.4), que
$$A \times B = \emptyset \iff A = \emptyset \text{ ó } B = \emptyset$$

♦

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 4.15

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)

$$(A \cup B) \times C = \{(1,3),(1,4),(1,7),(2,3),(2,4),(2,7),(3,3),(3,4),(3,7),(4,3),(4,4),(4,7),(5,3),(5,4),(5,7)\}$$

(e)

$$(A \times C) \cup (B \times C) = \{(1,3),(1,4),(1,7),(2,3),(2,4),(2,7),(3,3),(3,4),(3,7),(4,3),(4,4),(4,7),(5,3),(5,4),(5,7)\}$$

♦

Ejemplo 4.16

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 4.17

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 4.18

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 4.19

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 4.20

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 II

Teoría de Números

Lección 5

Divisibilidad. Algoritmo de la División

Dios hizo los enteros, el resto es obra del hombre.

Leopold Kronecker (1823-1891)

5.1 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 $12 = 2 \cdot 6$.

5.1.1 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 $a \mid b$, es decir,

$$a \mid b \iff \exists q \in \mathbb{Z} : b = aq$$

♦

Nota 5.1 Observemos lo siguiente:

$$a \text{ divide a } b \iff b = aq;\ q \in \mathbb{Z} \iff b \text{ es múltiplo de } a$$

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 $a \mid b$.

♦

Ejemplo 5.1

(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 $5 = 3 \cdot q$.

♦

Nota 5.2 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.

♦

5.1.2 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 $|a| = |b|$.

(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, $1 \mid a$.

(ii) Sea a cualquier número entero. Entonces,

$$0 = a \cdot 0, \text{ con } 0 \in \mathbb{Z}$$

luego, $a \mid 0$

(iii) $a\big|b$ y $b\big|a \iff |a| = |b|, \forall a, b \in \mathbb{Z} \setminus \{0\}$

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 $a\big|b$ y $b\big|a \implies |a| = |b|, \forall a, b \in \mathbb{Z} \setminus \{0\}$ En efecto,

$$\left.\begin{array}{l} a\big|b \iff \exists q_1 \in \mathbb{Z} : b = aq_1 \\ \text{y} \\ b\big|a \iff \exists q_2 \in \mathbb{Z} : a = bq_2 \end{array}\right\} \implies b = bq_1q_2 \implies b(1 - q_1q_2) = 0$$

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 $|a| = |b| \implies a\big|b$ y $b\big|a$

En efecto,

$$|a| = |b| \implies \begin{cases} a = b \implies \begin{cases} a = b \cdot 1,\ 1 \in \mathbb{Z} \implies b|a \\ \text{y} \\ b = a \cdot 1,\ 1 \in \mathbb{Z} \implies a|b \end{cases} \\ \text{o} \\ a = -b \implies \begin{cases} a = b(-1),\ -1 \in \mathbb{Z} \implies b\big|a \\ \text{y} \\ b = a(-1),\ -1 \in \mathbb{Z} \implies a\big|b \end{cases} \end{cases}$$

(iv) $a\big|b$ y $b\big|c \Longrightarrow a\big|c$. En efecto,

$$\left.\begin{array}{l} a\big|b \Longleftrightarrow \exists q_1 \in \mathbb{Z} : b = aq_1 \\ \text{y} \\ b\big|c \Longleftrightarrow \exists q_2 \in \mathbb{Z} : c = bq_2 \end{array}\right\} \Longrightarrow \quad c = aq_1q_2, \text{ con } q_1q_2 \in \mathbb{Z} \quad \Longleftrightarrow \quad a\big|c$$

(v) $a\big|b$ y $a\big|c \Longrightarrow a\big|pb + qc,\ \forall p, q \in \mathbb{Z}$. En efecto,

$$\left.\begin{array}{l} a\big|b \Longleftrightarrow \exists q_1 \in \mathbb{Z} : b = aq_1 \Longrightarrow pb = paq_1 \\ \text{y} \\ a\big|c \Longleftrightarrow \exists q_2 \in \mathbb{Z} : c = aq_2 \Longrightarrow qc = qaq_2 \end{array}\right\} \Longrightarrow pb + qc = a(pq_1 + qq_2),\ pq_1 + qq_2 \in \mathbb{Z} \Longleftrightarrow a\big|pb + qc$$

♦

Ejemplo 5.2

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,

$$\left.\begin{array}{l} a\big|b \\ \text{y} \\ a\big|c \end{array}\right\} \Longrightarrow \quad a\big|pb + qc,\ \forall p, q \in \mathbb{Z} \quad \{5.1.2\ (v)\}$$

$$\Longrightarrow \left\{\begin{array}{ll} a\big|b + c & \{\text{Tomando } p = q = 1\} \\ \text{y} & \\ a\big|b - c & \{\text{Tomando } p = 1 \text{ y } q = -1\} \end{array}\right.$$

♦

Ejemplo 5.3

Sean a, b, c y d números enteros con $a \neq 0$ y $c \neq 0$. Demuéstrese que

(a) Si $a\big|b$ y $c\big|d$, entonces $ac\big|bd$.

(b) $ac\big|bc$ si, y sólo si $a\big|b$.

Solución.

(a) Si $a\big|b$ y $c\big|d$, entonces $ac\big|bd$.
En efecto,

$$\left.\begin{array}{l} a\big|b \Longleftrightarrow \exists q_1 \in \mathbb{Z} : b = aq_1 \\ \text{y} \\ c\big|d \Longleftrightarrow \exists q_2 \in \mathbb{Z} : d = cq_2 \end{array}\right\} \Longrightarrow bd = acq_1q_2, \text{ con } q_1q_2 \in \mathbb{Z} \Longleftrightarrow ac\big|bd$$

(b) $ac \mid bc$ si, y sólo si $a \mid b$.

"Sólo si." En efecto, supongamos que $ac \mid bc$. 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,

$$a \mid b$$

"Si." En efecto, si $a \mid b$, como $c \mid c$, por el apartado (a) se sigue que $ac \mid bc$.

♦

Ejemplo 5.4

Sean a y b dos números enteros positivos. Probar que si $b \mid a$ y $b \mid (a+2)$, entonces $b = 1$ ó $b = 2$.

Solución.

Aplicando el resultado obtenido en el ejemplo 5.2,

$$\left.\begin{array}{l} b \mid a \\ \text{y} \\ b \mid a+2 \end{array}\right\} \Longrightarrow b \mid a + 2 - a \Longrightarrow b \mid 2 \Longrightarrow b = 1 \text{ o } b = 2$$

♦

Ejemplo 5.5

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 cualesquiera, probaremos que

$$\left.\begin{array}{l} a \text{ es impar} \\ \text{y} \\ b \text{ es impar} \end{array}\right\} \Longrightarrow a^2 + b^2 \text{ es múltiplo de } 2$$

En efecto,

$$\left.\begin{array}{l} a \text{ impar} \Rightarrow \exists q_1 \in \mathbb{Z}_0^+ : a = 2q_1 + 1 \Rightarrow a^2 = (2q_1+1)^2 \\ \text{y} \\ b \text{ impar} \Rightarrow \exists q_2 \in \mathbb{Z}_0^+ : b = 2q_2 + 1 \Rightarrow b^2 = (2q_2+1)^2 \end{array}\right\} \Longrightarrow \quad a^2 + b^2 = 4q_1^2 + 4q_1 + 4q_2^2 + 4q_2 + 2$$

$$\Longrightarrow \quad a^2 + b^2 = 2(2q_1^2 + 2q_1 + 2q_2^2 + 2q_2 + 1)$$

$$\left[\text{Tomando } q = 2q_1^2 + 2q_1 + 2q_2^2 + 2q_2 + 1\right]$$

$$\Longrightarrow \quad \exists q \in \mathbb{Z}^+ : a^2 + b^2 = 2q$$

$$\Longrightarrow \quad a^2 + b^2 \text{ es múltiplo de } 2$$

Comprobaremos ahora que a^2+b^2 no es múltiplo de 4, es decir

$$\left.\begin{array}{l} a \text{ es impar} \\ \text{y} \\ b \text{ es impar} \end{array}\right\} \Longrightarrow a^2+b^2 \text{ no es múltiplo de } 4$$

Lo probaremos por contradicción. En efecto, supongamos que la proposición es falsa, es decir,

$$a \text{ y } b \text{ son impares y } a^2+b^2 \text{ es múltiplo de } 4$$

o lo que es lo mismo

$$a \text{ y } b \text{ son impares y } 4\Big|a^2+b^2$$

Pues bien, si hacemos lo mismo que hicimos antes, tendremos que

$$\begin{aligned} a^2+b^2=4q_1^2+4q_1+1+4q_2^2+4q_2+1 \quad &\Longrightarrow \quad a^2+b^2-2=4(q_1^2+q_1+q_2^2+q_2), \\ &\big[\text{Tomando } q=q_1^2+q_1+q_2^2+q_2\big] \\ &\Longrightarrow \quad \exists q\in\mathbb{Z}^+ : a^2+b^2-2=4q \\ &\Longrightarrow \quad 4\Big|a^2+b^2-2. \end{aligned}$$

Así pues,

$$\left.\begin{array}{l} 4\Big|a^2+b^2 \\ \text{y} \\ 4\Big|(a^2+b^2)-2 \end{array}\right\} \overset{(5.2)}{\Longrightarrow} 4\Big|(a^2+b^2)-\big[(a^2+b^2)-2\big] \Longrightarrow 4\Big|2$$

lo cual, obviamente, es falso y, consecuentemente, la suposición hecha es falsa y,

$$a^2+b^2 \text{ no es múltiplo de } 4$$

♦♦♦

5.2 Algoritmo de la División

En este apartado veremos que cuando dividimos un entero por otro, existe un cociente y un resto y que ambos son únicos.

5.2.1 Existencia y Unicidad de Cociente y Resto

Si a y b son dos números enteros con $b>0$, entonces existen q y r, enteros y únicos, tales que $a=bq+r$, con $0\leqslant r<b$. Los números a, b, q y r se llaman, 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,

$$\begin{aligned} \left.\begin{array}{l} a=bq+r \\ \text{y} \\ 0\leqslant r<b \end{array}\right\} \quad &\Longrightarrow \quad \left.\begin{array}{l} r=a-bq \\ \text{y} \\ 0\leqslant r<b \end{array}\right\} \\ &\Longrightarrow \quad 0\leqslant a-bq<b \\ &\Longrightarrow \quad bq\leqslant a<b+bq \\ &\Longrightarrow \quad bq\leqslant a<b(q+1) \end{aligned}$$

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.

♦

5.2.2 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.

♦

Nota 5.3 Si quisiéramos dividir $-a$ entre b, podríamos hacer lo siguiente:

$$\begin{aligned} a = bq + r, \text{ con } 0 < r < b \quad &\Longrightarrow \quad -a = -bq - r, \text{ con } -b < -r < 0 \\ &\quad \{-r \text{ no es el resto, ya que este no puede ser negativo.}\} \\ &\Longrightarrow \quad -a = b(-q) - r + b - b, \text{ con } b - b < b - r < b \\ &\quad \{\text{Sumamos y restamos el divisor}\} \\ &\Longrightarrow \quad -a = b(-q-1) + b - r, \text{ con } 0 < b - r < b \\ &\quad \{\text{El resto es } b - r\} \end{aligned}$$

♦

Ejemplo 5.6

1. Sean $a = 17$ y $b = 3$.

   El mayor múltiplo de 3 menor o igual que 17 es $3 \cdot 5$, luego tomando $q = 5$ y $r = 17 - 3 \cdot 5 = 2$, tendremos que

   $$17 = 3 \cdot 5 + 2, \text{ con } 0 \leqslant 2 < 3$$

2. Sean $a = 17$ y $b = -3$.

   El mayor múltiplo de -3 menor o igual que 17 es $-3(-5)$, luego si $q = -5$ y $r = 17 - (-3)(-5) = 2$, tendremos que

   $$17 = (-3)(-5) + 2, \text{ con } 0 \leqslant 2 < 3 = |-3|$$

   Otra forma sería hacerlo como si los dos, a y b, fueran positivos y luego utilizar los signos de b y el cociente.

   $$17 = 3 \cdot 5 + 2 \Longrightarrow 17 = (-3)(-5) + 2, \text{ con } 0 \leqslant 2 < 3 = |-3|$$

3. Sean $a = -17$ y $b = 3$.

   El mayor múltiplo de 3 menor o igual que -17 es $3(-6)$, luego si $q = -6$ y $r = -17 - 3(-5) = 1$, tendremos que

   $$-17 = 3(-6) + 1, \text{ con } 0 \leqslant 1 < 3$$

   Otra forma sería hacerlo como hemos visto en la nota anterior.

   $$\begin{aligned} 17 = 3 \cdot 5 + 2 \quad &\Longrightarrow \quad -17 = -3 \cdot 5 - 2 \\ &\Longrightarrow \quad -17 = 3(-5) - 2 \qquad \{-2 \text{ no es el resto, ya que no puede ser negativo.}\} \\ &\Longrightarrow \quad -17 = 3(-5) - 2 + 3 - 3 \quad \{\text{Sumamos y restamos el divisor}\} \\ &\Longrightarrow \quad -17 = 3(-6) + 1 \qquad \text{con } 0 \leqslant 1 < 3 \end{aligned}$$

4. Sean $a = -17$ y $b = -3$.

   El mayor múltiplo de -3 menor o igual que -17 es $-3 \cdot 6$, luego si $q = 6$ y $r = -17 - (-3)6 = 1$, tendremos que

   $$-17 = -3 \cdot 6 + 1, \text{ con } 0 \leqslant 1 < 3$$

   Otra forma sería hacerlo como hemos visto en la nota anterior.

   $$\begin{aligned} 17 = 3 \cdot 5 + 2 &\implies -17 = -3 \cdot 5 - 2 && \{-2 \text{ no es el resto, ya que no puede ser negativo.}\} \\ &\implies -17 = -3 \cdot 5 - 2 + 3 - 3 && \{\text{Sumamos y restamos el divisor}\} \\ &\implies -17 = -3 \cdot 6 + 1 && \text{con } 0 \leqslant 1 < 3 = |-3| \end{aligned}$$

5. Sean $a = 3$ y $b = 17$.

   El mayor múltiplo de 17 menor o igual que 3 es $17 \cdot 0$, luego si $q = 0$ y $r = 3 - 17 \cdot 0 = 3$, se sigue que

   $$3 = 17 \cdot 0 + 3, \text{ con } 0 \leqslant 3 < 17$$

6. Sean $a = -3$ y $b = 17$.

   El mayor múltiplo de 17 menor o igual que -3 es $17(-1)$, luego si $q = -1$ y $r = -3 - 17(-1) = 14$, se sigue que

   $$-3 = 17(-1) + 14, \text{ con } 0 \leqslant 14 < 17$$

   Otra forma sería hacerlo como hemos visto en la nota anterior.

   $$\begin{aligned} 3 = 17 \cdot 0 + 3 &\implies -3 = -17 \cdot 0 - 3 \\ &\implies -3 = -17 \cdot 0 - 3 + 17 - 17 && \{\text{Sumamos y restamos el divisor}\} \\ &\implies -3 = 17(-1) + 14 && \text{con } 0 \leqslant 14 < 17 \end{aligned}$$

7. Sean $a = 3$ y $b = -17$.

   El mayor múltiplo de -17 menor o igual que 3 es $-17 \cdot 0$, luego si $q = 0$ y $r = 3 - 17 \cdot 0 = 3$, se sigue que

   $$3 = -17 \cdot 0 + 3, \text{ con } 0 \leqslant 3 < 17 = |-17|$$

8. Sean $a = -3$ y $b = -17$.

   El mayor múltiplo de -17 menor o igual que -3 es $-17 \cdot 1$, luego si $q = 1$ y $r = -3 - (-17)1 = 14$, se sigue que

   $$-3 = -17 \cdot 1 + 14, \text{ con } 0 \leqslant 14 < 17 = |-17|$$

   Otra forma sería hacerlo como hemos visto en la nota anterior.

   $$\begin{aligned} 3 = 17 \cdot 0 + 3 &\implies -3 = -17 \cdot 0 - 3 \\ &\implies -3 = -17 \cdot 0 - 3 + 17 - 17 && \{\text{Sumamos y restamos el divisor}\} \\ &\implies -3 = -17 \cdot 1 + 14 && \text{con } 0 \leqslant 14 < 17 = |-17| \end{aligned}$$

♦

Ejemplo 5.7

Demuéstrese que el cuadrado de cualquier número impar puede escribirse en la forma

(a) $4q + 1$

(b) $8q + 1$

siendo $q \in \mathbb{Z}$.

Solución.

En efecto, sea a cualquier número entero.

(a) Probaremos que

$$a \text{ es impar} \Longrightarrow \exists q \in \mathbb{Z} : a^2 = 4q + 1$$

En efecto,

$$\begin{aligned} a \text{ es impar} &\Longrightarrow \exists q_1 \in \mathbb{Z} : a = 2q_1 + 1 \\ &\Longrightarrow \exists q_1 \in \mathbb{Z} : a^2 = 4q_1^2 + 4q_1 + 1 \\ &\Longrightarrow \exists q_1 \in \mathbb{Z} : a^2 = 4(q_1^2 + q_1) + 1 \\ &\quad \left[\text{Tomando } q = q_1^2 + q_1\right] \\ &\Longrightarrow \exists q \in \mathbb{Z} : a^2 = 4q + 1 \end{aligned}$$

(b) Probaremos ahora que

$$a \text{ es impar} \Longrightarrow \exists q \in \mathbb{Z} : a^2 = 8q + 1$$

En efecto,

$$\begin{aligned} a \text{ es impar} &\Longrightarrow \exists q_1 \in \mathbb{Z} : a = 2q_1 + 1 \\ &\Longrightarrow \exists q_1 \in \mathbb{Z} : a^2 = 4q_1^2 + 4q_1 + 1 \\ &\Longrightarrow \exists q_1 \in \mathbb{Z} : a^2 = 4q_1(q_1 + 1) + 1 \\ &\quad \left[\begin{array}{l} \text{Uno de los dos números } q_1 \text{ o } q_1 + 1 \\ \text{ha de ser par, luego } q_1(q_1 + 1) \text{ es par,} \\ \text{de aquí que } \exists q \in \mathbb{Z} : q_1(q_1 + 1) = 2q \end{array}\right] \\ &\Longrightarrow \exists q \in \mathbb{Z} : a^2 = 4 \cdot 2q + 1 \\ &\Longrightarrow \exists q \in \mathbb{Z} : a^2 = 8q + 1 \end{aligned}$$

♦

Ejemplo 5.8

Demuéstrese que si un número entero es a la vez un cuadrado y un cubo, entonces puede escribirse en la forma $7q$ ó $7q + 1$ con $q \in \mathbb{Z}$.

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 5.2.1, 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 5.2.1, $k_1 = k_2$ 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,

$$a^2 = b^3 \Longleftrightarrow a^2 \text{ y } b^3 \text{ son de la forma } 7q \text{ ó } 7q + 1$$

Por tanto,

$$n \text{ es cuadrado y cubo} \Longrightarrow n = 7q \text{ ó } n = 7q + 1$$

♦

Ejemplo 5.9

Demostrar que

(a) El cuadrado de cualquier número entero es de la forma $3q$ o $3q + 1$, $q \in \mathbb{Z}$.

(b) El cubo de cualquier número entero es de la forma $9q$, $9q + 1$ o $9q + 8$, $q \in \mathbb{Z}$.

Solución.

Sea a un entero cualquiera.

(a) Probaremos que

$$a \in \mathbb{Z} \Longrightarrow \exists q \in \mathbb{Z} : a^2 = 3q \text{ o } a^2 = 3q + 1$$

En efecto, por 5.2.1,

$$\begin{aligned}
a \in \mathbb{Z} &\Longrightarrow \exists q_1, r \in \mathbb{Z} : a = 3q_1 + r, \text{ con } 0 \leqslant r < 3 \\
&\Longrightarrow \exists q_1, r \in \mathbb{Z} : a^2 = 9q_1^2 + 6q_1 + r^2, \text{ con } 0 \leqslant r < 3 \\
&\Longrightarrow \begin{cases} \text{Para } r = 0, \ a^2 = 3(3q_1^2 + 2q_1) \\ \text{Para } r = 1, \ a^2 = 3(3q_1^2 + 2q_1) + 1 \\ \text{Para } r = 2, \ a^2 = 3(3q_1^2 + 2q_1 + 1) + 1 \end{cases} \\
&\Longrightarrow \begin{cases} \text{Tomando } q = 3q_1^2 + 2q_1, \exists q \in \mathbb{Z} : a^2 = 3q \\ \text{Tomando } q = 3q_1^2 + 2q_1, \exists q \in \mathbb{Z} : a^2 = 3q + 1 \\ \text{Tomando } q = 3q_1^2 + 2q_1 + 1, \exists q \in \mathbb{Z} : a^2 = 3q + 1 \end{cases}
\end{aligned}$$

(b) Probaremos que

$$a \in \mathbb{Z} \Longrightarrow \exists q \in \mathbb{Z} : a^3 = 9q, \ a^3 = 9q + 1 \text{ o } a^3 = 9q + 8$$

En efecto, por 5.2.1,

$$\begin{aligned}
a \in \mathbb{Z} &\Longrightarrow \exists q_1, r \in \mathbb{Z} : a = 3q_1 + r, \text{ con } 0 \leqslant r < 3 \\
&\Longrightarrow \exists q_1, r \in \mathbb{Z} : a^3 = 27q_1^3 + 27q_1^2 r + 9q_1 r^2 + r^3, \text{ con } 0 \leqslant r < 3 \\
&\Longrightarrow \exists q_1, r \in \mathbb{Z} : a^3 = 9(3q_1^3 + 3q_1^2 r + q_1 r^2) + r^3, \text{ con } 0 \leqslant r < 3 \\
&\quad \left[\text{Tomando } q = 3q_1^3 + 3q_1^2 r + q_1 r^2\right] \\
&\Longrightarrow \exists q, r \in \mathbb{Z} : a^3 = 9q + r^3, \text{ con } 0 \leqslant r < 3 \\
&\Longrightarrow \begin{cases} \text{Para } r = 0, \exists q \in \mathbb{Z} : a^3 = 9q \\ \text{Para } r = 1, \exists q \in \mathbb{Z} : a^3 = 9q + 1 \\ \text{Para } r = 2, \exists q \in \mathbb{Z} : a^3 = 9q + 8 \end{cases}
\end{aligned}$$

♦

Ejemplo 5.10

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:

$$a(a+1)(a+2)$$
$$(a-1)a(a+1)$$
$$(a-2)(a-1)a$$

Estudiaremos, únicamente, la primera ya que un razonamiento similar se puede utilizar en las otras dos.

Por el teorema de existencia y unicidad de cociente y resto, (5.2.1), 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,

$$a(a+1)(a+2) = 2q_1(a+1)(a+2) = 2q_2,\ \text{siendo } q_2 = q_1(a+1)(a+2) \in \mathbb{Z}$$

2 $a = 2q_1 + 1$
En tal caso,

$$a(a+1)(a+2) = a(2q_1+2)(a+2) = 2a(q_1+1)(a+2) = 2q_2,\ \text{siendo } q_2 = a(q_1+1)(a+2) \in \mathbb{Z}$$

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, (5.2.1), 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,

$$a(a+1)(a+2) = 3q_1(a+1)(a+2) = 3q_3,\ \text{siendo } q_3 = q_1(a+1)(a+2) \in \mathbb{Z}$$

2 $a = 3q_1 + 1$.
En este caso, tendremos,

$$a(a+1)(a+2) = a(a+1)(3q_1+3) = 3a(a+1)(q_1+1) = 3q_3,\ \text{siendo } q_3 = a(a+1)(q_1+1) \in \mathbb{Z}$$

3 $a = 3q_1 + 2$.
En tal caso,

$$a(a+1)(a+2) = a(3q_1+3)(a+2) = 3a(q_1+1)(a+2) = 3q_3,\ \text{siendo } q_3 = a(q_1+1)(a+2) \in \mathbb{Z}$$

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,

$$\left.\begin{array}{l} a(a+1)(a+2) = 2q_2 \\ \text{y} \\ a(a+1)(a+2) = 3q_3 \end{array}\right\} \implies a(a+1)(a+2) = \text{m.c.m}(2,3)\cdot q \implies a(a+1)(a+2) = 6q,\ q \in \mathbb{Z}$$

Es decir, el producto de tres enteros consecutivos es múltiplo de 6.

♦

Ejemplo 5.11

Probar que si a es un número entero, entonces $\dfrac{a(a+1)(2a+1)}{6}$ también lo es.

Solución.

En efecto,

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

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,

$$\frac{a(a+1)(2a+1)}{6} = \frac{(a-1)a(a+1) + a(a+1)(a+2)}{6} = \frac{6q}{6} = q,\ \text{siendo } q \in \mathbb{Z}$$

♦♦♦

5.3 Máximo Común Divisor

Ahora estudiamos los divisores comunes de dos números enteros.

5.3.1 Definición

Sean a y b números enteros cualesquiera. El entero $d > 0$ es el máximo común divisor de a y b si es divisor de ambos números y cualquier otro divisor de a y b es, también, divisor de d.

$$d = m.c.d.(a,b) \iff \left\{\begin{array}{l} 1.\quad d\,|\,a \quad y \quad d\,|\,b \\ \quad y \\ 2.\quad c\,|\,a \quad y \quad c\,|\,b \implies c\,|\,d \end{array}\right.$$

♦

5.3.2 Propiedades

Sean a y b, enteros, ambos no iguales a 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.

1. Por la definición de divisibilidad, cualquier entero se divide a sí mismo, entonces $a\big|a$ y por (ii) de las propiedades de la divisibilidad, (5.1.2), $a\big|0$, es decir,
$$a\big|a \text{ y } a\big|0$$
2. Además, si c es cualquier entero, entonces
$$c\big|a \text{ y } c\big|0 \Longrightarrow c\big|a$$

De 1. y 2. se sigue que $\text{m.c.d.}(a,0) = a$, y como el máximo común divisor es estrictamente mayor que cero, tendremos
$$\text{m.c.d.}(a,0) \;=\; \left\{\begin{array}{ll} a & \text{si, } a>0 \\ \text{y} & \\ -a & \text{si, } a<0 \end{array}\right\} \;=\; |a|$$

(ii) Veamos ahora que $\text{m.c.d.}\,(a,b) = \text{m.c.d.}\,(|a|,|b|)$.

En efecto, como a y b son cualesquiera distintos de cero, estudiaremos los cuatro casos que pueden darse. Llamaremos, en todos los casos,
$$d_1 = \text{m.c.d.}(a,b) \quad \text{y} \quad d_2 = \text{m.c.d.}\,(|a|,|b|)$$

$\boxed{1}$ $a>0$ y $b>0$.
$$\begin{aligned} d_1 = \text{m.c.d.}(a,b) &\Longrightarrow d_1\big|a \text{ y } d_1\big|b \\ &\Longrightarrow d_1\big||a| \text{ y } d_1\big||b| \qquad \{|a|=a,\ |b|=b\} \\ &\Longrightarrow d_1\big|\text{m.c.d.}\,(|a|,|b|) \\ &\Longrightarrow d_1\big|d_2 \end{aligned}$$

Recíprocamente,
$$\begin{aligned} d_2 = \text{m.c.d.}\,(|a|,|b|) &\Longrightarrow d_2\big||a| \text{ y } d_2\big||b| \\ &\Longrightarrow d_2\big|a \text{ y } d_2\big|b \qquad \{|a|=a,\ |b|=b\} \\ &\Longrightarrow d_2\big|\text{m.c.d.}(a,b) \\ &\Longrightarrow d_2\big|d_1 \end{aligned}$$

Por la propiedad (iii) de (5.1.2) y teniendo en cuenta que $d_1>0$ y $d_2>0$,
$$\left.\begin{array}{l} d_1\big|d_2 \\ \text{y} \\ d_2\big|d_1 \end{array}\right\} \Longrightarrow d_1 = d_2$$

2 $a > 0$ y $b < 0$.

$$\begin{aligned} d_1 = \text{m.c.d.}(a,b) &\implies d_1 \big| a \text{ y } d_1 \big| b \\ &\implies d_1 \big| a \text{ y } d_1 \big| -b \qquad \{(v) \text{ de } 5.1.2\} \\ &\implies d_1 \big| \, |a| \text{ y } d_1 \big| \, |b| \qquad \{|a| = a,\ |b| = -b\} \\ &\implies d_1 \big| \text{m.c.d.}\left(|a|, |b|\right) \\ &\implies d_1 \big| d_2 \end{aligned}$$

Recíprocamente,

$$\begin{aligned} d_2 = \text{m.c.d.}\left(|a|, |b|\right) &\implies d_2 \big| \, |a| \text{ y } d_2 \big| \, |b| \\ &\implies d_2 \big| a \text{ y } d_2 \big| -b \qquad \{|a| = a,\ |b| = -b\} \\ &\implies d_2 \big| a \text{ y } d_2 \big| b \qquad \{(v) \text{ de } 5.1.2\} \\ &\implies d_2 \big| \text{m.c.d.}(a,b) \\ &\implies d_2 \big| d_1 \end{aligned}$$

Por (iii) en 5.1.2) y teniendo en cuenta que $d_1 > 0$ y $d_2 > 0$,

$$\left.\begin{array}{l} d_1 \big| d_2 \\ \text{y} \\ d_2 \big| d_1 \end{array}\right\} \implies d_1 = d_2$$

3 $a < 0$ y $b > 0$. Se comprueba de forma análoga a los casos anteriores.

4 $a < 0$ y $b < 0$. Se comprueba de forma análoga a los casos anteriores.

Obsérvese que de este resultado se sigue que si a y b son enteros positivos cualesquiera,

$$\begin{aligned} \text{m.c.d.}(-a,b) &= \text{m.c.d.}\left(|-a|, |b|\right) &&= \text{m.c.d.}(a,b) \\ \text{m.c.d.}(a,-b) &= \text{m.c.d.}\left(|a|, |-b|\right) &&= \text{m.c.d.}(a,b) \\ \text{m.c.d.}(-a,-b) &= \text{m.c.d.}\left(|-a|, |-b|\right) &&= \text{m.c.d.}(a,b) \end{aligned}$$

por lo tanto,

$$\text{m.c.d.}(-a,b) = \text{m.c.d.}(a,-b) = \text{m.c.d.}(-a,-b) = \text{m.c.d.}(a,b)$$

♦

5.3.3 Principio de la Buena Ordenación

Todo subconjunto no vacío de enteros positivos tiene elemento mínimo.

♦

5.3.4 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,

$$C = \{ma + nb \in \mathbb{Z}^+ : m, n \in \mathbb{Z}\}$$

⊛ C no es vacío. En efecto,

$$|a| = \begin{cases} a = 1 \cdot a + 0 \cdot b, \text{ si } a \geqslant 0 \\ -a = -1 \cdot a + 0 \cdot b, \text{ si } a < 0 \end{cases}$$

Por lo tanto, $|a|$, al menos, estaría en C y C sería un subconjunto no vacío de $\mathbb{Z}^+$. 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,

$$\left.\begin{array}{rcrcl} a & = & dq & + & r \\ d & = & sa & + & tb \end{array}\right\} \Longrightarrow a = (sa + tb)\, q + r$$

$$\Longrightarrow r = a - (sa + tb)\, q$$

$$\Longrightarrow r = (1 - sq)\, a + (-tq)\, b > 0, \text{ con } 1 - sq \text{ y } -tq \text{ enteros.}$$

$$\Longrightarrow r \in C.$$

   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, $d \big| a$.

   Con un razonamiento idéntico se prueba que $d \big| b$.
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 (5.1.2), dividirá a cualquier combinación lineal con coeficientes enteros de a y b, luego, $c \big| sa + tb$ es decir, $c \big| d$.

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,

$$\left.\begin{array}{r} d \text{ es el máximo de los divisores comunes de } a \text{ y } b \\ \text{y} \\ d' \text{ es un divisor común de } a \text{ y } b \end{array}\right\} \Longrightarrow d' \big| d$$

$$\left.\begin{array}{r} d' \text{ es el máximo de los divisores comunes de } a \text{ y } b \\ \text{y} \\ d \text{ es un divisor común } a \text{ y } b \end{array}\right\} \Longrightarrow d \big| d'$$

$$\left.\begin{array}{r} d' \big| d \\ \text{y} \\ d \big| d' \end{array}\right\} \overset{d>0,\ d'>0}{\Longrightarrow} d = d'$$

♦

5.3.5 Corolario. Identidad de Bezout

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.

$$d = m.c.d.(a,b) \Longrightarrow \exists p, q \in \mathbb{Z} : d = pa + qb$$

Los coeficientes p y q se llaman Coeficientes de Bezout.

Demostración.

Se sigue directamente del teorema anterior.

♦

Nota 5.4 ¿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,

$$6 = 2 \cdot 27 + (-3) \cdot 16$$

y, sin embargo,

$$\text{m.c.d.}\,(27,16) = 1 \neq 6.$$

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.

♦

5.3.6 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

$$d \Big| a \text{ y } d \Big| b$$

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,

$$\left.\begin{array}{l} c \Big| a \\ \text{y} \\ c \Big| b \end{array}\right\} \Longrightarrow c \Big| pa + qb, \text{ con } p \text{ y } q \text{ enteros} \Longrightarrow c \Big| d.$$

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.

5.3.7 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 5.3.5, 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, $1\big|a$ y $1\big|b$. Aplicamos la proposición anterior y m.c.d. $(a,b)=1$.

♦

Ejemplo 5.12

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, (5.3.7),

$$\left.\begin{array}{l}\text{m.c.d.}\,(a,b)=1 \iff \exists p_1,q_1\in\mathbb{Z}: p_1a+q_1b=1\\ \text{y}\\ \text{m.c.d.}\,(a,c)=1 \iff \exists p_2,q_2\in\mathbb{Z}: p_2a+q_2c=1\end{array}\right\} \implies (p_1a+q_1b)(p_2a+q_2c)=1$$

$$\implies (p_1p_2a+p_1q_2c+p_2q_1b)\,a+(q_1q_2)\,bc=1$$

[Tomando $p=p_1p_2a+p_1q_2c+p_2q_1b$ y $q=q_1q_2$]

$$\implies \exists p,q\in\mathbb{Z}: pa+qbc=1 \quad \{5.3.7\}$$

$$\iff \text{m.c.d.}(a,bc)=1$$

♦

5.3.8 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 m.c.d. $(a,b)=d$, entonces m.c.d. $\left(\frac{a}{d},\frac{b}{d}\right)=1$

En efecto,

$$\begin{array}{rll} d=\text{m.c.d.}(a,b) & \implies & \exists p,q\in\mathbb{Z}: pa+qb=d \quad \{\text{Corolario 5.3.5}\}\\ & \iff & \exists p,q\in\mathbb{Z}: p\frac{a}{d}+q\frac{b}{d}=1\\ & \iff & \text{m.c.d.}\left(\frac{a}{d},\frac{b}{d}\right)=1 \quad \{\text{Corolario 5.3.7}\}\end{array}$$

(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,

$$d = \text{m.c.d.}(a, b) \implies \exists p, q \in \mathbb{Z} : pa + qb = d \quad \{\text{Corolario } 5.3.5\}$$

Veamos que kd es el máximo común divisor de ka y kb.

1. kd es divisor de ka y kb.
   En efecto,
$$d = \text{m.c.d.}\,(a, b) \implies \begin{cases} d\big|a \implies kd\big|ka \\ \text{y} \\ d\big|b \implies kd\big|kb \end{cases}$$

2. Sea c cualquier otro divisor común de ka y kb. Entonces,
$$\left.\begin{array}{c} c\big|ka \\ \text{y} \\ c\big|kb \end{array}\right\} \implies c\big|pka + qkb \text{ con } p, q \in \mathbb{Z} \implies c\big|k(pa + qb) \text{ con } p, q \in \mathbb{Z} \implies c\big|kd$$

Luego,

$$\text{m.c.d.}\,(ka, kb) = kd = k\text{m.c.d.}\,(a, b)$$

♦

Ejemplo 5.13

Demostrar que si $\text{m.c.d.}\,(a, b) = 1$, entonces $\text{m.c.d.}\,(a + b, a - b) = 1$ ó 2.

Solución.

Sea $d = \text{m.c.d.}\,(a + b, a - b)$. Entonces,

$$\left.\begin{array}{l} d\big|a + b \\ \text{y} \\ d\big|a - b \end{array}\right\} \implies d\big|(a + b) + (a - b) \implies d\big|2a$$

y también,

$$\left.\begin{array}{l} d\big|a + b \\ \text{y} \\ d\big|a - b \end{array}\right\} \implies d\big|(a + b) - (a - b) \implies d\big|2b$$

y si $d\big|2a$ y $d\big|2b$, entonces d divide al máximo común divisor de $2a$ y $2b$, es decir,

$$d\big|\text{m.c.d.}\,(2a, 2b) \implies d\big|2 \cdot \text{m.c.d.}\,(a, b) \implies d\big|2$$

pero los únicos divisores positivos de 2 son 1 y 2, luego

$$d = 1 \text{ o } d = 2$$

o sea,

$$\text{m.c.d.}\,(a + b, a - b) = 1 \text{ ó } 2$$

♦

Ejemplo 5.14

Demuéstrese que $d = \text{m.c.d.}\,(a,b)$ si, y sólo si $d\big|a, d\big|b$ y $\text{m.c.d.}\left(\frac{a}{d}, \frac{b}{d}\right) = 1$.

Solución.

"Sólo si". Esta demostración la hicimos en (i) de 5.3.8. Ahora la haremos utilizando (ii) de dicha proposición.

Si $d = \text{m.c.d.}\,(a,b)$, es obvio que $d\big|a$ y $d\big|b$, 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,

$$\begin{aligned} \text{m.c.d.}\,(a,b) = d &\implies \text{m.c.d.}\left(d \cdot \frac{a}{d}, d \cdot \frac{b}{d}\right) = d \\ &\implies d \cdot \text{m.c.d.}\left(\frac{a}{d}, \frac{b}{d}\right) = d \\ &\implies \text{m.c.d.}\left(\frac{a}{d}, \frac{b}{d}\right) = 1 \end{aligned}$$

Veamos ahora que la hipótesis de que $d\big|a$ y $d\big|b$, permite probar el recíproco también.

"Si". En efecto, como $d\big|a$ y $d\big|b$, 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 5.15

Probar que si $d\big|a$ y $d\big|b$, entonces $\text{m.c.d.}\left(\frac{a}{d}, \frac{b}{d}\right) = \frac{1}{d} \cdot \text{m.c.d.}(a,b)$.

Solución.

Por hipótesis $d\big|a$ y $d\big|b$ luego $\frac{a}{d}$ y $\frac{b}{d}$ son números enteros y existe $\text{m.c.d.}\left(\frac{a}{d}, \frac{b}{d}\right)$. Pues bien, aplicando (ii) de 5.3.8,

$$d \cdot \text{m.c.d.}\left(\frac{a}{d}, \frac{b}{d}\right) = \text{m.c.d.}\left(d \cdot \frac{a}{d}, d \cdot \frac{b}{d}\right) \implies d \cdot \text{m.c.d.}\left(\frac{a}{d}, \frac{b}{d}\right) = \text{m.c.d.}\,(a,b)$$

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 5.16

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:

$$\begin{aligned} D_{144} &= \{1,2,4,8,16,3,6,12,24,48,9,18,36,72,144\} \\ \text{y} & \\ D_{180} &= \{1,2,4,3,6,12,9,18,36,5,10,20,15,30,60,45,90,180\} \\ \text{y} & \\ D_{240} &= \{1,2,4,8,16,3,6,12,24,48,5,10,20,40,80,15,30,60,120,240\} \end{aligned}$$

Por lo tanto, el conjunto de los divisores comunes a los tres números será

$$D_{144} \cap D_{180} \cap D_{240} = \{1,2,4,3,6,12\}$$

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

$$N = \frac{144}{6} + \frac{180}{6} + \frac{240}{6} = 94$$

♦♦♦

5.4 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.

5.4.1 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.

[1] Matemático Griego del siglo tercero antes de Cristo.

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 5.1.2,

$$d \Big| a + (-q)b$$

es decir,

$$d \Big| r.$$

Por lo tanto,

$$d \Big| b \text{ y } d \Big| r. \tag{5.1}$$

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 (v) de 5.1.2,

$$c \Big| bq + r$$

es decir,

$$c \Big| a$$

luego,

$$c \Big| a \text{ y } c \Big| b$$

y, consecuentemente, ha de dividir al máximo común divisor de a y b, es decir,

$$c \Big| d. \tag{5.2}$$

De (5.1) y (5.2) se sigue que

$$\text{m.c.d.}\,(b, r) = d$$

y, por lo tanto,

$$\text{m.c.d.}\,(a, b) = \text{m.c.d.}\,(b, r)$$

♦

5.4.2 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 5.2.1, 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 5.2.1, obtenemos q_2 y r_2 tales que

$$b = r_1 q_2 + r_2 : 0 \leqslant r_2 < r_1$$

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 5.2.1 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 5.17

Hallar el máximo común divisor de 2597 y 1369 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 5.3.5,

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.

$$\left.\begin{aligned} 1 &= 1 \cdot 3 + (-1)\, 2 \\ 2 &= 5 - 1 \cdot 3 \end{aligned}\right\} \implies 1 = 1 \cdot 3 + (-1)\,(5 - 1 \cdot 3)$$

$$\implies 1 = -1 \cdot 5 + 2 \cdot 3$$

$$\left.\begin{aligned} 1 &= -1 \cdot 5 + 2 \cdot 3 \\ 3 &= 18 - 3 \cdot 5 \end{aligned}\right\} \implies 1 = -1 \cdot 5 + 2\,(18 - 3 \cdot 5)$$

$$\implies 1 = 2 \cdot 18 + (-7)\, 5$$

$$\left.\begin{aligned} 1 &= 2 \cdot 18 + (-7)\, 5 \\ 5 &= 41 - 2 \cdot 18 \end{aligned}\right\} \implies 1 = 2 \cdot 18 + (-7)\,(41 - 2 \cdot 18)$$

$$\implies 1 = -7 \cdot 41 + 16 \cdot 18$$

$$\left.\begin{aligned} 1 &= -7 \cdot 41 + 16 \cdot 18 \\ 18 &= 100 - 2 \cdot 41 \end{aligned}\right\} \implies 1 = -7 \cdot 41 + 16\,(100 - 2 \cdot 41)$$

$$\implies 1 = 16 \cdot 100 + (-39)\, 41$$

$$\left.\begin{aligned} 1 &= 16 \cdot 100 + (-39)\, 41 \\ 41 &= 141 - 1 \cdot 100 \end{aligned}\right\} \implies 1 = 16 \cdot 100 + (-39)\,(141 - 1 \cdot 100)$$

$$\implies 1 = -39 \cdot 141 + 55 \cdot 100$$

$$\left.\begin{aligned} 1 &= -39 \cdot 141 + 55 \cdot 100 \\ 100 &= 1228 - 8 \cdot 141 \end{aligned}\right\} \implies 1 = -39 \cdot 141 + 55\,(1228 - 8 \cdot 141)$$

$$\implies 1 = 55 \cdot 1228 + (-479)\, 141$$

$$\left.\begin{array}{l} 1 = 55 \cdot 1228 + (-479)\,141 \\ 141 = 1369 - 1 \cdot 1228 \end{array}\right\} \implies 1 = 55 \cdot 1228 + (-479)\,(1369 - 1 \cdot 1228)$$

$$\implies 1 = -479 \cdot 1369 + 534 \cdot 1228$$

$$\left.\begin{array}{l} 1 = -479 \cdot 1369 + 534 \cdot 1228 \\ 1228 = 2597 - 1 \cdot 1369 \end{array}\right\} \implies 1 = -479 \cdot 1369 + 534\,(2597 - 1 \cdot 1369)$$

$$\implies 1 = 534 \cdot 2597 + (-1013)\,1369$$

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

$$\begin{aligned} 1 &= 534 \cdot 2597 + (-1013) \cdot 1369 \\ &= 534 \cdot 2597 + (-1013) \cdot 1369 + (-1369k) \cdot 2597 + (2597k) \cdot 1369 \\ &= (534 - 1369k)2597 + (-1013 + 2597k)1369 \end{aligned}$$

Obsérvese también que

$$\text{m.c.d.}\,(2597, -1369) = 1$$

$$\text{m.c.d.}\,(-2597, 1369) = 1$$

$$\text{m.c.d.}\,(-2597, -1369) = 1$$

y en tales casos las combinaciones lineales con coeficientes enteros serían:

$$1 = 534 \cdot 2597 + 1013\,(-1369)$$

$$1 = (-534)\,(-2597) + (-1013)\,1369$$

$$1 = (-534)\,(-2597) + 1013\,(-1369)$$

♦

Ejemplo 5.18

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.

$$\left.\begin{array}{l} 7 = 1 \cdot 203 + (-7)\, 28 \\ 28 = 231 - 1 \cdot 203 \end{array}\right\} \implies 7 = 1 \cdot 203 + (-7)\,(231 - 1 \cdot 203)$$

$$\implies 7 = -7 \cdot 231 + 8 \cdot 203$$

$$\left.\begin{array}{l} 7 = -7 \cdot 231 + 8 \cdot 203 \\ 203 = 1820 - 7 \cdot 231 \end{array}\right\} \implies 7 = -7 \cdot 231 + 8\,(1820 - 7 \cdot 231)$$

$$\implies 7 = 8 \cdot 1820 + (-63)\, 231$$

es decir, la combinación lineal pedida es

$$7 = 8 \cdot 1820 + (-63)\, 231$$

♦

Ejemplo 5.19

¿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 5.2.1, existirán q_1 y q_2, enteros, tales que

$$\left.\begin{array}{rcl} 68130 = aq_1 + 27 \\ \text{y} \\ 107275 = aq_2 + 49 \end{array}\right\} \implies \left.\begin{array}{rcl} 68103 = aq_1, \text{ con } q_1 \in \mathbb{Z} \\ \text{y} \\ 107226 = aq_2, \text{ con } q_2 \in \mathbb{Z} \end{array}\right\}$$

$$\implies a \mid 68103 \text{ y } a \mid 107226$$

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	2	1	6
107226	68103	39123	28980	10143	8694	1449
39123	28980	10143	8694	1449	0	

luego, $a = 1449$

♦

Ejemplo 5.20

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 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 $b = 364$.

♦♦♦

5.5 Mínimo Común Múltiplo

En esta sección estudiaremos los múltiplos comunes a un par de enteros.

5.5.1 Definición

Sean a y b dos enteros cualesquiera. El número entero $m > 0$ es el mínimo común múltiplo de a y b si es múltiplo de ambos y cualquier otro múltiplo de a y b es, también, múltiplo de m. Es decir,

$$m = m.c.m.(a,b) \iff \begin{cases} 1.\ a \mid m \ \text{ y } \ b \mid m \\ \text{y} \\ 2.\ \forall c,\ a \mid c \ \text{ y } \ b \mid c \Longrightarrow m \mid c \end{cases}$$

♦

5.5.2 Propiedades

Sean a y b dos números enteros distintos de cero. Se verifica:

(a) Si $m.c.d.(a,b) = 1$, entonces $m.c.m.(a,b) = |ab|$.

(b) $m.c.m.(ka,kb) = k \cdot m.c.m.(a,b),\ \forall k \in \mathbb{Z}^+$

(c) $m.c.d.(a,b) \cdot m.c.m.(a,b) = |ab|$

Demostración.

(a) Si m.c.d.$(a,b) = 1$, entonces m.c.m.$(a,b) = |ab|$.

Sea $m > 0$ el mínimo común múltiplo de a y b. Entonces,

$$
\begin{aligned}
m = \text{m.c.m}(a,b) &\implies \left\{ \begin{array}{l} a \big| m \\ \text{y} \\ b \big| m \end{array} \right. \\
&\implies \left\{ \begin{array}{l} \exists q_1 \in \mathbb{Z} : m = aq_1 \\ \text{y} \\ \exists q_2 \in \mathbb{Z} : m = bq_2 \end{array} \right. \\
&\implies aq_1 = bq_2 \\
&\iff \frac{q_1}{q_2} = \frac{b}{a} \\
&\qquad \left\{ \begin{array}{l} \exists q \in \mathbb{Z}^+ : \text{m.c.d.}(q_1, q_2) = q \\ \text{m.c.d.}(a,b) = 1 \end{array} \right\} \\
&\iff \frac{\frac{q_1}{q}}{\frac{q_2}{q}} = \frac{b}{a} \\
&\iff \left\{ \begin{array}{ll} \dfrac{q_1}{q} = b & \\ \text{y} & \{\text{Fracciones Irreducibles}\} \\ \dfrac{q_2}{q} = a & \end{array} \right. \\
&\iff \left\{ \begin{array}{l} \exists q \in \mathbb{Z}^+ : q_1 = bq \\ \text{y} \\ \exists q \in \mathbb{Z}^+ : q_2 = aq \end{array} \right. \\
&\implies \exists q \in \mathbb{Z}^+ : m = abq \\
&\implies ab \big| m
\end{aligned}
$$

Por otra parte,

$$
\left. \begin{array}{l} a \big| ab \\ \text{y} \\ b \big| ab \end{array} \right\} \implies \text{m.c.m.}(a,b) \big| ab \implies m \big| ab
$$

Finalmente,

$$
\left. \begin{array}{l} ab \big| m \\ \text{y} \\ m \big| ab \end{array} \right\} \implies |m| = |ab| \overset{m>0}{\implies} m = |ab|
$$

(b) 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.
$$m = \text{m.c.m.}\,(a,b) \Longrightarrow \begin{cases} a \mid m \Longrightarrow ka \mid km \\ \text{y} \\ b \mid m \Longrightarrow kb \mid km \end{cases}$$
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,
$$ka \mid c \Longleftrightarrow \exists q_1 \in \mathbb{Z} : c = ka \cdot q_1 \Longrightarrow \frac{c}{k} = a \cdot q_1 \Longleftrightarrow a \mid \frac{c}{k}$$
y
$$kb \mid c \Longleftrightarrow \exists q_2 \in \mathbb{Z} : c = kb \cdot q_2 \Longrightarrow \frac{c}{k} = b \cdot q_2 \Longleftrightarrow b \mid \frac{c}{k}$$
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
$$m \mid \frac{c}{k} \Longleftrightarrow \exists q \in \mathbb{Z} : \frac{c}{k} = m \cdot q \Longleftrightarrow c = km \cdot q \Longleftrightarrow km \mid c$$
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) $\text{m.c.d.}(a,b) \cdot \text{m.c.m.}(a,b) = |ab|$.

En efecto, sea $d = \text{m.c.d.}(a,b)$, entonces
$$\begin{aligned} \text{m.c.d.}(a,b) \cdot \text{m.c.m.}(a,b) &= d \cdot \text{m.c.m.}(a,b) \\ &= d \cdot \text{m.c.m.}\left(d\frac{a}{d}, d\frac{b}{d}\right) \\ &= d \cdot d \cdot \text{m.c.m.}\left(\frac{a}{d}, \frac{b}{d}\right) \\ &\quad \left[\text{m.c.d.}\left(\frac{a}{d}, \frac{b}{d}\right) = 1 \ \{5.3.8\ (i)\}\right] \\ &= d^2 \left|\frac{a}{d} \cdot \frac{b}{d}\right| \ \{\text{Apartado (a)}\} \\ &= \frac{d^2}{d^2}\,|ab| \\ &= |ab| \end{aligned}$$

♦

Ejemplo 5.21

Sean a y b dos números enteros distintos de cero. Demostrar que las tres condiciones siguientes son equivalentes:

(i) $a \mid b$

(ii) $\text{m.c.d.}(a,b) = |a|$

(iii) $\text{m.c.m.}(a,b) = |b|$

Solución.

$(i) \Longrightarrow (ii)$.

En efecto, $a \big| a$ y como, por hipótesis, $a \big| b$, tendremos que a es divisor común a a y a b, luego ha de dividir a su máximo común divisor, es decir,

$$a \big| \text{m.c.d.}(a, b).$$

Por otro lado,

$$\text{m.c.d.}(a, b) \big| a$$

y por (iii) de 5.1.2, al ser g.c.d.$(a, b) > 0$,

$$\text{g.c.d.}(a, b) = |a|$$

$(ii) \Longrightarrow (iii)$.

En efecto, si m.c.d.$(a, b) = |a|$, entonces aplicando (iii) de 5.5.2, tendremos

$$\begin{aligned} \text{m.c.d.}(a, b) \cdot \text{m.c.m.}(a, b) = |ab| &\Longrightarrow |a| \cdot \text{m.c.m.}(a, b) = |ab| \\ &\Longrightarrow \text{m.c.m.}(a, b) = \frac{|a|\,|b|}{|a|} \\ &\Longrightarrow \text{m.c.m.}(a, b) = |b| \end{aligned}$$

$(iii) \Longrightarrow (i)$.

En efecto, si 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 $|b|$ y, por lo tanto, de b, es decir,

$$a \big| b$$

♦

Ejemplo 5.22

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) 4001 y 2689

(b) 7983 y 7982

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.

$$\left.\begin{array}{l} 1 = 1 \cdot 5 + (-2)\,2 \\ 2 = 12 - 2 \cdot 5 \end{array}\right\} \implies 1 = 1 \cdot 5 + (-2)\,(12 - 2 \cdot 5)$$

$$\implies 1 = -2 \cdot 12 + 5 \cdot 5$$

$$\left.\begin{array}{l} 1 = -2 \cdot 12 + 5 \cdot 5 \\ 5 = 65 - 5 \cdot 12 \end{array}\right\} \implies 1 = -2 \cdot 12 + 5\,(65 - 5 \cdot 12)$$

$$\implies 1 = 5 \cdot 65 + (-27)\,12$$

$$\left.\begin{array}{l} 1 = 5 \cdot 65 + (-27)\,12 \\ 12 = 1312 - 20 \cdot 65 \end{array}\right\} \implies 1 = 5 \cdot 65 + (-27)\,(1312 - 20 \cdot 65)$$

$$\implies 1 = -27 \cdot 1312 + 545 \cdot 65$$

$$\left.\begin{array}{l} 1 = -27 \cdot 1312 + 545 \cdot 65 \\ 65 = 2689 - 2 \cdot 1312 \end{array}\right\} \implies 1 = -27 \cdot 1312 + 545\,(2689 - 2 \cdot 1312)$$

$$\implies 1 = 545 \cdot 2689 + (-1117)\,1312$$

$$\left.\begin{array}{l} 1 = 545 \cdot 2689 + (-1117)\,1312 \\ 1312 = 4001 - 1 \cdot 2689 \end{array}\right\} \implies 1 = 545 \cdot 2689 + (-1117)\,(4001 - 1 \cdot 2689)$$

$$\implies 1 = -1117 \cdot 4001 + 1662 \cdot 2689$$

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 7983 y 7982.

	1	7982
7983	7982	1
1	0	

luego,

$$\text{m.c.d.}\,(7983, 7982) = 1$$

y

$$\text{m.c.m.}\,(7983, 7982) = 7983 \cdot 7982 = 63720306$$

siendo la combinación lineal buscada:

$$1 = 1 \cdot 7983 + (-1)\,7982$$

♦

Ejemplo 5.23

Para cada $a \in \mathbb{Z}^+$, ¿Cuál es el mínimo común múltiplo y el máximo común divisor de a y $a+1$?

Solución.

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 5.24

Sean a, b y c tres números enteros positivos tales que a y b son primos entre sí. Probar que si $a \mid c$ y $b \mid c$, entonces $ab \mid c$. ¿Se verifica también si a y b no son primos entre sí?

Solución.

En efecto,

$$\left.\begin{array}{l} a \mid c \iff c \text{ es múltiplo de } a \\ \text{y} \\ b \mid c \iff c \text{ es múltiplo de } b \end{array}\right\} \implies c \text{ es múltiplo del m.c.m.}\,(a, b)$$

$$\{\text{m.c.m.}\,(a, b) = ab\}$$

$$\implies c \text{ es múltiplo de } ab$$

$$\iff ab \mid c$$

Si a y b no son primos entre sí, no se verifica la proposición. Por ejemplo

$$4 \mid 16 \quad \text{y} \quad 8 \mid 16$$

sin embargo 32 no divide a 16.

♦

Ejemplo 5.25

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 el denominador de la fracción pedida y sea d el máximo común divisor de ambos números. La fracción $\frac{a}{b}$ puede ser positiva o negativa dependiendo de los signos de a y b. Tomaremos valores absolutos para considerar todos los casos.

$$\frac{|a|}{|b|} = \frac{|a|+20}{|b|+25} \iff |ab| + 25\,|a| = |ab| + 20\,|b| \iff \frac{|a|}{|b|} = \frac{20}{25}$$

Y si dividimos numerador y denominador de ambas fracciones por su máximo común divisor, tendremos,

$$\frac{\frac{|a|}{d}}{\frac{|b|}{d}} = \frac{\frac{20}{5}}{\frac{25}{5}} \Longrightarrow \frac{\frac{|a|}{d}}{\frac{|b|}{d}} = \frac{4}{5} \iff \left\{ \begin{array}{l} \frac{|a|}{d} = 4 \\ \text{y} \\ \frac{|b|}{d} = 5 \end{array} \right. \Longrightarrow \frac{|ab|}{d^2} = 20 \Longrightarrow |ab| = 20d^2$$

Por otra parte,

$$\text{m.c.d.}\,(a,b) \cdot \text{m.c.m.}\,(a,b) = |ab| \Longrightarrow |ab| = 340d$$

luego,

$$\left. \begin{array}{l} |ab| = 20d^2 \\ \text{y} \\ |ab| = 340d \end{array} \right\} \Longrightarrow \quad 20d^2 = 340d \quad \Longrightarrow \quad 20d = 340 \quad \Longrightarrow \quad d = \frac{340}{20} \quad \Longrightarrow \quad d = 17$$

de aquí que,

$$\left. \begin{array}{l} \frac{|a|}{d} = 4 \\ \text{y} \\ d = 17 \end{array} \right\} \Longrightarrow \quad |a| = 68 \quad \Longrightarrow \quad a = 68 \text{ o } a = -68$$

$$\left. \begin{array}{l} \frac{|b|}{d} = 5 \\ \text{y} \\ d = 17 \end{array} \right\} \Longrightarrow \quad |b| = 85 \quad \Longrightarrow \quad b = 85 \text{ o } b = -85$$

y habrá cuatro opciones,

$$\frac{68}{85},\ \frac{68}{-85},\ \frac{-68}{85},\ \frac{-68}{-85}$$

y, por lo tanto, las fracciones pedidas son,

$$\frac{68}{85} \quad \text{y} \quad -\frac{68}{85}$$

♦

Ejemplo 5.26

Probar que si dos números enteros son primos entre sí, entonces su suma y su producto también lo son.

Solución.

Sean a y b enteros 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 (5.3.7), podremos encontrar dos enteros p y q tales que

$$pa+qb=1$$

de aquí que

$$\begin{array}{rcl} pa^2 & + & qab = a \\ \text{y} & & \\ pab & + & qb^2 = b \end{array}$$

Pues bien, sea d un divisor común a ab y $a+b$. Entonces,

$$\left.\begin{array}{l} d\big|ab \\ \text{y} \\ d\big|a+b \implies d\big|a\,(a+b) \end{array}\right\} \implies d\big|ab \text{ y } d\big|a\,(a+b)-ab$$

$$\begin{aligned} &\implies d\big|ab \text{ y } d\big|a^2+ab-ab \\ &\implies d\big|ab \text{ y } d\big|a^2 \\ &\implies d\big|pa^2+qab \\ &\implies d\big|a \end{aligned}$$

Por otro lado,

$$\left.\begin{array}{l} d\big|ab \\ \text{y} \\ d\big|a+b \implies d\big|b\,(a+b) \end{array}\right\} \implies d\big|ab \text{ y } d\big|b\,(a+b)-ab$$

$$\begin{aligned} &\implies d\big|ab \text{ y } d\big|b^2+ab-ab \\ &\implies d\big|ab \text{ y } d\big|b^2 \\ &\implies d\big|pab+qb^2 \\ &\implies d\big|b \end{aligned}$$

Por tanto, d es un divisor común a a y b, luego será divisor del máximo común divisor de ambos, es decir,

$$d\big|\text{m.c.d.}(a,b) \implies d\big|1 \implies d=1$$

por lo tanto,

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

♦

Ejemplo 5.27

Hallar dos números enteros positivos sabiendo que su suma es 240 y su mínimo común múltiplo, 1768.

Solución.

Sean a y b los números buscados y sea d su máximo común divisor. Entonces, $a+b=240$ y

$$\text{m.c.d.}(a,b)\cdot\text{m.c.m.}(a,b)=|ab| \iff |ab|=1768d$$

y al ser positivos ambos números, $|ab|=ab$, luego,

$$\left.\begin{array}{l} a+b=240 \\ ab=1768d \end{array}\right\}$$

Por otra parte, utilizando el hecho de que *"si dos números son primos entre sí, entonces su suma y su producto también lo son"*,

$$\begin{aligned} \text{m.c.d.}(a,b)=d &\implies \text{m.c.d.}\left(\frac{a}{d},\frac{b}{d}\right)=1 \\ &\implies \text{m.c.d.}\left(\frac{a}{d}\cdot\frac{b}{d},\frac{a}{d}+\frac{b}{d}\right)=1 \\ &\implies \text{m.c.d.}\left(\frac{ab}{d^2},\frac{a+b}{d}\right)=1 \\ &\implies \frac{\frac{ab}{d^2}}{\frac{a+b}{d}} \text{ es irreducible.} \end{aligned}$$

Sustituyendo,

$$\begin{aligned} \frac{\frac{ab}{d^2}}{\frac{a+b}{d}}=\frac{\frac{1768d}{d^2}}{\frac{240}{d}} &\implies \frac{\frac{ab}{d^2}}{\frac{a+b}{d}}=\frac{1768}{240} \\ &\implies \frac{\frac{ab}{d^2}}{\frac{a+b}{d}}=\frac{\frac{1768}{8}}{\frac{240}{8}} \quad \{\text{m.c.d.}(1768,240)=8\} \\ &\implies \frac{\frac{ab}{d^2}}{\frac{a+b}{d}}=\frac{221}{30} \\ &\implies \left\{\begin{array}{l} \frac{ab}{d^2}=221 \\ \text{y} \\ \frac{a+b}{d}=30 \end{array}\right. \quad \{\text{Fracciones irreducibles}\} \\ &\implies \left\{\begin{array}{l} \frac{a}{d}\cdot\frac{b}{d}=221 \\ \text{y} \\ \frac{a}{d}+\frac{b}{d}=30 \end{array}\right. \end{aligned}$$

luego $\frac{a}{d}$ y $\frac{b}{d}$ han de ser, ambos, divisores positivos de 221, es decir, pertenecen al conjunto,

$$D_{221} = \{1, 13, 17, 221\}$$

son primos entre sí, su producto es 221 y su suma ha de ser 30. Veamos los casos que pueden presentarse.

$\frac{a}{d}$	1	13
$\frac{b}{d}$	221	17
$\frac{a}{d} \cdot \frac{b}{d}$	221	221
m.c.d. $\left(\frac{a}{d}, \frac{b}{d}\right)$	1	1
$\frac{a}{d} + \frac{b}{d}$	222	30

Eliminando las opciones que no son posibles,

$\frac{a}{d}$	1	13
$\frac{b}{d}$	221	17
$\frac{a}{d} \cdot \frac{b}{d}$	221	221
m.c.d. $\left(\frac{a}{d}, \frac{b}{d}\right)$	1	1
$\frac{a}{d} + \frac{b}{d}$	222	30

y

$$\frac{a}{d} + \frac{b}{d} = 30 \Longrightarrow d = \frac{a+b}{30} \Longrightarrow d = \frac{240}{30} \Longrightarrow d = 8$$

luego,

a	104
b	136

♦

Ejemplo 5.28

Hallar dos números enteros sabiendo que su diferencia es -184 y su mínimo común múltiplo, 864.

Solución.

Sean a y b los números buscados y sea d su máximo común divisor. Entonces, $a - b = -184$ y

$$\text{m.c.d.}(a, b) \cdot \text{m.c.m.}(a, b) = |ab| \Longleftrightarrow |ab| = 864d$$

Por otra parte, utilizando el hecho de que "*si dos números son primos entre sí, entonces su diferencia y su producto también lo son*",

$$\begin{aligned}
\text{m.c.d.}(a,b)=d &\implies \text{m.c.d.}\left(\frac{a}{d},\frac{b}{d}\right)=1\\
&\implies \text{m.c.d.}\left(\frac{a}{d}\cdot\frac{b}{d},\frac{a}{d}-\frac{b}{d}\right)=1\\
&\implies \text{m.c.d.}\left(\frac{ab}{d^2},\frac{a-b}{d}\right)=1\\
&\implies \text{m.c.d.}\left(\frac{|ab|}{d^2},\frac{a-b}{d}\right)=1\\
&\implies \frac{\frac{|ab|}{d^2}}{\frac{a-b}{d}} \text{ es irreducible.}
\end{aligned}$$

Sustituyendo,

$$\begin{aligned}
\frac{\frac{|ab|}{d^2}}{\frac{a-b}{d}}=\frac{\frac{864d}{d^2}}{\frac{-184}{d}} &\implies \frac{\frac{|ab|}{d^2}}{\frac{a-b}{d}}=\frac{864}{-184}\\
&\implies \frac{\frac{|ab|}{d^2}}{\frac{a-b}{d}}=\frac{\frac{864}{8}}{\frac{-184}{8}} \quad \{\text{m.c.d.}(864,-184)=8\}\\
&\implies \frac{\frac{|ab|}{d^2}}{\frac{a-b}{d}}=\frac{108}{-23}\\
&\implies \begin{cases} \dfrac{|ab|}{d^2}=108\\ \text{y} \qquad \{\text{Fracciones irreducibles}\}\\ \dfrac{a-b}{d}=-23 \end{cases}\\
&\implies \begin{cases} \dfrac{ab}{d^2}=108 \text{ o } \dfrac{ab}{d^2}=-108\\ \text{y} \qquad \{\text{Fracciones irreducibles}\}\\ \dfrac{a-b}{d}=-23 \end{cases}\\
&\implies \begin{cases} \dfrac{a}{d}\cdot\dfrac{b}{d}=108 \text{ o } \dfrac{a}{d}\cdot\dfrac{b}{d}=-108\\ \text{y}\\ \dfrac{a}{d}-\dfrac{b}{d}=-23 \end{cases}
\end{aligned}$$

luego $\frac{a}{d}$ y $\frac{b}{d}$ han de ser, ambos, divisores de 108, es decir, pertenecen al conjunto,

$$D_{108}=\{\pm1,\pm2,\pm3,\pm4,\pm6,\pm9,\pm12,\pm18,\pm27,\pm36,\pm54,\pm108\}$$

son primos entre sí, su producto es 108 o -108 y su diferencia ha de ser -23. Veamos los casos que pueden presentarse.

※ $\dfrac{a}{d}\cdot\dfrac{b}{d}=108$.

$\frac{a}{d}$	1	2	3	4	6	9	12	18	27	36	54	108
$\frac{b}{d}$	108	54	36	27	18	12	9	6	4	3	2	1
$\frac{a}{d}\cdot\frac{b}{d}$	108	108	108	108	108	108	108	108	108	108	108	108
m.c.d. $\left(\frac{a}{d},\frac{b}{d}\right)$	1	2	3	1	6	3	3	6	1	3	2	1
$\frac{a}{d}-\frac{b}{d}$	−107	−52	−33	−23	−12	−3	3	12	23	33	52	107
$\frac{a}{d}$	−108	−54	−36	−27	−18	−12	−9	−6	−4	−3	−2	−1
$\frac{b}{d}$	−1	−2	−3	−4	−6	−9	−12	−18	−27	−36	−54	−108
$\frac{a}{d}\cdot\frac{b}{d}$	108	108	108	108	108	108	108	108	108	108	108	108
m.c.d. $\left(\frac{a}{d},\frac{b}{d}\right)$	1	2	3	1	6	3	3	6	1	3	2	1
$\frac{a}{d}-\frac{b}{d}$	−107	−52	−33	−23	−12	−3	3	12	23	33	52	107

Eliminando las opciones que no son posibles,

$\frac{a}{d}$	1	2	3	4	6	9	12	18	27	36	54	108
$\frac{b}{d}$	108	54	36	27	18	12	9	6	4	3	2	1
$\frac{a}{d}\cdot\frac{b}{d}$	108	108	108	108	108	108	108	108	108	108	108	108
m.c.d. $\left(\frac{a}{d},\frac{b}{d}\right)$	1	2	3	1	6	3	3	6	1	3	2	1
$\frac{a}{d}-\frac{b}{d}$	−107	−52	−33	−23	−12	−3	3	12	23	33	52	107
$\frac{a}{d}$	−108	−54	−36	−27	−18	−12	−9	−6	−4	−3	−2	−1
$\frac{b}{d}$	−1	−2	−3	−4	−6	−9	−12	−18	−27	−36	−54	−108
$\frac{a}{d}\cdot\frac{b}{d}$	108	108	108	108	108	108	108	108	108	108	108	108
m.c.d. $\left(\frac{a}{d},\frac{b}{d}\right)$	1	2	3	1	6	3	3	6	1	3	2	1
$\frac{a}{d}-\frac{b}{d}$	−107	−52	−33	−23	−12	−3	3	12	23	33	52	107

y

$$\frac{a}{d}-\frac{b}{d}=-23\Longrightarrow d=\frac{a-b}{-23}\Longrightarrow d=\frac{-184}{-23}\Longrightarrow d=8$$

luego,

a	32	−216
b	216	−32

serán las soluciones en este caso.

※ $\dfrac{a}{d}\cdot\dfrac{b}{d}=-108$.

$\frac{a}{d}$	1	2	3	4	6	9	12	18	27	36	54	108
$\frac{b}{d}$	−108	−54	−36	−27	−18	−12	−9	−6	−4	−3	−2	−1
$\frac{a}{d}\cdot\frac{b}{d}$	−108	−108	−108	−108	−108	−108	−108	−108	−108	−108	−108	−108
m.c.d. $\left(\frac{a}{d},\frac{b}{d}\right)$	1	2	3	1	6	3	3	6	1	3	2	1
$\frac{a}{d}-\frac{b}{d}$	109	56	39	31	24	21	21	24	31	39	56	109
$\frac{a}{d}$	−108	−54	−36	−27	−18	−12	−9	−6	−4	−3	−2	−1
$\frac{b}{d}$	1	2	3	4	6	9	12	18	27	36	54	108
$\frac{a}{d}\cdot\frac{b}{d}$	−108	−108	−108	−108	−108	−108	−108	−108	−108	−108	−108	−108
m.c.d. $\left(\frac{a}{d},\frac{b}{d}\right)$	1	2	3	1	6	3	3	6	1	3	2	1
$\frac{a}{d}-\frac{b}{d}$	−109	−56	−39	−31	−24	−21	−21	−24	−31	−39	−56	−109

Eliminando las opciones que no son posibles,

$\frac{a}{d}$	1	2	3	4	6	9	12	18	27	36	54	108
$\frac{b}{d}$	−108	−54	−36	−27	−18	−12	−9	−6	−4	−3	−2	−1
$\frac{a}{d}\cdot\frac{b}{d}$	−108	−108	−108	−108	−108	−108	−108	−108	−108	−108	−108	−108
m.c.d. $\left(\frac{a}{d},\frac{b}{d}\right)$	1	2	3	1	6	3	3	6	1	3	2	1
$\frac{a}{d}-\frac{b}{d}$	109	56	39	31	24	21	21	24	31	39	56	109
$\frac{a}{d}$	−108	−54	−36	−27	−18	−12	−9	−6	−4	−3	−2	−1
$\frac{b}{d}$	1	2	3	4	6	9	12	18	27	36	54	108
$\frac{a}{d}\cdot\frac{b}{d}$	−108	−108	−108	−108	−108	−108	−108	−108	−108	−108	−108	−108
m.c.d. $\left(\frac{a}{d},\frac{b}{d}\right)$	1	2	3	1	6	3	3	6	1	3	2	1
$\frac{a}{d}-\frac{b}{d}$	−109	−56	−39	−31	−24	−21	−21	−24	−31	−39	−56	−109

luego en este caso no hay solución.

♦

Ejemplo 5.29

Hallar dos números enteros positivos sabiendo que su producto es 5376 y su mínimo común múltiplo, 672.

Solución.

Sean a y b los números buscados. Entonces,

$$\text{m.c.d.}(a,b)\cdot\text{m.c.m.}(a,b)=|ab|$$

y llamando d al m.c.d.(a,b), tendremos

$$672d=5376\Longrightarrow d=\frac{5376}{672}\Longrightarrow d=8$$

Por otra parte,

$$\text{m.c.d.}(a,b)=d\Longrightarrow\text{m.c.d.}\left(\frac{a}{d},\frac{b}{d}\right)=1$$

Como los números han de ser positivos, $|ab| = ab$. Entonces,

$$\frac{|ab|}{d^2} = \frac{5376}{64} \implies \frac{|ab|}{d^2} = 84 \implies \frac{ab}{d^2} = 84 \implies \frac{a}{d} \cdot \frac{b}{d} = 84$$

es decir, $\frac{a}{d}$ y $\frac{b}{d}$ han de ser, ambos, divisores positivos de 84, es decir, pertenecen al conjunto,

$$D_{84} = \{1, 2, 3, 4, 6, 7, 12, 14, 21, 28, 42, 84\}$$

son primos entre sí y su producto ha de ser 84. Las opciones son:

$\frac{a}{d}$	1	2	3	4	6	7
$\frac{b}{d}$	84	42	28	21	14	12
$\frac{a}{d} \cdot \frac{b}{d}$	84	84	84	84	84	84
m.c.d. $\left(\frac{a}{d}, \frac{b}{d}\right)$	1	2	1	1	2	1

Eliminando las que no son posibles,

$\frac{a}{d}$	1	~~2~~	3	4	~~6~~	7
$\frac{b}{d}$	84	~~42~~	28	21	~~14~~	12
$\frac{a}{d} \cdot \frac{b}{d}$	84	~~84~~	84	84	~~84~~	84
m.c.d. $\left(\frac{a}{d}, \frac{b}{d}\right)$	1	~~2~~	1	1	~~2~~	1

Las soluciones serán, por tanto,

a	8	24	32	56
b	672	224	168	96

♦

Ejemplo 5.30

Hallar dos números enteros sabiendo que el valor absoluto de su producto es 5376 y su mínimo común múltiplo, 672.

Solución.

Sean a y b los números buscados. Entonces,

$$\text{m.c.d.}(a, b) \cdot \text{m.c.m.}(a, b) = |ab|$$

y llamando d al m.c.d.(a,b), tendremos

$$672d = 5376 \Longrightarrow d = \frac{5376}{672} \Longrightarrow d = 8$$

Por otra parte,

$$\text{m.c.d.}(a,b) = d \Longrightarrow \text{m.c.d.}\left(\frac{a}{d}, \frac{b}{d}\right) = 1$$

Pues bien,

$$\frac{|ab|}{d^2} = \frac{5376}{64} \quad \Longrightarrow \quad \frac{|ab|}{d^2} = 84$$

$$\Longrightarrow \quad \begin{cases} \dfrac{ab}{d^2} = 84 \\ \text{o} \\ \dfrac{ab}{d^2} = -84 \end{cases}$$

$$\Longrightarrow \quad \begin{cases} \dfrac{a}{d} \cdot \dfrac{b}{d} = 84 \\ \text{o} \\ \dfrac{a}{d} \cdot \dfrac{b}{d} = -84 \end{cases}$$

es decir, $\dfrac{a}{d}$ y $\dfrac{b}{d}$ han de ser, ambos, Divisores de 84, es decir, pertenecen al conjunto,

$$D_{84} = \{\pm 1, \pm 2, \pm 3, \pm 4, \pm 6, \pm 7, \pm 12, \pm 14, \pm 21, \pm 28, \pm 42, \pm 84\}$$

son primos entre sí y su producto ha de ser 84. Veamos los casos que pueden presentarse.

※ $\dfrac{a}{d} \cdot \dfrac{b}{d} = 84$.

$\frac{a}{d}$	1	2	3	4	6	7
$\frac{b}{d}$	84	42	28	21	14	12
$\frac{a}{d} \cdot \frac{b}{d}$	84	84	84	84	84	84
m.c.d. $\left(\frac{a}{d}, \frac{b}{d}\right)$	1	2	1	1	2	1

$\frac{a}{d}$	-84	-42	-28	-21	-14	-12
$\frac{b}{d}$	-1	-2	-3	-4	-6	-7
$\frac{a}{d} \cdot \frac{b}{d}$	84	84	84	84	84	84
m.c.d. $\left(\frac{a}{d}, \frac{b}{d}\right)$	1	2	1	1	2	1

Eliminando las opciones que no son posibles,

$\frac{a}{d}$	1	~~2~~	3	4	~~6~~	7
$\frac{b}{d}$	84	~~42~~	28	21	~~14~~	12
$\frac{a}{d} \cdot \frac{b}{d}$	84	~~84~~	84	84	~~84~~	84
m.c.d. $\left(\frac{a}{d}, \frac{b}{d}\right)$	1	~~2~~	1	1	~~2~~	1

$\frac{a}{d}$	-84	~~-42~~	-28	-21	~~-14~~	-12
$\frac{b}{d}$	-1	~~-2~~	-3	-4	~~-6~~	-7
$\frac{a}{d} \cdot \frac{b}{d}$	84	~~84~~	84	84	~~84~~	84
m.c.d. $\left(\frac{a}{d}, \frac{b}{d}\right)$	1	~~2~~	1	1	~~2~~	1

Las soluciones, en este caso, serán:

a	8	24	32	56	-672	-224	-168	-96
b	672	224	168	96	-8	-24	-32	-56

※ $\frac{a}{d} \cdot \frac{b}{d} = -84$.

$\frac{a}{d}$	1	2	3	4	6	7	12	14	21	28	42	84
$\frac{b}{d}$	-84	-42	-28	-21	-14	-12	-7	-6	-4	-3	-2	-1
$\frac{a}{d} \cdot \frac{b}{d}$	-84	-84	-84	-84	-84	-84	-84	-84	-84	-84	-84	-84
m.c.d. $\left(\frac{a}{d}, \frac{b}{d}\right)$	1	2	1	1	2	1	1	2	1	1	2	1

Eliminando las opciones que no son posibles,

$\frac{a}{d}$	1	~~2~~	3	4	~~6~~	7	12	~~14~~	21	28	~~42~~	84
$\frac{b}{d}$	-84	~~-42~~	-28	-21	~~-14~~	-12	-7	~~-6~~	-4	-3	~~-2~~	-1
$\frac{a}{d} \cdot \frac{b}{d}$	-84	~~-84~~	-84	-84	~~-84~~	-84	-84	~~-84~~	-84	-84	~~-84~~	-84
m.c.d. $\left(\frac{a}{d}, \frac{b}{d}\right)$	1	~~2~~	1	1	~~2~~	1	1	~~2~~	1	1	~~2~~	1

Las soluciones, en este caso, serán:

a	8	24	32	56	96	168	224	672
b	-672	-224	-168	-96	-56	-32	-24	-8

♦

Ejemplo 5.31

Hallar dos números enteros sabiendo que su máximo común divisor es 8 y su mínimo común múltiplo, 2520.

Solución.

Sean a y b los números buscados. Entonces,

$$\text{m.c.d.}(a,b) \cdot \text{m.c.m.}(a,b) = |ab| \Longrightarrow |ab| = 8 \cdot 2520 \Longrightarrow |ab| = 20160$$

Por otra parte, si llamamos d al máximo común divisor de a y b,

$$\text{m.c.d.}(a,b) = d \Longrightarrow \text{m.c.d.}\left(\frac{a}{d}, \frac{b}{d}\right) = 1$$

Entonces,

$$\begin{aligned} \frac{|ab|}{d^2} = \frac{20160}{64} \quad &\Longrightarrow \quad \frac{|ab|}{d^2} = 315 \\ &\Longrightarrow \quad \begin{cases} \dfrac{ab}{d^2} = 315 \\ \text{o} \\ \dfrac{ab}{d^2} = -315 \end{cases} \\ &\Longrightarrow \quad \begin{cases} \dfrac{a}{d} \cdot \dfrac{b}{d} = 315 \\ \text{o} \\ \dfrac{a}{d} \cdot \dfrac{b}{d} = -315 \end{cases} \end{aligned}$$

luego $\dfrac{a}{d}$ y $\dfrac{b}{d}$ han de ser, ambos, divisores de 315, es decir, pertenecen al conjunto,

$$D_{315} = \{\pm 1, \pm 3, \pm 5, \pm 7, \pm 9, \pm 15, \pm 21, \pm 35, \pm 45, \pm 63, \pm 105, \pm 315\}$$

son primos entre sí y su producto ha de ser 315 o -315. Veamos los casos que pueden presentarse.

※ $\dfrac{a}{d} \cdot \dfrac{b}{d} = 315$.

$\frac{a}{d}$	1	3	5	7	9	15
$\frac{b}{d}$	315	105	63	45	35	21
$\frac{a}{d} \cdot \frac{b}{d}$	315	315	315	315	315	315
m.c.d. $\left(\frac{a}{d}, \frac{b}{d}\right)$	1	3	1	1	1	3

$\frac{a}{d}$	-315	-105	-63	-45	-35	-21
$\frac{b}{d}$	-1	-3	-5	-7	-9	-15
$\frac{a}{d} \cdot \frac{b}{d}$	315	315	315	315	315	315
m.c.d. $\left(\frac{a}{d}, \frac{b}{d}\right)$	1	3	1	1	1	3

Eliminando las opciones que no son posibles,

$\frac{a}{d}$	1	~~3~~	5	7	9	~~15~~
$\frac{b}{d}$	315	~~105~~	63	45	35	~~21~~
$\frac{a}{d} \cdot \frac{b}{d}$	315	~~315~~	315	315	315	~~315~~
m.c.d. $\left(\frac{a}{d}, \frac{b}{d}\right)$	1	~~3~~	1	1	1	~~3~~

$\frac{a}{d}$	-315	-105	-63	-45	-35	-21
$\frac{b}{d}$	-1	-3	-5	-7	-9	-15
$\frac{a}{d}\cdot\frac{b}{d}$	315	315	315	315	315	315
m.c.d. $\left(\frac{a}{d},\frac{b}{d}\right)$	1	3	1	1	1	3

Las soluciones, en este caso, serán:

a	8	40	56	72	-2520	-504	-360	-280
b	2520	504	360	280	-8	-40	-56	-72

$\frac{a}{d}\cdot\frac{b}{d}=-315$.

$\frac{a}{d}$	1	3	5	7	9	15	21	35	45	63	105	315
$\frac{b}{d}$	-315	-105	-63	-45	-35	-21	-15	-9	-7	-5	-3	-1
$\frac{a}{d}\cdot\frac{b}{d}$	-315	-315	-315	-315	-315	-315	-315	-315	-315	-315	-315	-315
m.c.d. $\left(\frac{a}{d},\frac{b}{d}\right)$	1	3	1	1	1	3	3	1	1	1	3	1

Eliminando las opciones que no son posibles,

$\frac{a}{d}$	1	3	5	7	9	15	21	35	45	63	105	315
$\frac{b}{d}$	-315	-105	-63	-45	-35	-21	-15	-9	-7	-5	-3	-1
$\frac{a}{d}\cdot\frac{b}{d}$	-315	-315	-315	-315	-315	-315	-315	-315	-315	-315	-315	-315
m.c.d. $\left(\frac{a}{d},\frac{b}{d}\right)$	1	3	1	1	1	3	3	1	1	1	3	1

Las soluciones, en este caso, serán:

a	8	40	56	72	280	360	504	2520
b	-2520	-504	-360	-280	-72	-56	-40	-8

♦

Ejemplo 5.32

Hallar dos números enteros sabiendo que su mínimo común múltiplo es 288 y la suma de sus cuadrados, 6208.

Solución.

Sean a y b los enteros que buscamos y sea d el máximo común divisor de a y b. Entonces,

$$\text{m.c.d.}(a,b)=d \Longrightarrow \text{m.c.d.}\left(\frac{a}{d},\frac{b}{d}\right)=1 \Longrightarrow \text{m.c.d.}\left(\frac{a^2}{d^2},\frac{b^2}{d^2}\right)=1 \Longrightarrow \text{m.c.d.}\left(\frac{|ab|^2}{d^4},\frac{a^2+b^2}{d^2}\right)=1$$

Por otra parte, según los datos del enunciado,

$$\text{m.c.d.}(a,b)\cdot\text{m.c.m.}(a,b)=|ab| \Longrightarrow 288d=|ab| \Longrightarrow |ab|^2=288^2d^2 \Longrightarrow \frac{|ab|^2}{d^4}=\frac{82944}{d^2}$$

además,

$$a^2+b^2=6208 \Longrightarrow \frac{a^2+b^2}{d^2}=\frac{6208}{d^2}$$

Por lo tanto,

$$\frac{\frac{|ab|^2}{d^4}}{\frac{a^2+b^2}{d^2}}=\frac{\frac{82944}{d^2}}{\frac{6208}{d^2}} \quad\Longrightarrow\quad \frac{\frac{|ab|^2}{d^4}}{\frac{a^2+b^2}{d^2}}=\frac{82944}{6208}$$

$$\Longrightarrow\quad \frac{\frac{|ab|^2}{d^4}}{\frac{a^2+b^2}{d^2}}=\frac{\frac{82944}{64}}{\frac{6208}{64}} \qquad \{\text{m.c.d.}(82944,6208)=64\}$$

$$\Longrightarrow\quad \frac{\left(\frac{|ab|}{d^2}\right)^2}{\frac{a^2+b^2}{d^2}}=\frac{1296}{97}$$

$$\Longrightarrow\quad \begin{cases} \left(\dfrac{|ab|}{d^2}\right)^2=1296 \\ \text{y} \qquad\qquad\qquad\qquad \{\text{Fracciones irreducibles}\} \\ \dfrac{a^2}{d^2}+\dfrac{b^2}{d^2}=97 \end{cases}$$

$$\Longrightarrow\quad \begin{cases} \dfrac{|ab|}{d^2}=36 \\ \text{y} \\ \dfrac{a^2}{d^2}+\dfrac{b^2}{d^2}=97 \end{cases}$$

$$\Longrightarrow\quad \begin{cases} \dfrac{a}{d}\cdot\dfrac{b}{d}=36 \text{ o } \dfrac{a}{d}\cdot\dfrac{b}{d}=-36 \\ \text{y} \\ \dfrac{a^2}{d^2}+\dfrac{b^2}{d^2}=97 \end{cases}$$

luego, $\dfrac{a}{d}$ y $\dfrac{b}{d}$ han de ser, ambos, divisores de 36, primos entre sí, su producto ha de ser 36 o -36 y la suma de sus cuadrados, 97.

$$D_{36}=\{\pm1,\ \pm2,\ \pm3,\ \pm4,\ \pm6,\ \pm9,\ \pm12,\ \pm18,\ \pm36\}$$

Veamos los casos que pueden presentarse.

* $\frac{a}{d}\cdot\frac{b}{d}=36$.

$\frac{a}{d}$	1	2	3	4	6
$\frac{b}{d}$	36	18	12	9	6
$\frac{a}{d}\cdot\frac{b}{d}$	36	36	36	36	36
m.c.d. $\left(\frac{a}{d},\frac{b}{d}\right)$	1	2	3	1	6
$\frac{a^2}{d^2}+\frac{b^2}{d^2}$	1297	328	153	97	72

$\frac{a}{d}$	-36	-18	-12	-9	-6
$\frac{b}{d}$	-1	-2	-3	-4	-6
$\frac{a}{d}\cdot\frac{b}{d}$	36	36	36	36	36
m.c.d. $\left(\frac{a}{d},\frac{b}{d}\right)$	1	2	3	1	6
$\frac{a^2}{d^2}+\frac{b^2}{d^2}$	1297	328	153	97	72

Eliminando las opciones que no son posibles,

$\frac{a}{d}$	~~1~~	~~2~~	~~3~~	4	~~6~~
$\frac{b}{d}$	~~36~~	~~18~~	~~12~~	9	~~6~~
$\frac{a}{d}\cdot\frac{b}{d}$	~~36~~	~~36~~	~~36~~	36	~~36~~
m.c.d. $\left(\frac{a}{d},\frac{b}{d}\right)$	~~1~~	~~2~~	~~3~~	1	~~6~~
$\frac{a^2}{d^2}+\frac{b^2}{d^2}$	~~1297~~	~~328~~	~~153~~	97	~~72~~

$\frac{a}{d}$	~~-36~~	~~-18~~	~~-12~~	-9	~~-6~~
$\frac{b}{d}$	~~-1~~	~~-2~~	~~-3~~	-4	~~-6~~
$\frac{a}{d}\cdot\frac{b}{d}$	~~36~~	~~36~~	~~36~~	36	~~36~~
m.c.d. $\left(\frac{a}{d},\frac{b}{d}\right)$	~~1~~	~~2~~	~~3~~	1	~~6~~
$\frac{a^2}{d^2}+\frac{b^2}{d^2}$	~~1297~~	~~328~~	~~153~~	97	~~72~~

y

$$\frac{a^2}{d^2}+\frac{b^2}{d^2}=97\Longrightarrow d^2=\frac{a^2+b^2}{97}\Longrightarrow d^2=\frac{6208}{97}\Longrightarrow d^2=64\Longrightarrow d=8$$

luego,

a	32	-72
b	72	-32

serán las soluciones en este caso.

* $\frac{a}{d}\cdot\frac{b}{d}=-36$.

$\frac{a}{d}$	1	2	3	4	6	9	12	18	36
$\frac{b}{d}$	-36	-18	-12	-9	-6	-4	-3	-2	-1
$\frac{a}{d}\cdot\frac{b}{d}$	-36	-36	-36	-36	-36	-36	-36	-36	-36
m.c.d. $\left(\frac{a}{d},\frac{b}{d}\right)$	1	2	3	1	6	1	3	2	1
$\frac{a^2}{d^2}+\frac{b^2}{d^2}$	1297	328	153	97	72	97	153	328	1297

Eliminando las soluciones que no son posibles,

$\frac{a}{d}$	1	2	3	4	6	9	12	18	36
$\frac{b}{d}$	-36	-18	-12	-9	-6	-4	-3	-2	-1
$\frac{a}{d}\cdot\frac{b}{d}$	-36	-36	-36	-36	-36	-36	-36	-36	-36
m.c.d. $\left(\frac{a}{d},\frac{b}{d}\right)$	1	2	3	1	6	1	3	2	1
$\frac{a^2}{d^2}+\frac{b^2}{d^2}$	1297	328	153	97	72	97	153	328	1297

y

$$\frac{a^2}{d^2}+\frac{b^2}{d^2}=97\Longrightarrow d^2=\frac{a^2+b^2}{97}\Longrightarrow d^2=\frac{6208}{97}\Longrightarrow d^2=64\Longrightarrow d=8$$

luego,

a	32	72
b	-72	-32

serán las soluciones en este caso.

♦

Ejemplo 5.33

Hallar dos números enteros sabiendo que su mínimo común múltiplo es 360 y la suma de sus cuadrados, 5409.

Solución.

Sean a y b los enteros que buscamos y sea d el máximo común divisor de a y b. Entonces,

$$\text{m.c.d.}(a,b)=d\Longrightarrow\text{m.c.d.}\left(\frac{a}{d},\frac{b}{d}\right)=1\Longrightarrow\text{m.c.d.}\left(\frac{a^2}{d^2},\frac{b^2}{d^2}\right)=1\Longrightarrow\text{m.c.d.}\left(\frac{|ab|^2}{d^4},\frac{a^2+b^2}{d^2}\right)=1$$

Por otra parte, según los datos del enunciado,

$$\text{m.c.d.}(a,b)\cdot\text{m.c.m.}(a,b)=|ab|\Longrightarrow 360d=|ab|\Longrightarrow|ab|^2=360^2d^2\Longrightarrow\frac{|ab|^2}{d^4}=\frac{129600}{d^2}$$

además,

$$a^2+b^2=5409\Longrightarrow\frac{a^2+b^2}{d^2}=\frac{5409}{d^2}$$

Por lo tanto,

$$\frac{\frac{|ab|^2}{d^4}}{\frac{a^2+b^2}{d^2}} = \frac{\frac{129600}{d^2}}{\frac{5409}{d^2}} \implies \frac{\frac{|ab|^2}{d^4}}{\frac{a^2+b^2}{d^2}} = \frac{129600}{5409}$$

$$\implies \frac{\frac{|ab|^2}{d^4}}{\frac{a^2+b^2}{d^2}} = \frac{\frac{129600}{9}}{\frac{5409}{9}} \quad \{\text{m.c.d.}(129600, 5409) = 9\}$$

$$\implies \frac{\left(\frac{|ab|}{d^2}\right)^2}{\frac{a^2+b^2}{d^2}} = \frac{14400}{601}$$

$$\implies \begin{cases} \left(\frac{|ab|}{d^2}\right)^2 = 14400 \\ \text{y} \qquad \{\text{Fracciones irreducibles}\} \\ \frac{a^2}{d^2} + \frac{b^2}{d^2} = 601 \end{cases}$$

$$\implies \begin{cases} \frac{|ab|}{d^2} = 120 \\ \text{y} \\ \frac{a^2}{d^2} + \frac{b^2}{d^2} = 601 \end{cases}$$

$$\implies \begin{cases} \frac{a}{d} \cdot \frac{b}{d} = 120 \text{ o } \frac{a}{d} \cdot \frac{b}{d} = -120 \\ \text{y} \\ \frac{a^2}{d^2} + \frac{b^2}{d^2} = 601 \end{cases}$$

luego, $\frac{a}{d}$ y $\frac{b}{d}$ han de ser, ambos, divisores de 120, primos entre sí, su producto ha de ser 120 o -120 y la suma de sus cuadrados, 601.

$$D_{120} = \{\pm 1, \pm 2, \pm 3, \pm 4, \pm 5, \pm 6, \pm 8, \pm 10, \pm 12, \pm 15, \pm 20, \pm 24, \pm 30, \pm 40, \pm 60, \pm 120\}$$

Veamos los casos que pueden presentarse.

※ $\frac{a}{d} \cdot \frac{b}{d} = 120$.

$\frac{a}{d}$	1	2	3	4	5	6	8	10
$\frac{b}{d}$	120	60	40	30	24	20	15	12
$\frac{a}{d} \cdot \frac{b}{d}$	120	120	120	120	120	120	120	120
m.c.d. $\left(\frac{a}{d}, \frac{b}{d}\right)$	1	2	1	2	1	2	1	2
$\frac{a^2}{d^2} + \frac{b^2}{d^2}$	14401	3604	1609	916	601	436	289	244

$\frac{a}{d}$	-120	-60	-40	-30	-24	-20	-15	-12
$\frac{b}{d}$	-1	-2	-3	-4	-5	-6	-8	-10
$\frac{a}{d} \cdot \frac{b}{d}$	120	120	120	120	120	120	120	120
m.c.d. $\left(\frac{a}{d}, \frac{b}{d}\right)$	1	2	1	2	1	2	1	2
$\frac{a^2}{d^2} + \frac{b^2}{d^2}$	14401	3604	1609	916	601	436	289	244

Eliminando las opciones que no son posibles,

$\frac{a}{d}$	1	2	3	4	5	6	8	10
$\frac{b}{d}$	120	60	40	30	24	20	15	12
$\frac{a}{d}\cdot\frac{b}{d}$	120	120	120	120	120	120	120	120
m.c.d. $\left(\frac{a}{d},\frac{b}{d}\right)$	1	2	1	2	1	2	1	2
$\frac{a^2}{d^2}+\frac{b^2}{d^2}$	14401	3604	1609	916	601	436	289	244

$\frac{a}{d}$	-120	-60	-40	-30	-24	-20	-15	-12
$\frac{b}{d}$	-1	-2	-3	-4	-5	-6	-8	-10
$\frac{a}{d}\cdot\frac{b}{d}$	120	120	120	120	120	120	120	120
m.c.d. $\left(\frac{a}{d},\frac{b}{d}\right)$	1	2	1	2	1	2	1	2
$\frac{a^2}{d^2}+\frac{b^2}{d^2}$	14401	3604	1609	916	601	436	289	244

y

$$\frac{a^2}{d^2}+\frac{b^2}{d^2}=601\Longrightarrow d^2=\frac{a^2+b^2}{601}\Longrightarrow d^2=\frac{5409}{601}\Longrightarrow d^2=9\Longrightarrow d=3$$

luego,

a	15	-72
b	72	-15

serán las soluciones en este caso.

※ $\frac{a}{d}\cdot\frac{b}{d}=-120$.

$\frac{a}{d}$	1	2	3	4	5	6	8	10	12	15	20	24	30	40	60	120
$\frac{b}{d}$	-120	-60	-40	-30	-24	-20	-15	-12	-10	-8	-6	-5	-4	-3	-2	-1
$\frac{a}{d}\cdot\frac{b}{d}$	-120	-120	-120	-120	-120	-120	-120	-120	-120	-120	-120	-120	-120	-120	-120	-120
m.c.d. $\left(\frac{a}{d},\frac{b}{d}\right)$	1	2	1	2	1	2	1	2	2	1	2	1	2	1	2	1
$\frac{a^2}{d^2}+\frac{b^2}{d^2}$	14401	3604	1609	916	601	436	289	244	244	289	436	601	916	1609	3604	14401

Eliminando las soluciones que no son posibles,

$\frac{a}{d}$	1	2	3	4	5	6	8	10	12	15	20	24	30	40	60	120
$\frac{b}{d}$	-120	-60	-40	-30	-24	-20	-15	-12	-10	-8	-6	-5	-4	-3	-2	-1
$\frac{a}{d}\cdot\frac{b}{d}$	-120	-120	-120	-120	-120	-120	-120	-120	-120	-120	-120	-120	-120	-120	-120	-120
m.c.d. $\left(\frac{a}{d},\frac{b}{d}\right)$	1	2	1	2	1	2	1	2	2	1	2	1	2	1	2	1
$\frac{a^2}{d^2}+\frac{b^2}{d^2}$	14401	3604	1609	916	601	436	289	244	244	289	436	601	916	1609	3604	14401

y

$$\frac{a^2}{d^2}+\frac{b^2}{d^2}=601\Longrightarrow d^2=\frac{a^2+b^2}{601}\Longrightarrow d^2=\frac{5409}{601}\Longrightarrow d^2=9\Longrightarrow d=3$$

luego,

a	15	72
b	-72	-15

serán las soluciones en este caso.

♦♦♦

Lección 6

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 ejemplos siguientes aparecen en los *Elementos de Euclides*.

- Todo entero mayor que 1 puede escribirse como un producto único de números primos.
- Existen infinitos números primos.
- Podemos obtener una lista de los números primos por medio de la *Criba de Eratóstenes*.

6.1 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.

6.1.1 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.

♦

6.1.2 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.

♦

6.1.3 Proposición

$p \in \mathbb{Z}^+$ es primo si, y sólo si $p \neq ab,\ \forall a, b \in \mathbb{Z},\ 1 < a < p,\ 1 < b < p$

Demostración.

"Solo si."

$$p \in \mathbb{Z}^+ \text{ es primo} \Longrightarrow p \neq ab,\ \forall a, b \in \mathbb{Z},\ 1 < a < p,\ 1 < b < p$$

Lo haremos por contradicción. En efecto, supongamos que

$$p \in \mathbb{Z}^+ \text{ es primo y } \exists a, b \in \mathbb{Z},\ 1 < a < p,\ 1 < b < p \text{ tal que } p = ab.$$

Entonces,

$$\exists a \in \mathbb{Z} : p = ab \Longrightarrow a|p.$$

$$\exists b \in \mathbb{Z} : p = ab \Longrightarrow b|p.$$

Luego, en cualquier caso, p tendría más de dos divisores y, consecuentemente, no sería primo lo que contradice la hipótesis que asegura que si lo es.

"Si."

$$p \neq ab,\ \forall a, b \in \mathbb{Z},\ 1 < a < p,\ 1 < b < p \Longrightarrow p \in \mathbb{Z}^+ \text{ es primo}$$

En efecto, si $p \neq ab,\ \forall a, b \in \mathbb{Z},\ 1 < a < p,\ 1 < b < p$, entonces la definición de divisibilidad asegura que a no es divisor de p y b tampoco, por lo tanto los únicos divisores que tiene p son 1 y el propio p, es decir p es primo.

♦

Nota 6.1 Obsérvese que de la proposición anterior se sigue que

$$\begin{aligned} p \in \mathbb{Z}^+ \text{ es primo} &\iff p \neq ab,\ \forall a, b \in \mathbb{Z},\ 1 < a < p,\ 1 < b < p \\ &\iff \nexists a, b \in \mathbb{Z},\ 1 < a < p,\ 1 < b < p : p = ab \end{aligned}$$

o lo que es igual,

p es primo si, y sólo si es imposible escribir $p = ab$ con $a, b \in \mathbb{Z}$ y $1 < a, b < p$.

♦

6.1.4 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 $\mathbb{Z}^+$. Por el *Principio de la buena ordenación* (5.3.3), C tendrá un elemento mínimo, m. Pues bien,

$$\begin{aligned}
m \in C \quad &\Longrightarrow \quad \left\{ \begin{array}{l} m \text{ es compuesto.} \\ \text{y} \\ m \text{ no tiene divisores primos.} \end{array} \right. \\
&\Longrightarrow \quad \left\{ \begin{array}{l} m \text{ tiene más de 2 divisores.} \\ \text{y} \\ m \text{ no tiene divisores primos.} \end{array} \right. \\
&\Longrightarrow \quad \left\{ \begin{array}{l} \text{Hay, al menos, un } m_1 \in \mathbb{Z}^+, \text{ divisor de } m \text{ y distinto de 1 y de } m. \\ \text{y} \\ m_1 \text{ no es primo.} \end{array} \right. \\
&\Longrightarrow \quad \text{Hay, al menos, un } m_1 \in \mathbb{Z}^+, \text{ compuesto tal que } m_1 | m \text{ y } 1 < m_1 < m.
\end{aligned}$$

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.

6.1.5 Teorema

Existen infinitos números primos.

Demostración.

Utilizamos, de nuevo, la demostración por contradicción. En efecto, supongamos que la cantidad de números primos existente es finita, digamos, 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,

$$m > p_i, \text{ y } m \neq p_i, \ i = 1, 2, \ldots, k$$

es decir m 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.

La contradicción se sigue de la suposición de que existía únicamente una cantidad finita de números primos y, por lo tanto, existen infinitos números primos.

♦

Ejemplo 6.1

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 $p_1 \cdot p_2 \cdot \cdots\cdots \cdot p_n + 1$ 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,

$$a \in \mathbb{Z} \text{ es cuadrado perfecto} \iff \sqrt{a} \in \mathbb{Z}$$

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.

$$\begin{aligned}
a \text{ cuadrado perfecto} &\iff \sqrt{a} \in \mathbb{Z} \\
&\implies \exists q_1, r \in \mathbb{Z} : \sqrt{a} = 2q_1 + r, \text{ con } r = 0 \text{ ó } r = 1 \text{ (5.2.1)} \\
&\iff \exists q_1, r \in \mathbb{Z} : a = (2q_1 + r)^2, \text{ con } r = 0 \text{ ó } r = 1 \\
&\iff \exists q_1, r \in \mathbb{Z} : a = 4q_1^2 + 4q_1 r + r^2, \text{ con } r = 0 \text{ ó } r = 1 \\
&\iff \exists q_1, r \in \mathbb{Z} : a = 4\left(q_1^2 + q_1 r\right) + r^2, \text{ con } r = 0 \text{ ó } r = 1 \\
&\quad \left\{\text{Tomando } q \in \mathbb{Z} \text{ tal que } q = q_1^2 + q_1 r\right\} \\
&\iff \exists q \in \mathbb{Z} : \begin{cases} a = 4q \\ \text{o} \\ a = 4q + 1 \end{cases}
\end{aligned}$$

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

$$a \neq 4q \text{ y } a \neq 4q + 1, \forall q \in \mathbb{Z} \Longrightarrow a \text{ no es un cuadrado perfecto} \tag{6.1}$$

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.

$$\begin{aligned}
\exists q \in \mathbb{Z}_0^+ : p_2 \cdot p_3 \cdots p_n = 2q + 1 &\implies \exists q \in \mathbb{Z} : p_1 \cdot p_2 \cdot p_3 \cdots p_n + 1 = 2(2q + 1) + 1 \\
&\implies \exists q \in \mathbb{Z} : p_1 \cdot p_2 \cdot p_3 \cdots p_n + 1 = 4q + 3
\end{aligned}$$

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 (6.1),

$$a = p_1 \cdot p_2 \cdot p_3 \cdots p_n + 1 \Longrightarrow a \text{ no es un cuadrado perfecto}$$

es decir ningún número entero de la forma $p_1 \cdot p_2 \cdot p_3 \cdots p_n + 1$ es un cuadrado perfecto.

♦♦♦

6.2 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.

6.2.1 Teorema

Si $p > 1$ no tiene divisores primos menores o iguales que su raíz, entonces p es primo.

Demostración.

Sea p un entero estrictamente mayor que 1. Utilizamos el método de demostración por la contrarrecíproca.

Si p no es primo, entonces existe, al menos, un divisor primo de p menor o igual que su raíz.

En efecto, si p no es primo, entonces es compuesto luego existirán q_1 y q_2 tales que

$$p = q_1 q_2, \text{ siendo } 1 < q_1 < p \text{ y } 1 < q_2 < p$$

Pues bien, uno de los divisores de p, q_1 ó q_2, ha de ser menor o igual que la raíz de p, es decir, $q_1 \leqslant \sqrt{p}$ ó $q_2 \leqslant \sqrt{p}$ ya que si no fuera así tendríamos que

$$\left.\begin{array}{l} q_1 > \sqrt{p} \\ \text{y} \\ q_2 > \sqrt{p} \end{array}\right\} \implies q_1 q_2 > \sqrt{p}\sqrt{p} \implies p > p$$

lo cual, obviamente, es imposible. Supondremos, sin pérdida de generalidad, que $q_1 \leqslant \sqrt{p}$. Ahora puede ocurrir lo siguiente:

- Si q_1 es primo, entonces el teorema estará demostrado ya que

  $$q_1 \text{ es divisor primo de } p \text{ y } q_1 \leqslant \sqrt{p}$$

- Si q_1 no es primo, entonces por la proposición 6.1.2, q_1 tendrá, al menos, un divisor primo q, $1 < q < q_1$. Entonces,

  $$\left.\begin{array}{l} q | q_1 \\ \text{y} \\ q_1 | p \end{array}\right\} \implies q \big| p$$

  y hemos encontrado

  $$q \text{ divisor primo de } p \text{ y } q \leqslant \sqrt{p}$$

  es decir, el teorema estaría probado.

♦

[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.

Ejemplo 6.2

Aplicar directamente el teorema anterior para comprobar que el 11 es primo.

Solución.

Sea q cualquier entero. Entonces,

$$\left.\begin{array}{l} q \text{ es primo} \\ \text{y} \\ q < \sqrt{11} \end{array}\right\} \Longrightarrow \left.\begin{array}{l} q \text{ es primo} \\ \text{y} \\ q \leqslant 3 \end{array}\right\} \Longrightarrow \quad q = 2 \text{ o } q = 3$$

y como 11 no es múltiplo de 2 ni de 3, el teorema anterior asegura que el número 11 es primo.

♦

6.2.2 Criba de Eratóstenes

Veamos como se utiliza el teorema anterior para construir la criba de Eratóstenes y encontrar números primos.

Partiremos de que los enteros 2 y 3 son primos.

Sea p 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 tal que $2^2 \leqslant p < 3^2$. Entonces,

$$2^2 \leqslant p < 3^2 \Longrightarrow 2 \leqslant \sqrt{p} < 3$$

luego el único número primo menor o igual que $\sqrt{p}$ es el 2, así que por el teorema anterior,

si p 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~~

Ahora tomamos p de tal forma que esté entre el primer primo no considerado, 3, y el siguiente encontrado 5, sin que pueda ser el segundo, es decir tal que $3^2 \leqslant p < 5^2$. Entonces,

$$3^2 \leqslant p < 5^2 \Longrightarrow 3 \leqslant \sqrt{p} < 5$$

y los números primos que cumplen esta condición son el 2, el 3, luego por el teorema anterior,

si p no es múltiplo de 2, ni de 3, entonces es primo.

En la práctica procedemos igual que antes.

- Escribimos todos los números entre 9 y 25.

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 y, consecuentemente, son primos. Añadimos los que teníamos entre 2 y 8 y tendremos todos los números primos entre 9 y 25.

2 3 ~~4~~ 5 ~~6~~ 7 ~~8~~ ~~9~~ ~~10~~

11 ~~12~~ 13 ~~14~~ ~~15~~ ~~16~~ 17 ~~18~~ 19 ~~20~~

~~21~~ ~~22~~ 23 ~~24~~

Ahora tomamos p de tal forma que esté entre el primer primo no considerado, 5, y el siguiente encontrado 7, sin que pueda ser el segundo, es decir tal que $5^2 \leqslant p < 7^2$. Entonces,

$$5^2 \leqslant p < 7^2 \Longrightarrow 5 \leqslant \sqrt{p} < 7$$

y los números primos que cumplen esta condición son el 2, el 3 y el 5, luego por el teorema anterior,

si p no es múltiplo de 2, ni de 3, ni de 5, entonces es primo.

En la práctica procedemos 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.

				~~25~~	~~26~~	~~27~~	~~28~~	29	~~30~~
31	~~32~~	~~33~~	~~34~~	~~35~~	~~36~~	37	~~38~~	~~39~~	~~40~~
41	~~42~~	43	~~44~~	~~45~~	~~46~~	47	~~48~~		

- Los que quedan sin tachar no son múltiplos de 2, ni de 3, ni de 5 y, consecuentemente, estos números serán primos. Añadimos los que teníamos entre 2 y 24 y tendremos todos los números primos entre 2 y 48.

	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~~		

Ahora tomamos p de tal forma que esté entre el primer primo no considerado, 7, y el siguiente encontrado 11, sin que pueda ser el segundo, es decir tal que $7^2 \leqslant p < 11^2$. Entonces,

$$7^2 \leqslant p < 11^2 \Longrightarrow 7 \leqslant \sqrt{p} < 11$$

y los números primos que cumplen esta condición son el 2, el 3, el 5 y el 7, luego por el teorema anterior,

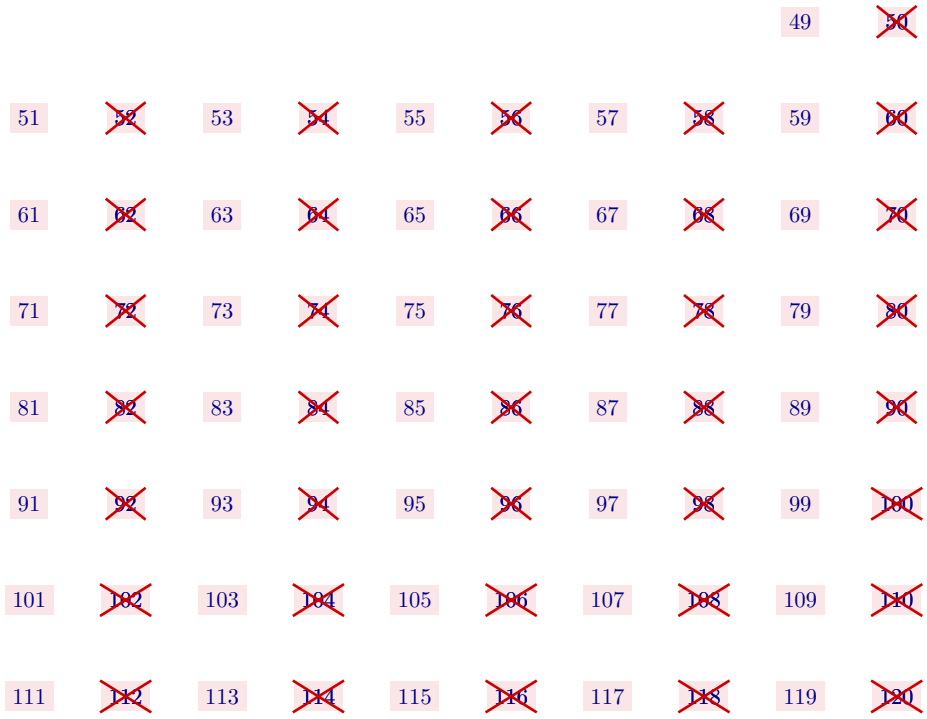
si p no es múltiplo de 2, ni de 3, ni de 5, ni de 7, entonces es primo.

En la práctica procedemos igual que en los casos anteriores.

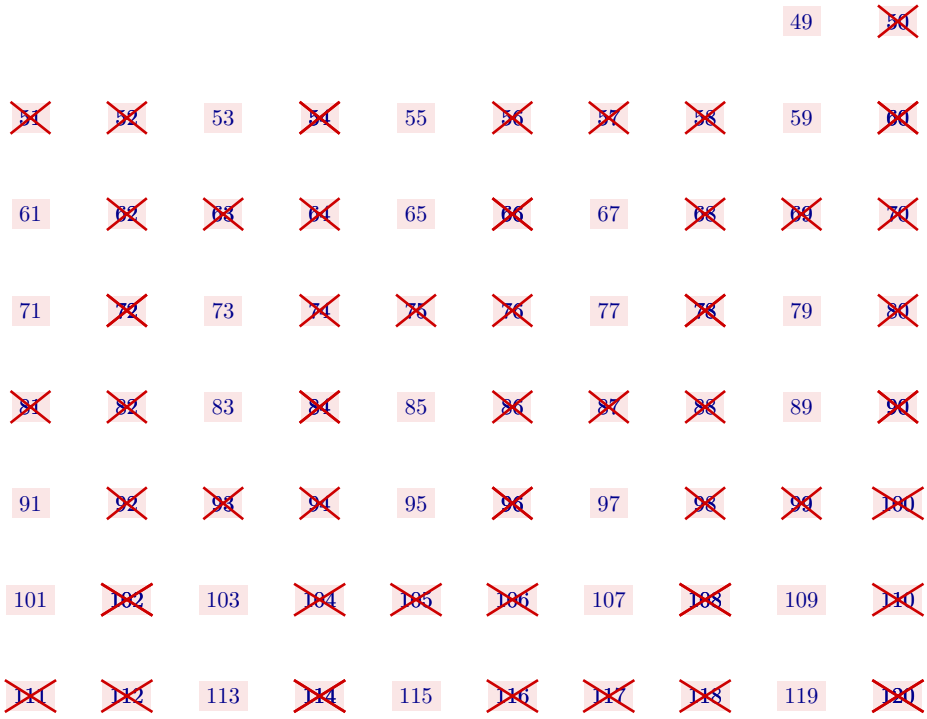
- Escribimos todos los números enteros entre 49 y 120.

								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

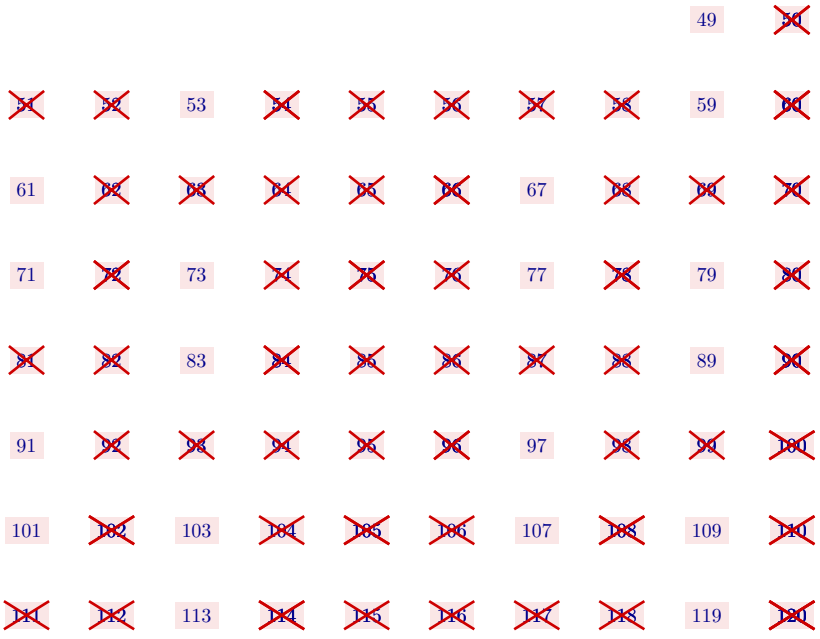
- Tachamos los que sean múltiplos de 2.



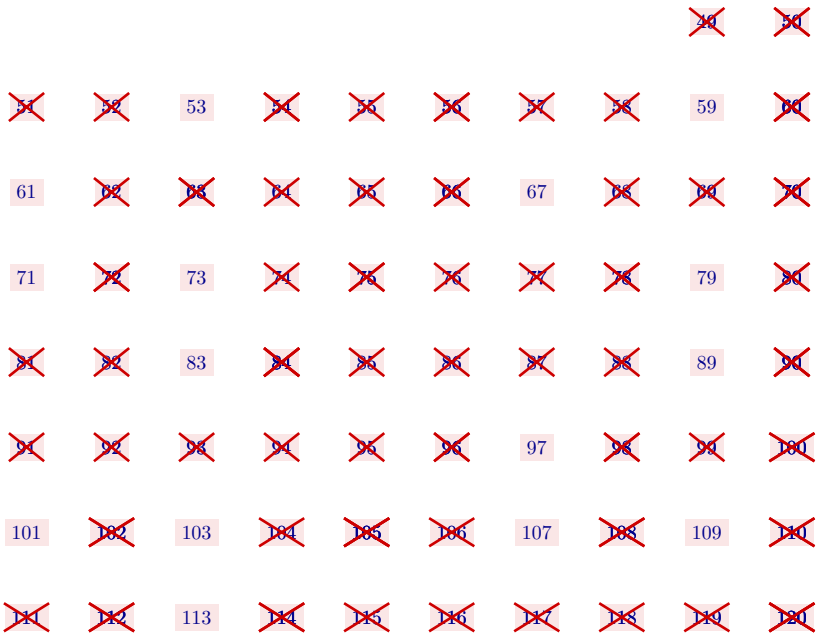
⁕ Tachamos los que sean múltiplos de 3.



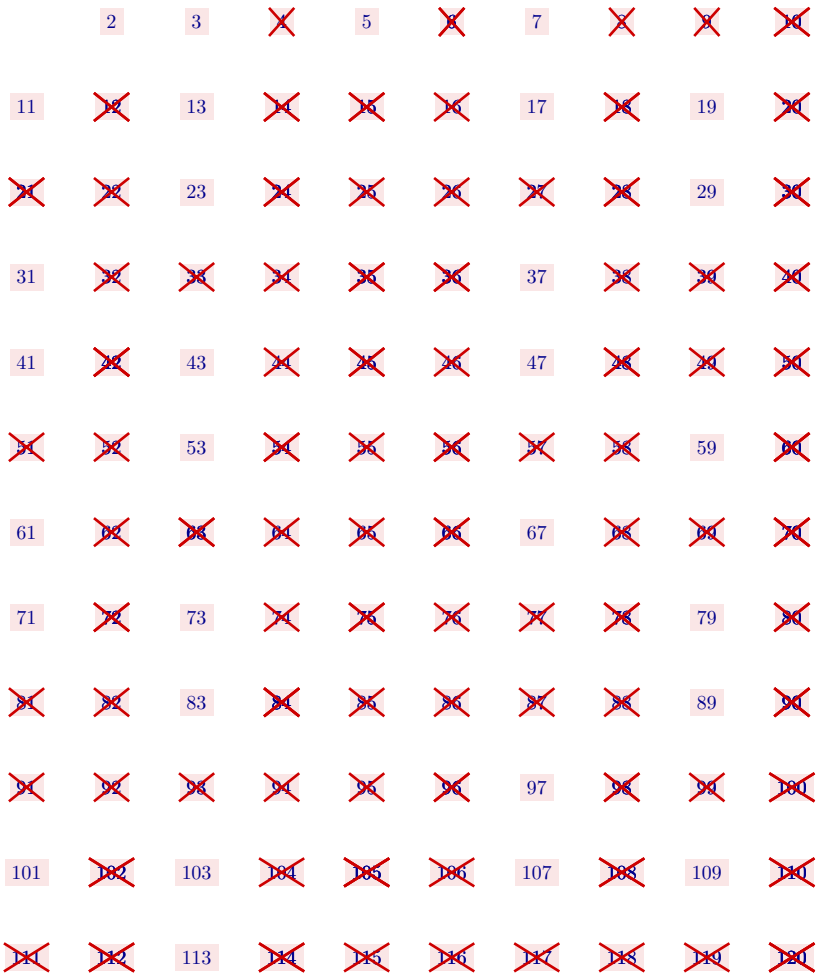
⁕ Tachamos los que sean múltiplos de 5.



⁕ Tachamos los que sean múltiplos de 7.



⁕ Los que quedan sin tachar no son múltiplos de 2, ni de 3, ni de 5, ni de 7 y, por lo tanto, primos. Añadimos los que teníamos entre 2 y 48 y tendremos todos los primos entre 2 y 120.



♦

Nota 6.2 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 $p \leqslant \sqrt{a}$ o $p^2 \leqslant a$.

♦

Ejemplo 6.3

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.

♦♦♦

6.3 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*".

6.3.1 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

$$a\big|bc \text{ y } \text{m.c.d.}(a,b) = 1 \Longrightarrow a\big|c$$

En efecto, como m.c.d. $(a,b) = 1$, por el corolario 5.3.7, existirán dos números enteros p y q tales que

$$pa + qb = 1$$

Entonces,

$$\left.\begin{array}{l} a\big|bc \\ \text{y} \\ a\big|a \Longrightarrow a\big|ac \end{array}\right\} \Longrightarrow a\big|pac + qbc \Longrightarrow a\big|\,(pa+qb)\,c \Longrightarrow a\big|c$$

♦

6.3.2 Teorema

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.

Sea p un entero mayor que 1. La proposición a probar sería,

$$p \text{ es primo} \longleftrightarrow \forall n_1, n_2 \in \mathbb{Z}\left(p\big|n_1n_2 \longrightarrow p\big|n_1 \text{ ó } p\big|n_2\right)$$

La condición es *necesaria*, es decir,

$$p \text{ es primo} \longrightarrow \forall n_1, n_2 \in \mathbb{Z}\left(p\big|n_1n_2 \longrightarrow p\big|n_1 \text{ ó } p\big|n_2\right)$$

Probaremos que si a y b dos enteros cualesquiera,

$$p \text{ es primo} \Longrightarrow \left(p\big|ab \Longrightarrow p\big|a \text{ o } p\big|b\right)$$

o lo que es igual,

$$p \text{ es primo} \Longrightarrow \Big(p\big|ab \text{ y } p\not\big|a \Longrightarrow p\big|b\Big)$$

En efecto, si p no es divisor de a, entonces, al ser p primo, el único divisor común de p y a es 1, es decir a y p son primos entre sí. Aplicando el *Lema de Euclides*,

$$\left.\begin{array}{l} \text{m.c.d.}(a,p)=1 \\ \text{y} \\ p\big|ab \end{array}\right\} \Longrightarrow p\big|b$$

Si p no fuera divisor de b, escribiríamos,

$$p \text{ es primo} \Longrightarrow \Big(p\big|ab \text{ y } p\not\big|b \Longrightarrow p\big|a\Big)$$

y siguiendo un proceso análogo llegaríamos a que $p\big|a$.

La condición es *suficiente*, es decir,

$$\forall n_1, n_2 \in \mathbb{Z}\ \Big(p\big|n_1n_2 \longrightarrow p\big|n_1 \text{ ó } p\big|n_2\Big) \longrightarrow p \text{ es primo}$$

y lo probaremos utilizando el método de demostración por la contrarrecíproca,

$$p \text{ no es primo} \longrightarrow \exists n_1, n_2 \in \mathbb{Z} : p\big|n_1n_2 \text{ y } p\not\big|n_1 \text{ y } p\not\big|n_2$$

En efecto, supongamos que p no es primo. Entonces, por 6.1.3,

$$\begin{array}{rcl} p \text{ no es primo} & \Longleftrightarrow & \exists a, b \in \mathbb{Z} : 1 < a < p \text{ y } 1 < b < p : p = ab \\ & \Longrightarrow & p\big|ab \text{ y } a\big|p \text{ y } b\big|p \end{array}$$

Además, p no puede dividir a a ni a b, ya que

- si p dividiese a a, entonces
$$p\big|a \Longrightarrow p\big|a \text{ y } a\big|p \Longrightarrow p = a$$
lo cual es imposible ya que $a \neq p$.
- si p dividiese a b, entonces
$$p\big|b \Longrightarrow p\big|b \text{ y } b\big|p \Longrightarrow p = b$$
lo cual es imposible ya que $b \neq p$.

Por lo tanto,

$$p \text{ no es primo} \Longrightarrow p\big|ab \text{ y } p\not\big|a \text{ y } p\not\big|b$$

luego, hemos encontrado dos enteros a y b tales que si p no es primo, p divide a ab y no divide a a ni a b.

♦

6.3.3 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

$$p\big|a_1 \cdot a_2 \cdot a_3 \cdot \cdots \cdot a_n \Longrightarrow \exists a_i : p\big|a_i,\ 1 \leqslant i \leqslant n$$

En efecto, supongamos que

$$p \mid a_1 \cdot a_2 \cdot a_3 \cdot \cdots \cdot a_n$$

entonces,

$$p \mid a_1 \, (a_2 \cdot a_3 \cdot \cdots \cdot a_n)$$

y aplicando el corolario anterior

$$p \mid a_1 \text{ ó } p \mid a_2 \cdot a_3 \cdot \cdots \cdot a_n$$

– Si $p \mid a_1$, el corolario está demostrado, de lo contrario

$$p \mid a_2 \cdot a_3 \cdot \cdots \cdot a_n$$

luego,

$$p \mid a_2 \, (a_3 \cdot \cdots \cdot a_n)$$

y, nuevamente por el corolario anterior,

$$p \mid a_2 \text{ ó } p \mid a_3 \cdot a_4 \cdot \cdots \cdot a_n$$

– Si $p \mid a_2$, el corolario está demostrado, de lo contrario

$$p \mid a_3 \cdot a_4 \cdot \cdots \cdot a_n$$

luego,

$$p \mid a_3 \, (a_4 \cdot \cdots \cdot a_n)$$

Repitiendo el proceso un número finito de veces, encontraremos, al menos, un a_i, $1 \leqslant i \leqslant n$, tal que $p \mid a_i$.

♦

Ejemplo 6.4

Demostrar que si $p, q_1, q_2, \ldots, q_r$ son primos y $p \mid q_1 \cdot q_2 \cdots q_r$, entonces existe algún $i = 1, 2, \ldots, r$ tal que $p = q_i$

Solución.

En efecto, por el corolario 6.3.3 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 6.5

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:

$$\sqrt{2} = \frac{a}{b} \Longrightarrow 2 = \frac{a^2}{b^2} \Longrightarrow a^2 = 2b^2 \Longrightarrow 2 \Big| a \cdot a$$

luego por el corolario 6.3.3

$$2 \Big| a$$

y, consecuentemente, existe un entero q tal que

$$a = 2q$$

entonces,

$$a = 2q \Longrightarrow a^2 = 4q^2 \Longrightarrow 2b^2 = 4q^2 \Longrightarrow b^2 = 2q^2 \Longrightarrow 2 \Big| b^2 \Longrightarrow 2 \Big| b \cdot b$$

y, nuevamente por el corolario 6.3.3, se sigue que

$$2 \Big| b$$

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 6.6

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

$$5 = \frac{a^3}{b^3} \Longrightarrow a^3 = 5b^3 \Longrightarrow 5 \Big| a^3$$

de donde se sigue, al ser 5 un número primo, que

$$5 \Big| a$$

luego existe un número entero q tal que

$$a = 5q \Longrightarrow a^3 = 5^3 q^3 \Longrightarrow 5b^3 = 5^3 q^3 \Longrightarrow b^3 = 5^2 q^3 \Longrightarrow 5 \Big| b^3$$

por tanto,

$$5 \Big| b$$

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.

♦

6.3.4 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.

Factorización.

- 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 6.1.4 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 6.1.4 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,

$$\begin{aligned} a = p_1(p_2p_3\cdots p_k) &\implies p_1 \Big| a \\ &\implies p_1 \Big| q_1q_2q_3\cdots q_r \\ &\implies p_1 \Big| q_j \text{ para algún } j \text{ entre 1 y } r. \ \{\text{Corolario 6.3.3}\} \\ &\implies p_1 = q_j, \text{ ya que } q_j \text{ es primo y } p_1 \neq 1. \end{aligned}$$

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

$$p_1p_2p_3\cdots p_k = p_1q_2q_3\cdots q_r$$

de donde, al ser $p_1 \neq 0$, se sigue que

$$p_2p_3\cdots p_k = q_2q_3\cdots q_r$$

Sea ahora

$$a_1 = p_2p_3\cdots p_k$$

y

$$a_1 = q_2q_3\cdots q_r.$$

Entonces $a_1 < a$, y

$$\begin{aligned} a_1 = p_2(p_3p_4\cdots p_k) &\implies p_2 \Big| a_1 \\ &\implies p_2 \Big| q_2q_3q_4\cdots q_r \\ &\implies p_2 \Big| q_j \text{ para algún } j \text{ entre 2 y } r. \ \{\text{Corolario 6.3.3}\} \\ &\implies p_2 = q_j, \text{ ya que } q_j \text{ es primo y } p_2 \neq 1. \end{aligned}$$

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,

$$\begin{aligned} a_{k-1} = p_k &\implies p_k \Big| a_{k-1} \\ &\implies p_k \Big| q_kq_{k+1}q_{k+2}\cdots q_r \\ &\implies p_k \Big| q_j \text{ para algún } j \text{ entre } k \text{ y } r. \ \{\text{Corolario 6.3.3}\} \\ &\implies p_k = q_j, \text{ ya que } q_j \text{ es primo y } p_k \neq 1 \end{aligned}$$

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

$$a = p_1 p_2 \cdot p_3 \cdots p_k$$

siendo única la factorización.

♦

6.3.5 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 factorizarse en números 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 factorización 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 6.7

Factorizar en números primos el número 720.

Solución.

Obtendremos una factorización 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

$$720 = 2^4 \cdot 3^2 \cdot 5$$

♦♦♦

6.4 Divisores de un número

6.4.1 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 factorización de a y b se sigue directamente del corolario 6.3.5.

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 6.8

Factorizar $a = 270$ y $b = 368$ en números 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.

♦

6.4.2 Criterio General de Divisibilidad

Sean a y b dos números enteros tales que $|a| > 1$ y $|b| > 1$. 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 (6.4.1) y podemos escribir b y q en la forma,

$$\begin{aligned} b &= p_1^{\beta_1} p_2^{\beta_2} \cdots p_k^{\beta_k}, \text{con } \beta_i \geqslant 0,\ 1 \leqslant i \leqslant k \\ q &= p_1^{\gamma_1} p_2^{\gamma_2} \cdots p_k^{\gamma_k}, \text{con } \gamma_i \geqslant 0,\ 1 \leqslant i \leqslant k \end{aligned} \tag{6.2}$$

donde en las factorizaciones anteriores se verifica:

$\beta_i = 0$, si p_i no está en la factorización en números primos de q,

y

$\gamma_i = 0$, si p_i no está en la factorización en números 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,

$$\alpha_i = \beta_i + \gamma_i,\ \text{con } \gamma_i \geqslant 0 \implies \alpha_i \geqslant \beta_i,\ \text{para } 1 \leqslant i \leqslant k$$

y a tiene, al menos, todos los factores primos de b ya que en la factorización (6.2) 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 factorización en números primos de b (6.3.5) 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 factorización 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

$$\alpha_i \geqslant \beta_i \implies \alpha_i - \beta_i \geqslant 0,\ \text{para } 1 \leqslant i \leqslant k$$

tendremos que $\dfrac{a}{b}$ 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 $-b$.

♦

6.4.3 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 6.3.5, a admite una factorización 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,

$$\begin{aligned} b \in D_a &\iff b \text{ es divisor de } a \\ &\iff a \text{ es divisible por } b \\ &\iff \begin{cases} a \text{ tiene en su factorización, al menos, todos los factores} \\ \text{primos de } b \text{ con exponentes iguales o mayores.} \end{cases} \\ &\iff \begin{cases} b \text{ tiene en su factorización, a lo sumo, todos los factores} \\ \text{primos de } a \text{ con exponentes iguales o menores.} \end{cases} \\ &\iff b = p_1^{\beta_1} \cdot p_2^{\beta_2} \cdot \cdots \cdot p_k^{\beta_k}, \text{con } 0 \leqslant \beta_i \leqslant \alpha_i,\ 1 \leqslant i \leqslant k \end{aligned}$$

y como b es entero, los β_i han de ser no negativos. Por tanto,

$$D_a = \left\{ p_1^{\beta_1} \cdot p_2^{\beta_2} \cdot \cdots \cdot p_k^{\beta_k}, \text{con } 0 \leqslant \beta_i \leqslant \alpha_i,\ 1 \leqslant i \leqslant k \right\}$$

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,

$$D_a = \left\{ -p_1^{\beta_1} \cdot p_2^{\beta_2} \cdot \cdots \cdot p_k^{\beta_k}, \text{con } 0 \leqslant \beta_i \leqslant \alpha_i,\ 1 \leqslant i \leqslant k \right\}$$

es el conjunto formado por los divisores negativos de a.

El conjunto de todos los divisores de a será, por tanto,

$$D_a = \left\{ \pm p_1^{\beta_1} \cdot p_2^{\beta_2} \cdot \cdots \cdot p_k^{\beta_k}, \text{con } 0 \leqslant \beta_i \leqslant \alpha_i,\ 1 \leqslant i \leqslant k \right\}$$

2. $a < -1$. En este caso,

$$a < -1 \Longrightarrow -a > 1$$

aplicamos todo lo que hicimos en el caso anterior a $-a$ y tendremos:

$$D_{-a} = \left\{ \pm p_1^{\beta_1} \cdot p_2^{\beta_2} \cdot \cdots \cdot p_k^{\beta_k}, \text{con } 0 \leqslant \beta_i \leqslant \alpha_i,\ 1 \leqslant i \leqslant k \right\}$$

De 1. y 2. se sigue que:

$$D_{|a|} = \left\{ \pm p_1^{\beta_1} \cdot p_2^{\beta_2} \cdot \cdots \cdot p_k^{\beta_k}, \text{con } 0 \leqslant \beta_i \leqslant \alpha_i,\ 1 \leqslant i \leqslant k \right\}$$

♦

6.4.4 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.

Sea a un entero tal que $|a| > 1$. Según hemos visto en el apartado anterior,

$$D_{|a|} = \left\{ \pm p_1^{\beta_1} \cdot p_2^{\beta_2} \cdot \cdots \cdot p_k^{\beta_k}, \text{con } 0 \leqslant \beta_i \leqslant \alpha_i,\ 1 \leqslant i \leqslant k \right\}$$

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 $p_1^{\beta_1} \cdot p_2^0 \cdot p_3^0 \cdot \cdots \cdot p_k^0$ 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	$\cdots\cdots$	$p_1^{\alpha_1}$
$\times p_2$	$p_1^0p_2$	p_1p_2	$p_1^2p_2$	$\cdots\cdots$	$p_1^{\alpha_1}p_2$
$\times p_2^2$	$p_1^0p_2^2$	$p_1p_2^2$	$p_1^2p_2^2$	$\cdots\cdots$	$p_1^{\alpha_1}p_2^2$
$\times p_2^3$	$p_1^0p_2^3$	$p_1p_2^3$	$p_1^2p_2^3$	$\cdots\cdots$	$p_1^{\alpha_1}p_2^3$
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots\quad\vdots$	$\vdots$
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots\quad\vdots$	$\vdots$
$\times p_2^{\alpha_2}$	$p_1^0p_2^{\alpha_2}$	$p_1p_2^{\alpha_2}$	$p_1^2p_2^{\alpha_2}$	$\cdots\cdots$	$p_1^{\alpha_1}p_2^{\alpha_2}$
$\times p_3$	$p_1^0p_3$	p_1p_3	$p_1^2p_3$	$\cdots\cdots$	$p_1^{\alpha_1}p_3$
	$p_1^0p_2p_3$	$p_1p_2p_3$	$p_1^2p_2p_3$	$\cdots\cdots$	$p_1^{\alpha_1}p_2p_3$
	$p_1^0p_2^2p_3$	$p_1p_2^2p_3$	$p_1^2p_2^2p_3$	$\cdots\cdots$	$p_1^{\alpha_1}p_2^2p_3$
	$p_1^0p_2^3p_3$	$p_1p_2^3p_3$	$p_1^2p_2^3p_3$	$\cdots\cdots$	$p_1^{\alpha_1}p_2^3p_3$
	$\vdots$	$\vdots$	$\vdots$	$\vdots\quad\vdots$	$\vdots$
	$\vdots$	$\vdots$	$\vdots$	$\vdots\quad\vdots$	$\vdots$
	$p_1^0p_2^{\alpha_2}p_3$	$p_1p_2^{\alpha_2}p_3$	$p_1^2p_2^{\alpha_2}p_3$	$\cdots\cdots$	$p_1^{\alpha_1}p_2^{\alpha_2}p_3$
$\times p_3^2$	$p_1^0p_3^2$	$p_1p_3^2$	$p_1^2p_3^2$	$\cdots\cdots$	$p_1^{\alpha_1}p_3^2$
	$p_1^0p_2p_3^2$	$p_1p_2p_3^2$	$p_1^2p_2p_3^2$	$\cdots\cdots$	$p_1^{\alpha_1}p_2p_3^2$
	$p_1^0p_2^2p_3^2$	$p_1p_2^2p_3^2$	$p_1^2p_2^2p_3^2$	$\cdots\cdots$	$p_1^{\alpha_1}p_2^2p_3^2$
	$p_1^0p_2^3p_3^2$	$p_1p_2^3p_3^2$	$p_1^2p_2^3p_3^2$	$\cdots\cdots$	$p_1^{\alpha_1}p_2^3p_3^2$
	$\vdots$	$\vdots$	$\vdots$	$\vdots\quad\vdots$	$\vdots$
	$\vdots$	$\vdots$	$\vdots$	$\vdots\quad\vdots$	$\vdots$
	$p_1^0p_2^{\alpha_2}p_3^2$	$p_1p_2^{\alpha_2}p_3^2$	$p_1^2p_2^{\alpha_2}p_3^2$	$\cdots\cdots$	$p_1^{\alpha_1}p_2^{\alpha_2}p_3^2$
	$\vdots$	$\vdots$	$\vdots$	$\vdots\quad\vdots$	$\vdots$
	$\vdots$	$\vdots$	$\vdots$	$\vdots\quad\vdots$	$\vdots$
$\times p_3^{\alpha_3}$	$p_1^0p_3^{\alpha_3}$	$p_1p_3^{\alpha_3}$	$p_1^2p_3^{\alpha_3}$	$\cdots\cdots$	$p_1^{\alpha_1}p_3^{\alpha_3}$
	$p_1^0p_2p_3^{\alpha_3}$	$p_1p_2p_3^{\alpha_3}$	$p_1^2p_2p_3^{\alpha_3}$	$\cdots\cdots$	$p_1^{\alpha_1}p_2p_3^{\alpha_3}$
	$p_1^0p_2^2p_3^{\alpha_3}$	$p_1p_2^2p_3^{\alpha_3}$	$p_1^2p_2^2p_3^{\alpha_3}$	$\cdots\cdots$	$p_1^{\alpha_1}p_2^2p_3^{\alpha_3}$
	$p_1^0p_2^3p_3^{\alpha_3}$	$p_1p_2^3p_3^{\alpha_3}$	$p_1^2p_2^3p_3^{\alpha_3}$	$\cdots\cdots$	$p_1^{\alpha_1}p_2^3p_3^{\alpha_3}$
	$\vdots$	$\vdots$	$\vdots$	$\vdots\quad\vdots$	$\vdots$
	$\vdots$	$\vdots$	$\vdots$	$\vdots\quad\vdots$	$\vdots$
	$p_1^0p_2^{\alpha_2}p_3^{\alpha_3}$	$p_1p_2^{\alpha_2}p_3^{\alpha_3}$	$p_1^2p_2^{\alpha_2}p_3^{\alpha_3}$	$\cdots\cdots$	$p_1^{\alpha_1}p_2^{\alpha_2}p_3^{\alpha_3}$

⁕ 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,

$$\begin{aligned}&0\leqslant\beta_1\leqslant\alpha_1\\&0\leqslant\beta_2\leqslant\alpha_2\\&0\leqslant\beta_3\leqslant\alpha_3\\&\cdots\cdots\cdots\\&0\leqslant\beta_k\leqslant\alpha_k\end{aligned}$$

♦

Ejemplo 6.9

Calcular todos los divisores de 604800.

Solución.

Factorizamos 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

♦

6.4.5 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 factorización en números 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 6.4.3, 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

$$\begin{array}{|c|}\hline p_1^0 \\ \hline p_1^1 \\ \hline p_1^2 \\ \hline \vdots \\ \hline p_1^{\alpha_1} \\ \hline \end{array} \Big\} (\alpha_1 + 1)$$

  es decir habrá un total de $\alpha_1 + 1$ de estos divisores.

- Los divisores de la forma $p_1^{\beta_1} \cdot p_2^{\beta_2}$, con $0 \leqslant \beta_2 \leqslant \alpha_2$ son:

$$\begin{array}{|c|c|}\hline p_1^0 & p_1^0 \cdot p_2^0 \\ \hline & p_1^0 \cdot p_2^1 \\ \hline & p_1^0 \cdot p_2^2 \\ \hline & \vdots \\ \hline & p_1^0 \cdot p_2^{\alpha_2} \\ \hline \end{array} \Big\} (\alpha_2 + 1)$$

$$\begin{array}{|c|c|}\hline p_1^1 & p_1^1 \cdot p_2^0 \\ \hline & p_1^1 \cdot p_2^1 \\ \hline & p_1^1 \cdot p_2^2 \\ \hline & \vdots \\ \hline & p_1^1 \cdot p_2^{\alpha_2} \\ \hline \end{array} \Big\} (\alpha_2 + 1)$$

$$\vdots$$

$$\begin{array}{|c|c|}\hline p_1^{\alpha_1} & p_1^{\alpha_1} \cdot p_2^0 \\ \hline & p_1^{\alpha_1} \cdot p_2^1 \\ \hline & p_1^{\alpha_1} \cdot p_2^2 \\ \hline & \vdots \\ \hline & p_1^{\alpha_1} \cdot p_2^{\alpha_2} \\ \hline \end{array} \Big\} (\alpha_2 + 1)$$

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

$$(\alpha_1+1)\,(\alpha_2+1)\,(\alpha_3+1)\cdots\cdots(\alpha_{k-1}+1)$$

⊛ 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

$$(\alpha_1+1)\,(\alpha_2+1)\,(\alpha_3+1)\cdots\cdots(\alpha_{k-1}+1)\,(\alpha_k+1)$$

Por lo tanto, el número total de divisores de a es:

$$N_a=(\alpha_1+1)\,(\alpha_2+1)\,(\alpha_3+1)\cdots\cdots(\alpha_{k-1}+1)\,(\alpha_k+1)$$

♦

Ejemplo 6.10

¿Cuántos divisores positivos tiene el número 604800?

Solución.

En un ejemplo anterior teníamos que

$$604800 = 2^7 \cdot 3^3 \cdot 5^2 \cdot 7$$

por lo tanto, según el apartado anterior,

$$N_{604800} = (7+1)(3+1)(2+1)(1+1) = 8 \cdot 4 \cdot 3 \cdot 2 = 192$$

es decir, el número 604800 tiene 192 divisores positivos.

♦

6.4.6 Suma de los divisores de un número compuesto

Si a es un entero de valor absoluto mayor que 1 y $a = p_1^{\alpha_1} p_2^{\alpha_2} p_3^{\alpha_3} \cdot \cdots \cdot p_k^{\alpha_k}$ es su factorización en números 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 6.4.3, 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.

$$\begin{aligned}
S_a &= \sum_{\beta_1=0}^{\alpha_1} \sum_{\beta_2=0}^{\alpha_2} \sum_{\beta_3=0}^{\alpha_3} \cdots \cdots \sum_{\beta_k=0}^{\alpha_k} p_1^{\beta_1} \cdot p_2^{\beta_2} \cdot p_3^{\beta_3} \cdots \cdots p_k^{\beta_k} \\
&= \sum_{\beta_1=0}^{\alpha_1} \sum_{\beta_2=0}^{\alpha_2} \sum_{\beta_3=0}^{\alpha_3} p_1^{\beta_1} \cdot p_2^{\beta_2} \cdot p_3^{\beta_3} \cdots \cdots \sum_{\beta_k=0}^{\alpha_k} p_k^{\beta_k} \\
&= \sum_{\beta_1=0}^{\alpha_1} \sum_{\beta_2=0}^{\alpha_2} p_1^{\beta_1} \cdot p_2^{\beta_2} \sum_{\beta_3=0}^{\alpha_3} \cdot p_3^{\beta_3} \cdots \cdots \sum_{\beta_k=0}^{\alpha_k} p_k^{\beta_k} \\
&= \sum_{\beta_1=0}^{\alpha_1} p_1^{\beta_1} \sum_{\beta_2=0}^{\alpha_2} p_2^{\beta_2} \sum_{\beta_3=0}^{\alpha_3} p_3^{\beta_3} \cdots \cdots \sum_{\beta_k=0}^{\alpha_k} p_k^{\beta_k} \\
&= \left(p_1^0 + p_1^1 + p_1^2 + \cdots + p_1^{\alpha_1}\right) \left(p_2^0 + p_2^1 + p_2^2 + \cdots + p_2^{\alpha_2}\right) \\
&\qquad \left(p_3^0 + p_3^1 + p_3^2 + \cdots + p_3^{\alpha_3}\right) \\
&\qquad \cdots\cdots\cdots\cdots\cdots\cdots \\
&\qquad \left(p_k^0 + p_k^1 + p_k^2 + \cdots + p_k^{\alpha_k}\right) \\
&= \frac{p_1^{\alpha_1+1} - 1}{p_1 - 1} \cdot \frac{p_2^{\alpha_2+1} - 1}{p_2 - 1} \cdot \frac{p_3^{\alpha_3+1} - 1}{p_3 - 1} \cdot \cdots \cdot \frac{p_k^{\alpha_k+1} - 1}{p_k - 1}
\end{aligned}$$

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 $p_1, p_2, p_3, \cdots, p_k$.

♦♦♦

6.5 Reglas para calcular el M.C.D. y el M.C.M. 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.

6.5.1 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 factorizaciones en números primos.

Demostración.

Sean a y b enteros cualesquiera. Por el lema 6.4.1, podemos escribir a y b en la forma:

$$\begin{aligned} a &= p_1^{\alpha_1} p_2^{\alpha_2} \cdot \cdots \cdot p_k^{\alpha_k},\ \alpha_i \geqslant 0,\ 1 \leqslant i \leqslant k \\ \text{y} & \\ b &= p_1^{\beta_1} p_2^{\beta_2} \cdot \cdots \cdot p_k^{\beta_k},\ \beta_i \geqslant 0,\ 1 \leqslant i \leqslant k \end{aligned}$$

siendo $\alpha_i = 0$, si el factor primo p_i de la factorización de b no aparece en la de a y $\beta_i = 0$ si el p_i de la factorización de a no aparece en la de b.

Sea c cualquier entero y sea

$$c = p_1^{\gamma_1} p_2^{\gamma_2} \cdot \cdots \cdot p_k^{\gamma_k},\ \gamma_i \geqslant 0,\ 1 \leqslant i \leqslant k$$

la factorización obtenida por aplicación del lema 6.4.1. Entonces, si c es divisor de a y de b, tendremos

$$\left.\begin{array}{lll} c \mid a & \Longrightarrow & \gamma_i \leqslant \alpha_i,\ 1 \leqslant i \leqslant k \\ \text{y} & & \\ c \mid b & \Longrightarrow & \gamma_i \leqslant \beta_i,\ 1 \leqslant i \leqslant k \end{array}\right\} \Longrightarrow \gamma_i \leqslant \text{mín}\,\{\alpha_i, \beta_i\}$$

luego los divisores comunes a a y a b tienen, todos, la forma,

$$c = p_1^{\gamma_1} p_2^{\gamma_2} \cdot \cdots \cdot p_k^{\gamma_k},\ \gamma_i \geqslant \text{mín}\,\{\alpha_i, \beta_i\}\ \ 1 \leqslant i \leqslant k$$

y el máximo de ellos, en el sentido de que sea múltiplo de todos, se obtendrá cuando $\gamma_i = \text{mín}\,\{\alpha_i, \beta_i\}$.

Pues bien, si

$$d = p_1^{\text{mín}\{\alpha_1,\beta_1\}} p_2^{\text{mín}\{\alpha_2,\beta_2\}} \cdot \cdots \cdot p_k^{\text{mín}\{\alpha_k,\beta_k\}}$$

entonces,

$$\begin{aligned} &1.\ d \mid a \text{ y } d \mid b \\ &\text{y} \\ &2.\ \forall c,\ c \mid a \text{ y } c \mid b \Longrightarrow d \mid c \end{aligned}$$

luego $d = \text{m.c.d.}(a, b)$.

Ahora, para cada i entre 1 y k, puede ocurrir lo siguiente:

$$\min\{\alpha_i,\beta_i\}=0 \implies \begin{cases} \alpha_i=0 \\ \text{ó} \\ \beta_i=0 \end{cases} \implies \begin{cases} p_i \text{ no está en la factorización en números primos de } a. \\ \text{ó} \\ p_i \text{ no está en la factorización en números primos de } b. \end{cases} \implies \text{El factor primo } p_i \text{ no es común a } a \text{ y a } b$$

ó

$$\min\{\alpha_i,\beta_i\}\neq 0 \implies \begin{cases} \alpha_i\neq 0 \\ \text{y} \\ \beta_i\neq 0 \end{cases} \implies \begin{cases} p_i \text{ está en la factorización en números primos de } a. \\ \text{y} \\ p_i \text{ está en la factorización en números primos de } b. \end{cases} \implies \text{El factor primo } p_i \text{ es común a } a \text{ y a } b$$

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 6.11

Calcular el máximo común divisor de 1548 y 18900.

Solución.

Lo calcularemos siguiendo los pasos del apartado anterior.

Descomponemos ambos números en factores primos.

1584	2
792	2
396	2
198	2
99	3
33	3
11	11
1	

$$\implies 1584=2^4\cdot 3^2\cdot 11$$

18900	2
9450	2
4725	3
1575	3
525	3
175	5
35	5
7	7
1	

$$\implies 18900=2^2\cdot 3^3\cdot 5^2\cdot 7$$

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 6.4.1).

$$\begin{aligned} 1584 &= 2^4 \cdot 3^2 \cdot 5^0 \cdot 7^0 \cdot 11 \\ 18900 &= 2^2 \cdot 3^3 \cdot 5^2 \cdot 7 \cdot 11^0 \end{aligned}$$

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).

♦

6.5.2 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 enteros cualesquiera. Por el lema 6.4.1, podemos escribir a y b en la forma:

$$\begin{aligned} a &= p_1^{\alpha_1} p_2^{\alpha_2} \cdot \cdots \cdot p_k^{\alpha_k},\ \alpha_i \geqslant 0,\ 1 \leqslant i \leqslant k \\ &\text{y} \\ b &= p_1^{\beta_1} p_2^{\beta_2} \cdot \cdots \cdot p_k^{\beta_k},\ \beta_i \geqslant 0,\ 1 \leqslant i \leqslant k \end{aligned}$$

siendo $\alpha_i = 0$, si el factor primo p_i de la factorización de b no aparece en la de a y $\beta_i = 0$ si el p_i de la factorización de a no aparece en la de b.

Sea c cualquier entero y sea

$$c = p_1^{\gamma_1} p_2^{\gamma_2} \cdot \cdots \cdot p_k^{\gamma_k},\ \gamma_i \geqslant 0,\ 1 \leqslant i \leqslant k$$

la factorización obtenida por aplicación del lema 6.4.1. Entonces, si c es múltiplo de a y de b, tendremos

$$\left.\begin{array}{ll} a \big| c & \Longrightarrow \gamma_i \geqslant \alpha_i,\ 1 \leqslant i \leqslant k \\ \text{y} & \\ b \big| c & \Longrightarrow \gamma_i \geqslant \beta_i,\ 1 \leqslant i \leqslant k \end{array}\right\} \Longrightarrow \gamma_i \geqslant \text{máx}\{\alpha_i, \beta_i\}$$

luego los múltiplos comunes a a y a b tienen, todos, la forma,

$$c = p_1^{\gamma_1} p_2^{\gamma_2} \cdot \cdots \cdot p_k^{\gamma_k},\ \gamma_i \geqslant \text{máx}\{\alpha_i, \beta_i\}\ \ 1 \leqslant i \leqslant k$$

y el mínimo de ellos, en el sentido de que sea divisor de todos, se obtendrá cuando $\gamma_i = \text{máx}\{\alpha_i, \beta_i\}$.

Pues bien, si

$$m = p_1^{\text{máx}\{\alpha_1,\beta_1\}} p_2^{\text{máx}\{\alpha_2,\beta_2\}} \cdot \cdots \cdot p_k^{\text{máx}\{\alpha_k,\beta_k\}}$$

entonces,

1. $a \big| m$ y $b \big| m$

y

2. $\forall c,\ a \big| c$ y $b \big| c \Longrightarrow m \big| c$

luego $m = \text{l.c.m.}(a, b)$.

Ahora, para cada i entre 1 y k, puede ocurrir lo siguiente:

$$\left.\begin{array}{l}\alpha_i = 0\\ \text{y}\\ \beta_i \neq 0\end{array}\right\} \Longrightarrow \text{El factor primo } p_i \text{ no es común a } a \text{ y a } b \text{ y máx}\{\alpha_i, \beta_i\} = \beta_i$$

ó

$$\left.\begin{array}{l}\alpha_i \neq 0\\ \text{y}\\ \beta_i = 0\end{array}\right\} \Longrightarrow \text{El factor primo } p_i \text{ no es común a } a \text{ y a } b \text{ y máx}\{\alpha_i, \beta_i\} = \alpha_i$$

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 6.12

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 6.4.1).

$$\begin{aligned} 1584 &= 2^4 \cdot 3^2 \cdot 5^0 \cdot 7^0 \cdot 11 \\ 18900 &= 2^2 \cdot 3^3 \cdot 5^2 \cdot 7 \cdot 11^0 \end{aligned}$$

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.

♦

Ejemplo 6.13

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 6.3.5, 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

$$a = p_1^{\alpha_1} p_2^{\alpha_2} p_3^{\alpha_3} \cdot \cdots \cdot p_k^{\alpha_k}$$

y

$$b = q_1^{\beta_1} q_2^{\beta_2} q_3^{\beta_3} \cdot \cdots \cdot q_m^{\beta_m}$$

Pues bien, según el enunciado, m.c.d.$(a,b) = 18$, es decir, 18 es divisor de a y de b luego por 6.4.2 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 $18 = 2 \cdot 3^2$,

$$\text{m.c.d.}(a,b) = 18 \implies \begin{cases} 18 \,|a \\ \text{y} \\ 18 \,|b \end{cases}$$

$$\implies \begin{cases} 2 \cdot 3^2 \,|a \\ \text{y} \\ 2 \cdot 3^2 \,|b \end{cases}$$

$$\implies \begin{cases} p_1 = 2 \text{ y } \alpha_1 \geqslant 1 \\ \text{y} \\ p_2 = 3 \text{ y } \alpha_2 \geqslant 2 \end{cases} \quad \begin{cases} q_1 = 2 \text{ y } \beta_1 \geqslant 1 \\ \text{y} \\ q_2 = 3 \text{ y } \beta_2 \geqslant 2 \end{cases}$$

Por otra parte, el número de divisores de a es 21. Entonces, utilizando el resultado de 6.4.5,

$$\begin{aligned} N_a = 21 &\implies (\alpha_1 + 1)(\alpha_2 + 1)(\alpha_3 + 1) \cdots (\alpha_k + 1) = 21 \\ &\implies \alpha_1 + 1 \in D_{21},\ 1 \leqslant i \leqslant k \\ &\implies \alpha_1 + 1 \in \{1, 3, 7, 21\},\ 1 \leqslant i \leqslant k \\ &\quad \{\alpha_1 \geqslant 1 \implies \alpha_1 + 1 \geqslant 2\} \\ &\implies \alpha_1 + 1 \in \{3, 7, 21\} \end{aligned}$$

Habrá, pues, tres opciones.

1 $\alpha_1 + 1 = 3$. En este caso,

$$\left.\begin{aligned}(\alpha_1+1)(\alpha_2+1)(\alpha_3+1)\cdots(\alpha_k+1) &= 21\\ \alpha_1+1 &= 3\end{aligned}\right\} \implies 3(\alpha_2+1)(\alpha_3+1)\cdots(\alpha_k+1) = 21$$

$$\implies (\alpha_2+1)(\alpha_3+1)\cdots(\alpha_k+1) = 7$$

$$\implies \alpha_2+1 \in D_7$$

$$\implies \alpha_2+1 \in \{1,7\}$$

$$\{\alpha_2 \geqslant 2 \implies \alpha_2+1 \geqslant 3\}$$

$$\implies \alpha_2+1 = 7$$

Entonces,

$$\left.\begin{aligned}(\alpha_2+1)(\alpha_3+1)\cdots(\alpha_k+1) &= 7\\ \alpha_2+1 &= 7\end{aligned}\right\} \implies 7(\alpha_3+1)\cdots(\alpha_k+1) = 7$$

$$\implies (\alpha_3+1)\cdots(\alpha_k+1) = 1$$

$$\implies \alpha_i+1 = 1,\ 3 \leqslant i \leqslant k$$

Tendremos, pues,

$$\left.\begin{aligned}\alpha_1+1 = 3 &\implies \alpha_1 = 2\\ \alpha_2+1 = 7 &\implies \alpha_2 = 6\\ \alpha_i+1 = 1,\ 3 \leqslant i \leqslant k &\implies \alpha_i = 0,\ 3 \leqslant i \leqslant k\end{aligned}\right\} \implies a = 2^2 3^6$$

2 $\alpha_1 + 1 = 7$. En tal caso,

$$\left.\begin{aligned}(\alpha_1+1)(\alpha_2+1)(\alpha_3+1)\cdots(\alpha_k+1) &= 21\\ \alpha_1+1 &= 7\end{aligned}\right\} \implies 7(\alpha_2+1)(\alpha_3+1)\cdots(\alpha_k+1) = 21$$

$$\implies (\alpha_2+1)(\alpha_3+1)\cdots(\alpha_k+1) = 3$$

$$\implies \alpha_2+1 \in D_3$$

$$\implies \alpha_2+1 \in \{1,3\}$$

$$\{\alpha_2 \geqslant 2 \implies \alpha_2+1 \geqslant 3\}$$

$$\implies \alpha_2+1 = 3$$

Entonces,

$$\left.\begin{aligned}(\alpha_2+1)(\alpha_3+1)\cdots(\alpha_k+1) &= 3\\ \alpha_2+1 &= 3\end{aligned}\right\} \implies 3(\alpha_3+1)\cdots(\alpha_k+1) = 3$$

$$\implies (\alpha_3+1)\cdots(\alpha_k+1) = 1$$

$$\implies \alpha_i+1 = 1,\ 3 \leqslant i \leqslant k$$

Tendremos, pues,

$$\left.\begin{aligned}\alpha_1+1 = 7 &\implies \alpha_1 = 6\\ \alpha_2+1 = 3 &\implies \alpha_2 = 2\\ \alpha_i+1 = 1,\ 3 \leqslant i \leqslant k &\implies \alpha_i = 0,\ 3 \leqslant i \leqslant k\end{aligned}\right\} \implies a = 2^6 3^2$$

3 $\alpha_1 + 1 = 21$. En tal caso,

$$\left.\begin{array}{r}(\alpha_1+1)(\alpha_2+1)(\alpha_3+1)\cdots(\alpha_k+1)=21\\ \alpha_1+1=21\end{array}\right\} \implies 21(\alpha_2+1)(\alpha_3+1)\cdots(\alpha_k+1)=21$$
$$\implies (\alpha_2+1)(\alpha_3+1)\cdots(\alpha_k+1)=1$$
$$\implies \alpha_i+1=1,\ 2\leqslant i\leqslant k$$

lo cual es imposible, ya que $\alpha_2 \geqslant 2 \implies \alpha_2 + 1 \geqslant 3$.

Calculamos, ahora, el número b.

$$\begin{aligned} N_b = 10 &\implies (\beta_1+1)(\beta_2+1)(\beta_3+1)\cdots(\beta_m+1)=10\\ &\implies \beta_1+1\in D_{10},\ 1\leqslant i\leqslant m\\ &\implies \beta_1+1\in\{1,2,5,10\},\ 1\leqslant i\leqslant m\\ &\quad\ \{\beta_1\geqslant 1\implies \beta_1+1\geqslant 2\}\\ &\implies \beta_1+1\in\{2,5,10\}\end{aligned}$$

Habrá, pues, tres opciones.

1 $\beta_1 + 1 = 2$. En este caso,

$$\left.\begin{array}{r}(\beta_1+1)(\beta_2+1)(\beta_3+1)\cdots(\beta_m+1)=10\\ \beta_1+1=2\end{array}\right\} \implies 2(\beta_2+1)(\beta_3+1)\cdots(\beta_m+1)=10$$
$$\implies (\beta_2+1)(\beta_3+1)\cdots(\beta_m+1)=5$$
$$\implies \beta_2+1\in D_5$$
$$\implies \beta_2+1\in\{1,5\}$$
$$\{\beta_2\geqslant 2\implies \beta_2+1\geqslant 3\}$$
$$\implies \beta_2+1=5$$

Entonces,

$$\left.\begin{array}{r}(\beta_2+1)(\beta_3+1)\cdots(\beta_m+1)=5\\ \beta_2+1=5\end{array}\right\} \implies 5(\beta_3+1)\cdots(\beta_m+1)=4$$
$$\implies (\beta_3+1)\cdots(\beta_m+1)=1$$
$$\implies \beta_j+1=1,\ 3\leqslant j\leqslant m$$

Tendremos, pues,

$$\left.\begin{array}{rcl}\beta_1+1=2 &\implies& \beta_1=1\\ \beta_2+1=5 &\implies& \beta_2=4\\ \beta_j+1=1,\ 3\leqslant j\leqslant k &\implies& \beta_j=0,\ 3\leqslant j\leqslant k\end{array}\right\} \implies b=2\cdot 3^4$$

2 $\beta_1 + 1 = 5$. En este caso,

$$\left.\begin{array}{r}(\beta_1+1)(\beta_2+1)(\beta_3+1)\cdots(\beta_m+1)=10\\ \beta_1+1=5\end{array}\right\} \implies 5(\beta_2+1)(\beta_3+1)\cdots(\beta_m+1)=10$$
$$\implies (\beta_2+1)(\beta_3+1)\cdots(\beta_m+1)=2$$
$$\implies \beta_2+1\in D_2$$
$$\implies \beta_2+1\in\{1,2\}$$

lo cual es imposible, ya que $\beta_2 \geqslant 2 \implies \beta_2 + 1 \geqslant 3$.

3 $\beta_1 + 1 = 10$. En tal caso,

$$\left.\begin{array}{r}(\beta_1+1)(\beta_2+1)(\beta_3+1)\cdots(\beta_m+1)=10\\ \beta_1+1=10\end{array}\right\} \implies 10(\beta_2+1)(\beta_3+1)\cdots(\beta_k+1)=10$$
$$\implies (\beta_2+1)(\beta_3+1)\cdots(\beta_k+1)=1$$
$$\implies \beta_j+1=1,\ 2\leqslant j\leqslant k$$

lo cual es imposible, ya que $\beta_2 \geqslant 2 \implies \beta_2 + 1 \geqslant 3$.

Tenemos, pues, dos soluciones:

$$\left(a = 2^2\cdot 3^6 \text{ ó } a = 2^6\cdot 3^2\right) \text{ y } b = 2\cdot 3^4 \implies \left\{\begin{array}{l}1.\ a = 2^2\cdot 3^6 \text{ y } b = 2\cdot 3^4\\ \text{ó}\\ 2.\ a = 2^6\cdot 3^2 \text{ y } b = 2\cdot 3^4\end{array}\right.$$

Veamos cual de las dos es la que buscamos.

1. $a = 2^2\cdot 3^6$ y $b = 2\cdot 3^4$. En este caso,
$$\text{m.c.d.}(a,b) = 2\cdot 3^4 = 162$$
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 $b = 2\cdot 3^4$. En tal caso,
Al igual que en el caso anterior, por 6.4.3,
$$\text{m.c.d.}(a,b) = 2\cdot 3^2 = 18$$
que coincide con el dato proporcionado por el enunciado.

La solución correcta del ejercicio es, pues,

$$a = 576 \text{ y } b = 162$$

♦

Ejemplo 6.14

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 a tiene 8 divisores, $N_a = 8$, luego,

$$N_a = 8 \implies (\alpha_1+1)(\alpha_2+1) = 8$$
$$\implies \alpha_1+1 \text{ y } \alpha_2+1 \text{ son, ambos, divisores de 8}$$
$$\left[\ 8 = 2^3 \implies D_8 = \{1,2,4,8\}\ \right]$$
$$\implies \left\{\begin{array}{l}\alpha_1+1 \in \{1,2,4,8\}\\ \text{y}\\ \alpha_2+1 \in \{1,2,4,8\}\end{array}\right.$$

Representamos las posibles opciones en la tabla siguiente:

α_1+1	1	2	4	8
α_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,

$$\alpha_1+1=2 \implies \alpha_2+1=4$$

y

$$\alpha_2+1=8 \implies \alpha_1+1=1$$

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,

$$\left.\begin{array}{lll} \alpha_1+1=2 & \Longrightarrow & \alpha_1=1 \\ \text{y} & & \\ \alpha_2+1=4 & \Longrightarrow & \alpha_2=3 \end{array}\right\} \Longrightarrow \quad a=p_1p_2^3$$

2. $\alpha_1+1=4$ y $\alpha_2+1=2$. Entonces,

$$\left.\begin{array}{lll} \alpha_1+1=4 & \Longrightarrow & \alpha_1=3 \\ \text{y} & & \\ \alpha_2+1=1 & \Longrightarrow & \alpha_2=1 \end{array}\right\} \Longrightarrow \quad a=p_1^3p_2$$

Tenemos, pues, dos posibles soluciones. Estudiaremos cada una de ellas.

1. $a = p_1 p_2^3$.

   Según el enunciado, la suma de los divisores de a es 320. Pues bien, por 6.4.3,

   $$D_a = \left\{ p_1^\alpha p_2^\beta : 0 \leqslant \alpha \leqslant 1 \text{ y } 0 \leqslant \beta \leqslant 3 \right\}$$

   y podemos escribirlos todos utilizando el método que vimos en 6.4.4, es decir,

	1	p_1
$\times p_2$	p_2	$p_1 p_2$
$\times p_2^2$	p_2^2	$p_1 p_2^2$
$\times p_2^3$	p_2^3	$p_1 p_2^3$

   Calculamos ahora la suma de todos ellos, S_a. En efecto, sumando por columnas,

   $$\begin{aligned} S_a &= 1 + p_2 + p_2^2 + p_2^3 + p_1 + p_1 p_2 + p_1 p_2^2 + p_1 p_2^3 \\ &= (1 + p_1)\left(1 + p_2 + p_2^2 + p_2^3\right) \end{aligned}$$

   y, entonces,

   $$\begin{aligned} S_a = 320 &\implies (1 + p_1)\left(1 + p_2 + p_2^2 + p_2^3\right) = 320 \\ &\implies \begin{cases} 1 + p_1 \text{ es divisor de } 320 \\ \text{y} \\ 1 + p_2 + p_2^2 + p_2^3 \text{ es divisor de } 320 \end{cases} \end{aligned}$$

   y como $320 = 2^6 \cdot 5$, de nuevo por 6.4.3, tendremos que

   $$D_{320} = \left\{ 2^\gamma 3^\delta : 0 \leqslant \gamma \leqslant 6 \text{ y } 0 \leqslant \delta \leqslant 1 \right\}$$

   y por 6.4.4,

	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 $\Longrightarrow p_1 \geqslant 2 \Longrightarrow 1+p_1 \geqslant 3$, 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

$$1+p_2+p_2^2+p_2^3=40 \quad\Longrightarrow\quad p_2\left(1+p_2+p_2^2\right)=39$$

Entonces,

$$\left.\begin{array}{l} 39=3\cdot 13 \\ \text{y} \\ p_2\left(1+p_2+p_2^2\right)=39 \\ \text{y} \\ p_2 \text{ es primo} \end{array}\right\} \Longrightarrow \left\{\begin{array}{lll} p_2=3 & \Longrightarrow & 1+p_2+p_2^2=13 \\ \text{ó} & & \\ p_2=13 & \Longrightarrow & 1+p_2+p_2^2=183\neq 3 \end{array}\right.$$

y, consecuentemente, $p_2=3$.

Así pues, la primera solución es:

$$\left.\begin{array}{l} a=p_1p_2^3 \\ \text{y} \\ p_1=7 \\ \text{y} \\ p_2=3 \end{array}\right\} \Longrightarrow \quad a=7\cdot 3^3=189$$

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 6.4.3,

$$D_a=\left\{p_1^\alpha p_2^\beta : 0\leqslant\alpha\leqslant 3 \text{ y } 0\leqslant\beta\leqslant 1\right\}$$

y podemos escribirlos todos utilizando el método que vimos en 6.4.4, 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,

$$\begin{aligned} S_a=320 \quAD\Longrightarrow\quad & \left(1+p_1+p_1^2+p_1^3\right)(1+p_2)=320 \\ \Longrightarrow\quad & \left\{\begin{array}{l} 1+p_1+p_1^2+p_1^3 \text{ es divisor de } 320 \\ \text{y} \\ 1+p_2 \text{ es divisor de } 320 \end{array}\right. \end{aligned}$$

y como $320=2^6\cdot 5$, de nuevo por 6.4.3, 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 6.15

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 del número.

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,

$$\left.\begin{array}{rcl}(\alpha_1+1)(\alpha_3+1)(\alpha_2+2-\alpha_2-1) & = & 8\\ \text{y} & & \\ (\alpha_2+1)(\alpha_3+1)(\alpha_1+4-\alpha_1-1) & = & 18\end{array}\right\} \Longrightarrow \left\{\begin{array}{rcl}(\alpha_1+1)(\alpha_3+1) & = & 8\\ \text{y} & & \\ (\alpha_2+1)(\alpha_3+1) & = & 6\end{array}\right.$$

$$\Longrightarrow \left\{\begin{array}{l}\alpha_3+1 \text{ es divisor de } 8\\ \text{y}\\ \alpha_3+1 \text{ es divisor de } 6\end{array}\right.$$

$$\Longrightarrow \alpha_3+1 \,|\text{m.c.d.}(6,8)$$

$$\Longrightarrow \alpha_3+1\,|2$$

$$\Longrightarrow \left\{\begin{array}{l}\alpha_3+1=1\\ \text{ó}\\ \alpha_3+1=2\end{array}\right.$$

$$\Longrightarrow \left\{\begin{array}{l}\alpha_3=0.\text{ Imposible, ya que } \alpha_3\geqslant 1\\ \text{ó}\\ \alpha_3=1\end{array}\right.$$

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:

$$\left.\begin{array}{l}\alpha_1=3\\ \text{y}\\ \alpha_2=2\\ \text{y}\\ \alpha_3=1\\ \text{y}\\ a=2^{\alpha_1}5^{\alpha_2}7^{\alpha_3}\end{array}\right\} \Longrightarrow a=2^3 5^2 7 \Longrightarrow a=1400$$

Veamos ahora la suma de todos sus divisores. Por 6.4.6,

$$S=\frac{2^{3+1}-1}{2-1}\cdot\frac{5^{2+1}-1}{5-1}\cdot\frac{7^{1+1}-1}{7-1}=3720$$

♦

Ejemplo 6.16

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,

$$\frac{\alpha_1 + 1}{\alpha_1} = \frac{24}{18} \Longrightarrow \frac{\alpha_1 + 1}{\alpha_1} = \frac{4}{3} \Longrightarrow \alpha_1 = 3, \text{ ya que } \alpha_1 \text{ y } \alpha_1 + 1 \text{ son primos entre sí.}$$

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,

$$N_{3a} = 28 \Longrightarrow (3 + 1)(\alpha_2 + 1) \cdots (\alpha_k + 1)(1 + 1) = 28 \Longrightarrow 2(\alpha_2 + 1) \cdots (\alpha_k + 1) = 7 \Longrightarrow 2 \,|7$$

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,

$$\begin{aligned}
N_{3a} = 28 &\implies (3 + 1)(\alpha_2 + 2)(\alpha_3 + 1) \cdots (\alpha_k + 1) = 28 \\
&\implies (\alpha_2 + 2)(\alpha_3 + 1) \cdots (\alpha_k + 1) = 7 \\
&\implies \alpha_2 + 2 \in D_7 \\
&\implies \alpha_2 + 2 \in \{1, 7\} \\
&\quad \{\alpha_2 \geqslant 1 \implies \alpha_2 + 2 \geqslant 3\} \\
&\implies \alpha_2 + 2 = 7 \\
&\implies \alpha_2 = 5
\end{aligned}$$

Entonces,

$$\left.\begin{array}{r}(\alpha_2+2)(\alpha_3+1)\cdots(\alpha_k+1)=7\\ \alpha_2+2=7\end{array}\right\} \implies 7(\alpha_3+1)\cdots(\alpha_k+1)=7$$
$$\implies (\alpha_3+1)\cdots(\alpha_k+1)=1$$
$$\implies \alpha_i+1=1,\ 3\leqslant i\leqslant k$$
$$\implies \alpha_i=0,\ 3\leqslant i\leqslant k$$

Tendremos, pues,

$$\left.\begin{array}{l}\alpha_1=3\\ \alpha_2=5\\ \alpha_i=0,\ 3\leqslant i\leqslant k\end{array}\right\} \implies a=2^3 3^5 \implies a=1944$$

Veamos ahora cuales son sus divisores. Utilizando el método 6.4.4,

	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

Lección 7

Ecuaciones Diofánticas

7.1 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.

7.1.1 Definición

Una ecuación diofántica es una ecuación lineal con coeficientes enteros y que exige soluciones también enteras.

♦♦♦

7.2 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.

7.2.1 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.

"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

$$d = \text{m.c.d.}(a, b) \implies d \big| a \text{ y } d \big| b \implies d \big| ax_0 + by_0 \implies d \big| c$$

[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.

"Si". Recíprocamente, supongamos que $d = \text{m.c.d.}(a, b)$ es divisor de c. Entonces,

$$\begin{aligned} \text{m.c.d.}(a,b) = d &\implies \exists p, q \in \mathbb{Z} : pa + qb = d \qquad \{\text{Identidad de Bezout (5.3.5)}\} \\ &\iff \exists p, q \in \mathbb{Z} : p\frac{a}{d} + q\frac{b}{d}q = 1 \\ &\implies \exists p, q \in \mathbb{Z} : \frac{cp}{d}a + \frac{cq}{d}b = c \end{aligned}$$

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 7.1

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.

$$25 = 1 \cdot 525 + (-5)\,100$$

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

$$y_0 = \frac{50(-5)}{25} = -10$$

♦

7.2.2 Solución General

Sean a, b y c tres números enteros no nulos tales que d, 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. Entonces,

$$\text{m.c.d.}(a, b) = d \Longrightarrow \text{m.c.d.}\left(\frac{a}{d}, \frac{b}{d}\right) = 1$$

Además, d es divisor de c luego $\frac{c}{d}$ es entero y como $1 \left| \frac{c}{d} \right.$, por el teorema anterior, (7.2.1), la ecuación

$$\frac{a}{d}x + \frac{b}{d}y = \frac{c}{d}$$

tiene solución entera.

Pues bien, sea $x = x_1$ e $y = y_1$ cualquiera de esas soluciones. Entonces,

$$\frac{a}{d}x_1 + \frac{b}{d}y_1 = \frac{c}{d}$$

Por otra parte, como d, máximo común divisor de a y b, divide a c, el teorema anterior, (7.2.1), de nuevo, asegura la existencia de una solución $x = x_0$, $y = y_0$ de la ecuación $ax + by = c$. Entonces,

$$ax_0 + by_0 = c$$

de aquí que

$$\frac{a}{d}x_0 + \frac{b}{d}y_0 = \frac{c}{d}$$

Tendremos, pues,

$$\left.\begin{array}{l}\frac{a}{d}x_1+\frac{b}{d}y_1=\frac{c}{d}\\ \frac{a}{d}x_0+\frac{b}{d}y_0=\frac{c}{d}\end{array}\right\} \implies \frac{a}{d}(x_1-x_0)+\frac{b}{d}(y_1-y_0)=0$$

$$\implies \frac{a}{d}(x_1-x_0)=\frac{b}{d}(y_0-y_1)$$

$$\implies \frac{b}{d}\Big|\frac{a}{d}(x_1-x_0)$$

$$\left\{\text{m.c.d.}\left(\frac{b}{d},\frac{a}{d}\right)=1\right\}$$

$$\implies \frac{b}{d}\Big|(x_1-x_0) \qquad \{\text{Lema de Euclides (6.3.1)}\}$$

$$\implies \exists k\in\mathbb{Z}: x_1-x_0=k\frac{b}{d}$$

$$\implies x_1=x_0+k\frac{b}{d},\ \text{con } k\in\mathbb{Z}$$

Sustituyendo el valor de x_1-x_0 en $\frac{a}{d}(x_1-x_0)+\frac{b}{d}(y_1-y_0)=0$,

$$\left.\begin{array}{l}\frac{a}{d}(x_1-x_0)+\frac{b}{d}(y_1-y_0)=0\\ x_1-x_0=k\frac{b}{d}\end{array}\right\} \implies \frac{a}{d}k\frac{b}{d}+\frac{b}{d}(y_1-y_0)=0$$

$$\implies \frac{b}{d}(y_1-y_0)=-\frac{a}{d}k\frac{b}{d}$$

$$\implies y_1-y_0=-k\frac{a}{d}$$

$$\implies y_1=y_0-k\frac{a}{d}$$

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 7.1 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 la 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 7.2

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 7.2.1 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

$$22 = 1 \cdot 550 + (-8)\,66$$

luego,

$$22 = -8 \cdot 66 + 1 \cdot 550$$

es decir, $p = -8$ y $q = 1$, luego

$$x_0 = \frac{88(-8)}{22} = -32$$
$$y_0 = \frac{88 \cdot 1}{22} = 4$$

es una *solución particular* de la ecuación.

♢ Calculemos ahora la *solución general*.

Según lo visto en el teorema 7.2.2 si una solución particular de la misma es $x_0 = -32$ e $y_0 = 4$, entonces la solución general es:

$$x = -32 + k\frac{550}{22} = -32 + 25k$$

$$y = 4 - k\frac{66}{22} = 4 - 3k$$

siendo k cualquier número entero.

♦

Ejemplo 7.3

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 es 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

$$xy + 30x + 12y - xy = 1200$$

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.

$$6 = 1 \cdot 30 + (-2)\,12$$

luego entonces los coeficientes buscados son $p = 1$ y $q = -2$ 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 t ipo de leche.

Según lo visto hasta ahora, la cantidad de leche entera es

$$C_e = 200 + 2k, k \in \mathbb{Z}$$

Teniendo en cuenta que la cantidad de leche entera no puede ser cero y tampoco puede ser 12 ya que, en tal caso, no compraría leche desnatada,

$$\begin{aligned} 0 < C_e < 12 &\iff 0 < 200 + 2k < 12 \\ &\iff -200 < 2k < -188 \\ &\iff -100 < k < -94 \\ &\iff k \in \{-99, -98, -97, -96, -95\} \end{aligned}$$

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,

$$C_e = 200 + 2(-95) = 200 - 190 = 10$$
$$C_d = 12 - C_e = 2$$

o sea, se compraron 10 litros de leche entera y 2 litros de leche desnatada.

♦

Ejemplo 7.4

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,

$$84x + 990y = c \text{ tiene solución entera} \iff 6 \,|c \iff \exists q \in \mathbb{Z} : c = 6q$$

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

$$\left.\begin{array}{l} 6 = 1 \cdot 18 + (-1)\,12 \\ 12 = 66 - 3 \cdot 18 \end{array}\right\} \implies 6 = 1 \cdot 18 + (-1)\,(66 - 3 \cdot 18)$$

$$\implies 6 = -1 \cdot 66 + 4 \cdot 18$$

$$\left.\begin{array}{l} 6 = -1 \cdot 66 + 4 \cdot 18 \\ 18 = 84 - 1 \cdot 66 \end{array}\right\} \implies 6 = -1 \cdot 66 + 4\,(84 - 1 \cdot 66)$$

$$\implies 6 = 4 \cdot 84 + (-5)\,66$$

$$\left.\begin{array}{l} 6 = 4 \cdot 84 + (-5)\,66 \\ 66 = 990 - 11 \cdot 84 \end{array}\right\} \implies 6 = 4 \cdot 84 + (-5)\,(990 - 11 \cdot 84)$$

$$\implies 6 = -5 \cdot 990 + 59 \cdot 84$$

luego,

$$6 = 59 \cdot 84 + (-5)\,990$$

♢ 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 7.5

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.

Los enteros 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 7.6

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 está 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.

Calculamos el máximo común divisor de 3 y -4 utilizando el *Algoritmo de Euclides*,

	1	3
4	3	1
1	0	

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.*

Volviendo atrás el Algoritmo,

$$1=1\cdot 4+(-1)\,3$$

es decir,

$$1=-1\cdot 3+(-1)\,(-4)$$

luego $p=-1$ y $q=-1$ y

$$x_0=\frac{1(-1)}{1}=-1$$

$$y_0=\frac{1(-1)}{1}=-1$$

es una *solución particular* de la ecuación.

♢♢ *Solución general*

$$x=-1+\frac{-4}{1}k=-1-4k$$

$$y=1-\frac{3}{1}k=-1-3k$$

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,

$$100 < -12k - 1 < 110 \Longrightarrow \frac{101}{12} < -k < \frac{111}{12} \Longrightarrow \frac{-111}{12} < k < \frac{-101}{12} \Longrightarrow -9.25 < k < -8.42$$

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 7.7

Hallar el menor entero positivo que dividido por 4, 7 y 11 da resto 3, y que dividido por 13 da resto 1.

Solución.

Sea a el número buscado, entonces por el algoritmo de la división existen q_1, q_2 y q_3 tales que

$$\left.\begin{array}{l} a = 4q_1 + 3 \Longrightarrow a - 3 = 4q_1 \\ a = 7q_2 + 3 \Longrightarrow a - 3 = 7q_2 \\ a = 11q_3 + 3 \Longrightarrow a - 3 = 11q_3 \end{array}\right\} \Longrightarrow \exists x \in \mathbb{Z} : a - 3 = \text{m.c.m.}(4, 7, 11)x$$

$$\Longrightarrow a - 3 = 308x$$

$$\Longrightarrow a = 308x + 3$$

Por otro lado y también por el algoritmo de la división, existirá un entero y tal que

$$a = 13y + 1$$

por tanto,

$$\left.\begin{array}{l} a = 308x + 3 \\ a = 13y + 1 \end{array}\right\} \Longrightarrow 308x - 13y = -2$$

♢ 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.

$$\left.\begin{array}{l}1=1\cdot 9+(-2)\,4\\4=13-1\cdot 9\end{array}\right\}\implies 1=1\cdot 9+(-2)\,(13-1\cdot 9)$$

$$\implies 1=-2\cdot 13+3\cdot 9$$

$$\left.\begin{array}{l}1=-2\cdot 13+3\cdot 9\\9=308-23\cdot 13\end{array}\right\}\implies 1=-2\cdot 13+3\,(308-23\cdot 13)$$

$$\implies 1=3\cdot 308+(-71)\,13$$

luego $p=3$ y $q=71$ y

$$1=3\cdot 308+71\,(-13)$$

siendo,

$$x_0=\frac{(-2)3}{1}=-6$$

$$y_0=\frac{(-2)71}{1}=-142$$

una solución particular de la ecuación.

♢ *Solución general*

$$x=-6+k\frac{-13}{1}=-6-13k$$

$$y=-142-k\frac{308}{1}=-142-308k$$

donde k es cualquier número entero.

♢ Calculemos, finalmente, el número pedido.

$$x=-13k-6\Longrightarrow x=13(-k)-6+13-13\Longrightarrow x=13(-k-1)+7$$

Entonces,

$$\left.\begin{array}{l}x=13(-k-1)+7\\\text{y}\\a>0\end{array}\right\}\Longrightarrow -k-1\geqslant 0\Longrightarrow \exists q\in\mathbb{Z}_0^+:-k-1=q\Longrightarrow x=13q+9,\ q\in\mathbb{Z}_0^+$$

de aquí que,

$$\left.\begin{array}{l}a=308x+3\\\text{y}\\x=13q+7\end{array}\right\}\Longrightarrow a=308\,[13q+7]+3\Longrightarrow a=4004q+2159, q\geqslant 0$$

luego a es cualquier entero positivo que de resto 2159 al dividirlo por 4004. El menor de todos ellos se obtendrá cuando $q=0$. Entonces,

$$a=4004\cdot 0+2159=2159$$

y es el menor número entero que cumple las condiciones del enunciado.

♦

Ejemplo 7.8

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:

$$\left.\begin{array}{l} x+y+z=100 \\ 50x+1000y+5000z=100000 \end{array}\right\} \implies \left\{\begin{array}{l} z=100-x-y \\ 50x+1000y+5000z=100000 \end{array}\right.$$

$$\implies 50x+1000y+5000(100-x-y)=100000$$

$$\implies 4950x+4000y=400000$$

♢ Veamos si la ecuación propuesta tiene soluciones enteras.

Calculamos el máximo común divisor de 4950 y 4000 por el *Algoritmo de Euclides.*

	1	4	4	1	3
4950	4000	950	200	150	50
950	200	150	50	0	

luego,

$$\text{m.c.d.}\,(4950, 4000) = 50$$

y como 50 divide a 400000, término independiente de la ecuación, esta tiene soluciones enteras.

♢♢ Calculamos una *solución particular.*

Expresamos 50 como combinación lineal de 4950 y 4000 volviendo hacia atrás los cálculos en el *Algoritmo de Euclides.*

$$\left.\begin{array}{l} 50=1\cdot 200+(-1)\,150 \\ 150=950-4\cdot 200 \end{array}\right\} \implies 50=1\cdot 200+(-1)\,(950-4\cdot 200)$$

$$\implies 50=-1\cdot 950+5\cdot 200$$

$$\left.\begin{array}{l} 50=-1\cdot 950+5\cdot 200 \\ 200=4000-4\cdot 950 \end{array}\right\} \implies 50=-1\cdot 950+5\,(4000-4\cdot 950)$$

$$\implies 50=5\cdot 4000+(-21)\,950$$

$$\left.\begin{array}{l} 50=5\cdot 4000+(-21)\,950 \\ 950=4950-1\cdot 4000 \end{array}\right\} \implies 50=5\cdot 4000+(-21)\,(4950-1\cdot 4000)$$

$$\implies 50=-21\cdot 4950+26\cdot 4000$$

luego los *coeficientes de Bezout* serán

$$p=-21 \text{ y } q=26$$

por tanto,

$$x_0 = \frac{400000(-21)}{50} = -168000$$
$$y_0 = \frac{400000 \cdot 26}{50} = 208000$$

es una solución particular de la ecuación.

♢♢ La *solución general* será,

$$x = -168000 + k\frac{4000}{50} = 80k - 168000 \Longrightarrow x = 80(k - 2100)$$
$$y = 208000 - k\frac{4950}{50} = 208000 - 99k \Longrightarrow y = 99(-k + 2101) + 1$$

siendo k cualquier número entero.

♢ Veamos, finalmente, cuantos animales de cada clase compró.

Teniendo en cuenta que adquirió animales de las tres clases, tendremos

$$\left.\begin{array}{l} x > 0 \Longrightarrow 80(k - 2100) > 0 \Longrightarrow k - 2100 \geqslant 1 \Longrightarrow k \geqslant 2101 \\ y > 0 \Longrightarrow 99(-k + 2101) + 1 > 0 \Longrightarrow -k + 2101 \geqslant 0 \Longrightarrow k \leqslant 2101 \end{array}\right\} \Longrightarrow k = 2101$$

Así pues,

$$x = 80(2101 - 2100) = 80$$
$$y = 99(-2101 + 2101) + 1 = 1$$

y al ser

$$x + y + z = 100$$

será

$$z = 100 - 80 - 1 = 19$$

por tanto compró 80 pollos, 1 conejo y 19 terneros.

♦

Ejemplo 7.9

Demostrar, en $\mathbb{Z}_0^+$, que todos los números que dan resto 1 al dividirlos por 3 y resto 7 al dividirlos por 11 dan resto 7 al dividirlos por 33.

Solución.

Según el *Teorema de existencia y unicidad de cociente y resto* (5.2.1), los números que dan resto 1 al dividirlos por 3 son de la forma $3x + 1$ y los que dan resto 7 al dividirlos por 11, de la forma $11y + 7$, siendo x e y, enteros no negativos ya que estamos en $\mathbb{Z}_0^+$. Si $a \in \mathbb{Z}_0^+$, tendremos que probar, por tanto,

$$\left.\begin{array}{l} a = 3x + 1 \\ \text{y} \\ a = 11y + 7 \end{array}\right\} \Longrightarrow \exists q \in \mathbb{Z}_0^+ : a = 33q + 7$$

Pues bien,

$$\left.\begin{array}{l} a = 3x + 1 \\ \text{y} \\ a = 11y + 7 \end{array}\right\} \Longrightarrow 3x + 1 = 11y + 7 \Longrightarrow 3x - 11y = 6$$

♢ Veamos si esta ecuación tiene soluciones enteras.

Calculamos el máximo común divisor de 3 y -11 utilizando el algoritmo de Euclides.

	3	1	2
11	3	2	1
2	1	0	

luego,

$$\text{m.c.d.}(3,-11)=1$$

y como 1 divide a 6, término independiente de la ecuación, esta tiene soluciones enteras.

♢ Calculamos una solución particular.

Expresaremos 1 como combinación lineal de 3 y -11, obteniendo los coeficientes de la misma mediante la vuelta atrás del algoritmo de Euclides.

$$\left.\begin{array}{l} 1=1\cdot 3+(-1)\,2 \\ 2=11-3\cdot 3 \end{array}\right\} \implies 1=1\cdot 3+(-1)\,(11-3\cdot 3)$$

$$\implies 1=-1\cdot 11+4\cdot 3$$

es decir,

$$1=4\cdot 3+1(-11)$$

luego $p=4$ y $q=1$. Entonces,

$$x_0=\frac{6\cdot 4}{1}=24$$

e

$$y_0=\frac{6\cdot 1}{1}=6$$

♢ Obtenemos la solución general.

$$x=24-11k \implies x=11(-k)+11\cdot 2+2 \implies x=11(-k+2)+2$$

e

$$y=6-3k$$

siendo k un número entero.

♢ Probemos, finalmente, la conclusión.

Obsérvese que $x\in\mathbb{Z}_0^+$, pero si x fuera cero, entonces a sería 1, pero 1 no da resto 7 al dividirlo entre 11, luego $x>0$. Entonces,

$$\begin{aligned} x>0 &\implies 11(-k+2)+2>0 \\ &\implies -k+2\geqslant 0 \\ &\implies \exists q\in\mathbb{Z}_0^+ : q=-k+2 \\ &\implies \exists q\in\mathbb{Z}_0^+ : x=11q+2 \end{aligned}$$

y como $a=3x+1$,

$$\exists q\in\mathbb{Z}_0^+ : n=3(11q+2)+1 \implies \exists q\in\mathbb{Z}_0^+ : a=33q+7.$$

Que era lo que queríamos probar.

♦♦♦

Lección 8

Congruencias

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.

8.1 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.

8.1.1 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,

$$a \equiv b\ (mód\ m) \iff m \big| a-b$$

♦

Ejemplo 8.1

$80 \equiv 20$ (mód 15), ya que $15 \big| 60$

$-8 \equiv 16$ (mód 4), ya que $4 \big| -24$

$-5 \equiv -25$ (mód 10), ya que $10 \big| 20$

$12 \equiv -3$ (mód 5), ya que $5 \big| 15$

♦

Ejemplo 8.2

Encontrar cinco números enteros distintos, cada uno los cuales sea congruente con 13 módulo 11.

Solución.

Sea a cualquiera de los números buscados. Entonces,

$$\begin{aligned} a \equiv 13 \ (\text{mód } 11) &\iff 11 \mid a-13 \\ &\iff \exists q \in \mathbb{Z} : a-13 = 11q \\ &\iff \exists q \in \mathbb{Z} : a = 11q+13 \end{aligned}$$

Si ahora tomamos, por ejemplo, $q = -2,\ -1,\ 0,\ 1$ ó 2, tendremos los cinco números buscados:

$$\begin{aligned} a &= 11(-2)+13 = -9 \\ a &= 11(-1)+13 = 2 \\ a &= 11\cdot 0+13 = 13 \\ a &= 11\cdot 1+13 = 24 \\ a &= 11\cdot 2+13 = 35 \end{aligned}$$

♦

8.1.2 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,

$$\begin{aligned} a \in \mathbb{Z} \text{ y } m \in \mathbb{Z}^+ &\implies \exists q, r \in \mathbb{Z},\ \text{únicos} : a = mq + r,\ \text{siendo } 0 \leqslant r < m \ \{(5.2.1)\} \\ &\iff \exists q, r \in \mathbb{Z} : a - r = mq,\ \text{siendo } 0 \leqslant r < m \\ &\iff \exists r \in \mathbb{Z} : m \mid a-r,\ \text{siendo } 0 \leqslant r < m \\ &\iff \exists r \in \mathbb{Z} : a \equiv r \ (\text{mód } m),\ \text{siendo } 0 \leqslant r < m \\ &\iff \begin{cases} a \equiv 0 \ (\text{mód } m) \\ \text{ó} \\ a \equiv 1 \ (\text{mód } m) \\ \text{ó} \\ a \equiv 2 \ (\text{mód } m) \\ \vdots \\ \text{ó} \\ a \equiv m-1 \ (\text{mód } m) \end{cases} \end{aligned}$$

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, por (a), existirá $r \in \mathbb{Z},\ 0 \leqslant r < m$, único, tal que $a \equiv r \pmod{m}$. Entonces,

$$\begin{aligned} a \equiv r \pmod{m} &\iff m \mid a - r \ 0 \leqslant r < m && \{8.1.1\} \\ &\iff \exists q_1 \in \mathbb{Z} : a - r = mq_1,\ 0 \leqslant r < m && \{5.1.1\} \\ &\iff \exists q_1, r \in \mathbb{Z} : a = mq_1 + r,\ 0 \leqslant r < m \end{aligned}$$

luego por (5.2.1), el resto de dividir a entre m es r.
Veamos, ahora que si $a \equiv b \pmod{m}$, entonces b también da resto r al dividirlo entre m.
En efecto,

$$\begin{aligned} a \equiv b \pmod{m} &\iff m \mid a - b && \{8.1.1\} \\ &\iff \exists q_2 \in \mathbb{Z} : a - b = mq_2 && \{5.1.1\} \\ &\iff \exists q_2 \in \mathbb{Z} : b = a - mq_2 \\ &\implies \exists q_1, q_2, r \in \mathbb{Z} : b = mq_1 + r - mq_2,\ 0 \leqslant r < m && \{a = mq_1 + r\} \\ &\iff \exists q_1, q_2, r \in \mathbb{Z} : b = m(q_1 - q_2) + r,\ 0 \leqslant r < m \\ &\implies \exists q, r \in \mathbb{Z} : b = mq + r,\ 0 \leqslant r < m && \{q = q_1 - q_2\} \end{aligned}$$

por lo tanto, el *Teorema de existencia y unicidad de cociente y resto* (5.2.1) asegura que r también es el resto de dividir b entre 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,

$$\begin{aligned} &\left.\begin{array}{l} a = mq_1 + r \\ \text{y} \\ b = mq_2 + r \end{array}\right\} \implies a - b = m(q_1 - q_2) \\ &\implies \exists q \in \mathbb{Z} : a - b = mq \quad \{\text{Tomando } q = q_1 - q_2\} \\ &\iff m \mid a - b \\ &\iff a \equiv b \pmod{m} \qquad \{8.1.1\} \end{aligned}$$

♦

Ejemplo 8.3

Demuéstrese que todo número primo mayor o igual que 5 es congruente con 1 ó con 5, módulo 6.

Solución.

Sea p cualquier número entero. Probaremos que

$$\text{si } p \text{ es primo y } p \geqslant 5, \text{ entonces } p \equiv 1 \pmod{6} \text{ ó } p \equiv 5 \pmod{6}.$$

En efecto, supongamos que la proposición es falsa, es decir,

p es primo y $p \geqslant 5$ y, sin embargo, $p \not\equiv 1 \pmod 6$ y $p \not\equiv 5 \pmod 6$.

Entonces, por (a) del teorema anterior, (8.1.2), $p \equiv 0 \pmod m$ ó $p \equiv 2 \pmod m$ ó $p \equiv 3 \pmod m$ ó $p \equiv 4 \pmod m$.

Pues bien,

- Si $p \equiv 0 \pmod 6$, entonces $6 \mid p$ lo cual es imposible ya que p es primo.
- Si $p \equiv 2 \pmod 6$, entonces

$$\left.\begin{array}{l} 6 \mid p-2 \\ \text{y} \\ 2 \mid 6 \end{array}\right\} \Longrightarrow \left.\begin{array}{l} 2 \mid p-2 \\ \text{y} \\ 2 \mid 2 \end{array}\right\} \Longrightarrow 2 \mid p-2+2 \Longrightarrow 2 \mid p$$

  y esto contradice el que p sea primo.

- Si $p \equiv 3 \pmod 6$, entonces

$$\left.\begin{array}{l} 6 \mid p-3 \\ \text{y} \\ 3 \mid 6 \end{array}\right\} \Longrightarrow \left.\begin{array}{l} 3 \mid p-3 \\ \text{y} \\ 3 \mid 3 \end{array}\right\} \Longrightarrow 3 \mid p-3+3 \Longrightarrow 3 \mid p$$

  y esto contradice el que p sea primo.

- Si $p \equiv 4 \pmod 6$, entonces

$$\left.\begin{array}{l} 6 \mid p-4 \\ \text{y} \\ 2 \mid 6 \end{array}\right\} \Longrightarrow \left.\begin{array}{l} 2 \mid p-4 \\ \text{y} \\ 2 \mid 4 \end{array}\right\} \Longrightarrow 2 \mid p-4+4 \Longrightarrow 2 \mid p$$

  y, de nuevo, 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 8.4

Demuéstrese que si $d \mid m$ y $a \equiv b \pmod m$, entonces $a \equiv b \pmod d$.

Solución.

Por las propiedades de la divisibilidad, 5.1.2 (iv),

$$\left.\begin{array}{l} d \mid m \\ \text{y} \\ a \equiv b \pmod m \Longleftrightarrow m \mid a-b \end{array}\right\} \Longrightarrow d \mid a-b \Longleftrightarrow a \equiv b \pmod d$$

♦♦♦

8.2 Propiedades

Veremos a continuación algunas propiedades de las congruencias que son, con frecuencia, bastante útiles.

8.2.1 Teorema

Sean a, b, c y m cuatro enteros cualesquiera con $m > 0$. Se verifica:

(a) $a \equiv a \pmod{m}$.

(b) Si $a \equiv b \pmod{m}$, *entonces* $b \equiv a \pmod{m}$

(c) Si $a \equiv b \pmod{m}$ *y* $b \equiv c \pmod{m}$, *entonces* $a \equiv c \pmod{m}$

Demostración.

Utilizaremos las propiedades de la divisibilidad, (5.1.2).

(a) $a \equiv a \pmod{m}$
Teniendo en cuenta que $m \neq 0$,

$$m \mid 0 \iff m \mid a - a \iff a \equiv a \pmod{m}$$

(b) Si $a \equiv b \pmod{m}$, entonces $b \equiv a \pmod{m}$. En efecto,

$$a \equiv b \pmod{m} \iff m \mid a - b \iff m \mid (-1)(a - b) \implies m \mid b - a \iff b \equiv a \pmod{m}$$

(c) Si $a \equiv b \pmod{m}$ y $b \equiv c \pmod{m}$, entonces $a \equiv c \pmod{m}$. En efecto,

$$\left.\begin{array}{l} a \equiv b \pmod{m} \iff m \mid a - b \\ \text{y} \\ b \equiv c \pmod{m} \iff m \mid b - c \end{array}\right\} \implies m \mid (a - b) + (b - c) \implies m \mid a - c \implies a \equiv c \pmod{m}$$

♦

8.2.2 Teorema

Sean a, b, c, d, k y m, enteros con $k \neq 0$ y $m > 0$. Se verifica:

(a) si $a \equiv b \pmod{m}$ *y* $c \equiv d \pmod{m}$, *entonces* $a + c \equiv b + d \pmod{m}$.

(b) Si $a \equiv b \pmod{m}$ *y* $c \equiv d \pmod{m}$, *entonces* $ac \equiv bd \pmod{m}$.

(c) Si $a \equiv b \pmod{m}$, *entonces* $ka \equiv kb \pmod{m}$.

(d) Si $k \mid a$, $k \mid b$ *y* $a \equiv b \pmod{m}$, *entonces* $\frac{a}{k} \equiv \frac{b}{k} \pmod{\frac{m}{d}}$, *siendo* $d = m.c.d.(k, m)$.

Demostración.

Utilizaremos, al igual que en el teorema anterior, las propiedades de la divisibilidad (5.1.2).

(a) Si $a \equiv b \pmod{m}$ y $b \equiv c \pmod{m}$, entonces $a + c \equiv b + d \pmod{m}$ y $ac \equiv bd \pmod{m}$. En efecto,

$$\left.\begin{array}{l} a \equiv b \pmod{m} \iff m \big| a - b \\ \text{y} \\ c \equiv d \pmod{m} \iff m \big| c - d \end{array}\right\} \Longrightarrow m \big| (a - b) + (c - d) \Longrightarrow m \big| (a + c) - (b + d)$$

luego,

$$a + c \equiv b + d \pmod{m}.$$

(b) Si $a \equiv b \pmod{m}$ y $c \equiv d \pmod{m}$, entonces $ac \equiv bd \pmod{m}$. En efecto,

$$\left.\begin{array}{l} a \equiv b \pmod{m} \iff m \big| a - b \Longrightarrow m \big| ac - bc \\ \text{y} \\ c \equiv d \pmod{m} \iff m \big| c - d \Longrightarrow m \big| bc - bd \end{array}\right\} \Longrightarrow m \big| (ac - bc) + (bc - bd) \Longrightarrow m \big| ac - bd$$

por lo tanto,

$$ac \equiv bd \pmod{m}.$$

(c) Si $a \equiv b \pmod{m}$, entonces $ka \equiv kb \pmod{m}$. En efecto,

$$a \equiv b \pmod{m} \iff m \big| a - b \Longrightarrow m \big| k(a - b) \Longrightarrow m \big| ka - kb \iff ka \equiv kb \pmod{m}$$

(d) Si $k \big| a$, $k \big| b$ y $a \equiv b \pmod{m}$, entonces $\dfrac{a}{k} \equiv \dfrac{b}{k} \pmod{\dfrac{m}{d}}$, siendo $d = \text{m.c.d.}(k, m)$. En efecto, por 5.5.2,

$$\left.\begin{array}{rcl} \text{m.c.d.}(k, m) \cdot \text{m.c.m.}(k, m) & = & km \\ \text{m.c.d.}(k, m) & = & d \end{array}\right\} \Longrightarrow d \cdot \text{m.c.m.}(k, m) = km$$

$$\Longrightarrow \text{m.c.m.}(k, m) = \frac{km}{d}$$

Pues bien,

$$\left.\begin{array}{l} \left.\begin{array}{l} k \big| a \\ \text{y} \\ k \big| b \end{array}\right\} \Longrightarrow k \big| a - b \\ \text{y} \\ a \equiv b \pmod{m} \iff m \big| a - b \end{array}\right\} \Longrightarrow \text{m.c.m.}(k, m) \big| a - b$$

$$\Longrightarrow \frac{km}{d} \big| a - b$$

$$\Longrightarrow \exists q \in \mathbb{Z} : a - b = \frac{km}{d} q$$

$$\Longrightarrow \exists q \in \mathbb{Z} : \frac{a}{k} - \frac{b}{k} = \frac{mq}{d}$$

$$\Longrightarrow \frac{m}{d} \Big| \frac{a}{k} - \frac{b}{k}$$

$$\iff \frac{a}{k} \equiv \frac{b}{k} \pmod{\frac{m}{d}}$$

♦

Veamos ahora un corolario que generaliza algunos apartados del teorema anterior.

8.2.3 Corolario

Si $a_i \equiv b_i \pmod{m}$ para $1 \leqslant i \leqslant n$, entonces

(i) $\displaystyle\sum_{i=1}^{n} a_i \equiv \sum_{i=1}^{n} b_i \pmod{m}$

(ii) $\displaystyle\prod_{i=1}^{n} a_i \equiv \prod_{i=1}^{n} b_i \pmod{m}$

Demostración.

Procederemos, en ambos casos, por inducción.

(i) $\displaystyle\sum_{i=1}^{n} a_i \equiv \sum_{i=1}^{n} b_i \pmod{m}$

Paso básico. Veamos que es cierto para $n = 2$. En efecto, por el teorema anterior,

$$\left.\begin{array}{l} a_1 \equiv b_1 \pmod{m} \\ \text{y} \\ a_2 \equiv b_2 \pmod{m} \end{array}\right\} \Longrightarrow a_1 + a_2 \equiv b_1 + b_2 \pmod{m}$$

Paso inductivo. Supongamos que la proposición es cierta para $n = p$, es decir,

$$\text{si } a_i \equiv b_i \pmod{m},\ i = 1, 2, \ldots, p, \text{ entonces } \sum_{i=1}^{p} a_i \equiv \sum_{i=1}^{p} b_i \pmod{m}$$

Veamos que también se cumple para $n = p + 1$. En efecto, si

$$a_i \equiv b_i \pmod{m},\ i = 1, 2, \ldots, p, p+1$$

entonces por la hipótesis de inducción y por ser cierta la propiedad para $i = 2$, tendremos que

$$\left.\begin{array}{l} \displaystyle\sum_{i=1}^{p} a_i \equiv \sum_{i=1}^{p} b_i \pmod{m} \\ \text{y} \\ a_{p+1} \equiv b_{p+1} \pmod{m} \end{array}\right\} \Longrightarrow \sum_{i=1}^{p} a_i + a_{p+1} \equiv \sum_{i=1}^{p} b_i + b_{p+1} \pmod{m} \Longrightarrow \sum_{i=1}^{p+1} a_i \equiv \sum_{i=1}^{p+1} b_i \pmod{m}$$

y, consecuentemente, la proposición será cierta para todo n.

(ii) $\displaystyle\prod_{i=1}^{n} a_i \equiv \prod_{i=1}^{n} b_i \pmod{m}$

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 8.5

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 8.1.2 a es congruente módulo 3 con 0, 1 ó 2. Pues bien,

$$\begin{aligned}
a \equiv 0 \ (\text{mód } 3) &\implies a^2 \equiv 0 \ (\text{mód } 3) \ \{(8.2.2\ (b))\} \\
&\iff 3 \big| a^2 \\
&\iff a^2 \text{ es divisible por } 3 \\
&\text{ó} \\
a \equiv 1 \ (\text{mód } 3) &\implies a^2 \equiv 1 \ (\text{mód } 3) \ \{(8.2.2\ (b))\} \\
&\text{ó} \\
a \equiv 2 \ (\text{mód } 3) &\implies a^2 \equiv 4 \ (\text{mód } 3) \ \{(8.2.2\ (b))\} \\
&\iff \left\{ \begin{array}{l} a^2 \equiv 4 \ (\text{mód } 3) \\ \text{y} \\ 4 \equiv 1 \ (\text{mód } 3) \end{array} \right. \\
&\iff a^2 \equiv 1 \ (\text{mód } 3) \ \{8.2.1\ (c)\}
\end{aligned}$$

luego a^2 es divisible por 3 o es congruente con 1 módulo 3.

♦

Ejemplo 8.6

Demostrar:

(a) Si $a \equiv b \ (\text{mód } m)$, entonces $\text{m.c.d.}(a, m) = \text{m.c.d.}(b, m)$.

(b) Si $a \equiv b \ (\text{mód } m)$, entonces $a^n \equiv b^n \ (\text{mód } m)$ para cualquier entero positivo n.

(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 $d \big| a$ y $d \big| m$, entonces $d \big| b$.

Solución.

(a) Si $a \equiv b \ (\text{mód } m)$, entonces $\text{m.c.d.}(a, m) = \text{m.c.d.}(b, m)$. En efecto,

$$a \equiv b \ (\text{mód } m) \iff m \big| a - b$$

Pues bien, sea $d_1 = \text{m.c.d}(a, m)$ y $d_2 = \text{m.c.d}(b, m)$. Entonces,

$$d_1 = \text{m.c.d}(a, m) \implies \left\{ \begin{array}{l} d_1 \big| a \\ \text{y} \\ d_1 \big| m \implies d_1 \big| m \text{ y } m \big| a - b \implies d_1 \big| a - b \end{array} \right\} \implies d_1 \big| a - (a - b) \implies d_1 \big| b$$

Es decir, d_1 divide a b y a m, por tanto dividirá al máximo común divisor de ambos, luego

$$d_1 \big| d_2$$

Análogamente,

$$d_2 = \text{m.c.d}(b,m) \Longrightarrow \left\{ \begin{array}{l} d_2 \big| b \\ \text{y} \\ d_2 \big| m \Longrightarrow d_2 \big| m \text{ y } m \big| a-b \Longrightarrow d_2 \big| a-b \end{array} \right\} \Longrightarrow d_2 \big| b+(a-b) \Longrightarrow d_2 \big| a$$

O sea, d_2 divide a a y a m, luego dividirá al máximo común divisor de ambos, de aquí que

$$d_2 \big| d_1$$

Finalmente, como d_1 y d_2 son enteros positivos, por (iii) en 5.1.2, d_1 será igual a d_2, es decir,

$$\text{m.c.d.}(a,m) = \text{m.c.d.}(b,m)$$

(b) Si $a \equiv b \pmod{m}$, entonces $a^n \equiv b^n \pmod{m}$ 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 $a+b \equiv c \pmod{m}$, entonces $a \equiv c-b \pmod{m}$.
En efecto,

$$a+b \equiv c \pmod{m} \Longleftrightarrow m \big| a+b-c \Longleftrightarrow m \big| a-(c-b) \Longleftrightarrow a \equiv c-b \pmod{m}$$

(d) Si $a \equiv b \pmod{m}$ y $d \big| a$ y $d \big| m$, entonces $d \big| b$.
En efecto,

$$a \equiv b \pmod{m} \Longleftrightarrow m \big| a-b$$

y como $d \big| m$, por (iv) en 5.1.2, $d \big| a-b$. Así pues,

$$\left\{ \begin{array}{l} d \big| a \\ \text{y} \\ d \big| a-b \end{array} \right\} \Longrightarrow d \big| a-(a-b) \Longrightarrow d \big| b$$

♦

Ejemplo 8.7

Demostrar que el resto de dividir 20^{4572} entre 7 es 1.

Solución.

En efecto,

$$\left\{ \begin{array}{l} 20 \equiv 6 \pmod{7} \\ 6 \equiv -1 \pmod{7} \end{array} \right\} \Longrightarrow 20 \equiv -1 \pmod{7}$$

$$\Longrightarrow 20^{4572} \equiv (-1)^{4572} \pmod{7}$$

$$\Longrightarrow 20^{4572} \equiv 1 \pmod{7}$$

$$\Longrightarrow 7 \big| 20^{4572} - 1$$

$$\Longrightarrow \exists q \in \mathbb{Z} : 20^{4572} - 1 = 7q$$

$$\Longrightarrow \exists q \in \mathbb{Z} : 20^{4572} = 7q + 1$$

$$\Longrightarrow \text{El resto de dividir } 20^{4572} \text{ por 7 es 1}$$

♦

Ejemplo 8.8

Demostrar que para cualquier entero no negativo n, el número $3 \cdot 5^{2n+1} + 2^{3n+1}$ es divisible por 17.

Solución.

Observemos lo siguiente:

$$\left.\begin{array}{l} 3 \cdot 5^{2n+1} = 3 \cdot (5^2)^n \cdot 5 = 15 \cdot 25^n \\ 2^{3n+1} = (2^3)^n \cdot 2 = 2 \cdot 8^n \end{array}\right\} \implies 3 \cdot 5^{2n+1} + 2^{3n+1} = 15 \cdot 25^n + 2 \cdot 8^n$$

Por otra parte,

$$17 \equiv 0 \ (\text{mód } 17) \implies 15 + 2 \equiv 0 \ (\text{mód } 17) \implies 15 \equiv -2 \ (\text{mód } 17)$$

luego,

$$\left.\begin{array}{l} 15 \equiv -2 \ (\text{mód } 17) \\ \text{y} \\ 25 \equiv 8 \ (\text{mód } 17) \implies 25^n \equiv 8^n \ (\text{mód } 17) \end{array}\right\} \implies 15 \cdot 25^n \equiv -2 \cdot 8^n \ (\text{mód } 17)$$

entonces,

$$15 \cdot 25^n + 2 \cdot 8^n \equiv 0 \ (\text{mód } 17)$$

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 8.9

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,

$$\begin{aligned} 1461 = 730 \cdot 2 + 1 &\implies 1461 \equiv 1 (\text{mód } 730) \\ &\implies 1461^{2n} \equiv 1^{2n} \ (\text{mód } 730) \\ &\implies 1461^{2n} \equiv 1 \ (\text{mód } 730) \\ &\implies 1461^{2n} \cdot 3 \equiv 3 \ (\text{mód } 730) \\ &\iff 3^{2n+1} \cdot 487^{2n} \equiv 3 \ (\text{mód } 730) \end{aligned}$$

de aquí que,

$$9^{6n+1} + 3^{2n+1} \cdot 487^{2n} \equiv 12 \pmod{730}$$

es decir,

$$9^{6n+1} + 3^{2n+1} \cdot 487^{2n} - 10 \equiv 2 \pmod{730}$$

y, por tanto,

$$\begin{aligned} 730 \left| 9^{6n+1} + 3^{2n+1} \cdot 487^{2n} - 10 - 2 \right. &\iff \exists q \in \mathbb{Z} : 9^{6n+1} + 3^{2n+1} \cdot 487^{2n} - 10 - 2 = 730q \\ &\implies \exists q \in \mathbb{Z} : 9^{6n+1} + 3^{2n+1} \cdot 487^{2n} - 10 = 730q + 2 \end{aligned}$$

y, consecuentemente, el resto de dividir el número dado entre 730 es 2.

♦

Ejemplo 8.10

Demostrar que para cualquier entero no negativo n, el número $10^n(9n-1)+1$ es divisible por 9.

Solución.

En efecto,

$$10 = 9 \cdot 1 + 1 \implies 10 \equiv 1 \pmod{9} \implies 10^n \equiv 1 \pmod{9}$$

y

$$9n \equiv 0 \pmod{9} \implies \left\{ \begin{array}{l} 9n \equiv 0 \pmod{9} \\ \text{and} \\ -1 \equiv -1 \pmod{9} \end{array} \right\} \implies 9n - 1 \equiv -1 \pmod{9}$$

entonces,

$$\left. \begin{array}{l} 10^n \equiv 1 \pmod{9} \\ \text{and} \\ 9n - 1 \equiv -1 \pmod{9} \end{array} \right\} \implies 10^n(9n-1) \equiv -1 \pmod{9}$$

por lo tanto,

$$\left. \begin{array}{l} 10^n(9n-1) \equiv -1 \pmod{9} \\ \text{and} \\ 1 \equiv 1 \pmod{9} \end{array} \right\} \implies 10^n(9n-1) + 1 \equiv 0 \pmod{9}$$

y, consecuentemente, el resto de dividir el número dado por 9 es cero.

♦♦♦

8.3 Congruencias Lineales

A continuación, proponemos congruencias del tipo $ax \equiv b \pmod{m}$ donde a y b son enteros y x es la indeterminada. Resolver estas congruencias significa obtener todos los números en $\mathbb{Z}$ que cuando se escriben en lugar de la indeterminada, la verifican.

Veremos que encontrar las soluciones de este tipo de congruencias es equivalente a la resolución de una Ecuación Diofántica.

8.3.1 Teorema

Sean a y b dos enteros cualesquiera y m un entero positivo. La congruencia lineal $ax \equiv b \pmod{m}$ tiene solución en $\mathbb{Z}$ si, y solo si el máximo común divisor de a y m divide a b. El número de soluciones no congruentes módulo m es igual al m.c.d.(a, m).

Demostración.

En efecto, sean a y b enteros cualesquiera. Entonces,

$$\begin{aligned}
ax \equiv b \pmod{m} \text{ tiene solución en } \mathbb{Z} &\iff \exists x \in \mathbb{Z} : ax \equiv b \pmod{m} \\
&\iff \exists x \in \mathbb{Z} : m \Big| ax - b \\
&\iff \exists x \in \mathbb{Z} : m \Big| b - ax \\
&\iff \exists x, y \in \mathbb{Z} : b - ax = my \\
&\iff \exists x, y \in \mathbb{Z} : ax + my = b \\
&\iff \text{La ecuación Diofántica } ax + my = b \text{ tiene solución} \\
&\iff \text{m.c.d.}(a, m) \Big| b \ \{7.2.1\}
\end{aligned}$$

Sea $d = \text{m.c.d.}(a, m)$. Si $d \Big| b$, entonces la Ecuación Diofántica $ax + my = b$ tiene una solución particular, x_0, y por (7.2.2) su solución general viene dada por la expresión,

$$x = x_0 + k\frac{m}{d}, \text{ con } k \in \mathbb{Z}$$

Veremos que para cada $0 \leqslant k < d$ puede encontrarse una solución no congruente módulo m, es decir no hay dos soluciones que sean congruentes módulo m. En efecto, supongamos que lo contrario es cierto, esto es, existen

$$x_1 = x_0 + k_1\frac{m}{d}$$

y

$$x_2 = x_0 + k_2\frac{m}{d}$$

con $0 \leqslant k_1, k_2 < d$ y $x_1 \equiv x_2 \pmod{m}$. Entonces,

$$\left.\begin{array}{l} 0 \leqslant k_1 < d \\ -d < -k_2 \leqslant 0 \end{array}\right\} \implies -d < k_1 - k_2 < d \implies |k_1 - k_2| < d$$

y

$$\begin{aligned}
x_1 \equiv x_2 \pmod{m} &\implies x_0 + k_1\frac{m}{d} \equiv x_0 + k_2\frac{m}{d} \pmod{m} \\
&\implies k_1\frac{m}{d} \equiv k_2\frac{m}{d} \pmod{m} \\
&\implies m \Big| (k_1 - k_2)\frac{m}{d} \\
&\implies (k_1 - k_2)\frac{m}{d} = mq, \ q \in \mathbb{Z} \\
&\implies k_1 - k_2 = dq \\
&\implies |k_1 - k_2| = d\,|q| \\
&\implies d \Big| |k_1 - k_2|
\end{aligned}$$

pero esto es imposible porque $|k_1 - k_2| < d$ y un número no puede tener divisores mayores que él.

A continuación, veremos que ocurre cuando $k \geqslant d$.

Por el *Teorema de existencia y unicidad de cociente y resto*, (5.2.1), existen q y r tales que $k = dq + r$, con $0 \leqslant r < d$. Si x_1 y x_2 son, respectivamente, las soluciones de $ax \equiv b \pmod{m}$ para k y r, tendremos,

$$\left.\begin{array}{l} x_1 = x_0 + k\dfrac{m}{d} \\ \text{y} \\ x_2 = x_0 + r\dfrac{m}{d} \end{array}\right\} \implies x_1 - x_2 = x_0 + k\frac{m}{d} - x_0 + r\frac{m}{d}$$

$$\implies x_1 - x_2 = (k - r)\frac{m}{d}$$

$$\implies x_1 - x_2 = dq\frac{m}{d}$$

$$\implies x_1 - x_2 = mq$$

$$\implies x_1 \equiv x_2 \pmod{m}$$

Por lo tanto, para cada solución de la congruencia existe una solución módulo m con ella,

$$x = x_0 + k\frac{m}{d}, \text{con } 0 \leqslant k < d$$

es decir el número de soluciones no congruentes módulo m es, exactamente, d.

♦

8.3.2 Corolario

Sea a cualquier entero y $m > 1$. La congruencia lineal $ax \equiv 1 \pmod{m}$ tiene solución si, y solo si a y m son primos entre sí. Existe una única solución no congruente módulo m.

Demostración.

Efectivamente, si a y m son primos entre sí, entonces m.c.d.$(a, m) = 1$ y por el teorema anterior, la congruencia lineal $ax \equiv 1 \pmod{m}$ tiene solución.

Además, si $d = $ m.c.d.(a, m) y x_0 es una solución particular de la Ecuación Diofántica $ax + my = 1$,

$$\left.\begin{array}{l} x = x_0 + k\dfrac{m}{d} \\ \text{y} \\ d = 1 \\ \text{y} \\ 0 \leqslant k < d \end{array}\right\} \implies \left.\begin{array}{l} x = x_0 + km \\ \text{y} \\ k = 0 \end{array}\right\} \implies x = x_0$$

A esta solución se le llama el *inverso de a módulo m*.

♦

Ejemplo 8.11

Resolver las siguientes congruencias lineales.

(a) $5x \equiv 8 \pmod{6}$.

(b) $15x \equiv 6 \pmod{21}$.

(c) $3x \equiv 27 \pmod{6}$.

(d) $3x \equiv 8 \pmod 6$.

(e) $12x \equiv 45 \pmod 3$

Solución.

(a) $5x \equiv 8 \pmod 6$

Por el teorema previo, (8.3.1),

$$ax \equiv b \pmod m \text{ tiene solución en } \mathbb{Z} \Longleftrightarrow \text{m.c.d.}(a,m) \Big| b$$

y, en tal caso, si $d = \text{m.c.d.}(a,m)$, las soluciones no congruentes módulo m de $ax \equiv b \pmod m$ son

$$x = x_0 + k\frac{m}{d}, \text{ con } 0 \leqslant k < d$$

siendo x_0 la solución particular de la Ecuación Diofántica $ax + my = b$,

$$x_0 = \frac{bp}{d}$$

y p el Coeficiente de Bezout (5.3.5).

Pues bien, en nuestro caso,

◊ m.c.d.$(5,6)$.

Calculamos el máximo común divisor de 5 y 6 mediante el Algoritmo de Euclides,

	1	5
6	5	1
1	0	

es decir, m.c.d.$(5,6) = 1$ y como 1 divide a 8, nuestra congruencia lineal, $5x \equiv 8 \pmod 6$ tiene solución en $\mathbb{Z}$.

◊ Coeficiente de Bezout.

Por 5.3.5,

$$1 = \text{m.c.d.}(5,6) \Longrightarrow \exists p, q \in \mathbb{Z} : 1 = 5p + 6q$$

y podemos obtener p y q volviendo atrás el Algoritmo de Euclides,

$$1 = 1 \cdot 6 + (-1)\,5$$

luego,

$$1 = (-1)\,5 + 1 \cdot 6$$

es decir $p = -1$.

◊ Solución particular de $5x + 6y = 8$.

$$x_0 = \frac{8(-1)}{1} \Longrightarrow x_0 = -8$$

◊ Solución general de $5x + 6y = 8$.

$$x = x_0 + k\frac{m}{d} \Longrightarrow x = -8 + 6k,\ k \in \mathbb{Z}$$

◊ Solución $5x \equiv 8$ (mód 6).

$$\left.\begin{array}{l} x = -8 + 6k \\ \text{y} \\ 0 \leqslant k < 1 \end{array}\right\} \Longrightarrow x = -8$$

◊ Veamos, finalmente, si la solución encontrada es correcta. Efectivamente,

$$5(-8) = -40 \equiv 8 \text{ (mód 6)}$$

(b) $15x \equiv 6$ (mód 21)

Por el teorema previo, (8.3.1),

$$ax \equiv b \text{ (mód } m) \text{ tiene solución en } \mathbb{Z} \Longleftrightarrow \text{m.c.d.}(a, m) \Big| b$$

y, en tal caso, si $d = \text{m.c.d.}(a, m)$, las soluciones no congruentes módulo m de $ax \equiv b$ (mód m) son

$$x = x_0 + k\frac{m}{d}, \text{ con } 0 \leqslant k < d$$

siendo x_0 la solución particular de la Ecuación Diofántica $ax + my = b$,

$$x_0 = \frac{bp}{d}$$

y p el Coeficiente de Bezout (5.3.5).

Pues bien, en nuestro caso,

◊ m.c.d.$(15, 21)$.

Calculamos el máximo común divisor de 15 y 21 mediante el Algoritmo de Euclides,

	1	2	2
21	15	6	3
6	3	0	

es decir, m.c.d.$(15, 21) = 3$ y como 3 divide a 21, nuestra congruencia lineal, $15x \equiv 6$ (mód 21) tiene solución en $\mathbb{Z}$.

◊ Coeficiente de Bezout.

Por 5.3.5,

$$3 = \text{m.c.d.}(15, 21) \Longrightarrow \exists p, q \in \mathbb{Z} : 3 = 15p + 21q$$

y podemos obtener p y q volviendo atrás el Algoritmo de Euclides,

$$\left.\begin{array}{l} 3 = 1 \cdot 15 + (-2)\, 6 \\ 6 = 21 - 1 \cdot 15 \end{array}\right\} \Longrightarrow 3 = 1 \cdot 15 + (-2)\,(21 - 1 \cdot 15)$$

$$\Longrightarrow 3 = -2 \cdot 21 + 3 \cdot 15$$

es decir,

$$3 = 3 \cdot 15 + (-2)\, 21$$

luego $p = 3$.

◊ Solución particular de $15x + 21y = 6$.

$$x_0 = \frac{6 \cdot 3}{3} \Longrightarrow x_0 = 6$$

◊ Solución general de $15x + 21y = 6$.

$$x = x_0 + k\frac{m}{d} \Longrightarrow x = 6 + 7k,\ k \in \mathbb{Z}$$

◊ Solución de $15x \equiv 6$ (mód 21).

$$\left.\begin{array}{l} x = 6 + 7k \\ \text{y} \\ 0 \leqslant k < 3 \end{array}\right\} \Longrightarrow \left.\begin{array}{l} x = 6 \\ x = 13 \\ x = 20 \end{array}\right\}$$

◊ Veamos, finalmente, si las soluciones encontradas son correctas. En efecto,

$$15 \cdot 6 = 90 \equiv 6 \text{ (mód 21)}$$
$$15 \cdot 13 = 195 \equiv 6 \text{ (mód 21)}$$
$$15 \cdot 20 = 300 \equiv 6 \text{ (mód 21)}$$

(c) $3x \equiv 27$ (mód 6)

Por el teorema previo, (8.3.1),

$$ax \equiv b \text{ (mód } m) \text{ tiene solución en } \mathbb{Z} \Longleftrightarrow \text{m.c.d.}(a, m) \Big| b$$

y, en tal caso, si $d = \text{m.c.d.}(a, m)$, las soluciones no congruentes módulo m de $ax \equiv b$ (mód m) son

$$x = x_0 + k\frac{m}{d},\ \text{con } 0 \leqslant k < d$$

siendo x_0 la solución particular de la Ecuación Diofántica $ax + my = b$,

$$x_0 = \frac{bp}{d}$$

y p el Coeficiente de Bezout (5.3.5).

Pues bien, en nuestro caso,

◊ m.c.d.$(3, 6)$.

	2
6	3
0	

es decir, m.c.d.$(3, 6) = 3$ y como 3 divide a 27, nuestra congruencia lineal, $3x \equiv 27$ (mód 6) tiene solución en $\mathbb{Z}$.

◊ Coeficiente de Bezout. Por 5.3.5,

$$3 = \text{m.c.d.}(3, 6) \Longrightarrow \exists p, q \in \mathbb{Z} : 3 = 3p + 6q$$

y podemos obtener p y q volviendo atrás el Algoritmo de Euclides,

$$3 = 1 \cdot 6 + (-1)\, 3$$

es decir,

$$3 = -1 \cdot 3 + 1 \cdot 6$$

luego $p = -1$.

◊ Solución particular de $3x + 6y = 27$.

$$x_0 = \frac{27(-1)}{3} \Longrightarrow x_0 = -9$$

◊ Solución general de $3x + 6y = 27$.

$$x = x_0 + k\frac{m}{d} \Longrightarrow x = -9 + 2k,\ k \in \mathbb{Z}$$

◊ Solución de $3x \equiv 27$ (mód 6).

$$\left.\begin{array}{l} x = -9 + 2k \\ \text{y} \\ 0 \leqslant k < 3 \end{array}\right\} \Longrightarrow \left.\begin{array}{l} x = -9 \\ x = -7 \\ x = -5 \end{array}\right\}$$

◊ Veamos, finalmente, si las soluciones encontradas son correctas. Efectivamente,

$$3(-9) = -27 \equiv 27 \text{ (mód 6)}$$
$$3(-7) = -21 \equiv 27 \text{ (mód 6)}$$
$$3(-5) = -15 \equiv 27 \text{ (mód 6)}$$

(d) $3x \equiv 8$ (mód 6)

Por el teorema previo, (8.3.1),

$$ax \equiv b \text{ (mód } m) \text{ tiene solución en } \mathbb{Z} \Longleftrightarrow \text{m.c.d.}(a, m) \Big| b$$

y, en tal caso, si $d = \text{m.c.d.}(a, m)$, las soluciones no congruentes módulo m de $ax \equiv b$ (mód m) son

$$x = x_0 + k\frac{m}{d},\ \text{con } 0 \leqslant k < d$$

siendo x_0 la solución particular de la Ecuación Diofántica $ax + my = b$,

$$x_0 = \frac{bp}{d}$$

y p el Coeficiente de Bezout (5.3.5).

Pues bien, en nuestro caso,

◊ m.c.d.$(3, 6)$.

$$\text{m.c.d.}(3, 6) = \text{m.c.d.}(6, 3) = \text{m.c.d.}(3, 0) = 3$$

es decir, m.c.d.$(6, 3) = 3$ y como 3 no divide a 8, nuestra congruencia lineal, $3x \equiv 8$ (mód 6) no tiene solución en $\mathbb{Z}$.

(e) $12x \equiv 45$ (mód 3).

Por el teorema previo, (8.3.1),

$$ax \equiv b \text{ (mód } m) \text{ tiene solución en } \mathbb{Z} \Longleftrightarrow \text{m.c.d.}(a, m) \Big| b$$

y, en tal caso, si $d = \text{m.c.d.}(a, m)$, las soluciones no congruentes módulo m de $ax \equiv b$ (mód m) son

$$x = x_0 + k\frac{m}{d},\ \text{con } 0 \leqslant k < d$$

siendo x_0 la solución particular de la Ecuación Diofántica $ax + my = b$,

$$x_0 = \frac{bp}{d}$$

y p el Coeficiente de Bezout (5.3.5).

Pues bien, en nuestro caso,

◊ m.c.d.$(12, 3)$.

		4
12		3
0		

es decir, m.c.d.$(12, 3) = 3$ y como 3 divide a 45, nuestra congruencia lineal, $12x \equiv 45 \pmod 3$ tiene solución en $\mathbb{Z}$.

◊ Coeficiente de Bezout. Por 5.3.5,

$$3 = \text{m.c.d.}(12, 3) \Longrightarrow \exists p, q \in \mathbb{Z} : 3 = 12p + 3q$$

y volviendo atrás el algoritmo de Euclides

$$3 = 1 \cdot 12 + (-3)\, 3$$

luego $p = 1$.

◊ Solución particular de $12x + 3y = 45$.

$$x_0 = \frac{45 \cdot 1}{3} \Longrightarrow x_0 = 15$$

◊ Solución general de $12x + 3y = 45$.

$$x = x_0 + k\frac{m}{d} \Longrightarrow x = 15 + k,\ k \in \mathbb{Z}$$

◊ Solución de $12x \equiv 45 \pmod 3$.

$$\left.\begin{array}{l} x = 15 + k \\ \text{y} \\ 0 \leqslant k < 3 \end{array}\right\} \Longrightarrow \left.\begin{array}{l} x = 15 \\ x = 16 \\ x = 17 \end{array}\right\}$$

◊ Veamos, finalmente, si las soluciones encontradas son correctas. En efecto,

$$12 \cdot 15 = 180 \equiv 45 \pmod 3$$
$$12 \cdot 16 = 192 \equiv 45 \pmod 3$$
$$12 \cdot 17 = 204 \equiv 45 \pmod 3$$

♦

En el siguiente punto, estudiaremos el *Teorema Chino del Resto*, un resultado que aparece en los más importantes manuscritos Chinos de la antigüedad, así como en los trabajos de Sun Tsu en el siglo primero. También, y al mismo tiempo, es conocido por el Neopitagórico Nicómaco.

8.3.3 Teorema Chino del Resto

Si $m_1, m_2, \cdots, m_n$ son enteros mayores que 1, primos entre sí dos a dos, y $a_1, a_2, \ldots, a_m$ enteros cualesquiera, entonces el sistema de congruencias lineales,

$$x \equiv a_1 \ (\textit{mód}\ m_1)$$
$$x \equiv a_2 \ (\textit{mód}\ m_2)$$
$$\vdots$$
$$x \equiv a_n \ (\textit{mód}\ m_n)$$

tiene una solución única módulo $m_1 \cdot m_2 \cdots m_n$.

Demostración.

Existencia. Probemos que existe una solución describiendo una forma de construirla.

Bien, sea $m = m_1 \cdot m_2 \cdots m_n$ y M_i el producto de todos los módulos excepto m_i, esto es,

$$M_i = \frac{m}{m_i}$$

Veamos que m.c.d.$(M_i, m_i) = 1$. En efecto, aplicando repetidamente el ejercicio 5.12,

$$\left.\begin{array}{l} \text{m.c.d.}(m_2, m_1) = 1 \\ \text{y} \\ \text{m.c.d.}(m_3, m_1) = 1 \end{array}\right\} \Longrightarrow \text{m.c.d.}(m_2 m_3, m_1) = 1$$

y,

$$\left.\begin{array}{l} \text{m.c.d.}(m_2 m_3, m_1) = 1 \\ \text{y} \\ \text{m.c.d.}(m_4, m_1) = 1 \end{array}\right\} \Longrightarrow \text{m.c.d.}(m_2 m_3 m_4, m_1) = 1$$

así sucesivamente, obtendríamos,

$$\text{m.c.d.}(m_2 m_3 \cdots m_n, m_1) = 1 \Longrightarrow \text{m.c.d.}(M_1, m_1) = 1$$

Procediendo de la misma forma, obtendríamos,

$$\begin{array}{c} \text{m.c.d.}(M_1, m_1) = 1 \\ \text{m.c.d.}(M_2, m_2) = 1 \\ \text{m.c.d.}(M_3, m_3) = 1 \\ \vdots \end{array}$$

esto es,

$$\text{m.c.d.}(M_i, m_i) = 1, i = 1, 2, \ldots, n$$

y por el corolario 8.3.2, sabemos que existe y_i, inverso de M_i módulo m_i, es decir,

$$\exists y_i \in \mathbb{Z} : M_i y_i \equiv 1 \ (\text{mód } m_i), \ i = 1, 2, \ldots, n$$

Además,

$$\begin{array}{l} M_1 = m_2 m_3 \cdots m_n \Longrightarrow M_1 \text{ es múltiplo de } m_i, \text{ para } i \neq 1 \Longrightarrow M_1 \equiv 0 \ (\text{mód } m_i), \text{ para } i \neq 1 \\ M_2 = m_1 m_3 \cdots m_n \Longrightarrow M_2 \text{ es múltiplo de } m_i, \text{ para } i \neq 2 \Longrightarrow M_2 \equiv 0 \ (\text{mód } m_i), \text{ para } i \neq 2 \\ M_3 = m_1 m_2 \cdots m_n \Longrightarrow M_3 \text{ es múltiplo de } m_i, \text{ para } i \neq 3 \Longrightarrow M_3 \equiv 0 \ (\text{mód } m_i), \text{ para } i \neq 3 \\ \vdots \end{array}$$

esto es,

$$M_j \equiv 0 \ (\text{mód } m_i) \text{ para } i \neq j$$

Ahora, construiremos una solución simultánea formando la suma,

$$x = a_1 M_1 y_1 + a_2 M_2 y_2 + \cdots + a_n M_n y_n$$

Veamos que x es una solución de todas las congruencias lineales. En efecto,

$$\left.\begin{array}{rcl} M_1y_1 \equiv 1 \pmod{m_1} & \Longrightarrow & a_1M_1y_1 \equiv a_1 \pmod{m_1} \\ M_2 \equiv 0 \pmod{m_1} & \Longrightarrow & a_2M_2y_2 \equiv 0 \pmod{m_1} \\ \vdots & & \vdots \\ M_n \equiv 0 \pmod{m_1} & \Longrightarrow & a_nM_ny_n \equiv 0 \pmod{m_1} \end{array}\right\}$$

y sumando miembro a miembro,

$$a_1M_1y_1 + a_2M_2y_2 + \cdots + a_nM_ny_n \equiv a_1 \pmod{m_1} \quad \Longrightarrow \quad x \equiv a_1 \pmod{m_1}$$

Procediendo análogamente,

$$\begin{array}{rcl} a_1M_1y_1 + a_2M_2y_2 + \cdots + a_nM_ny_n \equiv a_1 \pmod{m_2} & \Longrightarrow & x \equiv a_2 \pmod{m_2} \\ a_1M_1y_1 + a_2M_2y_2 + \cdots + a_nM_ny_n \equiv a_3 \pmod{m_3} & \Longrightarrow & x \equiv a_3 \pmod{m_3} \\ \vdots & & \\ a_1M_1y_1 + a_2M_2y_2 + \cdots + a_nM_ny_n \equiv a_n \pmod{m_n} & \Longrightarrow & x \equiv a_n \pmod{m_n} \end{array}$$

y, por lo tanto,

$$x = a_1M_1y_1 + a_2M_2y_2 + \cdots + a_nM_ny_n$$

es una solución del sistema de congruencias lineales propuesto.

Unicidad. Veamos, ahora, que la solución encontrada es única, es decir todas las demás soluciones son congruentes módulo m con ella.

Supongamos que existe x' que también satisface todas las congruencias lineales del sistema. Entonces,

$$\left.\begin{array}{l} x \equiv a_i \pmod{m_i} \\ \text{y} \\ x' \equiv a_i \pmod{m_i} \end{array}\right\} \quad \Longrightarrow \quad x \equiv x' \pmod{m_i} \quad \Longrightarrow \quad m_i \big| x - x', \text{ para } i = 1, 2, \ldots, n$$

Pues bien,

$$\left.\begin{array}{l} m_1 \big| x - x' \\ \text{y} \\ m_2 \big| x - x' \end{array}\right\} \quad \Longrightarrow \quad \text{m.c.m.}(m_1, m_2) \big| x - x' \quad \Longrightarrow \quad m_1m_2 \big| x - x', \text{ ya que m.c.d.}(m_1, m_2) = 1$$

y,

$$\left.\begin{array}{l} m_1m_2 \big| x - x' \\ \text{y} \\ m_3 \big| x - x' \end{array}\right\} \quad \Longrightarrow \quad \text{m.c.m.}(m_1m_2, m_3) \big| x - x' \quad \Longrightarrow \quad m_1m_2m_3 \big| x - x', \text{ ya que m.c.d.}(m_1m_2, m_3) = 1$$

y así sucesivamente, obtendríamos

$$m_1m_2 \cdots m_n \big| x - x' \Longrightarrow m \big| x - x' \Longrightarrow x \equiv x' \pmod{m}$$

y la solución que hemos construido es única módulo m.

♦

El ejemplo siguiente se debe a Sun Tsu.

Ejemplo 8.12

Encontrar el entero positivo más pequeño que dividido por 3 da 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,

$$\left.\begin{array}{l} x = 3q_1 + 2 \\ \text{y} \\ x = 5q_2 + 3 \\ \text{y} \\ x = 7q_3 + 2 \end{array}\right\} \iff \left\{\begin{array}{l} x - 2 = 3q_1 \\ \text{y} \\ x - 3 = 5q_2 \\ \text{y} \\ x - 2 = 7q_3 \end{array}\right.$$

$$\iff \left\{\begin{array}{l} 3 \mid x - 2 \\ \text{y} \\ 5 \mid x - 3 \\ \text{y} \\ 7 \mid x - 2 \end{array}\right.$$

$$\iff \left\{\begin{array}{l} x \equiv 2 \pmod 3 \\ \text{y} \\ x \equiv 3 \pmod 5 \\ \text{y} \\ x \equiv 2 \pmod 7 \end{array}\right.$$

Tendremos que encontrar, pues, un número que satisfaga este sistema de congruencias lineales.

Los números 3, 5 y 7 son dos a dos primos entre sí, entonces podemos usar el *Teorema Chino del resto*, (8.3.3), para encontrar una solución única módulo $3 \cdot 5 \cdot 7 = 105$.

En efecto, sea $m = 3 \cdot 5 \cdot 7 = 105$ y,

$$M_1 = \frac{m}{3} = \frac{105}{3} = 35$$

$$M_2 = \frac{m}{5} = \frac{105}{5} = 21$$

$$M_3 = \frac{m}{7} = \frac{105}{7} = 15$$

Pues bien,

$$\text{m.c.d.}(M_1, 3) = \text{m.c.d.}(35, 3) = 1 \implies \exists y_1 \in \mathbb{Z} : 35y_1 \equiv 1 \pmod 3$$

$$\text{m.c.d.}(M_2, 5) = \text{m.c.d.}(21, 5) = 1 \implies \exists y_2 \in \mathbb{Z} : 21y_2 \equiv 1 \pmod 5$$

$$\text{m.c.d.}(M_3, 7) = \text{m.c.d.}(15, 7) = 1 \implies \exists y_3 \in \mathbb{Z} : 15y_3 \equiv 1 \pmod 7$$

Resolveremos estas congruencias lineales. Observemos que por el corolario 8.3.2,

$$ax \equiv 1 \pmod m \text{ tiene solución en } \mathbb{Z} \iff a \text{ y } m \text{ son primos entre sí}$$

y, en tal caso, la única solución no congruente módulo m de $ax \equiv 1 \pmod m$ es

$$x = x_0$$

siendo x_0 la solución particular de la Ecuación Diofántica $ax + my = 1$,

$$x_0 = p$$

es decir,

$$x = p$$

con p el coeficiente de Bezout, (5.3.5).

✳ Inverso de 35. $35y_1 \equiv 1$ (mód 3).

◊ m.c.d.$(35, 3)$.
Calculamos el máximo común divisor de 35 y 3 mediante el Algoritmo de Euclides,

	11	1	2
35	3	2	1
2	1	0	

luego m.c.d.$(35, 3) = 1$, es decir 35 y 3 son primos entre sí y la congruencia lineal $35y_1 \equiv 1$ (mód 3) tiene solución en $\mathbb{Z}$.

◊ Coeficiente de Bezout.
Por 5.3.5,

$$1 = \text{m.c.d.}(35, 3) \iff \exists p, q \in \mathbb{Z} : 1 = 35p + 3q$$

y podemos obtener p y q volviendo atrás el Algoritmo de Euclides,

$$\left.\begin{array}{l} 1 = 1 \cdot 3 + (-1)\, 2 \\ 2 = 35 - 11 \cdot 3 \end{array}\right\} \implies 1 = 1 \cdot 3 + (-1)\,(35 - 11 \cdot 3)$$
$$\implies 1 = -1 \cdot 35 + 12 \cdot 3$$

Es decir, $p = -1$.

◊ Solución particular de $35y_1 + 3y = 1$.

$$x_0 = \frac{1 \cdot p}{1} \implies x_0 = -1$$

◊ Solución de $35y_1 \equiv 1$ (mód 3).

$$\left.\begin{array}{l} y_1 = x_0 \\ \text{y} \\ x_0 = -1 \end{array}\right\} \implies y_1 = -1$$

✳ Inverso de 21. $21y_2 \equiv 1$ (mód 5).

◊ m.c.d.$(21, 5)$.
Calculamos el máximo común divisor de 21 y 5 por el Algoritmo de Euclides,

	4	5
21	5	1
1	0	

luego m.c.d.$(21, 5) = 1$, es decir 21 y 5 son primos entre sí y la congruencia lineal $21y_2 \equiv 1$ (mód 5) tiene solución en $\mathbb{Z}$.

◊ Coeficiente de Bezout.
Por 5.3.5,

$$1 = \text{m.c.d.}(21, 5) \iff \exists p, q \in \mathbb{Z} : 1 = 21p + 5q$$

y podemos obtener p y q volviendo atrás el Algoritmo de Euclides,

$$1 = 1 \cdot 21 + (-4)\, 5$$

Es decir, $p = 1$.

◊ Solución particular de $21y_2 + 5y = 1$.

$$x_0 = \frac{1 \cdot p}{1} \Longrightarrow x_0 = 1$$

◊ Solución de $21y_2 \equiv 1$ (mód 5).

$$\left.\begin{array}{l} y_2 = x_0 \\ \text{y} \\ x_0 = 1 \end{array}\right\} \Longrightarrow y_2 = 1$$

✳ Inverso de 15. $15y_3 \equiv 1$ (mód 7)

◊ m.c.d.$(15, 7)$.
Calculamos el máximo común divisor de 15 y 7 por el Algoritmo de Euclides,

	2	7
15	7	1
1	0	

luego m.c.d.$(15, 7) = 1$, es decir 15 y 7 son primos entre sí y la congruencia lineal $15y_3 \equiv 1$ (mód 7) tiene solución en $\mathbb{Z}$.

◊ Coeficiente de Bezout.
Por 5.3.5,

$$1 = \text{m.c.d.}(15, 7) \Longleftrightarrow \exists p, q \in \mathbb{Z} : 1 = 15p + 7q$$

y podemos obtener p y q volviendo atrás el Algoritmo de Euclides,

$$1 = 1 \cdot 15 + (-2)\, 7$$

Es decir, $p = 1$.

◊ Solución particular de $15y_3 + 7y = 1$.

$$x_0 = \frac{1 \cdot p}{1} \Longrightarrow x_0 = 1$$

◊ Solución de $15y_3 \equiv 1$ (mód 7).

$$\left.\begin{array}{l} y_3 = x_0 \\ \text{y} \\ x_0 = 1 \end{array}\right\} \Longrightarrow y_3 = 1$$

La única solución módulo 105 del sistema de congruencias lineales es x tal que

$$\begin{aligned} x = a_1 M_1 y_1 + a_2 M_2 y_2 + a_3 M_3 y_3 \quad &\Longrightarrow \quad x = 2 \cdot 35(-1) + 3 \cdot 21 \cdot 1 + 2 \cdot 15 \cdot 1 \\ &\Longrightarrow \quad x = 23 \end{aligned}$$

luego $x = 23$ es la solución buscada.

Por lo tanto,

$$\left.\begin{array}{l} 23 \equiv 2 \ (\text{mód } 3) \\ \text{y} \\ 23 \equiv 3 \ (\text{mód } 5) \\ \text{y} \\ 23 \equiv 2 \ (\text{mód } 7) \end{array}\right\} \iff \left\{\begin{array}{l} 3 \mid 23-2 \\ \text{y} \\ 5 \mid 23-3 \\ \text{y} \\ 7 \mid 23-2 \end{array}\right.$$

$$\iff \left\{\begin{array}{l} \exists q_1 \in \mathbb{Z} : 23-2 = 3q_1 \\ \text{y} \\ \exists q_2 \in \mathbb{Z} : 23-3 = 5q_2 \\ \text{y} \\ \exists q_3 \in \mathbb{Z} : 23-2 = 7q_3 \end{array}\right.$$

$$\iff \left\{\begin{array}{l} \exists q_1 \in \mathbb{Z} : 23 = 3q_1+2 \\ \text{y} \\ \exists q_2 \in \mathbb{Z} : 23 = 5q_2+3 \\ \text{y} \\ \exists q_3 \in \mathbb{Z} : 23 = 7q_3+2 \end{array}\right.$$

y podemos concluir que 23 es el entero positivo más pequeño que da resto 2 cuando lo dividimos por 3, un resto igual a 3 cuando lo dividimos por 5, y resto 2 cuando se divide por 7.

♦

Ejemplo 8.13

Encontrar el entero positivo más pequeño cuyos restos cuando lo dividimos por 3, 4, 5 y 6 son, respectivamente, 2, 3, 4 y 5. (Brahmagupta[1]).

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,

[1]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 cuadrática $x^2 + 1 + py^2$, 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.

enteros, tales que $x = 3q_1 + 2$, $x = 4q_2 + 3$ y $x = 5q_3 + 4$. Entonces,

$$\left.\begin{array}{l} x = 3q_1 + 2 \\ \text{y} \\ x = 4q_2 + 3 \\ \text{y} \\ x = 5q_3 + 4 \end{array}\right\} \iff \left\{\begin{array}{l} x - 2 = 3q_1 \\ \text{y} \\ x - 3 = 4q_2 \\ \text{y} \\ x - 4 = 5q_3 \end{array}\right.$$

$$\iff \left\{\begin{array}{l} 3 \mid x - 2 \\ \text{y} \\ 4 \mid x - 3 \\ \text{y} \\ 5 \mid x - 4 \end{array}\right.$$

$$\iff \left\{\begin{array}{l} x \equiv 2 \ (\text{mód } 3) \\ \text{y} \\ x \equiv 3 \ (\text{mód } 4) \\ \text{y} \\ x \equiv 4 \ (\text{mód } 5) \end{array}\right.$$

Tendremos que encontrar, pues, un número que satisfaga este sistema de congruencias lineales.

Obsérvese que los números 3, 4 y 5 son dos a dos primos entre sí, sin embargo 3 no es primo con 6 y lo mismo ocurre con 4. Aplicaremos el *Teorema Chino del resto* a las tres congruencias y calcularemos una solución única módulo $3 \cdot 4 \cdot 5$, es decir, módulo 60.

En efecto, sea $m = 3 \cdot 4 \cdot 5 = 60$ y,

$$M_1 = \frac{m}{3} = \frac{60}{3} = 20$$

$$M_2 = \frac{m}{4} = \frac{60}{4} = 15$$

$$M_3 = \frac{m}{5} = \frac{60}{5} = 12$$

Pues bien,

$$\text{m.c.d.}(M_1, 3) = \text{m.c.d.}(20, 3) = 1 \implies \exists y_1 \in \mathbb{Z} : 20y_1 \equiv 1 \ (\text{mód } 3)$$

$$\text{m.c.d.}(M_2, 4) = \text{m.c.d.}(15, 4) = 1 \implies \exists y_2 \in \mathbb{Z} : 15y_2 \equiv 1 \ (\text{mód } 4)$$

$$\text{m.c.d.}(M_3, 5) = \text{m.c.d.}(12, 5) = 1 \implies \exists y_3 \in \mathbb{Z} : 12y_3 \equiv 1 \ (\text{mód } 5)$$

Resolveremos estas congruencias lineales. Observemos que por el corolario 8.3.2,

$$ax \equiv 1 \ (\text{mód } m) \text{ tiene solución en } \mathbb{Z} \iff a \text{ y } m \text{ son primos entre sí}$$

y, en tal caso, la única solución no congruente módulo m de $ax \equiv 1 \ (\text{mód } m)$ es

$$x = x_0$$

siendo x_0 la solución particular de la Ecuación Diofántica $ax + my = 1$,

$$x_0 = p$$

es decir,

$$x = p$$

donde p es el coeficiente de Bezout, (5.3.5).

- ✳ Inverso de 20. $20y_1 \equiv 1 \ (\text{mód } 3)$.
  - ◊ m.c.d.$(20, 3)$.
    Calculamos el máximo común divisor de 20 y 3 mediante el Algoritmo de Euclides,

	6	1	2
20	3	2	1
2	1	0	

luego m.c.d.$(20,3)=1$, es decir 20 y 3 son primos entre sí y $20y_1 \equiv 1$ (mód 3) tiene solución en $\mathbb{Z}$.

◊ Coeficiente de Bezout.
Por 5.3.5,

$$1 = \text{m.c.d.}(20,3) \Longleftrightarrow \exists p, q \in \mathbb{Z} : 1 = 20p + 3q$$

y podemos obtener p y q volviendo atrás el Algoritmo de Euclides,

$$\left.\begin{array}{l} 1 = 1 \cdot 3 + (-1)\, 2 \\ 2 = 20 - 6 \cdot 3 \end{array}\right\} \Longrightarrow 1 = 1 \cdot 3 + (-1)\,(20 - 6 \cdot 3)$$

$$\Longrightarrow 1 = -1 \cdot 20 + 7 \cdot 3$$

Es decir, $p = -1$.

◊ Solución particular de $20y_1 + 3y = 1$.

$$x_0 = \frac{1 \cdot p}{1} \Longrightarrow x_0 = -1$$

◊ Solución de $20y_1 \equiv 1$ (mód 3).

$$\left.\begin{array}{l} y_1 = x_0 \\ \text{y} \\ x_0 = -1 \end{array}\right\} \Longrightarrow y_1 = -1$$

✳ Inverso de 15. $15y_2 \equiv 1$ (mód 4)

◊ m.c.d.$(15,4)$.
Calculamos el máximo común divisor de 15 y 4 mediante el Algoritmo de Euclides,

	3	1	3
15	4	3	1
3	1	0	

luego m.c.d.$(15,4)=1$, es decir 15 y 4 son primos entre sí y la congruencia lineal $15y_2 \equiv 1$ (mód 4) tiene solución en $\mathbb{Z}$.

◊ Coeficiente de Bezout.
Por 5.3.5,

$$1 = \text{m.c.d.}(15,4) \Longleftrightarrow \exists p, q \in \mathbb{Z} : 1 = 15p + 4q$$

y podemos obtener p y q volviendo atrás el Algoritmo de Euclides,

$$\left.\begin{array}{l} 1 = 1 \cdot 4 + (-1)\, 3 \\ 3 = 15 - 3 \cdot 4 \end{array}\right\} \Longrightarrow 1 = 1 \cdot 4 + (-1)\,(15 - 3 \cdot 4)$$

$$\Longrightarrow 1 = -1 \cdot 15 + 4 \cdot 4$$

Es decir,$p = -1$.

◊ Solución particular de $15y_2 + 4y = 1$.

$$x_0 = \frac{1 \cdot p}{1} \Longrightarrow x_0 = -1$$

◊ Solución de $15y_2 \equiv 1$ (mód 4).

$$\left.\begin{array}{l} y_2 = x_0 \\ \text{y} \\ x_0 = -1 \end{array}\right\} \Longrightarrow y_2 = -1$$

✳ Inverso de 12. $12y_3 \equiv 1$ (mód 5)

◊ m.c.d.$(12, 5)$.
Calculamos el máximo común divisor de 12 y 5 por el Algoritmo de Euclides,

	2	2	2
12	5	2	1
2	1	0	

luego m.c.d.$(12, 5) = 1$, es decir 12 y 5 son primos entre sí y $12y_3 \equiv 1$ (mód 5) tiene solución en $\mathbb{Z}$.

◊ Coeficiente de Bezout.
Por 5.3.5,

$$1 = \text{m.c.d.}(12, 5) \Longleftrightarrow \exists p, q \in \mathbb{Z} : 1 = 12p + 5q$$

y podemos calcular p y q volviendo atrás el Algoritmo de Euclides,

$$\left.\begin{array}{l} 1 = 1 \cdot 5 + (-2)\, 2 \\ 2 = 12 - 2 \cdot 5 \end{array}\right\} \Longrightarrow 1 = 1 \cdot 5 + (-2)\,(12 - 2 \cdot 5)$$
$$\Longrightarrow 1 = -2 \cdot 12 + 5 \cdot 5$$

Es decir, $p = -2$.

◊ Solución particular de $12y_3 + 5y = 1$.

$$x_0 = \frac{1 \cdot p}{1} \Longrightarrow x_0 = -2$$

◊ Solución de $12y_3 \equiv 1$ (mód 5).

$$\left.\begin{array}{l} y_3 = x_0 \\ \text{y} \\ x_0 = -2 \end{array}\right\} \Longrightarrow y_3 = -2$$

La solución única módulo 60 del sistema de congruencias lineales es x tal que,

$$x = a_1M_1y_1 + a_2M_2y_2 + a_3M_3y_3 \Longrightarrow x = 2 \cdot 20(-1) + 3 \cdot 15(-1) + 4 \cdot 12(-2)$$
$$\Longrightarrow x = -181$$

Del enunciado se sigue que el número buscado da resto 5 cuando se divide por 6, luego por el *Teorema de existencia y unicidad de cociente y resto*,

$$\exists s \in \mathbb{Z} : x = 6s + 5$$

Por otra parte, x tiene que ser congruente módulo 60 con -181, luego,

$$x \equiv -181 \ (\text{mód } 60) \Longrightarrow 60 \mid x+181 \Longrightarrow \exists t \in \mathbb{Z} : x+181 = 60t \Longrightarrow \exists t \in \mathbb{Z} : x = 60t - 181$$

Pues bien,

$$\left.\begin{array}{l} x = 6s+5 \\ \text{y} \\ x = 60t-181 \end{array}\right\} \Longrightarrow 6s+5 = 60t-181 \Longrightarrow 6s-60t = -186$$

Ahora resolvemos la Ecuación Diofántica $6s - 60t = -186$.

- Hallamos el máximo común divisor de 6 y -60 utilizando el *Algoritmo de Euclides.*

	10	
60	6	
0		

- Volvemos atrás el Algoritmo para obtener el coeficiente de Bezout.

$$6 = 1 \cdot 60 + (-9)\, 6$$

es decir,

$$6 = -9 \cdot 6 + (-1)\,(-60)$$

luego $p = -9$.

- Calculamos la solución particular.

$$s_0 = \frac{-186(-9)}{6} \Longrightarrow s_0 = 279$$

- Solución general.

$$s = 279 - 10k, \ k \in \mathbb{Z}$$

Pues bien, s no puede ser igual a cero ya que, en tal caso, $x = 5$ y x no satisfaría las condiciones del enunciado, por lo tanto $s > 0$.

$$\begin{aligned} s > 0 &\Longrightarrow 279 - 10k > 0 \\ &\Longrightarrow 10(-k) + 10 \cdot 27 + 9 > 0 \\ &\Longrightarrow 10(27-k) + 9 > 0 \\ &\Longrightarrow 27 - k \geqslant 0 \\ &\Longrightarrow \exists q \in \mathbb{Z}_0^+ : q = 27 - k \\ &\Longrightarrow \exists q \in \mathbb{Z}_0^+ : s = 10q + 9 \end{aligned}$$

Entonces,

$$\left.\begin{array}{l} x = 6s+5 \\ \text{y} \\ s = 10q+9 \end{array}\right\} \Longrightarrow x = 6(10q+9)+5 \Longrightarrow x = 60q+59$$

y el número más pequeño que verifica esta igualdad se obtendrá para $q = 0$, es decir, $x = 59$, y podremos concluir que 59 es el entero positivo más pequeño que da resto 2 cuando lo dividimos por 3, resto 3 cuando lo dividimos por 4, resto 4 cuando se divide por 5, y resto 5 cuando lo dividimos por 6.

♦♦♦

8.4 Euler, Fermat y Wilson

Estudiaremos en este apartado tres importantes teoremas sobre congruencias. Previamente, introduciremos la función de Euler[2] que nos permitirá probar dichos teoremas.

8.4.1 Función de Euler

Dado un entero positivo m, definimos la función $\phi(m)$ como el número de enteros positivos no mayores que m y primos con m. Su expresión es

$$\phi(m) = \sum_{0<r\leqslant m} 1$$

siendo $m.c.d.(r, m) = 1$. Llamaremos a $\phi(m)$, Función de Euler de m.

♦

Ejemplo 8.14

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 8.1 Obsérvese que si p es un número primo, entonces todos los enteros positivos menores que p son primos con p, entonces

$$\phi(p) = p - 1$$

♦

[2]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 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.

8.4.2 Teorema de Euler

Si a y m son primos entre sí, entonces $a^{\phi(m)} \equiv 1 \pmod{m}$.

Demostración.

Supongamos que $\phi(m) = k$, es decir, existen k enteros positivos menores que m y primos con m. Sean $r_1, r_2, \ldots, r_k$ esos números. Entonces,

$$\text{m.c.d.}(r_i, m) = 1,\ 1 \leqslant i \leqslant k$$

Pues bien, por hipótesis $\text{m.c.d.}(a, m) = 1$, de aquí que,

$$\left.\begin{array}{l}\text{m.c.d.}(a,m)=1\\ \text{y}\\ \text{m.c.d.}(r_i,m)=1\end{array}\right\} \overset{(5.12)}{\Longrightarrow} \text{m.c.d.}(ar_i, m) = 1$$

Veamos ahora que existen, también, k números de la forma ar_i, o lo que es igual, veamos que los números ar_i son diferentes módulo m dos a dos, es decir,

$$i \neq j \Longrightarrow ar_i \not\equiv ar_j \pmod{m}$$

Lo probaremos por contradicción. Efectivamente, si $i \neq j$ y $ar_i \equiv ar_j \pmod{m}$, y llamamos $\overline{a}$ al inverso de a módulo m, tendremos,

$$ar_i \equiv ar_j \pmod{m} \Longrightarrow \overline{a}ar_i \equiv \overline{a}ar_j \pmod{m} \Longrightarrow r_i \equiv r_j \pmod{m}$$

y esto es imposible ya que $r_i \not\equiv r_j \pmod{m}$.

Por otra parte, el teorema 8.1.2, (a), asegura que existe r tal que $ar_i \equiv r \pmod{m}$ con $0 \leqslant r < m$. Entonces,

$$\begin{aligned} ar_i \equiv r \pmod{m} &\overset{(8.6)}{\Longrightarrow} \text{m.c.d.}(ar_i, m) = \text{m.c.d.}(m, r)\\ &\Longrightarrow \text{m.c.d.}(m, r) = 1\\ &\Longrightarrow r \text{ es primo con } m, \text{ siendo } 0 \leqslant r < m\\ &\Longrightarrow \exists j : r = r_j, 1 \leqslant j \leqslant m,\ j \neq i \end{aligned}$$

Por lo tanto, $ar_i \equiv r_j \pmod{m}$, $i \neq j$ y multiplicando miembro a miembro para $1 \leqslant i, j \leqslant k$ y reordenando,

$$ar_1 \cdot ar_2 \cdots ar_k \equiv r_1 \cdot r_2 \cdots r_k \pmod{m}$$

esto es,

$$a^k r_1 \cdot r_2 \cdots r_k \equiv r_1 \cdot r_2 \cdots r_k \pmod{m}$$

y como,

$$\text{m.c.d.}(r_1 \cdot r_2 \cdots r_k, m) = 1 \ (5.12)$$

el número $r_1 \cdot r_2 \cdots r_k$ tiene inverso módulo m y bastaría multiplicar ambos miembros por su inverso para obtener,

$$a^k \equiv 1 \pmod{m}$$

es decir,

$$a^{\phi(m)} \equiv 1 \pmod{m}$$

♦

8.4.3 Pequeño Teorema de Fermat

Si p es primo y a es un entero no divisible por p, entonces

$$a^{p-1} \equiv 1 \ (mód\ p)$$

Demostración.

En efecto, como p es primo, será $\phi(p) = p - 1$. Además, si a no es divisible por p, al ser p primo, se sigue m.c.d.$(a, p) = 1$. Por el *Teorema de Euler* para $m = p$,

$$a^{p-1} \equiv 1 \ (\text{mód } p)$$

♦

Ejemplo 8.15

Encontrar el resto de dividir 23^{2587} por 7.

Solución.

Como 7 es primo y m.c.d.$(23, 7) = 1$, entonces por *Pequeño Teorema de Fermat*,

$$23^6 \equiv 1 \ (\text{mód } 7)$$

Por otra parte,

$$2587 = 6 \cdot 431 + 1$$

luego,

$$23^{2587} = \left(23^6\right)^{431} \cdot 23.$$

Pues bien,

$$\left.\begin{array}{l} 23^6 \equiv 1 \ (\text{mód } 7) \Longrightarrow \left(23^6\right)^{431} \equiv 1 \ (\text{mód } 7) \\ \text{y} \\ 23 \equiv 2 \ (\text{mód } 7) \end{array}\right\} \Longrightarrow \left(23^6\right)^{431} \cdot 23 \equiv 2 \ (\text{mód } 7) \Longrightarrow 23^{2587} \equiv 2 \ (\text{mód } 7)$$

así que el resto buscado es 2.

♦

Ejemplo 8.16

Calcular el resto de dividir 3^{47} por 23.

Solución.

Los números 3 y 23 son primos entre sí y 23 es primo, luego por el *Pequeño Teorema de Fermat*,

$$3^{22} \equiv 1 \ (\text{mód } 23)$$

Por otra parte,

$$47 = 22 \cdot 2 + 3$$

luego,

$$3^{47} = \left(3^{22}\right)^2 \cdot 3^3$$

y

$$\left.\begin{array}{l} 3^{22} \equiv 1 \ (\text{mód } 23) \Longrightarrow \left(3^{22}\right)^2 \equiv 1 \ (\text{mód } 23) \\ \text{y} \\ 3^3 \equiv 4 \ (\text{mód } 23) \end{array}\right\} \Longrightarrow \left(3^{22}\right)^2 \cdot 3^3 \equiv 4 \ (\text{mód } 23) \Longrightarrow 3^{47} \equiv 4 \ (\text{mód } 23)$$

y, consecuentemente, el resto pedido es 4.

♦

Ejemplo 8.17

Probar que el número $\left(27^4\right)^9 - \left(25^3\right)^6$ es divisible por 37.

Solución.

Efectivamente,

$$\left(27^4\right)^9 - \left(25^3\right)^6 = 27^{36} - 5^{36}$$

y como 37 es primo, $27 < 37$ y $5 < 37$, 27 y 5 son primos con 37. Por el *Pequeño Teorema de Fermat*,

$$\left.\begin{array}{l} 27^{36} \equiv 1 \pmod{37} \\ \text{y} \\ 5^{36} \equiv 1 \pmod{37} \end{array}\right\} \Longrightarrow 27^{36} - 5^{36} \equiv 0 \pmod{37} \Longrightarrow \left(27^4\right)^9 - \left(25^3\right)^6 \equiv 0 \pmod{37}$$

es decir, el número propuesto es divisible por 37.

♦

Ejemplo 8.18

Probar:

(a) Si $a \equiv b \pmod{m_i}$ $1 \leqslant i \leqslant k$, entonces $a \equiv b \pmod{\text{m.c.m.}(m_1, m_2, \ldots, m_k)}$

(b) $2^{132} - 1$ es divisible $3 \cdot 13 \cdot 23$

Solución.

(a) Si $a \equiv b \pmod{m_i}$ $1 \leqslant i \leqslant k$, entonces $a \equiv b \pmod{\text{m.c.m.}(m_1, m_2, \ldots, m_k)}$
En efecto,

$$\begin{aligned} a \equiv b \pmod{m_i},\ i = 1, 2, \ldots, k &\iff m_i \mid a - b,\ i = 1, 2, \ldots, k \\ &\Longrightarrow \text{m.c.m.}(m_1, m_2, \ldots, m_k) \mid a - b \\ &\iff a \equiv b \pmod{\text{m.c.m.}(m_1, m_2, \ldots, m_k)} \end{aligned}$$

(b) $2^{132} - 1$ es divisible por $3 \cdot 13 \cdot 23$.
Efectivamente, como 3, 13 y 23 son primos, y 2 no es divisible por 3, ni por 13, ni por 23, por el *Pequeño Teorema de Fermat*,

$$\begin{aligned} 2^2 &\equiv 1 \pmod{3} \\ 2^{12} &\equiv 1 \pmod{13} \\ 2^{22} &\equiv 1 \pmod{23} \end{aligned}$$

y,

$$\begin{aligned} 2^2 \equiv 1 \pmod{3} &\Longrightarrow \left(2^2\right)^{66} \equiv 1 \pmod{3} \Longrightarrow 2^{132} \equiv 1 \pmod{3} \\ 2^{12} \equiv 1 \pmod{13} &\Longrightarrow \left(2^{12}\right)^{11} \equiv 1 \pmod{13} \Longrightarrow 2^{132} \equiv 1 \pmod{13} \\ 2^{22} \equiv 1 \pmod{23} &\Longrightarrow \left(2^{22}\right)^{6} \equiv 1 \pmod{23} \Longrightarrow 2^{132} \equiv 1 \pmod{23} \end{aligned}$$

Por (a),

$$2^{132} \equiv 1 \pmod{\text{m.c.m.}(3, 13, 23)}$$

y como m.c.m. $(3, 13, 23) = 3 \cdot 13 \cdot 23$, tendremos

$$2^{132} \equiv 1 \text{ (mód } 3 \cdot 13 \cdot 23)$$

es decir,

$$2^{132} - 1 \equiv 0 \text{ (mód } 3 \cdot 13 \cdot 23)$$

y, consecuentemente, $2^{132} - 1$ es divisible por $3 \cdot 13 \cdot 23$.

♦

Ejemplo 8.19

Probar que para cualquier entero positivo, n, 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 de cociente y resto* existirán enteros 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, únicos, tales que,

$$\begin{aligned}
n &= 37q_1 + r_1,\ 0 \leqslant r_1 < 37 \\
n &= 19q_2 + r_2,\ 0 \leqslant r_2 < 19 \\
n &= 13q_3 + r_3,\ 0 \leqslant r_3 < 13 \\
n &= 7q_4 + r_4,\ 0 \leqslant r_4 < 7 \\
n &= 3q_5 + r_5,\ 0 \leqslant r_5 < 3 \\
n &= 2q_1 + r_6,\ 0 \leqslant r_6 < 2
\end{aligned}$$

y, por la definición de congruencia, esto significa que,

$$\begin{aligned}
n &\equiv r_1 \text{ (mód } 37) \\
n &\equiv r_2 \text{ (mód } 19) \\
n &\equiv r_3 \text{ (mód } 13) \\
n &\equiv r_4 \text{ (mód } 7) \\
n &\equiv r_5 \text{ (mód } 3) \\
n &\equiv r_6 \text{ (mód } 2)
\end{aligned}$$

Ahora como 37, 19, 13, 7, 3 y 2 son primos,

$$\begin{aligned}
&\text{m.c.d.}(r_1, 37) = 1 \\
&\text{m.c.d.}(r_2, 19) = 1 \\
&\text{m.c.d.}(r_3, 13) = 1 \\
&\text{m.c.d.}(r_4, 7) = 1 \\
&\text{m.c.d.}(r_5, 3) = 1 \\
&\text{m.c.d.}(r_6, 2) = 1
\end{aligned}$$

Aplicamos el *Pequeño Teorema de Fermat* y,

$$\begin{aligned}
&r_1^{36} \equiv 1 \pmod{37} \\
r_2^{18} \equiv 1 \pmod{19} &\implies r_2^{36} \equiv 1 \pmod{19} \\
r_3^{12} \equiv 1 \pmod{13} &\implies r_3^{36} \equiv 1 \pmod{13} \\
r_4^{6} \equiv 1 \pmod{7} &\implies r_4^{36} \equiv 1 \pmod{7} \\
r_5^{2} \equiv 1 \pmod{3} &\implies r_5^{36} \equiv 1 \pmod{3} \\
r_6 \equiv 1 \pmod{2} &\implies r_6^{36} \equiv 1 \pmod{2}
\end{aligned}$$

y

$$\begin{aligned}
n \equiv r_1 \pmod{37} &\implies n^{36} \equiv r_1^{36} \pmod{37} \\
n \equiv r_2 \pmod{19} &\implies n^{36} \equiv r_2^{36} \pmod{19} \\
n \equiv r_3 \pmod{13} &\implies n^{36} \equiv r_3^{36} \pmod{13} \\
n \equiv r_4 \pmod{7} &\implies n^{36} \equiv r_4^{36} \pmod{7} \\
n \equiv r_5 \pmod{3} &\implies n^{36} \equiv r_5^{36} \pmod{3} \\
n \equiv r_6 \pmod{2} &\implies n^{36} \equiv r_6^{36} \pmod{2}
\end{aligned}$$

por lo tanto,

$$\left.\begin{aligned}
n^{36} &\equiv 1 \pmod{37} \\
n^{36} &\equiv 1 \pmod{19} \\
n^{36} &\equiv 1 \pmod{13} \\
n^{36} &\equiv 1 \pmod{7} \\
n^{36} &\equiv 1 \pmod{3} \\
n^{36} &\equiv 1 \pmod{2}
\end{aligned}\right\} \implies n^{36} \equiv 1 \pmod{\text{m.c.m.}(37, 19, 13, 7, 3, 2)}$$

$$\begin{aligned}
&\implies n^{36} \equiv 1 \pmod{37 \cdot 19 \cdot 13 \cdot 7 \cdot 3 \cdot 2} \\
&\implies n^{36} \equiv 1 \pmod{383838}
\end{aligned}$$

y como,

$$n \equiv n \pmod{383838}$$

tendremos que,

$$n^{37} \equiv n \pmod{383838}$$

y, consecuentemente,

$$n^{37} - n \equiv 0 \pmod{383838}$$

o lo que es lo mismo,

$$n^{37} - n \text{ es divisible por } 383838$$

♦

Ejemplo 8.20

Probar que $10! \equiv -1 \pmod{11}$.

Solución.

Sea a un entero tal que $0 < a < 11$. Entones, como 11 es primo, a y 11 son primos entre sí, es decir $\text{m.c.d.}(a, 11) = 1$, luego, por 8.3.2, las congruencias lineales $ax \equiv 1 \pmod{11}$ tienen una solución única

módulo 11, así que para cada a, existe $\overline{a}$, con $0 < \overline{a} < 11$, tal que $a\overline{a} \equiv 1$ (mód 11). Pues bien,

$$\left.\begin{array}{l} \text{Si } a = 2, \text{entonces } \overline{a} = 6, \text{ ya que } 2 \cdot 6 \equiv 1 \text{ (mód 11)} \\ \text{Si } a = 3, \text{entonces } \overline{a} = 4, \text{ ya que } 3 \cdot 4 \equiv 1 \text{ (mód 11)} \\ \text{Si } a = 5, \text{entonces } \overline{a} = 9, \text{ ya que } 5 \cdot 9 \equiv 1 \text{ (mód 11)} \\ \text{Si } a = 7, \text{entonces } \overline{a} = 8, \text{ ya que } 7 \cdot 8 \equiv 1 \text{ (mód 11)} \end{array}\right\} \implies 2 \cdot 3 \cdot 4 \cdot 5 \cdot 6 \cdot 7 \cdot 8 \cdot 9 \equiv 1 \text{ (mód 11)}$$

De aquí que,

$$\left.\begin{array}{l} 2 \cdot 3 \cdot 4 \cdot 5 \cdot 6 \cdot 7 \cdot 8 \cdot 9 \equiv 1 \text{ (mód 11)} \\ \text{y} \\ 10 \equiv -1 \text{ (mód 11)} \end{array}\right\} \implies 2 \cdot 3 \cdot 4 \cdot 5 \cdot 6 \cdot 7 \cdot 8 \cdot 9 \cdot 10 \equiv -1 \text{ (mód 11)}$$

$$\implies 10! \equiv -1 \text{ (mód 11)}$$

♦

En el siguiente teorema usaremos cualquier número primo p.

En 1770 Edward Waring anunció la publicación del siguiente teorema por su alumno John Wilson. Ni Waring ni Wilson pudieron probarlo, pero ahora se puede encontrar en cualquier texto elemental de Teoría de Números.

8.4.4 Teorema de Wilson

Si p primo, entonces $(p-1)! \equiv -1$ (mód p).

Demostración.

Si a es un entero tal que $0 < a < p$, entonces, como p es primo, m.c.d.$(a, p) = 1$ y, consecuentemente, por 8.3.2, la congruencia lineal $ax \equiv 1$ (mód p) tiene solución única módulo p. Es decir, existe un único número $0 < \overline{a} < p$ tal que $a\overline{a} \equiv 1$ (mód p). Este número, $\overline{a}$, es el inverso de a módulo p.

Además, a y su inverso módulo p, $\overline{a}$, únicamente coinciden cuando $a = 1$ o $a = p - 1$.

Efectivamente, supongamos que $a = \overline{a}$. Entonces,

$$\begin{aligned}
\overline{a} \text{ es el inverso de } a \text{ módulo } p &\iff a\overline{a} \equiv 1 \pmod{p} \\
&\overset{\overline{a}=a}{\iff} a \cdot a \equiv 1 \pmod{p} \\
&\iff a^2 \equiv 1 \pmod{p} \\
&\iff p \big| a^2 - 1 \\
&\iff p \big| (a-1)(a+1) \\
&\iff p \big| a-1 \text{ o } p \big| a+1 \ \{p \text{ es primo}\} \\
&\iff \exists q \in \mathbb{Z} : \begin{cases} a = pq + 1 \\ \text{o} \\ a = pq - 1 \end{cases} \\
&\iff \exists q \in \mathbb{Z} : \begin{cases} a = pq + 1 \\ \text{o} \\ a = p(q-1) + p - 1 \end{cases} \\
&\iff \begin{cases} a \text{ da resto 1 cuando se divide por } p \\ \text{o} \\ a \text{ da resto } p-1 \text{ cuando se divide por } p \end{cases} \\
&\overset{0<a<p}{\iff} \begin{cases} a = 1 \\ \text{o} \\ a = p - 1 \end{cases}
\end{aligned}$$

Por lo tanto,

$$a \neq \overline{a} \iff \begin{cases} a \neq 1 \\ \text{y} \\ a \neq p-1 \end{cases}$$

entonces,

$$\text{para cada } a \in \{2, 3, \ldots, p-2\} \text{ habrá un único } \overline{a} \in \{2, 3, \ldots, p-2\} : \overline{a} \neq a \text{ y } a\overline{a} \equiv 1 \pmod{p}$$

así que hay $\dfrac{p-3}{2}$ congruencias de la forma $a\overline{a} \equiv 1 \pmod{p}$ y multiplicándolas todas, tendremos

$$2 \cdot 3 \cdots (p-2) \equiv 1 \pmod{p}$$

y como,

$$p - 1 \equiv -1 \pmod{p}$$

Bastaría multiplicar y,

$$2 \cdot 3 \cdots (p-2)(p-1) \equiv -1 \pmod{p}$$

es decir,

$$(p-1)! \equiv -1 \pmod{p}$$

♦

Ejemplo 8.21

Demostrar que $138! + 197^{138}$ es divisible por 139.

Solución.

Probaremos que $138! + 197^{138} \equiv 0 \pmod{139}$.

En efecto, 139 es primo, entonces por el *Teorema de Wilson*,

$$(139-1)! \equiv -1 \pmod{139}$$

es decir,

$$138! \equiv -1 \pmod{139}$$

Por otra parte, 139 y 197 son primos entre sí, luego por el *Pequeño Teorema de Fermat*

$$197^{139-1} \equiv 1 \pmod{139}$$

esto es,

$$197^{138} \equiv 1 \pmod{139}$$

y sumando ambos resultados,

$$138! + 197^{138} \equiv 0 \pmod{139}$$

Consecuentemente, $138! + 197^{138}$ es divisible por 139.

♦♦♦

Unidad Temática III

Relaciones y Funciones

Lección 9

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.

9.1 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.

9.1.1 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 9.1

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

$$\begin{aligned} A_1 \times A_2 \times A_3 = \{&(a,1,p),(a,1,q),(a,1,r),(a,2,p),(a,2,q),(a,2,r),\\ &(a,3,p),(a,3,q),(a,3,r),(b,1,p),(b,1,q),(b,1,r),\\ &(b,2,p),(b,2,q),(b,2,r),(b,3,p),(b,3,q),(b,3,r)\} \end{aligned}$$

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 9.2

Sea $A = \{\text{huevos, leche, maíz}\}$ y $B = \{\text{vacas, cabras, gallinas}\}$. Escribir la relación $\mathscr{R}$ de A a B definida por:

$$(a, b) \in \mathscr{R} \iff a \text{ es producido por } b$$

Solución.

La relación sería:

$$\mathscr{R} = \{(\text{huevos,gallinas}),(\text{leche,vacas}),(\text{leche,cabras})\}$$

♦

9.1.2 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.

♦

9.1.3 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,

$$\begin{aligned} \text{Dom}(\mathscr{R}) &= \{1,3\} \\ \text{e} & \\ \text{Img}(\mathscr{R}) &= \{2,3\} \end{aligned}$$

♦

Ejemplo 9.3

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.

$$\mathscr{R} = \{(2,10),(2,12),(2,14),(3,12),(4,12),(5,10),(6,12),(7,14)\}$$

♦♦♦

9.2 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 9.4

(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,

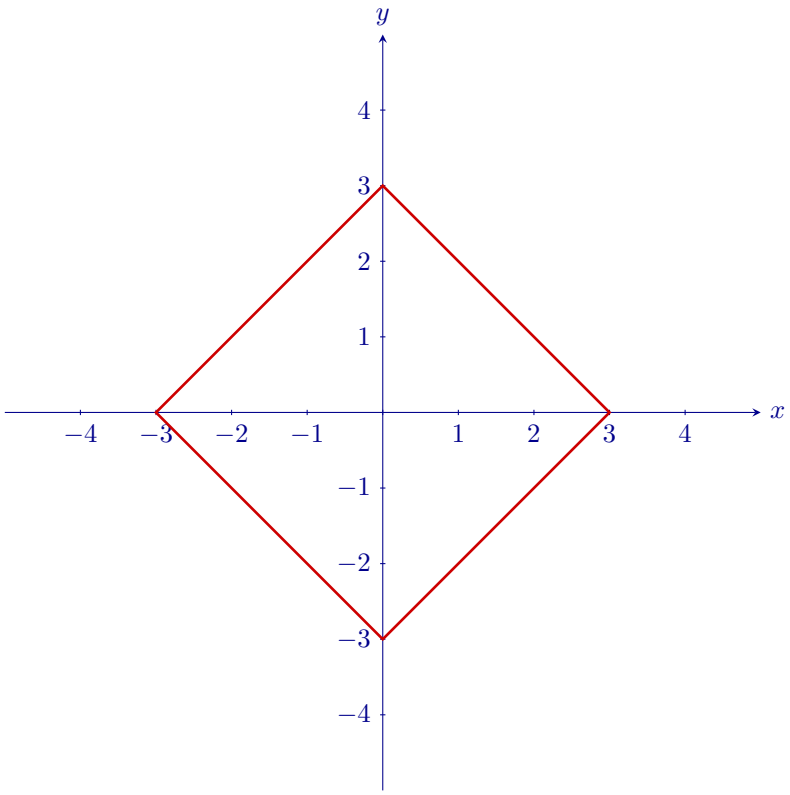
$4\mathscr{R}2$ pero $2\not\mathscr{R}4$, es decir 4 es múltiplo de 2, pero 2 no es múltiplo de 4.

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 9.5

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

$$1\mathscr{R}2,\ 1\mathscr{R}3,\ 3\mathscr{R}2,\ \text{pero}\ 1\not\mathscr{R}1,\ 2\not\mathscr{R}1,\ 2\not\mathscr{R}2,\ 2\not\mathscr{R}3,\ 3\not\mathscr{R}1,\ 3\not\mathscr{R}3$$

♦♦♦

9.3 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.

9.3.1 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:

$$M_{\mathscr{R}} = (r_{ij}) : r_{ij} = \begin{cases} 1, & si\ (a_i, b_j) \in \mathscr{R} \\ 0, & si\ (a_i, b_j) \notin \mathscr{R} \end{cases}$$

donde $i = 1, 2, \ldots\ldots, m$; $j = 1, 2, \ldots\ldots, n$.

♦

Ejemplo 9.6

Sea $A = \{1, 2, 3, 4\}$ y definimos la relación

$$a \mathscr{R} b \iff b \text{ es múltiplo de } a,\ \forall a, b \in A$$

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 9.1

- 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.

♦♦♦

9.4 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.

9.4.1 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.*

♦

9.4.2 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.

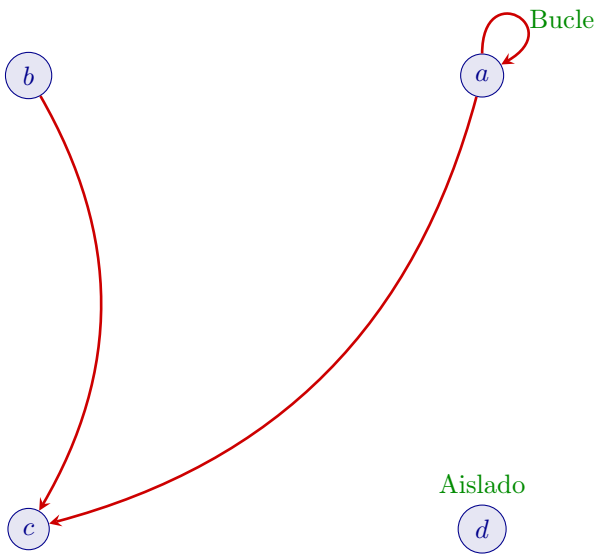
Grado de entrada de un vértice es el número de aristas que llegan hasta él. Representaremos por $gr_e(a)$ al del vértice a.

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 9.7

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:

$$\mathrm{gr}_e\,(a)=1,\ \mathrm{gr}_e\,(b)=0,\ \mathrm{gr}_e\,(c)=2,\ \mathrm{gr}_e\,(d)=0$$

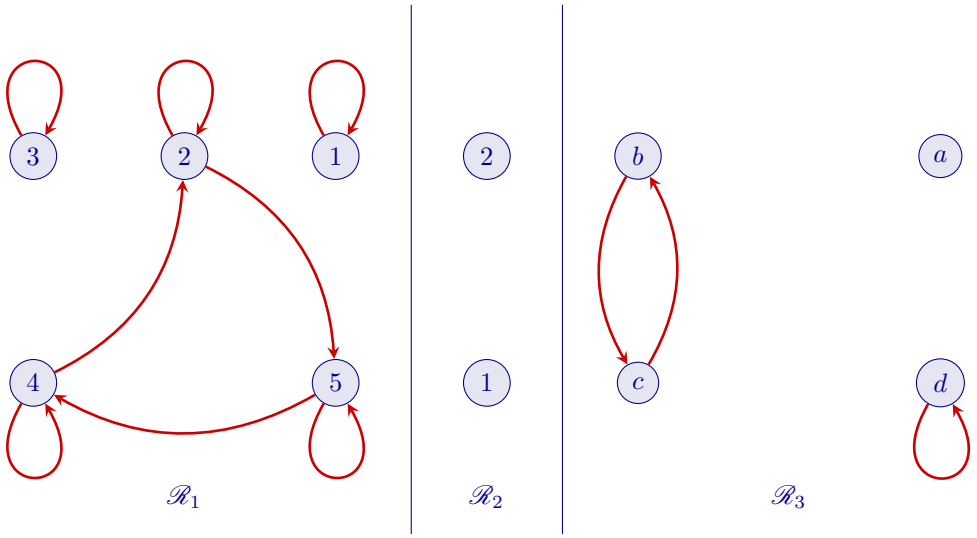
y los de salida,

$$\mathrm{gr}_s\,(a)=2,\ \mathrm{gr}_s\,(b)=1,\ \mathrm{gr}_s\,(c)=0,\ \mathrm{gr}_s\,(d)=0$$

♦

Ejemplo 9.8

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 9.9

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.

$$\mathscr{R} = \left\{(a, a+2) : a \in \mathbb{Z}^+\right\}$$

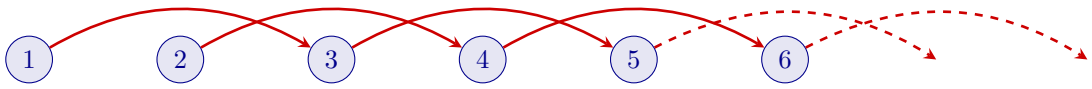
Observemos que la relación puede escribirse también, en la forma,

$$a\mathscr{R}b \Longleftrightarrow b = a+2$$

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.

♦♦♦

9.5 Propiedades de las Relaciones

Las relaciones binarias, es decir definidas sobre un único conjunto A, pueden tener ciertas propiedades que expondremos en este apartado.

9.5.1 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 9.10

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 9.11

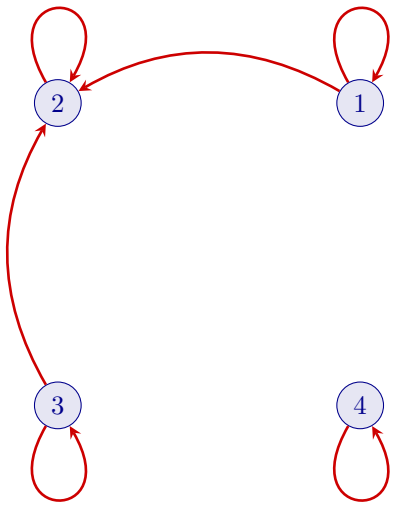
Sea $A = \{1, 2, 3, 4\}$ y $\mathscr{R} = \{(1, 1), (1, 2), (2, 2), (3, 3), (3, 2), (4, 4)\}$ una relación definida en A.

¿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 9.2 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 9.12

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 9.13

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,

$$a\mathscr{R}b \iff b \text{ es divisible por } a.$$

Analicemos el significado exacto de b "es divisible por" a. En efecto,

$$\begin{aligned} b \text{ es divisible por } a &\iff \frac{b}{a} \in \mathbb{Z}^+ \\ &\iff \exists q \in \mathbb{Z}^+ : \frac{b}{a} = q \\ &\iff b = aq, \text{ siendo } q \in \mathbb{Z}^+. \end{aligned}$$

La definición de $\mathscr{R}$ será, por tanto,

$$a\mathscr{R}b \iff b = aq, \text{ siendo } q \in \mathbb{Z}^+$$

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.

♦

9.5.2 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,

$$\mathscr{R} \text{ es simétrica} \iff \forall x, y \in A\,(x\mathscr{R}y \longrightarrow y\mathscr{R}x)$$

♦

Ejemplo 9.14

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.

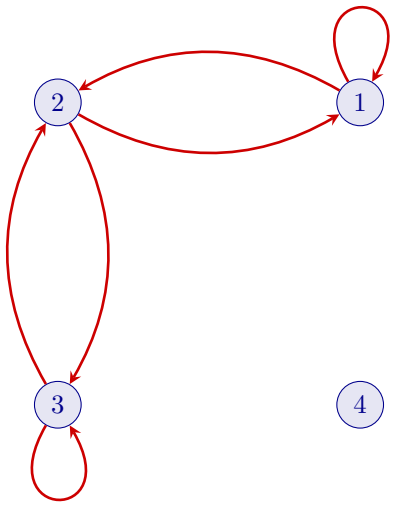
¿Es simétrica? Dibujar el digrafo y escribir la matriz de la relación.

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,

$$\begin{array}{ccc} (1,1) \in \mathscr{R} & \text{y} & (1,1) \in \mathscr{R} \\ (1,2) \in \mathscr{R} & \text{y} & (2,1) \in \mathscr{R} \\ (2,3) \in \mathscr{R} & \text{y} & (3,2) \in \mathscr{R} \\ (3,3) \in \mathscr{R} & \text{y} & (3,3) \in \mathscr{R} \end{array}$$

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 9.3 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

  $$\mathscr{R} \text{ es simétrica} \iff r_{ij} = r_{ji}, \forall i,j$$

  y

  $$\mathscr{R} \text{ es no simétrica} \iff \exists i,j : r_{ij} \neq r_{ji}$$

♦

9.5.3 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,

$$\mathscr{R} \text{ es antisimétrica} \Longleftrightarrow \forall x, y, (x \mathscr{R} y \ \wedge \ y \mathscr{R} x \longrightarrow x = y)$$

♦

Nota 9.4 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 9.5 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

$$\mathscr{R} \text{ es antisimétrica} \Longleftrightarrow \forall x, y \left[\neg \left(x \mathscr{R} y \ \wedge \ y \mathscr{R} x\right) \ \vee \ (x = y)\right]$$

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 9.15

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 $2 \not\mathscr{R} 4 \ \wedge 4 \not\mathscr{R} 2$.

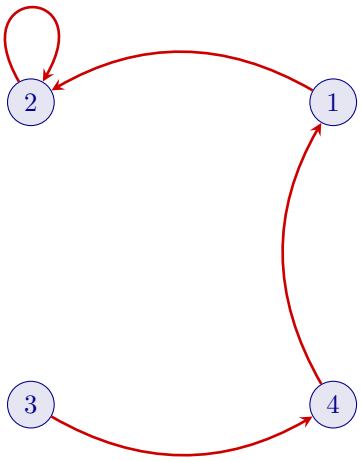
$3 \neq 4$ y $(3,4) \in \mathscr{R}$, pero $(4,3) \notin \mathscr{R}$, es decir $3 \mathscr{R} 4 \ \wedge \ 4 \not\mathscr{R} 3$.

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 9.6 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,

  $$\mathscr{R} \text{ es antisimétrica} \iff \forall i \neq j, r_{ij} = 0 \ \vee r_{ji} = 0$$

  y

  $$\mathscr{R} \text{ es no antisimétrica} \iff \exists i, j : r_{ij} = 1 \ \wedge \ r_{ji} = 1 \ \wedge \ i \neq j$$

♦

Ejemplo 9.16

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 9.12, 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,

$$\begin{array}{rcl} a\neq b & \Longleftrightarrow & b-a\neq 0 \\ & \Longleftrightarrow & b-a\in\mathbb{Z}\setminus\{0\} \\ & \Longleftrightarrow & b-a\in\mathbb{Z}^+\cup\mathbb{Z}^- \\ & \Longleftrightarrow & \left\{\begin{array}{l} b-a\in\mathbb{Z}^+ \quad \text{y} \quad a-b\in\mathbb{Z}^- \\ \text{ó} \\ b-a\in\mathbb{Z}^- \quad \text{y} \quad a-b\in\mathbb{Z}^+ \end{array}\right. \\ & \Longleftrightarrow & \left\{\begin{array}{l} a\mathscr{R}b \quad \text{y} \quad b\not\mathscr{R}\, a \\ \text{ó} \\ a\not\mathscr{R}\, b \quad \text{y} \quad b\mathscr{R}a \end{array}\right. \end{array}$$

Por lo tanto, la relación "menor o igual que" definida en el conjunto de los enteros es antisimétrica.

♦

Ejemplo 9.17

Estudiar la antisimetría de la relación de divisibilidad definida en el conjunto de los números enteros positivos.

Solución.

Según vimos en el ejemplo 9.13 la relación de divisibilidad en el conjunto de los enteros positivos se definía de la siguiente forma:

$$a\mathscr{R}b \Longleftrightarrow b = aq, \text{ siendo } q \in \mathbb{Z}^+, \ \forall a, b \in \mathbb{Z}^+$$

Pues bien, sean a y b dos enteros positivos cualesquiera y supongamos que $a\mathscr{R}b$ y $b\mathscr{R}a$. Entonces,

$$\left.\begin{array}{lll} a\mathscr{R}b & \Longleftrightarrow & b = aq_1, \text{ siendo } q_1 \in \mathbb{Z}^+ \\ y & & \\ b\mathscr{R}a & \Longleftrightarrow & a = bq_2, \text{ siendo } q_2 \in \mathbb{Z}^+ \end{array}\right\} \Longrightarrow b = bq_1q_2 \Longrightarrow q_1q_2 = 1 \Longrightarrow q_1 = q_2 = 1$$

luego,

$$a = b$$

y, consecuentemente, la relación propuesta es antisimétrica.

♦

9.5.4 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,

$$\mathscr{R} \text{ es transitiva} \Longleftrightarrow \forall x, y, z \, (x\mathscr{R}y \ \wedge \ y\mathscr{R}z \longrightarrow x\mathscr{R}z)$$

♦

Nota 9.7 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 $x\not\mathscr{R}z$.

♦

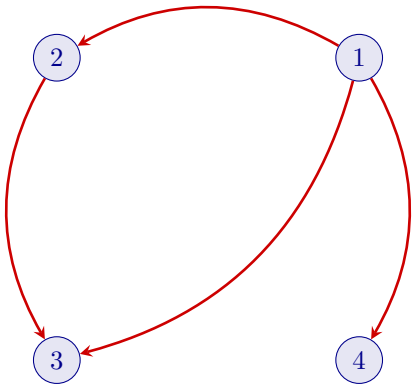
Ejemplo 9.18

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 9.8 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 $M_{\mathscr{R}} = (r_{ij})$,

$$\mathscr{R} \text{ es transitiva } \iff (r_{ij} = 1 \ \wedge \ r_{jk} = 1 \Longrightarrow r_{ik} = 1)$$

y

$$\mathscr{R} \text{ es no transitiva } \iff r_{ij} = 1 \ \wedge \ r_{jk} = 1 \ \wedge r_{ik} = 0$$

♦

Ejemplo 9.19

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 9.12, la relación puede definirse en la forma:

$$a\mathscr{R}b \iff b - a = k, \text{ siendo } k \in \mathbb{Z}_0^+$$

Pues bien, supongamos que $a\mathscr{R}b$ y $b\mathscr{R}c$, entonces

$$\left.\begin{array}{lll} a\mathscr{R}b & \iff & b - a = k_1, \text{ siendo } k_1 \in \mathbb{Z}_0^+ \\ \text{y} & & \\ b\mathscr{R}c & \iff & c - b = k_2, \text{ siendo } k_2 \in \mathbb{Z}_0^+ \end{array}\right\} \Longrightarrow c - a = k_1 + k_2, \text{ siendo } k_1 + k_2 \in \mathbb{Z}_0^+$$

luego,

$$a\mathscr{R}c$$

y, consecuentemente, la relación "menor o igual" definida en el conjunto de los números enteros es transitiva.

♦

Ejemplo 9.20

Estudiar la transitividad de la relación de divisibilidad definida en el conjunto de los números enteros positivos.

Solución.

Según vimos en el ejemplo 9.13 la relación de divisibilidad en el conjunto de los enteros positivos se definía de la siguiente forma:

$$a\mathscr{R}b \Longleftrightarrow b = aq, \text{ siendo } q \in \mathbb{Z}^+, \ \forall a, b \in \mathbb{Z}^+$$

Pues bien, sean a, b y c tres enteros positivos cualesquiera y supongamos que $a\mathscr{R}b$ y $b\mathscr{R}c$. Entonces,

$$\left.\begin{array}{lcl} a\mathscr{R}b & \Longleftrightarrow & b = aq_1, \text{ siendo } q_1 \in \mathbb{Z}^+ \\ y & & \\ b\mathscr{R}c & \Longleftrightarrow & c = bq_2, \text{ siendo } q_2 \in \mathbb{Z}^+ \end{array}\right\} \Longrightarrow c = aq_1q_2, \text{ siendo } q_1q_2 \in \mathbb{Z}^+ \Longrightarrow a\mathscr{R}c$$

luego,

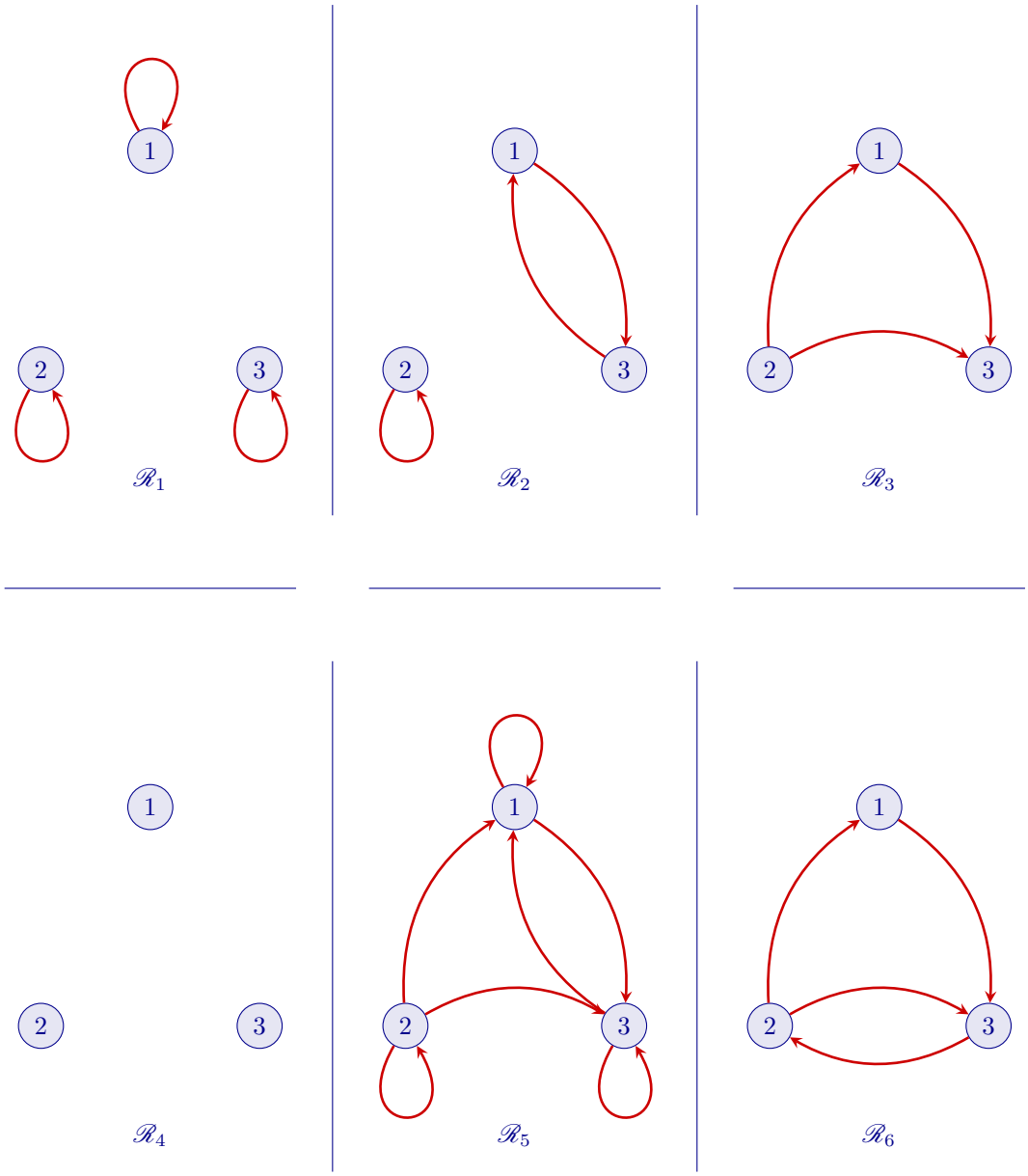
$$a\mathscr{R}c$$

y, consecuentemente, la relación de divisibilidad es transitiva.

♦

Ejemplo 9.21

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 9.22

Dibujar el grafo dirigido de las relaciones siguientes:

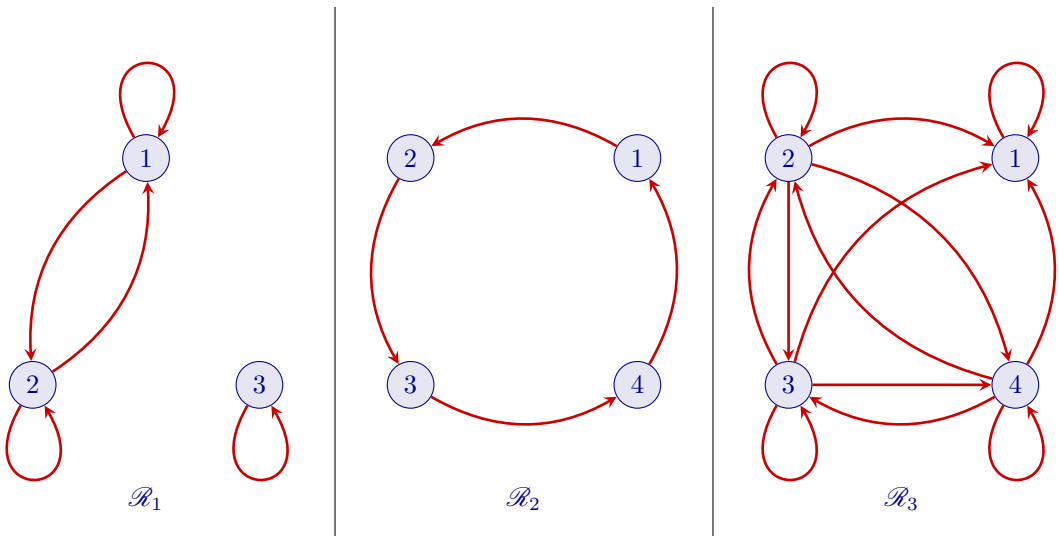
(a) La relación $\mathscr{R}_1 = \{(1,2),(2,1),(3,3),(1,1),(2,2)\}$ definida en $A = \{1,2,3\}$.

(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 9.23

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 10

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

10.1 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.

10.1.1 Definición

Una relación binaria $\mathscr{R}$ definida sobre un conjunto A se dice que es de equivalencia cuando es reflexiva, simétrica y transitiva.

♦

Ejemplo 10.1

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 10.2

(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.

♦

10.1.2 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,*

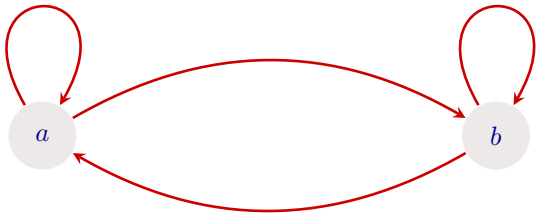
$$\forall a, (a \in A \longrightarrow a \mathscr{R} a)$$

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:

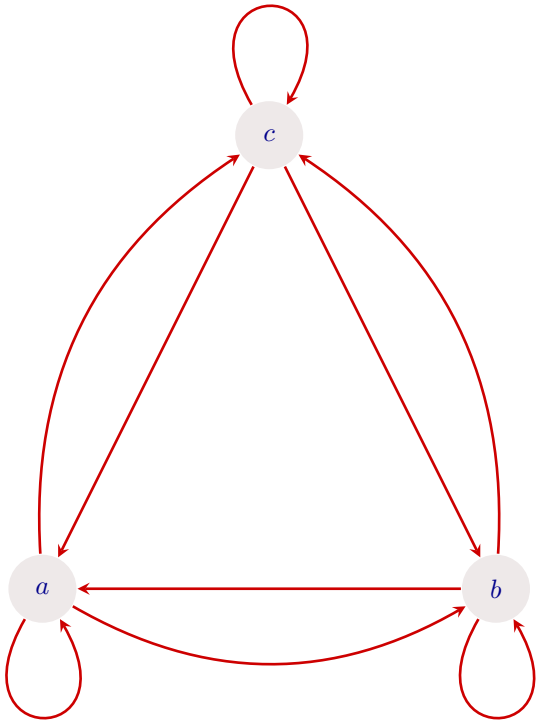
$$\mathscr{R} \text{ es simétrica} \Longleftrightarrow \forall a, b, (b \not\mathscr{R} a \longrightarrow a \not\mathscr{R} b)$$

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.



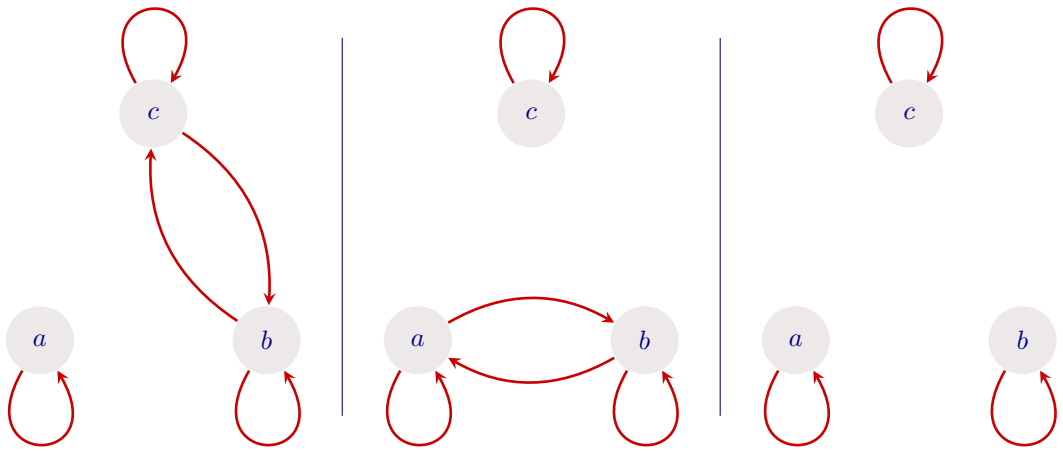
Utilizando el contrarrecíproco podemos definir, también, la transitividad en la siguiente forma:

$$\mathscr{R} \text{ es transitiva} \iff \forall a,b,c,(a\not\mathscr{R}\, c \Longrightarrow a\not\mathscr{R}\, b \text{ ó } b\not\mathscr{R}\, c)$$

$$\iff \forall a,b,c, a\not\mathscr{R}\, c \Longrightarrow \begin{cases} a\not\mathscr{R}\, b \text{ y } b\mathscr{R} c \\ \text{ó} \\ a\mathscr{R} b \text{ y } b\not\mathscr{R}\, c \\ \text{ó} \\ a\not\mathscr{R}\, b \text{ y } b\not\mathscr{R}\, c \end{cases}$$

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.*



♦

10.1.3 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 10.3

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,

$$\begin{aligned} r_{22}=1 \quad \text{y} \quad r_{23}=1 \quad &\Longrightarrow \quad r_{23}=1 \\ r_{23}=1 \quad \text{y} \quad r_{33}=1 \quad &\Longrightarrow \quad r_{23}=1 \\ r_{32}=1 \quad \text{y} \quad r_{22}=1 \quad &\Longrightarrow \quad r_{32}=1 \\ r_{33}=1 \quad \text{y} \quad r_{32}=1 \quad &\Longrightarrow \quad r_{32}=1 \end{aligned}$$

luego,

$$\text{si } r_{ij}=1 \text{ y } r_{jk}=1, \text{ entonces } r_{ik}=1$$

y

$$r_{12}=0 \quad \Longrightarrow \quad \begin{cases} r_{11}=1 \quad \text{y} \quad r_{12}=0 \\ r_{12}=0 \quad \text{y} \quad r_{22}=1 \\ r_{13}=0 \quad \text{y} \quad r_{32}=1 \end{cases}$$

$$r_{13}=0 \quad \Longrightarrow \quad \begin{cases} r_{11}=1 \quad \text{y} \quad r_{13}=0 \\ r_{12}=0 \quad \text{y} \quad r_{23}=1 \\ r_{13}=0 \quad \text{y} \quad r_{33}=1 \end{cases}$$

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.

♦♦♦

10.2 Clases de Equivalencia

10.2.1 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 $a \in [a]$.

♦

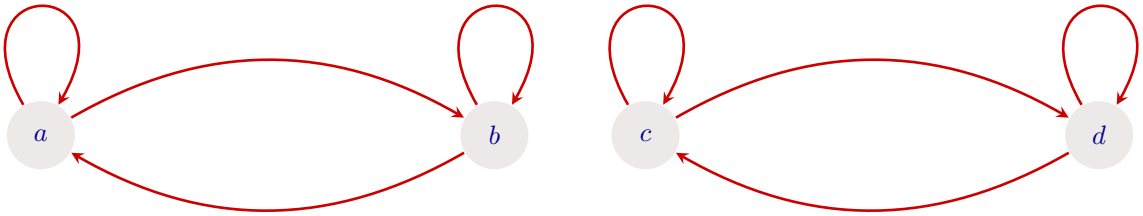
Ejemplo 10.4

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.

♦

10.2.2 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

$$\begin{aligned} x \in [a] &\iff x\mathscr{R}a \\ &\implies x\mathscr{R}a \text{ y } a\mathscr{R}b \quad \{\text{Hipótesis}\} \\ &\implies x\mathscr{R}b \quad \{\text{Transitividad de } \mathscr{R}\} \\ &\iff x \in [b] \end{aligned}$$

tenemos, pues, que

$$\forall x, (x \in [a] \longrightarrow x \in [b])$$

es decir, $[a] \subseteq [b]$.

Por otra parte,

$$\begin{aligned} x \in [b] &\iff x \mathscr{R} b \\ &\implies x \mathscr{R} b \text{ y } b \mathscr{R} a && \{\text{Hipótesis y Simetría de } \mathscr{R}\} \\ &\implies x \mathscr{R} a && \{\text{Transitividad de } \mathscr{R}\} \\ &\iff x \in [a] \end{aligned}$$

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.

♦♦♦

10.3 Conjunto Cociente

10.3.1 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,

$$A = \bigcup_{a\in A}[a]$$

♦

10.3.2 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 10.5

Sea $A = \{a, b, c, d, e, f\}$ y la relación de equivalencia definida en él,

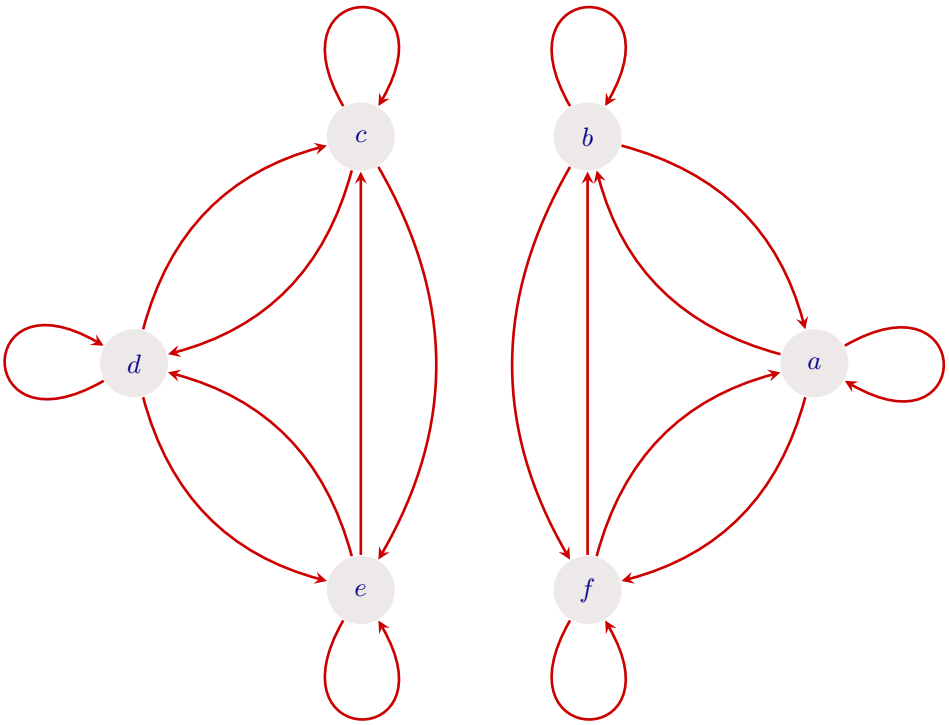
$$\begin{aligned}\mathscr{R} \;=\; \{&(a,a),(a,b),(a,f),(b,b),(b,a),(b,f),(c,c),(c,d),(c,e),\\ &(d,c),(d,e),(d,d),(e,c),(e,d),(e,e),(f,a),(f,b),(f,f)\}\end{aligned}$$

(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 10.6

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 $\mathbb{Z}$.

c) Clasificar, con la relación dada, el conjunto de los números enteros de valor absoluto menor o igual que 10 en el caso de $m = 3$.

Solución.

a) Probar que $\mathscr{R}$ es una relación de equivalencia.

Veamos si $\mathscr{R}$ es reflexiva, simétrica y transitiva.

Reflexiva. Sea a cualquier entero. Entonces,

$$a = a \iff a - a = 0 \Longrightarrow a - a = m \cdot 0, 0 \in \mathbb{Z} \iff a\mathscr{R}a$$

luego, dado cualquier número entero, n, $n\mathscr{R}n$, 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,

$$\begin{aligned} a\mathscr{R}b &\iff \exists q_1 \in \mathbb{Z} : a - b = mq_1 \\ &\iff \exists q_1 \in \mathbb{Z} : b - a = m(-q_1) \\ &\iff \exists q \in \mathbb{Z} : b - a = mq \ \ \{q = -q_1\} \\ &\iff b\mathscr{R}a \end{aligned}$$

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,

$$\left.\begin{array}{l} a\mathscr{R}b \\ \text{y} \\ b\mathscr{R}c \end{array}\right\} \iff \left\{\begin{array}{l} \exists q_1 \in \mathbb{Z} : a - b = mq_1 \\ \text{y} \\ \exists q_2 \in \mathbb{Z} : b - c = mq_2 \end{array}\right.$$

$$\begin{aligned} &\iff \exists q_1, q_2 \in \mathbb{Z} : a - b + b - c = mq_1 + mq_2 \\ &\iff \exists q_1, q_2 \in \mathbb{Z} : a - c = m(q_1 + q_2) \\ &\Longrightarrow \exists q \in \mathbb{Z} : a - c = mq \ \ \{q = q_1 + q_2\} \\ &\iff a\mathscr{R}c \end{aligned}$$

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) Obtener el conjunto cociente que la relación $\mathscr{R}$ determina en $\mathbb{Z}$.

Según la definición de conjunto cociente, 10.3.2,

$$\mathbb{Z}\Big/_{\mathscr{R}} = \{[a] : a \in \mathbb{Z}\}$$

Tendremos que hallar, pues, las clases de equivalencia.

Sea a cualquier número entero. Obtendremos $[a]$.

Por el teorema de existencia y unicidad de cociente y resto, (5.2.1), 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,

$$\begin{aligned}
b \in [a] &\iff b\mathscr{R}a \\
&\iff \exists q_1 \in \mathbb{Z} : b - a = mq_1 \\
&\iff \exists q_1 \in \mathbb{Z} : b - mq_2 - r = mq_1 \\
&\implies \exists q_1, q_2 \in \mathbb{Z} : b - r = mq_1 + mq_2,\ \text{siendo } 0 \leqslant r < m \\
&\iff \exists q_1, q_2 \in \mathbb{Z} : b - r = m(q_1 + q_2),\ \text{siendo } 0 \leqslant r < m \\
&\implies \exists q \in \mathbb{Z} : b - r = mq,\ \text{siendo } 0 \leqslant r < m\ \{\text{Tomando } q = q_1 + q_2\} \\
&\iff b\mathscr{R}r \\
&\iff b \in [r]
\end{aligned}$$

Por lo tanto, y al ser b cualquier entero, hemos probado que la proposición,

$$\forall n, (n \in [a] \longrightarrow n \in [r])$$

es verdadera y, consecuentemente,

$$[a] \subseteq [r]$$

Recíprocamente,

$$\begin{aligned}
b \in [r] &\iff b\mathscr{R}r \\
&\iff \exists q_1 \in \mathbb{Z} : b - r = mq_1 \\
&\implies \exists q_1, q_2 \in \mathbb{Z} : b - a + mq_2 = mq_1 \\
&\iff \exists q_1, q_2 \in \mathbb{Z} : b - a = m(q_1 - q_2) \\
&\implies \exists q \in \mathbb{Z} : b - a = mq\ \{\text{Tomando } q = q_1 - q_2\} \\
&\iff b\mathscr{R}a \\
&\iff b \in [a]
\end{aligned}$$

Nuevamente, por la arbitrariedad de b, la proposición,

$$\forall n, (n \in [r] \longrightarrow n \in [a])$$

es verdadera y, consecuentemente,

$$[r] \subseteq [a]$$

De la doble inclusión obtenida, se sigue que

$$[a] = [r]$$

es decir, la clase de equivalencia de un entero cualquiera, a es igual a la clase de equivalencia de r, resto de dividir a entre m, siendo,

$$\begin{aligned}
[r] &= \{n \in \mathbb{Z} : n\mathscr{R}r\} \\
&= \{n \in \mathbb{Z} : n - r = mq,\ q \in \mathbb{Z}\} \\
&= \{n \in \mathbb{Z} : n = mq + r,\ q \in \mathbb{Z}\}
\end{aligned}$$

Como r es un número entero entre 0 y $m-1$, habrá m clases de equivalencia distintas,

$$\begin{aligned}
[0] &= \{n : n = mq, q \in \mathbb{Z}\} \\
[1] &= \{n : n = mq + 1, q \in \mathbb{Z}\} \\
[2] &= \{n : n = mq + 2, q \in \mathbb{Z}\} \\
\vdots & \qquad\qquad \vdots \\
[m-1] &= \{n : n = mq + m - 1, q \in \mathbb{Z}\}
\end{aligned}$$

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 ... o $m-1$, luego,

$$[a] = [0] = \{n : n = mq,\ q \in \mathbb{Z}\}$$

o

$$[a] = [1] = \{n : n = mq + 1,\ q \in \mathbb{Z}\}$$

o

$$[a] = [2] = \{n : n = mq + 2,\ q \in \mathbb{Z}\}$$

o

$$\vdots$$

o

$$[a] = [m-1] = \{n : n = mq + m - 1,\ q \in \mathbb{Z}\}$$

Ahora podemos escribir el conjunto cociente. En efecto, según la definición de conjunto cociente, 10.3.2,

$$\mathbb{Z}\Big/_{\mathscr{R}} = \{[a] : a \in \mathbb{Z}\}$$

Pues bien, sea N cualquier subconjunto de números enteros. Entonces,

$$\begin{aligned}
N \in \mathbb{Z}\Big/_{\mathscr{R}} &\iff \exists a \in \mathbb{Z} : N = [a] \\
&\iff N = [r]\,, \text{ siendo } 0 \leqslant r < m-1 \\
&\iff N = [0] \ \vee\ N = [1] \ \vee\ N = [2] \ \vee\ \ldots \ \vee\ N = [m-1] \\
&\iff N \in \{[0]\,, [1]\,, [2]\,, \ldots, [m-1]\}
\end{aligned}$$

luego,

$$\mathbb{Z}\Big/_{\mathscr{R}} = \{[0]\,, [1]\,, [2]\,, \ldots, [m-1]\}$$

c) En este caso,

$$\forall n_1, n_2, (n_1 \mathscr{R} n_2 \text{ si, y solo si } n_1 - n_2 \text{ es múltiplo de } 3)$$

y tenemos que clasificar, es decir obtener el conjunto cociente que la relación $\mathscr{R}$ determina en el conjunto

$$A = \{n : |n| \leqslant 10\}$$

Pues bien, según el apartado anterior,

$$\mathbb{A}\Big/_{\mathscr{R}} = \{[0]\,, [1]\,, [2]\}$$

Tendremos que hallar, pues, [0], [1] y [2].

Sea a cualquier número entero. Entonces,

$$
\begin{aligned}
a \in [0] &\iff \begin{cases} a \mathscr{R} 0 \\ \text{y} \\ a \in A \end{cases} \\
&\iff \begin{cases} \exists q \in \mathbb{Z} : a - 0 = 3q \\ \text{y} \\ |a| \leqslant 10 \end{cases} \\
&\iff \begin{cases} \exists q \in \mathbb{Z} : a = 3q \\ \text{y} \\ |3q| \leqslant 10 \end{cases} \\
&\qquad \left[\begin{array}{lll} |3q| \leqslant 10 & \iff & -10 \leqslant 3q \leqslant 10 \\ & \iff & -10 < 3q < 10 \ \{3q \neq -10 \text{ y } 3q \neq 10\} \\ & \iff & \dfrac{-10}{3} < q < \dfrac{10}{3} \\ & \iff & -3 - \dfrac{1}{3} < q < 3 + \dfrac{1}{3} \\ & \iff & -3 \leqslant q \leqslant 3 \\ & \iff & |q| \leqslant 3 \end{array} \right] \\
&\iff \begin{cases} a = 3q \\ \text{y} \\ |q| \leqslant 3 \end{cases} \\
&\iff a \in \{-9, -6, -3, 0, 3, 6, 9\}
\end{aligned}
$$

Como a era la cualquiera, hemos probado la veracidad de la proposición

$$\forall n, (n \in [0] \longleftrightarrow n \in \{-9, -6, -3, 0, 3, 6, 9\})$$

y el axioma extensión asegura que

$$[0] = \{-9, -6, -3, 0, 3, 6, 9\}$$

Veamos ahora la clase de equivalencia del 1.

$$
\begin{aligned}
a \in [1] &\iff \begin{cases} a \mathscr{R} 1 \\ \text{y} \\ a \in A \end{cases} \\
&\iff \begin{cases} \exists q \in \mathbb{Z} : a - 1 = 3q \\ \text{y} \\ |a| \leqslant 10 \end{cases} \\
&\iff \begin{cases} \exists q \in \mathbb{Z} : a = 3q + 1 \\ \text{y} \\ |3q+1| \leqslant 10 \end{cases} \\
&\qquad \left[\begin{array}{lll} |3q+1| \leqslant 10 & \iff & -10 \leqslant 3q+1 \leqslant 10 \\ & \iff & -10 < 3q+1 \leqslant 10 \ \ \{3q+1 \neq -10\} \\ & \iff & -11 < 3q \leqslant 9 \\ & \iff & \dfrac{-11}{3} < q \leqslant \dfrac{9}{3} \\ & \iff & -3 - \dfrac{2}{3} < q \leqslant 3 \\ & \iff & -3 \leqslant q \leqslant 3 \\ & \iff & |q| \leqslant 3 \end{array} \right] \\
&\iff \begin{cases} a = 3q + 1 \\ \text{y} \\ |q| \leqslant 3 \end{cases} \\
&\iff a \in \{-8, -5, -2, 1, 4, 7, 10\}
\end{aligned}
$$

Como a era la cualquiera, hemos probado la veracidad de la proposición

$$\forall n, (n \in [1] \longleftrightarrow n \in \{-8, -5, -2, 1, 4, 7, 10\})$$

y, de nuevo, por el axioma extensión,

$$[1] = \{-8, -5, -2, 1, 4, 7, 10\}$$

Calculemos, finalmente, la clase de equivalencia del 2.

$$
\begin{aligned}
a \in [2] &\iff \begin{cases} a \mathscr{R} 2 \\ \text{y} \\ a \in A \end{cases} \\
&\iff \begin{cases} \exists q \in \mathbb{Z} : a - 2 = 3q \\ \text{y} \\ |a| \leqslant 10 \end{cases} \\
&\iff \begin{cases} \exists q \in \mathbb{Z} : a = 3q + 2 \\ \text{y} \\ |3q + 2| \leqslant 10 \end{cases} \\
&\qquad \left[\begin{array}{lll} |3q+1| \leqslant 10 & \iff & -10 \leqslant 3q + 2 \leqslant 10 \\ & \iff & -10 \leqslant 3q + 2 < 10 \ \ \{3q + 2 \neq 10\} \\ & \iff & -12 \leqslant 3q \leqslant 8 \\ & \iff & \dfrac{-12}{3} \leqslant q < \dfrac{8}{3} \\ & \iff & -4 \leqslant q < 2 + \dfrac{2}{3} \\ & \iff & -4 \leqslant q \leqslant 2 \end{array} \right] \\
&\iff \begin{cases} a = 3q + 2 \\ \text{y} \\ -4 \leqslant q \leqslant 2 \end{cases} \\
&\iff a \in \{-10, -7, -4, -1, 2, 5, 8\}
\end{aligned}
$$

Como a era la cualquiera, hemos probado la veracidad de la proposición

$$\forall n, (n \in [1] \longleftrightarrow n \in \{-10, -7, -4, -1, 2, 5, 8\})$$

y por el axioma extensión,

$$[1] = \{-10, -7, -4, -1, 2, 5, 8\}$$

El conjunto A clasificado por la relación propuesta sería:

$$
\begin{aligned}
\mathbb{A}/_{\mathscr{R}} &= \{[0], [1], [2]\} \\
&= \{\{-9, -6, -3, 0, 3, 6, 9\}, \{-8, -5, -2, 1, 4, 7, 10\}, \{-10, -7, -4, -1, 2, 5, 8\}\}
\end{aligned}
$$

♦

Ejemplo 10.7

En el conjunto $\mathbb{Z}$ de los números enteros se considera la siguiente relación:

$$\forall n_1, n_2,\ n_1 \mathscr{R} n_2 \iff \begin{cases} n_1 - n_2 = 0 \\ \text{ó} \\ n_1 + n_2 = 3 \end{cases}$$

(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,

$$\left.\begin{array}{rcl} a\mathscr{R}b & \Longleftrightarrow & a-b=0 \quad \text{ó} \quad a+b=3 \\ \text{y} & & \text{y} \\ b\mathscr{R}c & \Longleftrightarrow & b-c=0 \quad \text{ó} \quad b+c=3 \end{array}\right\} \Longrightarrow \left\{\begin{array}{l} \left.\begin{array}{l} a-b=0 \quad \text{ó} \quad a+b=3 \\ \text{y} \\ b-c=0 \end{array}\right\} \\ \text{ó} \\ \left.\begin{array}{l} a-b=0 \quad \text{ó} \quad a+b=3 \\ \text{y} \\ b+c=3 \end{array}\right\} \end{array}\right.$$

$$\Longrightarrow \left\{\begin{array}{l} \left.\begin{array}{rcl} a-b & = & 0 \\ \text{y} & & \\ b-c & = & 0 \end{array}\right\} \\ \text{ó} \\ \left.\begin{array}{rcl} a+b & = & 3 \\ \text{y} & & \\ b-c & = & 0 \end{array}\right\} \\ \text{ó} \\ \left.\begin{array}{rcl} a-b & = & 0 \\ \text{y} & & \\ b+c & = & 3 \end{array}\right\} \\ \text{ó} \\ \left.\begin{array}{rcl} a+b & = & 3 \\ \text{y} & & \\ b+c & = & 3 \end{array}\right\} \end{array}\right.$$

$$\Longrightarrow \left\{\begin{array}{rcl} a-c & = & 0 \\ \text{ó} & & \\ a+c & = & 3 \\ \text{ó} & & \\ a+c & = & 3 \\ \text{ó} & & \\ a-c & = & 0 \end{array}\right.$$

$$\Longrightarrow \quad a\mathscr{R}c$$

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

$$\begin{aligned} A/_{\mathscr{R}} &= \{[0], [1], [2], [3], [4], [5], [6], [7], [8]\} \\ &= \{\{0, 3\}, \{1, 2\}, \{4, -1\}, \{5, -2\}, \{6, -3\}, \{7, -4\}, \{8, -5\}\} \end{aligned}$$

♦

Ejemplo 10.8

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,

$$\begin{aligned}\mathbb{Z}^+/_{\mathscr{R}} &= \left\{\left[a^2\right] : a \in \mathbb{Z}^+\right\} \\ &= \{\{1,2,3\},\{4,5,6,7,8\},\{9,10,11,12,13,14,15\},\ldots\}\end{aligned}$$

♦

10.3.3 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, 10.3.2,

$$\begin{aligned}
X \in A\Big/_{\mathscr{R}} &\Longleftrightarrow \exists a \in A : X = [a] \\
&\Longleftrightarrow \exists A_i \in \mathscr{P} : a \in A_i \text{ y } X = [a] \\
&\Longleftrightarrow \exists A_i \in \mathscr{P} : [a] = A_i \text{ y } X = [a] \\
&\Longleftrightarrow \exists A_i \in \mathscr{P} : X = A_i \\
&\Longleftrightarrow X \in \mathscr{P} \\
&\Longleftrightarrow X \in \{A_1, A_2, \ldots, A_n\}
\end{aligned}$$

luego,

$$A\Big/_{\mathscr{R}} = \{A_1, A_2, \ldots, A_n\}$$

♦

Ejemplo 10.9

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 10.10

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

$$\begin{aligned} \mathscr{R} = \{&(a,a), (a,c), (a,e), (c,a), (c,c), (c,e), (e,a), (e,c), (e,e), \\ &(b,b), (b,d), (b,f), (d,b), (d,d), (d,f), (f,b), (f,d), (f,f)\} \end{aligned}$$

♦

Ejemplo 10.11

En el conjunto universal de los números enteros, y siendo m un entero positivo, se consideran las siguientes relaciones de equivalencia:

$\mathscr{R}_1$: Conjunto formado por todos los pares de números enteros, (n_1, n_2), cuya diferencia sea múltiplo de m.

$\mathscr{R}_2$: Conjunto formado por todos los pares de números enteros, (n_1, n_2), que den el mismo resto al dividirlos por m.

(a) Comprobar que $\mathscr{R}_1 = \mathscr{R}_2$.

(b) Obtener la clase de equivalencia de un entero cualquiera a.

(c) Sean los conjuntos:

A_0: Conjunto formado por todos los múltiplos de 6.

A_2: Conjunto formado por todos los números que den resto 2 al dividirlos por 6.

A_4: Conjunto formado por todos los números que den resto 4 al dividirlos por 6.

(c.1) Comprobar que $\mathscr{P} = \{A_0, A_2, A_4\}$ es una partición del conjunto M_2 de los números pares.

(c.2) Clasificar el conjunto, M_2, de los números pares por la relación de equivalencia, $\mathscr{R}_3$, determinada por la partición anterior en dicho conjunto.

(c.3) Calcular, razonadamente, el número de elementos que tienen cada una de las clases de equivalencia en el caso del conjunto de los números pares cuyo valor absoluto sea menor o igual que 19000.

Solución.

(a) Comprobaremos que $\mathscr{R}_1 = \mathscr{R}_2$.

* $\mathscr{R}_1 \subseteq \mathscr{R}_2$.
Sea (a, b) cualquiera de $\mathbb{Z} \times \mathbb{Z}$. Entonces,

$$\begin{aligned}
(a,b) \in \mathscr{R}_1 &\iff \exists q_1 \in \mathbb{Z} : a - b = mq_1 \\
&\iff \exists q_1 \in \mathbb{Z} : a = mq_1 + b \\
&\qquad \left\{ \begin{array}{l} \text{Teorema de existencia y unicidad de cociente y resto.} \\ \exists q_2, r \in \mathbb{Z} : b = mq_2 + r,\ 0 \leqslant r < m \end{array} \right\} \\
&\implies \exists q_1, q_2, r \in \mathbb{Z} : a = mq_1 + mq_2 + r,\ 0 \leqslant r < m \\
&\iff \exists q_1, q_2, r \in \mathbb{Z} : a = m(q_1 + q_2) + r,\ 0 \leqslant r < m \\
&\implies \exists q, r \in \mathbb{Z} : a = mq + r,\ 0 \leqslant r < m \ \{q = q_1 + q_2\} \\
&\iff a \text{ y } b \text{ dan el mismo resto, } r, \text{ al dividirlos por } m \\
&\iff (a,b) \in \mathscr{R}_2
\end{aligned}$$

De la arbitrariedad en la elección de (a, b) se sigue que la proposición,

$$\forall (n_1, n_2), ((n_1, n_2) \in \mathscr{R}_1 \longrightarrow (n_1, n_2) \in \mathscr{R}_2)$$

es verdadera y, consecuentemente, $\mathscr{R}_1 \subseteq \mathscr{R}_2$.

* $\mathscr{R}_2 \subseteq \mathscr{R}_1$.

En efecto, si (a,b) es cualquiera de $\mathbb{Z}\times\mathbb{Z}$, entonces

$$\begin{aligned}
(a,b)\in\mathscr{R}_2 &\iff a \text{ y } b \text{ dan el mismo resto, } r, \text{ al dividir entre } m\\
&\iff \begin{cases} \exists q_1\in\mathbb{Z} : a = mq_1 + r,\ 0\leqslant r<m\\ \exists q_2\in\mathbb{Z} : b = mq_2 + r,\ 0\leqslant r<m\end{cases}\\
&\implies \exists q_1,q_2\in\mathbb{Z} : a-b = m(q_1-q_2)\\
&\implies \exists q\in\mathbb{Z} : a-b = mq\ \ \{q=q_1-q_2\}\\
&\iff (a,b)\in\mathscr{R}_1
\end{aligned}$$

Como (a,b) es cualquiera, esto significa que la proposición

$$\forall (n_1,n_2), ((n_1,n_2)\in\mathscr{R}_2 \longrightarrow (n_1,n_2)\in\mathscr{R}_1)$$

es verdadera y, por lo tanto, $\mathscr{R}_2\subseteq\mathscr{R}_1$.

De la doble inclusión, $\mathscr{R}_1\subseteq\mathscr{R}_2$ y $\mathscr{R}_2\subseteq\mathscr{R}_1$, se sigue que $\mathscr{R}_1=\mathscr{R}_2$.

(b) Obtener, de forma razonada, la clase de equivalencia de un entero cualquiera a.

Por el teorema de existencia y unicidad de cociente y resto, existirán dos enteros, q_2 y r tales que $a = mq_2 + r$, con $0\leqslant r<m$.

Sea b un entero elegido arbitrariamente. Entonces, si llamamos $\mathscr{R}$ a $\mathscr{R}_1$ (se podría hacer igual con $\mathscr{R}_2$, ya que son iguales),

$$\begin{aligned}
b\in[a] &\iff b\mathscr{R}a\\
&\iff \exists q_1\in\mathbb{Z} : b-a = mq_1\\
&\iff \exists q_1\in\mathbb{Z} : b = mq_1 + a\\
&\implies \exists q_1,q_2,r\in\mathbb{Z} : b = mq_1 + mq_2 + r,\ 0\leqslant r<m\\
&\iff \exists q_1,q_2,r\in\mathbb{Z} : b = m(q_1+q_2) + r,\ 0\leqslant r<m\\
&\implies \exists q,r\in\mathbb{Z} : b = mq + r,\ 0\leqslant r<m\ \ \{q=q_1+q_2\}\\
&\iff \exists q,r\in\mathbb{Z} : b-r = mq,\ 0\leqslant r<m\\
&\iff b\mathscr{R}r,\ 0\leqslant r<m\\
&\iff b\in[r]\,,\ 0\leqslant r<m
\end{aligned}$$

De la arbitrariedad de b se sigue que la proposición,

$$\forall n, (n\in[a]\longrightarrow n\in[r])$$

es verdadera y, consecuentemente, $[a]\subseteq[r]$.

Recíprocamente,

$$\begin{aligned}
b\in[r] &\iff \exists q_1\in\mathbb{Z} : b-r = mq_1\\
&\iff \exists q_1\in\mathbb{Z} : b = mq_1 + r\\
&\iff \exists q_1,q_2\in\mathbb{Z} : b = mq_1 + a - mq_2\\
&\iff \exists q_1,q_2\in\mathbb{Z} : b = m(q_1-q_2) + a\\
&\implies \exists q\in\mathbb{Z} : b = mq + a\ \ \{q=q_1-q_2\}\\
&\iff \exists q\in\mathbb{Z} : b-a = mq\\
&\iff b\mathscr{R}a\\
&\iff b\in[a]
\end{aligned}$$

Como b estaba elegido arbitrariamente en $\mathbb{Z}$, la proposición,

$$\forall n, (n \in [r] \longrightarrow n \in [a])$$

es verdadera y, consecuentemente, $[r] \subseteq [a]$.

Finalmente, de la doble inclusión se sigue que $[a] = [r]$.

También, como acabamos de ver,

$$[r] = \{n : n = mq + r,\ q \in \mathbb{Z} \text{ y } 0 \leqslant r < m\}$$

Por lo tanto,

$$[a] = \{n : n = mq + r,\ q \in \mathbb{Z} \text{ y } 0 \leqslant r < m\}$$

siendo r el resto de dividir a entre m. Habrá, pues, tantas clases de equivalencia diferentes como restos haya al dividir entre m, es decir,

$$\begin{aligned}
[0] &= \{n : n = mq,\ q \in \mathbb{Z}\} \\
[1] &= \{n : n = mq + 1,\ q \in \mathbb{Z}\} \\
[2] &= \{n : n = mq + 2,\ q \in \mathbb{Z}\} \\
\vdots & \qquad\qquad \vdots \\
\vdots & \qquad\qquad \vdots \\
[m-1] &= \{n : n = mq + m - 1,\ q \in \mathbb{Z}\}
\end{aligned}$$

(c) Sean los conjuntos:

A_0: Conjunto formado por todos los múltiplos de 6.

A_2: Conjunto formado por todos los números que den resto 2 al dividirlos por 6.

A_4: Conjunto formado por todos los números que den resto 4 al dividirlos por 6.

(c.1) Comprobaremos que $\mathscr{P} = \{A_0, A_2, A_4\}$ cumple las tres condiciones para ser una partición del conjunto M_2 de los números pares.
Según la definición de los conjuntos,

$$\begin{aligned}
A_0 &= \{n : n = 6q,\ q \in \mathbb{Z}\} \\
A_2 &= \{n : n = 6q + 2,\ q \in \mathbb{Z}\} \\
A_4 &= \{n : n = 6q + 4,\ q \in \mathbb{Z}\}
\end{aligned}$$

es decir,

$$A_i = \{n : n = 6q + i,\ q \in \mathbb{Z}\},\ i = 0, 2, 4$$

1 Los tres conjuntos que integran la partición, A_0, A_2 y A_4 son no vacíos.
En efecto, si los tres fueran vacíos, entonces,

$$A_i = \emptyset,\ i = 0, 2, 4 \Longrightarrow 6q + i \notin A_i, \forall q \in \mathbb{Z}$$

lo cual, obviamente, no es cierto ya que tomando, por ejemplo, $q = 0$, tendríamos que

$$6q + i = i,\ \text{e } i \in A_i,\ i = 0, 2, 4$$

Por lo tanto, $A_i \neq \emptyset,\ i = 0, 2, 4$

2 Los tres conjuntos integrantes de la partición son, dos a dos, disjuntos, es decir,

$$i \neq j \Longrightarrow A_i \cap A_j = \emptyset,\ i,j = 0,2,4$$

Probaremos el contrarrecíproco,

$$A_i \cap A_j \neq \emptyset \Longrightarrow i = j,\ i,j = 0,2,4$$

En efecto,

$$\begin{aligned} A_i \cap A_j \neq \emptyset,\ i,j = 0,2,4 &\iff \exists a \in M_2 : \begin{cases} a \in A_i \\ \text{y} \\ a \in A_j \end{cases} \\ &\iff \exists q \in \mathbb{Z} : \begin{cases} a = 6q + i \\ \text{y} \\ a = 6q + j \end{cases} \\ &\qquad \left\{ \begin{array}{l} \text{El teorema de existencia y unicidad de cociente y} \\ \text{resto asegura que el resto de dividir } a \text{ por } 6 \\ \text{es único.} \end{array} \right\} \\ &\Longrightarrow i = j,\ i,j = 0,2,4 \end{aligned}$$

3 La unión de los tres conjuntos que conforman la partición es el conjunto formado por todos los números pares, es decir,

$$M_2 = A_0 \cup A_2 \cup A_4$$

En efecto, sea a cualquier entero.

$$\begin{aligned} a \in M_2 &\iff \exists q_1 \in \mathbb{Z} : a = 2q_1 \\ &\qquad \left\{ \begin{array}{l} \text{Dividiendo } q_1 \text{ por } 3 \\ \exists q, r \in \mathbb{Z} : q_1 = 3q + r,\ 0 \leqslant r < 3 \end{array} \right\} \\ &\Longrightarrow \exists q, r \in \mathbb{Z} : a = 2(3q + r),\ 0 \leqslant r < 3 \\ &\iff \exists q, r \in \mathbb{Z} : a = 6q + 2r,\ 2r = 0,2 \text{ o } 4 \\ &\iff \exists q, i \in \mathbb{Z} : a = 6q + i,\ i = 0,2 \text{ o } 4\ \{i = 2r\} \\ &\iff a \in A_0\ \vee\ a \in A_2\ \vee a \in A_4 \\ &\iff a \in (A_0 \cup A_2 \cup A_4) \end{aligned}$$

Como a era cualquier entero, esto quiere decir que la proposición,

$$\forall n, (n \in M_2 \longrightarrow n \in (A_0 \cup A_2 \cup A_4))$$

es verdadera y, por lo tanto, $M_2 \subseteq (A_0 \cup A_2 \cup A_4)$.
Recíprocamente,

$$\begin{aligned} a \in (A_0 \cup A_2 \cup A_4) &\iff \exists i : a \in A_i,\ i = 0,2 \text{ o } 4 \\ &\iff \exists q_1, i \in \mathbb{Z} : a = 6q_1 + i,\ i = 0,2 \text{ o } 4 \\ &\iff \exists q_1, r \in \mathbb{Z} : a = 6q_1 + 2r,\ 2r = 0,2 \text{ o } 4\ \left\{ r = \frac{i}{2} \right\} \\ &\iff \exists q_1, r \in \mathbb{Z} : a = 2(3q_1 + r),\ 0 \leqslant r < 3 \\ &\Longrightarrow \exists q \in \mathbb{Z} : a = 2q\ \{q = 3q_1 + r\} \\ &\iff a \in M_2 \end{aligned}$$

La arbitrariedad de a asegura que la proposición,

$$\forall n, (n \in (A_0 \cup A_2 \cup A_4) \longrightarrow n \in M_2)$$

es verdadera y, consecuentemente, $(A_0 \cup A_2 \cup A_4) \subseteq M_2$.
Por la doble inclusión se sigue que $M_2 = A_0 \cup A_2 \cup A_4$.

(c.2) Clasificar el conjunto, M_2, de los números pares por la relación de equivalencia, $\mathscr{R}_3$, determinada por la partición anterior en dicho conjunto.

Definimos la relación $\mathscr{R}_3$ según el teorema 7.3.3,

$\mathscr{R}_3$: Conjunto formado por todos los pares de números enteros, (n_1, n_2), que pertenecen al mismo subconjunto de la partición.

Entonces, si (a, b) es cualquier pareja de números enteros,

$$\begin{aligned}
(a,b) \in \mathscr{R}_3 &\iff \exists i : a \in A_i \text{ y } b \in A_i,\ i = 0,2,4 \\
&\iff \left\{ \begin{array}{l} \exists q_1 \in \mathbb{Z} : a = 6q_1 + i,\ i = 0,2,4 \\ \text{y} \\ \exists q_2 \in \mathbb{Z} : a = 6q_2 + i,\ i = 0,2,4 \end{array} \right\} \\
&\iff a \text{ y } b \text{ dan el mismo resto, } i, \text{ al dividir entre 6} \\
&\iff (a,b) \in \mathscr{R}_2 \\
&\iff (a,b) \in \mathscr{R}_1 \ \{\mathscr{R}_1 = \mathscr{R}_2\} \\
&\iff a - b = 6q
\end{aligned}$$

Por lo tanto, por el teorema citado anteriormente, y también por el apartado (b), las clases de equivalencia son A_0, A_2 y A_4, luego la clasificación que la relación propuesta produce en el conjunto de los números pares es:

$$\begin{aligned}
M_2 \Big/ \mathscr{R} &= \{A_0, A_1, A_2\} \\
&= \{\{n : n = 6q,\ q \in \mathbb{Z}\}, \{n : n = 6q+2,\ q \in \mathbb{Z}\}, \{n : n = 6q+4,\ q \in \mathbb{Z}\}\}
\end{aligned}$$

(c.3) Calcularemos, ahora, el número de elementos que tienen cada una de las clases de equivalencia en el caso del conjunto,

$$M_2 = \{n : n = 2q,\ q \in \mathbb{Z} \text{ y } |n| \leqslant 19000\}$$

⊛ $A_0 = \{n : n = 6q,\ q \in \mathbb{Z} \text{ y } |n| \leqslant 19000\}$
Sea a cualquier entero. Entonces,

$$\begin{aligned}
a \in A_0 &\iff \exists q \in \mathbb{Z} : a = 6q \text{ y } |a| \leqslant 19000 \\
&\iff \exists q \in \mathbb{Z} : |6q| \leqslant 19000 \\
&\iff \exists q \in \mathbb{Z} : |6q| < 19000 \ \{19000 \text{ no es múltiplo de } 6\} \\
&\iff \exists q \in \mathbb{Z} : |q| < \frac{19000}{6} \\
&\iff \exists q \in \mathbb{Z} : |q| < 3166,6 \\
&\iff |q| \leqslant 3166
\end{aligned}$$

Luego,

$$A_0 = \{n : n = 6q,\ q \in \mathbb{Z} \text{ y } |q| \leqslant 3166\}$$

y, consecuentemente, la clase de equivalencia A_0 tendrá, además del 0, 3166 números positivos y 3166 negativos, es decir un total de 6333 elementos.

⊛ $A_2 = \{n : n = 6q + 2,\ q \in \mathbb{Z} \text{ y } |n| \leqslant 19000\}$
Sea a cualquier entero. Entonces,

$$\begin{aligned}
a \in A_2 &\iff \exists q \in \mathbb{Z} : a = 6q + 2 \text{ y } |a| \leqslant 19000 \\
&\iff \exists q \in \mathbb{Z} : |6q + 2| \leqslant 19000 \\
&\iff \exists q \in \mathbb{Z} : -19000 \leqslant 6q + 2 \leqslant 19000 \\
&\iff \exists q \in \mathbb{Z} : -19002 \leqslant 6q \leqslant 18998 \\
&\iff \exists q \in \mathbb{Z} : -19002 \leqslant 6q < 18998 \ \{18998 \text{ no es múltiplo de } 6\} \\
&\iff \exists q \in \mathbb{Z} : \frac{-19002}{6} \leqslant q < \frac{18998}{6} \\
&\iff \exists q \in \mathbb{Z} : -3167 \leqslant q < 3166,3 \\
&\iff \exists q \in \mathbb{Z} : -3167 \leqslant q \leqslant 3166
\end{aligned}$$

Luego,

$$A_2 = \{n : n = 6q + 2,\ q \in \mathbb{Z} \text{ y } -3167 \leqslant q \leqslant 3166\}$$

y, consecuentemente, la clase de equivalencia A_2 tendrá, además del 0, 3166 números positivos y 3167 negativos, es decir un total de 6334 elementos.

⊛ $A_4 = \{n : n = 6q + 4,\ q \in \mathbb{Z} \text{ y } |n| \leqslant 19000\}$
Sea a cualquier entero. Entonces,

$$\begin{aligned}
a \in A_4 &\iff \exists q \in \mathbb{Z} : a = 6q + 4 \text{ y } |a| \leqslant 19000 \\
&\iff \exists q \in \mathbb{Z} : |6q + 4| \leqslant 19000 \\
&\iff \exists q \in \mathbb{Z} : -19000 \leqslant 6q + 4 \leqslant 19000 \\
&\iff \exists q \in \mathbb{Z} : -19004 \leqslant 6q \leqslant 18996 \\
&\iff \exists q \in \mathbb{Z} : -19004 < 6q \leqslant 18996 \ \{-19004 \text{ no es múltiplo de } 6\} \\
&\iff \exists q \in \mathbb{Z} : \frac{-19004}{6} < q \leqslant \frac{18996}{6} \\
&\iff \exists q \in \mathbb{Z} : -3167,3 < q \leqslant 3166 \\
&\iff \exists q \in \mathbb{Z} : -3167 \leqslant q \leqslant 3166
\end{aligned}$$

Luego,

$$A_4 = \{n : n = 6q + 4,\ q \in \mathbb{Z} \text{ y } -3167 \leqslant q \leqslant 3166\}$$

y, consecuentemente, la clase de equivalencia A_4 tendrá, además del 0, 3166 números positivos y 3167 negativos, es decir un total de 6334 elementos.

♦

Lección 11

Relaciones de Orden

Estudiamos en esta lección una de las relaciones binarias más importantes que pueden definirse en un conjunto, las relaciones de orden.

11.1 Generalidades

Definiremos el concepto principal de la lección y resolveremos algunos ejemplos.

11.1.1 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 11.1 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 11.1

Probar que la relación "menor o igual" definida en el conjunto $\mathbb{Z}$ de los números enteros es de orden.

Solución.

Según vimos en 9.12, 9.16 y 9.19, 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.

♦♦♦

11.2 Conjuntos Ordenados

11.2.1 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,

$$a \text{ y } b \text{ no son comparables} \iff a \not\preccurlyeq b \text{ y } b \not\preccurlyeq a$$

♦

11.2.2 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 11.2

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 11.3

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 (9.13) 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 9.13, 9.17 y 9.20, 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 11.2.2, la relación de divisibilidad es de orden parcial.

♦

Ejemplo 11.4

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 3.2.6,

$$B \subseteq B$$

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,

$$\left.\begin{array}{ccc} B \preccurlyeq C & \iff & B \subseteq C \\ \wedge & & \wedge \\ C \preccurlyeq B & \iff & C \subseteq B \end{array}\right\} \overset{3.2.5}{\Longrightarrow} B = C$$

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,

$$\left.\begin{array}{ccc} B \preccurlyeq C & \Longleftrightarrow & B \subseteq C \\ \wedge & & \wedge \\ C \preccurlyeq D & \Longleftrightarrow & C \subseteq D \end{array}\right\} \overset{3.2.7}{\Longrightarrow} \quad B \subseteq D \quad \Longleftrightarrow \quad B \preccurlyeq D$$

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 11.5

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,

$$\begin{array}{lll} d \in D_a & \Longleftrightarrow & d \text{ es divisor de } a \\ & \Longleftrightarrow & (d \text{ es divisor de } a) \wedge (a \text{ es divisor de } b) \quad \{\text{Hipótesis}\} \\ & \Longrightarrow & d \text{ es divisor de } b \quad \{\text{Transitividad}\} \\ & \Longleftrightarrow & d \in D_b \end{array}$$

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, (3.2.1),

$$D_a \subseteq D_b$$

⁕ $D_a \subseteq D_b \Longrightarrow a$ 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 11.6

En el conjunto de los enteros positivos, $\mathbb{Z}^+$, se consideran dos relaciones:

1 La relación de orden de divisibilidad,

$$\forall n_1, n_2, (n_1 \succcurlyeq_1 n_2 \longleftrightarrow n_1 \text{ es múltiplo de } n_2)$$

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, $M_a = \{n : n \text{ es múltiplo de } a\} = \{n : n = aq, q \in \mathbb{Z}^+\}$.

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, (3.2.1),

$$M_a \subseteq M_b$$

⋇ $M_a \subseteq M_b \Longrightarrow a$ es múltiplo de b.

En efecto, por la reflexividad de la relación de orden de divisibilidad,

$$\begin{aligned} a \text{ es múltiplo de } a &\iff a \in M_a \\ &\Longrightarrow a \in M_b \qquad \{\text{Hipótesis}\} \\ &\iff a \text{ es múltiplo de } b \end{aligned}$$

Como a y b eran cualesquiera de $\mathbb{Z}^+$, hemos probado que

$$\forall n_1, n_2, (n_1 \text{ es múltiplo de } n_2 \longleftrightarrow M_{n_1} \subseteq M_{n_2})$$

es decir las relaciones de orden $\succcurlyeq_1$ y $\succcurlyeq_2$ son equivalentes.

♦

Ejemplo 11.7

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,

$$\left.\begin{array}{l} a \preccurlyeq b \iff b = a^{q_1}, q_1 \in \mathbb{Z}^+ \\ \text{y} \\ b \preccurlyeq a \iff a = b^{q_2}, q_2 \in \mathbb{Z}^+ \end{array}\right\} \Longrightarrow b = (b^{q_2})^{q_1}$$

$$\iff b = b^{q_1 q_2}$$

$$\Longrightarrow \begin{cases} q_1 q_2 = 1 \\ \text{ó} \\ b = 1 \\ \text{ó} \\ b = -1, \ q_1 \text{ impar y } q_2 \text{ impar} \end{cases}$$

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

$$\left.\begin{array}{rcl} b & = & a^{q_1} \\ \text{y} & & \\ b & = & 1 \end{array}\right\} \implies 1 = a^{q_1},\ q_1 \in \mathbb{Z}^+ \implies a = 1$$

$$\left.\begin{array}{rcl} a & = & b^{q_2} \\ \text{y} & & \\ b & = & 1 \end{array}\right\} \implies a = 1^{q_2},\ q_2 \in \mathbb{Z}^+ \implies a = 1$$

$$\left.\begin{array}{l} \\ \\ \\ \\ \\ \end{array}\right\} \implies a = b$$

– Si $b = -1$ y $q_1, q_2 \in \mathbb{Z}^+$, impares,

$$\left.\begin{array}{rcl} b & = & a^{q_1} \\ \text{y} & & \\ b & = & -1 \end{array}\right\} \implies -1 = a^{q_1},\ q_1 \text{ impar} \implies a = -1$$

$$\left.\begin{array}{rcl} a & = & b^{q_2} \\ \text{y} & & \\ b & = & -1 \end{array}\right\} \implies a = (-1)^{q_2},\ q_2 \text{ impar} \implies a = -1$$

$$\left.\begin{array}{l} \\ \\ \\ \\ \\ \end{array}\right\} \implies a = b$$

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.

♦

11.2.3 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 $\preccurlyeq$.

♦♦♦

11.3 Representación Gráfica

11.3.1 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.*

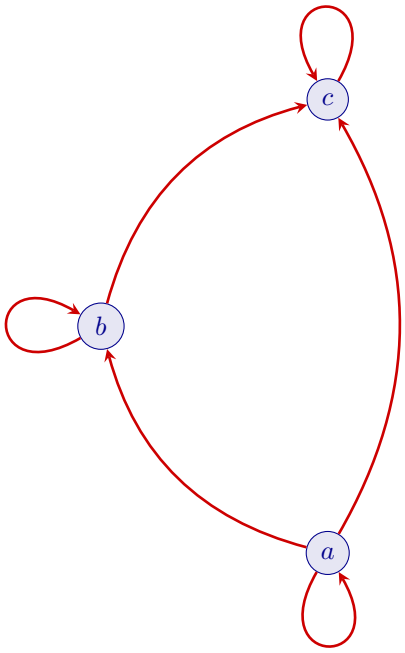
♦

Ejemplo 11.8

Consideremos definida en el conjunto $A = \{a, b, c\}$ la siguiente relación de orden

$$\preccurlyeq = \{(a,a), (a,b), (a,c), (b,b), (b,c), (c,c)\}\,.$$

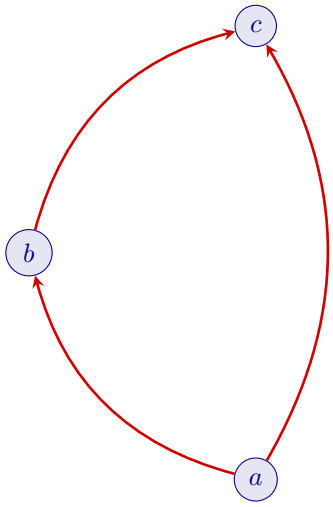
Su grafo dirigido sería:



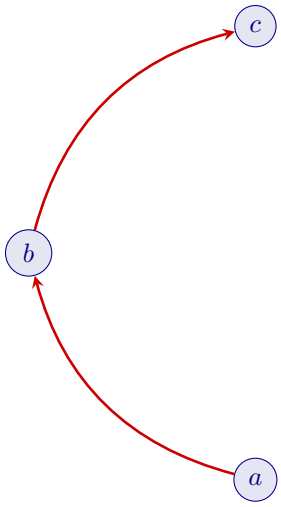
Obtener el diagrama de Hasse de la relación mediante la aplicación de los criterios anteriores.

Solución.

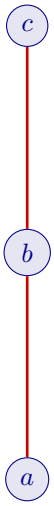
1. Eliminamos todos los bucles.



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.



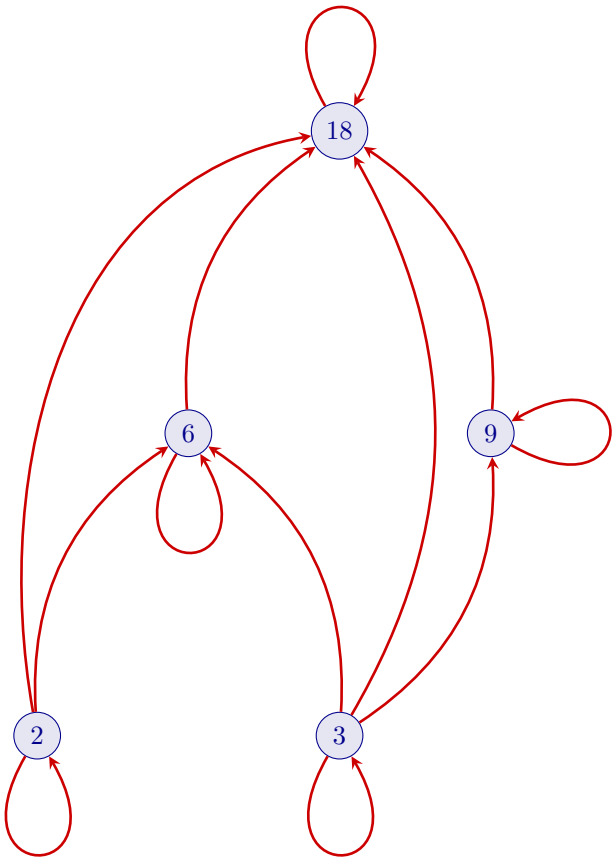
3. Eliminamos las direcciones y ya tenemos el diagrama de Hasse.



♦

Ejemplo 11.9

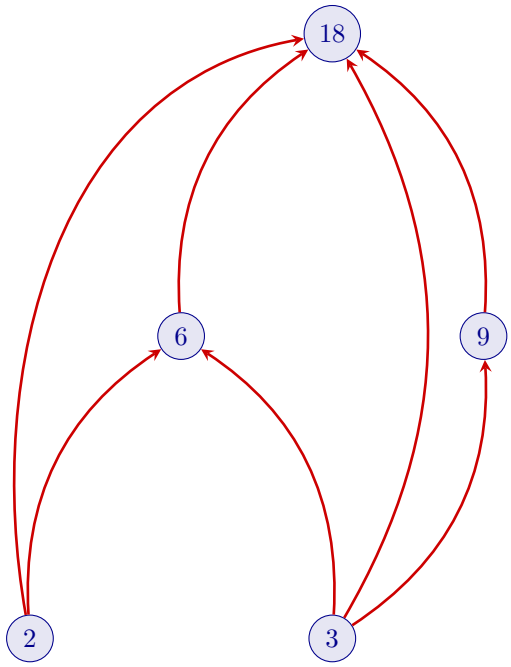
El siguiente grafo dirigido representa el conjunto $A = \{2, 3, 6, 9, 18\}$ ordenado por la relación de divisibilidad.



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.

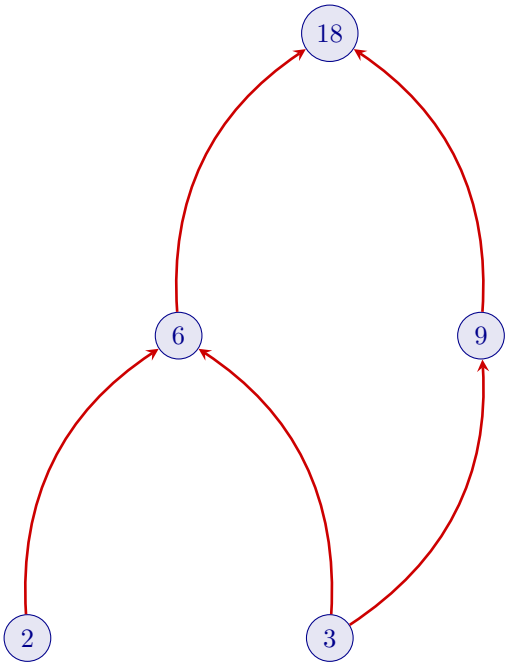


2. Eliminamos los cierres transitivos.

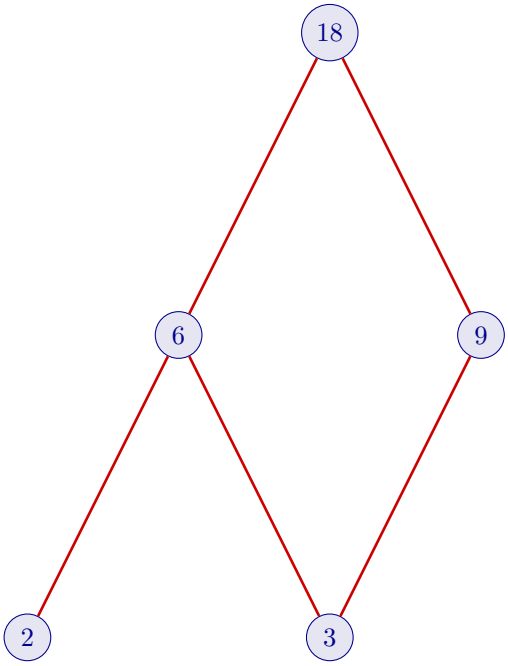
$$\left.\begin{array}{l}2 \text{ divide a } 6\\ \text{y}\\ 6 \text{ divide a } 18\end{array}\right\} \Longrightarrow \text{2 divide a 18. Eliminamos el arco que une 2 con 18.}$$

$$\left.\begin{array}{l}3 \text{ divide a } 6\\ \text{y}\\ 6 \text{ divide a } 18\end{array}\right\} \Longrightarrow \text{3 divide a 18. Eliminamos el arco que une 3 con 18.}$$

$$\left.\begin{array}{l}3 \text{ divide a } 9\\ \text{y}\\ 9 \text{ divide a } 18\end{array}\right\} \Longrightarrow \text{3 divide a 18. Eliminamos el arco que une 3 con 18.}$$



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 11.10

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) $\preccurlyeq = \{(1,1),(1,2),(2,2),(2,4),(1,3),(3,3),(3,4),(1,4),(4,4)\}$.

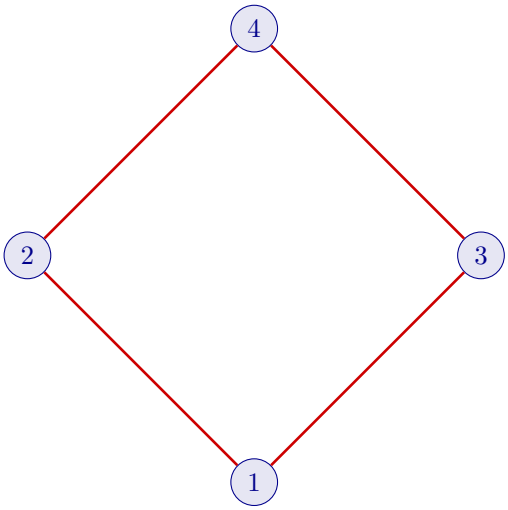
Observemos que

$$1 \preccurlyeq 2 \preccurlyeq 4$$

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,

$$a \preccurlyeq c \preccurlyeq d$$

$$a \preccurlyeq c \preccurlyeq e$$

$$b \preccurlyeq c \preccurlyeq e$$

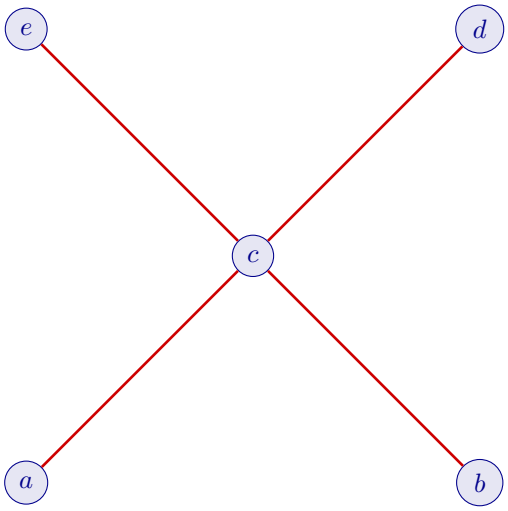
$$b \preccurlyeq c \preccurlyeq d$$

pero,

$$a \not\preccurlyeq b \quad \text{y} \quad b \not\preccurlyeq a$$

$$d \not\preccurlyeq e \quad \text{y} \quad e \not\preccurlyeq d$$

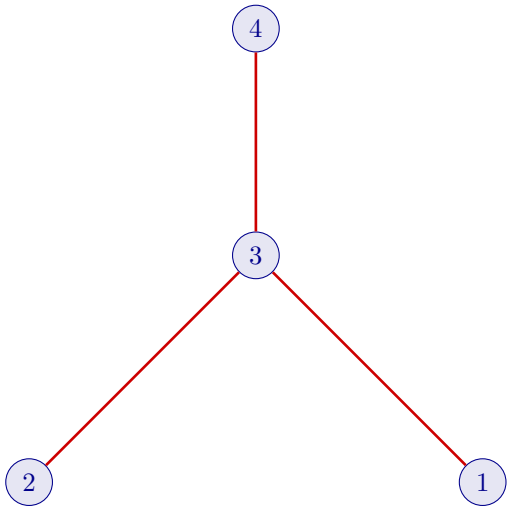
es decir, a y b no están relacionados y tampoco d y e. De todo esto se sigue que el diagrama de Hasse es:



♦

Ejemplo 11.11

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) $\preccurlyeq = \{(1,1),(1,2),(1,3),(1,4),(2,2),(2,3),(2,4),(3,3),(3,4),(4,4)\}$

♦♦♦

11.4 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 $(B \subseteq A)$.

11.4.1 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 11.12

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 una condición necesaria y suficiente para que $a \in \mathbb{Z}^+$ sea minimal de un conjunto de enteros positivos, A, 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,

$$\forall n_1, n_2, (n_1 \preccurlyeq n_2 \longleftrightarrow n_1 \in D_{n_2})\,.$$

Según la definición (11.4.1),

> *a es minimal de A respecto de la relación $\preccurlyeq$, si ningún elemento de A es estrictamente anterior al propio a.*

es decir,

$$a \text{ es minimal de } A \Longleftrightarrow \forall n, (n \in A \longrightarrow n \not\prec a)$$

Sea b cualquier entero positivo, entonces,

$$\begin{aligned}
b \in A \longrightarrow b \not\prec a &\iff b \in A \longrightarrow \neg\,(b \prec a)\\
&\iff b \in A \longrightarrow \neg\,(b \preccurlyeq a \wedge b \neq a)\\
&\iff b \in A \longrightarrow (\neg\,(b \preccurlyeq a) \vee b = a)\\
&\iff b \in A \longrightarrow (b \preccurlyeq a \longrightarrow b = a)\\
&\iff (b \in A \wedge b \preccurlyeq a) \longrightarrow b = a\\
&\iff (b \in A \wedge b \in D_a) \longrightarrow b \in \{a\}\\
&\iff b \in (A \cap D_a) \longrightarrow b \in \{a\}
\end{aligned}$$

y como b era cualquiera, tendremos que

$$\forall n, (n \in A \longrightarrow n \not\prec a) \Longleftrightarrow \forall n, (n \in (A \cap D_a) \longrightarrow n \in \{a\})$$

y, por definición de inclusión de conjuntos,

$$\forall n, (n \in (A \cap D_a) \longrightarrow n \in \{a\}) \Longleftrightarrow A \cap D_a \subseteq \{a\}$$

luego,

$$\forall n, (n \in A \longrightarrow n \not\prec a) \Longleftrightarrow A \cap D_a \subseteq \{a\}$$

Por otra parte,

$$\left.\begin{array}{l} a \in A \\ \text{y} \\ a \in D_a \end{array}\right\} \implies a \in A \cap D_a \implies \{a\} \subseteq A \cap D_a$$

de aquí que

$$A \cap D_a \subseteq \{a\} \Longleftrightarrow \left\{\begin{array}{l} A \cap D_a \subseteq \{a\} \\ \text{y} \\ \{a\} \subseteq A \cap D_a \end{array}\right\} \Longleftrightarrow A \cap D_a = \{a\}$$

y, por lo tanto,

$$\forall n, (n \in A \longrightarrow n \not\prec a) \Longleftrightarrow A \cap D_a = \{a\}$$

luego,

$$a \text{ es minimal de } A \Longleftrightarrow A \cap D_a = \{a\}$$

es decir,

> *Una condición necesaria y suficiente para que a sea minimal de A respecto a la relación de divisibilidad es que $A \cap D_a = \{a\}$*

siendo D_a el conjunto integrado por todos los divisores de a.

♦

Ejemplo 11.13

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 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,

$$4 \in D_{12}, \text{ por lo tanto, } 4 \preccurlyeq 12$$

$$6 \in D_{12}, \text{ por lo tanto, } 6 \preccurlyeq 12$$

$$12 \in D_{12}, \text{ por lo tanto, } 12 \preccurlyeq 12$$

Según el ejemplo anterior, 11.12, si a es un entero positivo cualquiera,

$$a \text{ es minimal de } A \iff A \cap D_a = \{a\}$$

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.

♦

11.4.2 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,

$$b \textit{ es maximal de } B \iff \forall x, (x \in B \longrightarrow x \not\succ b)$$

♦

Ejemplo 11.14

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 una condición necesaria y suficiente para que $a \in \mathbb{Z}^+$ sea maximal de un conjunto de enteros positivos, A, 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, $M_{n_1} = \{n : n = n_1 q; q \in \mathbb{Z}^+\}$.

Según la definición (11.4.2),

> *a es maximal de A respecto de la relación $\preccurlyeq$, si ningún elemento de A es estrictamente posterior a a.*

es decir,

$$a \text{ es maximal de } A \Longleftrightarrow \forall n, (n \in A \longrightarrow n \not\succ a)$$

Sea b cualquier entero positivo, entonces,

$$\begin{aligned}
b \in A \longrightarrow b \not\succ a \quad &\Longleftrightarrow \quad b \in A \longrightarrow \neg\,(b \succ a) \\
&\Longleftrightarrow \quad b \in A \longrightarrow \neg\,(b \succcurlyeq a \wedge b \neq a) \\
&\Longleftrightarrow \quad b \in A \longrightarrow (\neg\,(b \succcurlyeq a) \vee b = a) \\
&\Longleftrightarrow \quad b \in A \longrightarrow (b \succcurlyeq a \longrightarrow b = a) \\
&\Longleftrightarrow \quad (b \in A \wedge b \succcurlyeq a) \longrightarrow b = a \\
&\Longleftrightarrow \quad (b \in A \wedge b \in M_a) \longrightarrow b \in \{a\} \\
&\Longleftrightarrow \quad b \in (A \cap M_a) \longrightarrow b \in \{a\}
\end{aligned}$$

y como b era cualquiera, tendremos que

$$\forall n, (n \in A \longrightarrow n \not\succ a) \Longleftrightarrow \forall n, (n \in (A \cap M_a) \longrightarrow n \in \{a\})$$

y, por definición de inclusión de conjuntos,

$$\forall n, (n \in (A \cap M_a) \longrightarrow n \in \{a\}) \Longleftrightarrow A \cap M_a \subseteq \{a\}$$

luego,

$$\forall n, (n \in A \longrightarrow n \not\succ a) \Longleftrightarrow A \cap M_a \subseteq \{a\}$$

Por otra parte,

$$\left.\begin{array}{l} a \in A \\ \text{y} \\ a \in M_a \end{array}\right\} \implies a \in A \cap M_a \implies \{a\} \subseteq A \cap M_a$$

de aquí que

$$A \cap M_a \subseteq \{a\} \Longleftrightarrow \left\{ \begin{array}{l} A \cap M_a \subseteq \{a\} \\ \text{y} \\ \{a\} \subseteq A \cap M_a \Longleftrightarrow A \cap M_a = \{a\} \end{array} \right\}$$

y, por lo tanto,

$$\forall n, (n \in A \longrightarrow n \not\succ a) \Longleftrightarrow A \cap M_a = \{a\}$$

luego,

$$a \text{ es maximal de } A \Longleftrightarrow A \cap M_a = \{a\}$$

es decir,

> *Una condición necesaria y suficiente para que a sea maximal de A respecto a la relación de divisibilidad es que $A \cap M_a = \{a\}$*

siendo M_a el conjunto formado por todos los múltiplos de a.

♦

Ejemplo 11.15

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,

$$n_1 \preccurlyeq n_2 \longleftrightarrow n_1 \text{ es divisor de } n_2$$

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, $M_{n_1} = \{n : n = n_1 q; q \in \mathbb{Z}^+\}$.

Según el ejemplo anterior, 11.14, si a es un entero positivo cualquiera,

$$a \text{ es maximal de } A \Longleftrightarrow A \cap M_a = \{a\}$$

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.

♦

11.4.3 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.

♦

11.4.4 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 11.16

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, 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, (11.4.4),

> *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,

$$
\begin{aligned}
b \text{ es mínimo de } A &\iff (b \in A) \wedge (b \in D_a, \text{ para todos y cada uno de los } a \text{ de } A) \\
&\iff (b \in A) \wedge \left(b \in \bigcap_{a \in A} D_a \right) \\
&\iff (b \in A) \wedge (b \in D_6 \cap D_{12} \cap D_{18} \cap D_{24} \cap D_{36} \cap D_{54} \cap D_{72} \cap D_{108} \cap D_{216}) \\
&\qquad \left\{ \begin{array}{l} \text{Por (11.5), } D_6 \subseteq D_{12} \subseteq D_{36} \subseteq D_{72} \subseteq D_{216}, \text{ luego} \\ D_6 \cap D_{12} \cap D_{36} \cap D_{72} \cap D_{216} = D_6 \end{array} \right\} \\
&\implies (b \in A) \wedge (b \in D_6 \cap D_{18} \cap D_{24} \cap D_{54} \cap D_{108}) \\
&\qquad \left\{ \begin{array}{l} \text{Por (11.5), } D_6 \subseteq D_{18} \subseteq D_{54} \subseteq D_{108}, \text{ luego} \\ D_6 \cap D_{18} \cap D_{54} \cap D_{108} = D_6 \end{array} \right\} \\
&\implies (b \in A) \wedge (b \in D_6 \cap D_{24}) \\
&\qquad \left\{ \begin{array}{l} \text{Por (11.5), } D_6 \subseteq D_{24}, \text{ luego} \\ D_6 \cap D_{24} = D_6 \end{array} \right\} \\
&\iff (b \in A \cap D_6) \\
&\iff b \in (\{6, 12, 18, 24, 36, 54, 72, 108, 216\} \cap \{1, 2, 3, 6\}) \\
&\iff b \in \{6\} \\
&\iff b = 6
\end{aligned}
$$

Concluyendo, el mínimo del conjunto A ordenado por la relación de divisibilidad es el 6. Lo notaremos,

$$\text{Min}\,(A) = 6$$

♦

11.4.5 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 11.17

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,

$$n_1 \preccurlyeq n_2 \iff n_1 \text{ es divisor de } n_2$$

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 máximo, (11.4.5),

> *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,

$$\begin{aligned}
b \text{ es máximo de } A &\iff (b \in A) \wedge (b \in M_a, \text{ para todos y cada uno de los } a \text{ de } A) \\
&\iff (b \in A) \wedge \left(b \in \bigcap_{a \in A} M_a \right) \\
&\iff (b \in A) \wedge (b \in (M_{216} \cap M_{108} \cap M_{72} \cap M_{54} \cap M_{36} \cap M_{24} \cap M_{18} \cap M_{12} \cap M_6)) \\
&\qquad \left\{ \begin{array}{l} \text{Por (11.6), } M_{216} \subseteq M_{108} \subseteq M_{54} \subseteq M_{18} \subseteq M_6, \text{ luego} \\ M_{216} \cap M_{108} \cap M_{54} \cap M_{18} \cap M_6 = M_{216} \end{array} \right\} \\
&\iff (b \in A) \wedge (b \in (M_{216} \cap M_{72} \cap M_{36} \cap M_{24} \cap M_{18} \cap M_{12})) \\
&\qquad \left\{ \begin{array}{l} \text{Por (11.6), } M_{216} \subseteq M_{72} \subseteq M_{36} \subseteq M_{18}, \text{ luego} \\ M_{216} \cap M_{72} \cap M_{36} \cap M_{18} = M_{216} \end{array} \right\} \\
&\iff (b \in A) \wedge (M_{216} \cap M_{24} \cap M_{12}) \\
&\qquad \left\{ \begin{array}{l} \text{Por (11.6), } M_{216} \subseteq M_{24} \subseteq M_{12}, \text{ luego} \\ M_{216} \cap M_{24} \cap M_{12} = M_{216} \end{array} \right\} \\
&\iff (b \in A) \wedge (M_{216}) \\
&\iff b \in (A \cap M_{216}) \\
&\iff b \in (\{6, 12, 18, 24, 36, 54, 72, 108, 216\} \cap \{n : n = 216q, \ q \in \mathbb{Z}^+\}) \\
&\iff b \in \{216\} \\
&\iff b = 216
\end{aligned}$$

Concluyendo, el máximo del conjunto A ordenado por la relación de divisibilidad es el 216. Lo notaremos,

$$\text{Máx}\,(A) = 216$$

♦

11.4.6 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.

♦

11.4.7 Cotas Inferiores

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 11.18

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, 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 a cualquier entero positivo. Entonces, según la definición de cota inferior, (11.4.7),

> *a es cota inferior de A en $\mathbb{Z}^+$ respecto de la relación $\preccurlyeq$, si a es anterior a todos los elementos de A.*

y bastaría con que a 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,

> *a es cota inferior de A en $\mathbb{Z}^+$ respecto de la relación $\preccurlyeq$, si a es anterior a los elementos minimales de A.*

lo cual "traducido" a nuestra relación querrá decir,

> *a es cota inferior de A en $\mathbb{Z}^+$ respecto de la relación de divisibilidad, si a es divisor de los elementos minimales de A.*

Calculemos, pues, los elementos minimales del conjunto A. Por 11.12, si b es cualquier entero positivo,

$$b \text{ es minimal de } A \iff A \cap D_b = \{b\}\,.$$

Entonces,

$$A \cap D_{12} = \{12, 18, 24, 36, 54, 72, 108\} \cap \{1, 2, 3, 4, 6, 12\} = \{12\}$$

$$A \cap D_{18} = \{12, 18, 24, 36, 54, 72, 108\} \cap \{1, 2, 3, 6, 9, 18\} = \{18\}$$

y ninguno de los restantes números de A puede ser minimal ya que todos son múltiplos de 12 o de 18 lo cual significaría que bien el 12, bien el 18 serían estrictamente anteriores a ellos, luego el 12 y el 18 son los elementos minimales de A de aquí que

> *a es cota inferior de A en $\mathbb{Z}^+$ respecto de la relación de divisibilidad, si a es divisor de* 12 *y* 18.

Sea, pues, $C_{\text{inf}}(A)$ el conjunto formado por todas las cotas inferiores de A y sea a cualquier entero positivo. Entonces,

$$\begin{aligned}
a \in C_{\text{inf}}(A) &\iff \begin{cases} a \text{ es divisor de } 12 \\ \text{y} \\ a \text{ es divisor de } 18 \end{cases} \\
&\iff \begin{cases} a \in D_{12} \\ \text{y} \\ a \in D_{18} \end{cases} \\
&\iff a \in D_{12} \cap D_{18} \\
&\iff a \in \{1, 2, 3, 4, 6, 12\} \cap \{1, 2, 3, 6, 9, 18\} \\
&\iff a \in \{1, 2, 3, 6\}
\end{aligned}$$

Como a era cualquiera, tendremos que el conjunto de las cotas inferiores del conjunto A ordenado por la relación de divisibilidad es

$$C_{\text{inf}}(A) = \{1, 2, 3, 6\}$$

♦

11.4.8 Cotas Superiores

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 11.19

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 a cualquier entero positivo. Entonces, según la definición de cota inferior, (11.4.8),

> *a es cota superior de A en $\mathbb{Z}^+$ respecto de la relación $\preccurlyeq$, si a es posterior a todos los elementos de A.*

y bastaría con que a fuera posterior a los elementos maximales de A ya que, por definición de maximal, todos los demás elementos de A serán anteriores, o sea,

a es cota superior de A en $\mathbb{Z}^+$ respecto de la relación $\preccurlyeq$, si a es posterior a los elementos maximales de A.

lo cual "traducido" a nuestra relación querrá decir,

a es cota superior de A en $\mathbb{Z}^+$ respecto de la relación de divisibilidad, si a es múltiplo de los elementos maximales de A.

Calculamos, pues, los elementos maximales de A. Por 11.14, si b es cualquier entero positivo,

$$b \text{ es maximal de } A \iff A \cap M_b = \{b\}\,.$$

Entonces,

$$A \cap M_{72} = \{12, 18, 24, 36, 54, 72, 108\} \cap \{n : n = 72q,\ q \in \mathbb{Z}^+\} = 72$$
$$A \cap M_{108} = \{12, 18, 24, 36, 54, 72, 108\} \cap \{n : n = 108q,\ q \in \mathbb{Z}^+\} = 108$$

y ninguno de los restantes números de A puede ser maximal ya que todos son divisores de 72 o de 108 lo cual significaría que bien el 72, bien el 108 serían estrictamente posteriores a ellos, luego el 72 y el 108 son los elementos maximales de A de aquí que

a es cota superior de A en $\mathbb{Z}^+$ respecto de la relación de divisibilidad, si a 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 a cualquier entero positivo. Entonces,

$$\begin{aligned}
a \in C_{\sup}(A) &\iff \begin{cases} a \text{ es múltiplo de } 72 \\ \text{y} \\ a \text{ es múltiplo de } 108 \end{cases} \\
&\iff a \text{ es múltiplo del mínimo común múltiplo de } 72 \text{ y } 108 \\
&\iff \exists q \in \mathbb{Z}^+ : a = \text{m.c.m.}(72, 108) \cdot q \\
&\iff \exists q \in \mathbb{Z}^+ : a = \text{m.c.m.}(2^3 \cdot 3^2, 2^2 \cdot 3^3) \cdot q \\
&\iff \exists q \in \mathbb{Z}^+ : a = 2^3 \cdot 3^3 \cdot q \\
&\iff \exists q \in \mathbb{Z}^+ : a = 216 \cdot q \\
&\iff a \in \{n : n = 216q,\ q \in \mathbb{Z}^+\}
\end{aligned}$$

Consecuentemente, y al ser a 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,

$$C_{\sup}\,(A) = M_{216}$$

♦

11.4.9 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.

♦

11.4.10 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:

$$\begin{aligned} a \text{ es el ínfimo de } B \text{ en } A &\iff a \text{ es el máximo del conjunto de las cotas inferiores de } B \text{ en } A \\ &\iff (a \in C_{\inf}(B)) \wedge (\forall x, (x \in C_{\inf}(B) \longrightarrow a \succcurlyeq x)) \end{aligned}$$

♦

11.4.11 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 11.20

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, (11.4.10), 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 11.18 hemos obtenido que las cotas inferiores de A son los divisores de 6, es decir,

$$C_{\inf}(A) = D_6$$

tendremos que

$$\begin{aligned}
b \text{ es el ínfimo de } A \text{ en } \mathbb{Z}^+ &\iff (b \in C_{\inf}(A)) \wedge \left(b \in \bigcap_{a \in C_{\inf}(A)} M_a\right) \\
&\iff (b \in D_6) \wedge \left(b \in \bigcap_{a \in D_6} M_a\right) \\
&\iff b \in (D_6 \cap (M_1 \cap M_2 \cap M_3 \cap M_6)) \\
&\qquad \{M_6 \subseteq M_3 \subseteq M_1 \Longrightarrow M_1 \cap M_3 \cap M_6 = M_6\} \\
&\iff b \in (D_6 \cap (M_2 \cap M_6)) \\
&\qquad \{M_6 \subseteq M_2 \Longrightarrow M_2 \cap M_6 = M_6\} \\
&\iff b \in (D_6 \cap M_6) \\
&\iff b \in \{6\} \\
&\iff b = 6
\end{aligned}$$

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, (11.4.11), 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 11.19 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,

$$\text{Sup}\,(A) = 216$$

♦

11.4.12 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,

$$s_1 = s_2$$

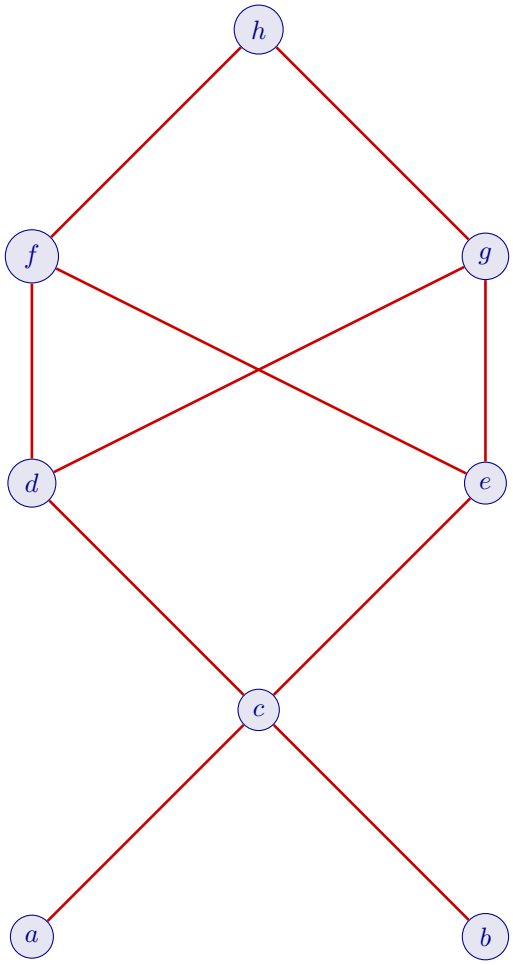
y el supremo, si existe, es único.

De una forma similar se prueba que el ínfimo de un conjunto ordenado, si existe, es único.

♦

Ejemplo 11.21

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

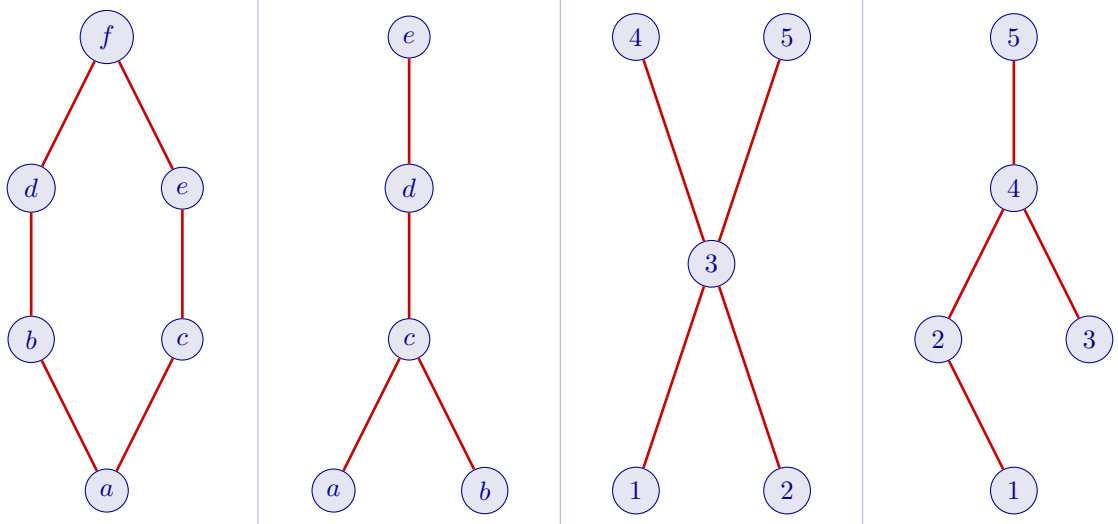
1. c es cota superior de B_2 en A.
2. c es el máximo del conjunto de las cotas inferiores.

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 11.22

Determinar maximales, minimales, máximo y mínimo de los conjuntos ordenados cuyo diagrama de Hasse es el siguiente:



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 11.23

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 11.24

Los elementos característicos del conjunto $A = \{12, 18, 24, 36, 54, 72, 108\}$ ordenado por la relación de divisibilidad son:

- ⁕ Minimales. 12 y 18.
- ⁕ Maximales. 72 y 108.
- ⁕ Cotas inferiores. $C_{\text{inf}}(A) = \{1, 2, 3, 6\}$.
- ⁕ Cotas superiores. $C_{\text{sup}}(A) = \{n : n = 216q,\ q \in \mathbb{Z}^+\}$.
- ⁕ Ínfimo. $\text{Ínf}(A) = 6$.
- ⁕ Supremo. $\text{Sup}(A) = 216$.

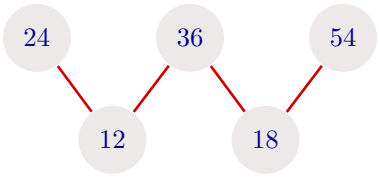
Hacer, de forma razonada, un diagrama de Hasse que represente la ordenación del conjunto anterior.

Solución.

Comenzaremos el diagrama situando en un primer nivel a los minimales del conjunto, 12 y 18.

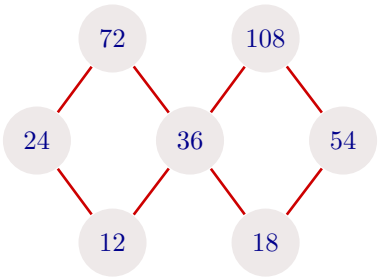
Situaremos ahora los elementos posteriores a los minimales.

- Inmediatamente posteriores al 12. Serán los primeros múltiplos de 12, es decir, $12 \cdot 2 = 24$ y $12 \cdot 3 = 36$.
- Inmediatamente posteriores al 18. Serán los primeros múltiplos de 18, es decir, $18 \cdot 2 = 36$ y $18 \cdot 3 = 54$.

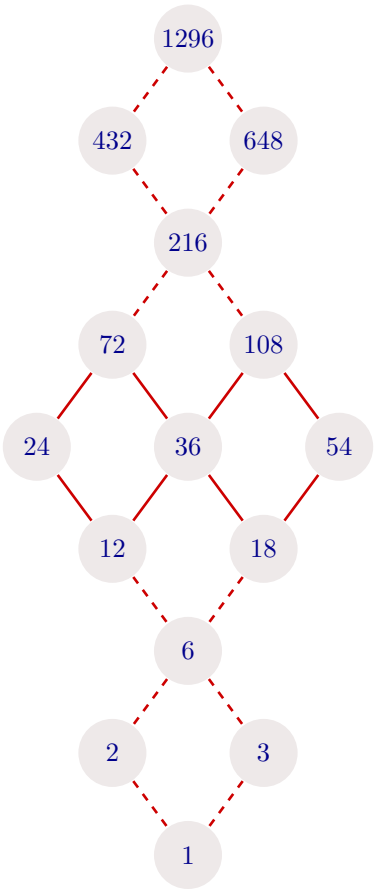


Ahora sólo quedan por situar los maximales.

- 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.


1296
432
648
216
72
108
24
36
54
12
18
6
2
3
1

♦♦♦

Lección 12

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.

12.1 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 $f, g, h, \ldots$.

12.1.1 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 $Dom(f) = A$, 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.

$$f : A \longrightarrow B \text{ es función} \iff \begin{cases} 1.\ \forall a \in A,\ \exists b \in B : f(a) = b \\ y \\ 2.\ \forall a \in A, [f(a) = b_1 \ \wedge\ f(a) = b_2 \longrightarrow b_1 = b_2] \end{cases}$$

♦

Nota 12.1 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 $f(a) \in B$.

12.1.2 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 12.1

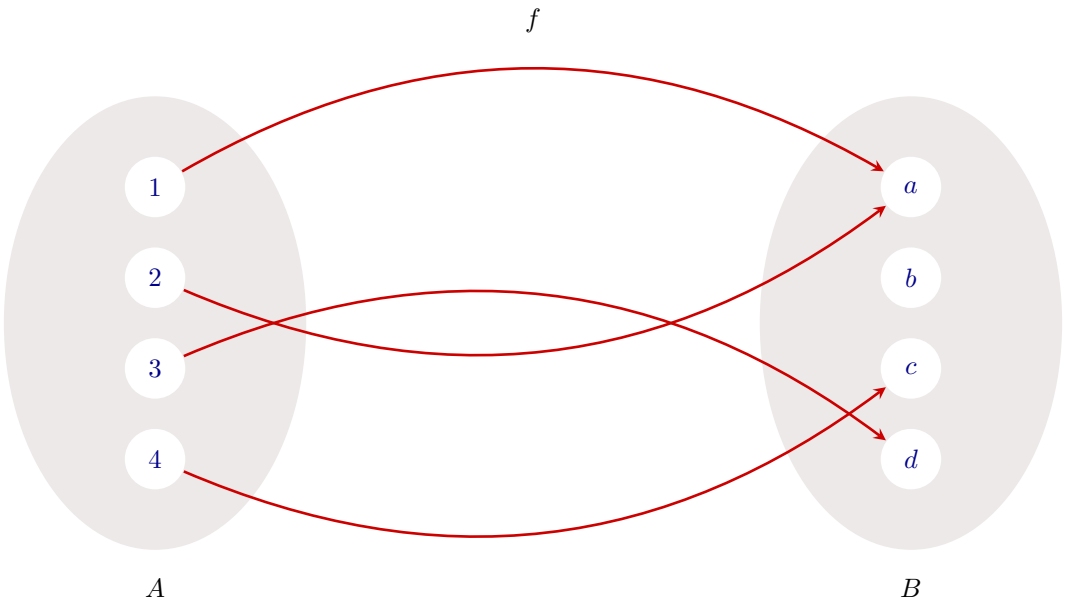
Sean $A = \{1, 2, 3, 4\}$, $B = \{a, b, c, d\}$ y $f = \{(1, a), (2, a), (3, d), (4, c)\}$. Comprobar que f es una función.

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 12.2

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 $\text{Dom}\,(f)$ en B.

♦

Ejemplo 12.3

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 12.4

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 12.5

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.

$$f : \mathbb{R} \longrightarrow \mathbb{Z} \text{ tal que } f(a) = \text{Máx}\left\{n \in \mathbb{Z} : n \leqslant a\right\},\ \forall a \in \mathbb{R}$$

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,

$$\text{Máx}\left\{n \in \mathbb{Z} : n \leqslant a\right\} = \text{Máx}\left\{n \in \mathbb{Z} : n \leqslant E(a)\right\} = E(a)$$

⁕ a es entero. En tal caso, $E(a) = a$, luego,

$$\text{Máx}\left\{n \in \mathbb{Z} : n \leqslant a\right\} = \text{Máx}\left\{n \in \mathbb{Z} : n \leqslant E(a)\right\} = E(a)$$

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,

$$f(a) = \text{Máx}\left\{n \in \mathbb{Z} : n \leqslant a\right\} = E(a) = b$$

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.

♦

12.1.3 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,

$$f = g \Longleftrightarrow f(a) = g(a),\ \forall a \in A$$

♦

12.1.4 Función Identidad

Dado un conjunto A, se define la identidad i_A como la función

$$i_A : A \longrightarrow A : i_A(a) = a,\ \forall a \in A$$

♦♦♦

12.2 Composición de Funciones

Estudiamos en este apartado una nueva función que se obtiene componiendo dos funciones conocidas. Introduciremos el concepto con un ejemplo.

Ejemplo 12.6

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

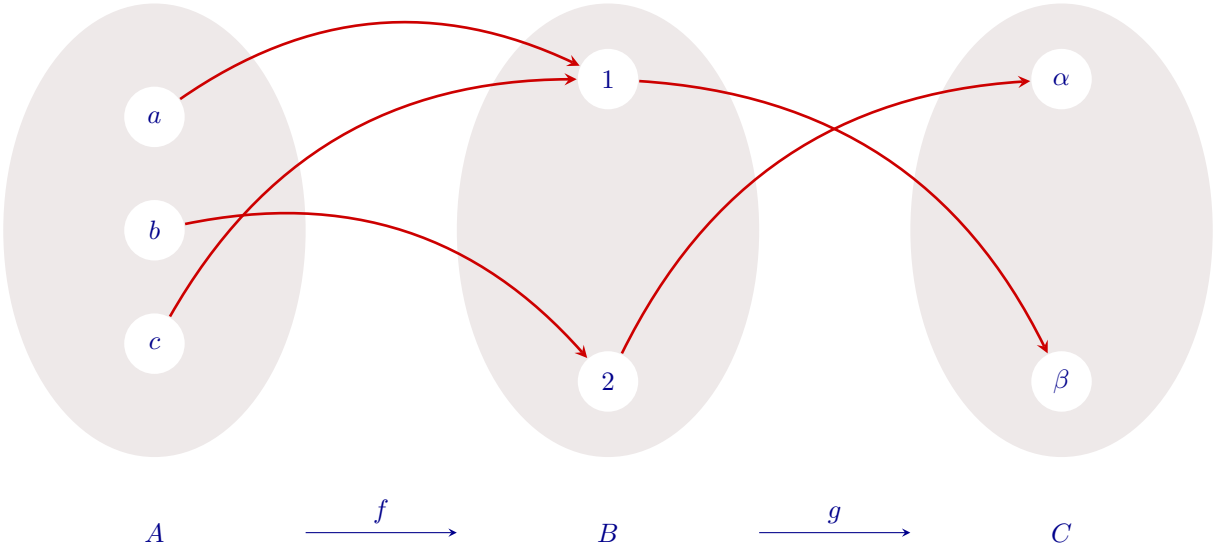
$$h : A \longrightarrow C : h(a)=\beta,\ h(b)=\alpha,\ \text{y}\ h(c)=\beta$$

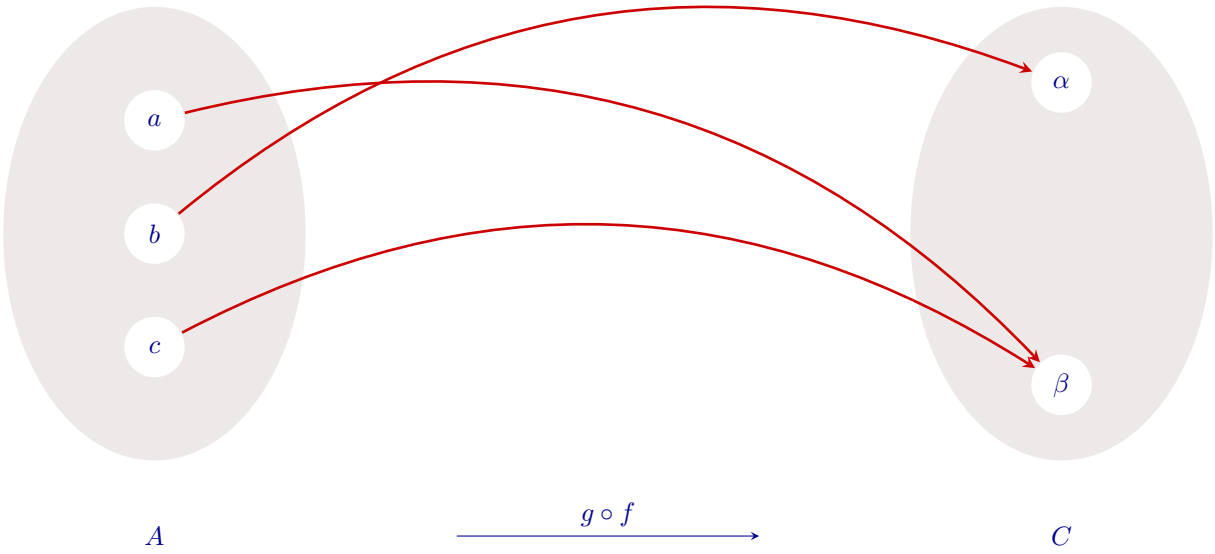
y comparamos con la anterior, tendremos

$$\begin{array}{rcl} h(a) & = & g\left[f(a)\right] \\ h(b) & = & g\left[f(b)\right] \\ h(c) & = & g\left[f(c)\right] \end{array}$$

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.





♦

12.2.1 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.

12.2.2 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,

$$\left.\begin{array}{l}(g \circ f)(a) = c_1 \\ \text{y} \\ (g \circ f)(a) = c_2\end{array}\right\} \implies \left\{\begin{array}{l} g\,[f(a)] = c_1 \\ \text{y} \\ g\,[f(a)] = c_2\end{array}\right.$$

$$\implies \left\{\begin{array}{ll} g(b) = c_1 & \\ \text{y} & \{f \text{ función } \implies \exists b \in B : f(a) = b\} \\ g(b) = c_2 & \end{array}\right.$$

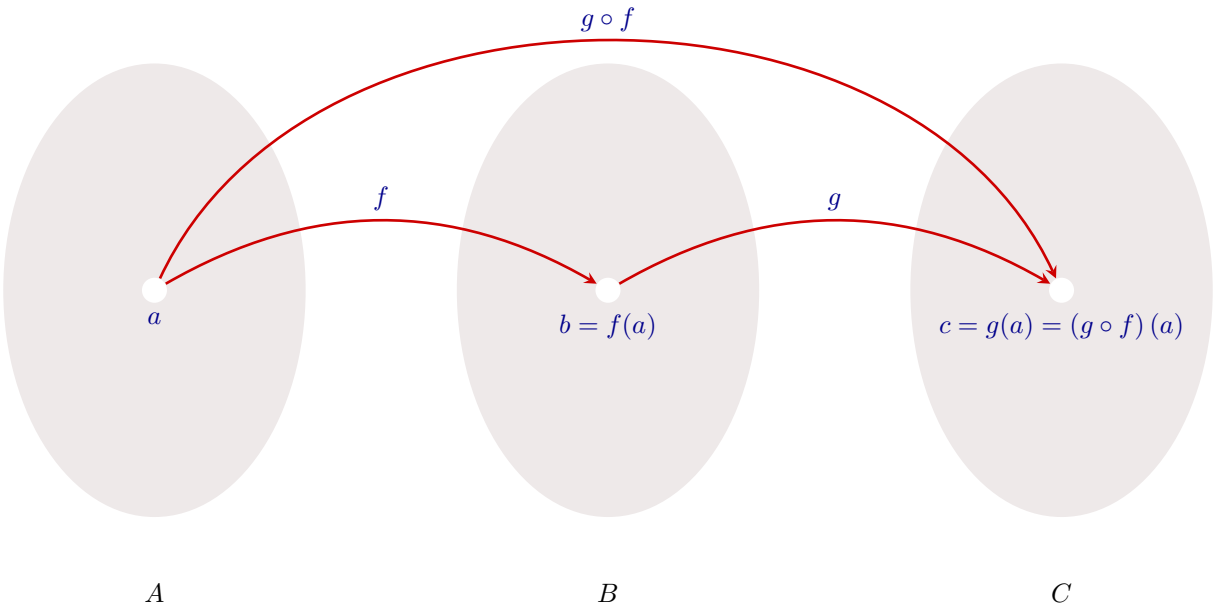
$$\implies c_1 = c_2 \qquad \{g \text{ es funcion}\}$$

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 12.7

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 12.8

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

$$(g \circ f)(x) = g\,[f(x)] = g(x^2) = x^2 + 5$$
$$(f \circ g)(x) = f\,[g(x)] = (x+5)^2 = x^2 + 10x + 25$$

luego

$$g \circ f : \mathbb{R} \longrightarrow \mathbb{R} : (g \circ f)(x) = x^2 + 5$$

y

$$f \circ g : \mathbb{R} \longrightarrow \mathbb{R} : (f \circ g)(x) = x^2 + 10x + 25$$

♦

Nota 12.2 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 12.9

Sean

$$f : \mathbb{Z}^+ \longrightarrow \mathbb{Z}^+ \text{ tal que } f(x) = x,\ \forall x \in \mathbb{Z}^+ \text{ y } g : \{0,1,2\} \longrightarrow \mathbb{Z}^+ \text{ tal que } g(x) = x,\ \forall x \in \{0,1,2\}$$

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:

$$f \circ g : \{0,1,2\} \longrightarrow \mathbb{Z}^+ \text{ tal que } (f \circ g)(x) = f\,[g(x)] = f(x) = x$$

En este caso, $f \circ g = g$.

♦

Ejemplo 12.10

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,

$$(g\circ f)(x)=g\left[f(x)\right]=\left\{\begin{array}{ll} g\left(\dfrac{x}{2}\right), & \text{si } x \text{ es par.}\\ g(0), & \text{en cualquier otro caso.}\end{array}\right\}=\begin{cases}2\dfrac{x}{2}=x, & \text{si } x \text{ es par.}\\ 2\cdot 0=0, & \text{en cualquier otro caso.}\end{cases}$$

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 $f\circ g=i_{\mathbb{Z}_0^+}$

♦

12.2.3 Asociatividad

Dadas tres aplicaciones

$$f:A\longrightarrow B \; g:B\longrightarrow C \; y \; h:C\longrightarrow D$$

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,

$$\left.\begin{array}{l} f:A\longrightarrow B\\ g:B\longrightarrow C\end{array}\right\}\Longrightarrow \left.\begin{array}{r} g\circ f:A\longrightarrow C\\ h:C\longrightarrow D\end{array}\right\}\Longrightarrow h\circ(g\circ f):A\longrightarrow D$$

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 12.11

Sean $A = B = C = \mathbb{R}$ y sean $f : A \longrightarrow B,\ g : B \longrightarrow C$ definidas por $f(a) = a - 1$ y $g(b) = b^2$. 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 12.12

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 12.13

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.

$$f_1(x) = x \qquad f_2(x) = 1 - x \qquad f_3(x) = \frac{1}{x}$$
$$f_4(x) = \frac{1}{1-x} \qquad f_5(x) = \frac{x}{x-1} \qquad f_6(x) = \frac{x-1}{x}$$

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 12.14

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,

$$\begin{array}{rcll} \forall c \in (g \circ f)(A) & \Longleftrightarrow & \exists a : a \in A\ \wedge\ (g \circ f)(a) = c & \\ & \Longleftrightarrow & \exists a : a \in A\ \wedge\ g\,[f(a)] = c & \{f \text{ es función, luego } \exists b : b \in B\ \wedge\ f(a) = b\} \\ & \Longrightarrow & \exists b : b \in B\ \wedge\ g(b) = c & \\ & \Longleftrightarrow & c \in g(B) & \end{array}$$

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,

$$\left.\begin{array}{l} (g \circ f)(x) = g\,[f(x)] = g(1) = \alpha \\ (g \circ f)(y) = g\,[f(y)] = g(2) = \alpha \end{array}\right\} \Longrightarrow (g \circ f)(A) = \{\alpha\}$$

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 12.15

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 12.16

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

$$f_X : \mathscr{U} \longrightarrow \{0,1\} \text{ tal que } f_X(x) = \left\{ \begin{array}{l} 1, \text{ si } x \in X \\ 0, \text{ si } x \notin X \end{array} \right\}$$

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

$$f_{A\setminus B} = f_A(1 - f_B)$$

12.3 Tipos de Funciones

Examinaremos en este apartado distintas clases especiales de funciones.

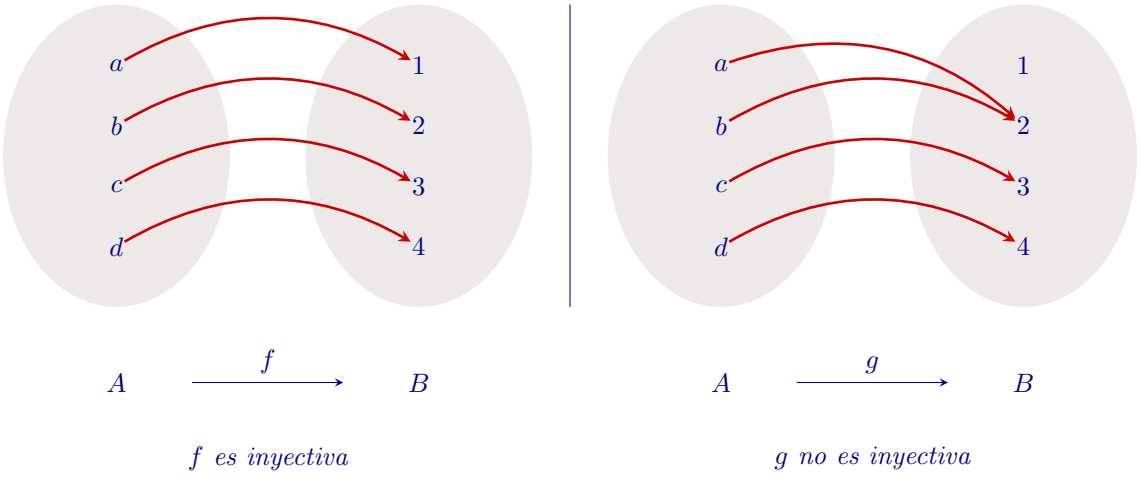
12.3.1 Función Inyectiva

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,

$$f : A \longrightarrow B \text{ es inyectiva} \Longleftrightarrow \forall a_1, a_2 \in A, [f(a_1) = f(a_2) \Longrightarrow a_1 = a_2]$$



♦

Ejemplo 12.17

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 12.18

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 12.3 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 12.19

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 12.20

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.

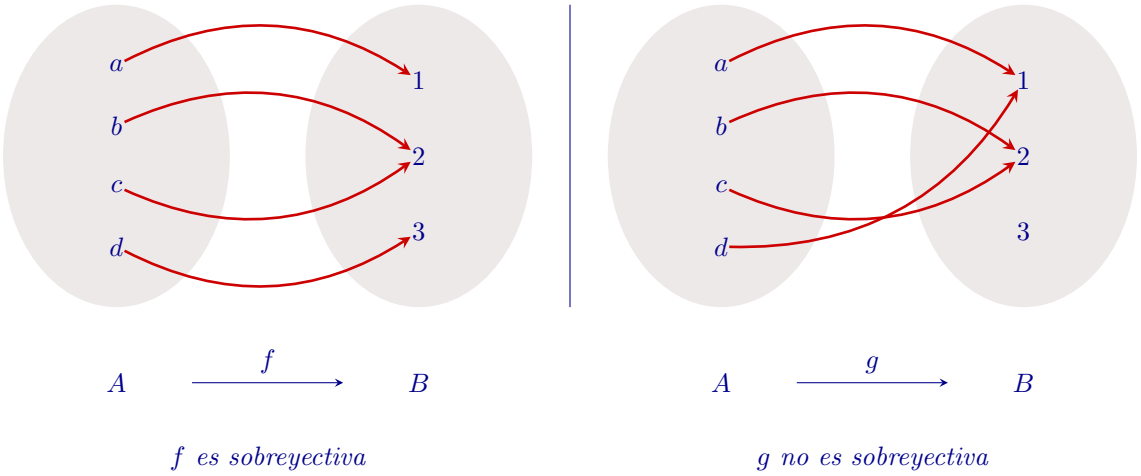
♦

12.3.2 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 12.21

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 12.4 Obsérvese lo siguiente:

$$f \text{ es suprayectiva} \iff \forall b \in B,\ \exists a \in A : f(a) = b$$

si negamos ambos miembros, tendremos

$$f \text{ no es suprayectiva} \iff \exists b \in B : f(a) \neq b, \forall a \in A$$

es decir, f no es suprayectiva si podemos encontrar un elemento en B tal que no es imagen de ningún elemento de A.

♦

Ejemplo 12.22

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.

♦

12.3.3 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 12.23

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,

$$y = 2x - 3 \iff 2x = y + 3 \iff x = \frac{y+3}{2}$$

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 12.24

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,

$$\begin{aligned} y = \frac{x}{x^2+1} &\iff x = x^2y + y \\ &\iff x^2y - x + y = 0 \\ &\iff x = \frac{1 \pm \sqrt{1-4y^2}}{2y} \end{aligned}$$

Ahora bien, si $1-4y^2<0$, entonces $x\notin\mathbb{R}$, y como

$$1-4y^2<0 \iff 4y^2>1 \iff y^2>\frac{1}{4} \iff y>\pm\frac{1}{2} \iff |y|>\frac{1}{2}$$

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 12.25

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,

$$\begin{aligned} f(x_1)=f(x_2) &\iff (b-a)x_1+a=(b-a)x_2+a \\ &\implies (b-a)x_1=(b-a)x_2 \qquad \{a\neq b\} \\ &\implies x_1=x_2 \end{aligned}$$

luego,

$$\forall x_1,x_2,\in[0,1]\ (f(x_1)=f(x_2)\implies x_1=x_2)$$

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,

$$y=(b-a)x+a \iff x=\frac{y-a}{b-a}$$

y al ser $a\neq b$, será $b-a\neq 0$, luego existe x, siendo

$$\begin{aligned} y\in[a,b] &\iff a\leqslant y\leqslant b \\ &\iff -b\leqslant -y\leqslant -a \\ &\iff a-b\leqslant a-y\leqslant a-a \\ &\iff 0\leqslant y-a\leqslant b-a \\ &\iff 0\leqslant \frac{y-a}{b-a}\leqslant 1 \\ &\iff 0\leqslant x\leqslant 1 \\ &\iff x\in[0,1] \end{aligned}$$

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 12.26

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 12.27

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.

♦

Ejemplo 12.28

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

$$\begin{aligned} f(x_1) = f(x_2) &\iff ax_1 + b = ax_2 + b \\ &\Longrightarrow ax_1 = ax_2,\ \forall b \in \mathbb{Z} \\ &\Longrightarrow x_1 = \frac{a}{a}x_2,\ \forall b \in \mathbb{Z} \\ &\Longrightarrow x_1 = x_2,\ \forall b \in \mathbb{Z},\ \text{y } \forall a \in \mathbb{Z} \setminus \{0\} \end{aligned}$$

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

$$x \in \mathbb{Z} \Longleftrightarrow \frac{y-b}{a} \in \mathbb{Z} \Longleftrightarrow \exists q \in \mathbb{Z} : y - b = aq \Longleftrightarrow \exists q \in \mathbb{Z} : b = a(-q) + y$$

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

$$\forall a \in \mathbb{Z} \setminus \{0\} \ \text{ y } \forall b : \frac{y-b}{a} \in \mathbb{Z}$$

♦

12.3.4 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

$$\begin{aligned} f(a_1) = f(a_2) &\implies g\,[f(a_1)] = g\,[f(a_2)] \\ &\implies (g \circ f)(a_1) = (g \circ f)(a_2) \quad \{g \circ f \text{ es inyectiva}\} \\ &\implies a_1 = a_2 \end{aligned}$$

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,

$$\begin{aligned} g(b_1) = g(b_2) &\iff g\,[f(a_1)] = g\,[f(a_2)] \\ &\iff (g \circ f)(a_1) = (g \circ f)(a_2) \quad \{g \circ f \text{ es inyectiva}\} \\ &\iff a_1 = a_2 \qquad\qquad\qquad\qquad \{f \text{ es función}\} \\ &\iff f(a_1) = f(a_2) \\ &\iff b_1 = b_2 \end{aligned}$$

(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,

$$g\,[f(a)] = g(b)$$

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.

♦

12.4 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.

12.4.1 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:

$$f^{-1} : B \longrightarrow A : f^{-1}(b) = a \Longleftrightarrow b = f(a),\ \forall b \in B$$

⧫

12.4.2 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,

$$\begin{aligned} f(a_1) = f(a_2) &\Longrightarrow b_1 = b_2 \\ &\Longrightarrow f^{-1}(b_1) = f^{-1}(b_2) \quad \{\text{Por ser } f^{-1} \text{ función}\} \\ &\Longleftrightarrow a_1 = a_2 \end{aligned}$$

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,

$$f^{-1}(b) = a \Longleftrightarrow f(a) = b$$

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,

$$f(a) = b \Longleftrightarrow f^{-1}(b) = a$$

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

$$\left.\begin{array}{l} f^{-1}(b) = a_1 \Longleftrightarrow f(a_1) = b \\ \wedge \\ f^{-1}(b) = a_2 \Longleftrightarrow f(a_2) = b \end{array}\right\} \Longrightarrow f(a_1) = f(a_2) \Longrightarrow a_1 = a_2$$

luego f^{-1} es una función y, por definición, f será invertible.

♦

Ejemplo 12.29

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 12.30

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 12.4.2, 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 12.31

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,

$$f^{-1} : B \longrightarrow A \text{ tal que } f^{-1}(y) = \sqrt[3]{y-2},\ \forall y \in B$$

♦♦♦

12.5 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.

12.5.1 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.

$$f \text{ es invertible } \iff \exists f^{-1} : B \longrightarrow A \text{ tal que } f^{-1}\circ f = i_A \text{ y } f\circ f^{-1} = i_B$$

$\Longrightarrow$) Supongamos que f es una función invertible y sea f^{-1} su función inversa. Teniendo en cuenta la definición de inversa, tendremos

$$f^{-1} : B \longrightarrow A \text{ tal que } f^{-1}(b) = a \iff b = f(a),\ \forall b \in B$$

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 12.4.2 tendremos que f es invertible.

♦

Nota 12.5 Obsérvese que además de caracterizar las funciones invertibles, con la proposición anterior hemos construido f^{-1}, inversa de la función f.

♦

Ejemplo 12.32

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 12.5.1, $f \circ f^{-1} = i_B$. 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.

♦

12.5.2 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,

$$f^{-1} : B \longrightarrow A \text{ tal que } f^{-1}(b) = a \iff b = f(a),\ \forall b \in B$$

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,

$$\begin{aligned} h = h \circ i_B = h \circ (f \circ f^{-1}) = (h \circ f) \circ f^{-1} = i_A \circ f^{-1} = f^{-1} \\ h = i_A \circ h = (f^{-1} \circ f) \circ h = f^{-1} \circ (f \circ h) = f^{-1} \circ i_B = f^{-1} \end{aligned}$$

es decir,

$$h = f^{-1}$$

Consecuentemente la inversa de f, si existe, es única.

♦

12.5.3 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,

$$\left.\begin{array}{l} f \text{ es invertible, luego es biyectiva} \\ g \text{ es invertible, luego es biyectiva} \end{array}\right\} \overset{(12.3.4)}{\Longrightarrow} g \circ f \text{ es biyectiva} \iff g \circ f \text{ es invertible}$$

(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,

$$(g \circ f) \circ (f^{-1} \circ g^{-1}) = i_C \tag{12.1}$$

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,

$$(f^{-1} \circ g^{-1}) \circ (g \circ f) = i_A \tag{12.2}$$

De (12.1), (12.2) y de 12.5.1 se sigue que

$$(g \circ f)^{-1} = f^{-1} \circ g^{-1}$$

♦

Ejemplo 12.33

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 12.34

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 12.5.1, 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 13

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

13.1 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 13.1

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, tendrían 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.

♦

13.1.1 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

$$a_2 = 1$$

♦♦♦

13.2 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.

13.2.1 Sucesión

Una sucesión es una función real definida en el conjunto de los enteros positivos, $\mathbb{Z}^+$.

♦

Ejemplo 13.2

(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 $f(n) = n^2 - 1$ o $\left\{n^2 - 1\right\}$ o $\{a_n\}$ tal que $a_n = n^2 - 1$.

♦

13.2.2 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 13.3

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 13.4

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 14

Ecuaciones de Recurrencia Lineales

14.1 Generalidades

14.1.1 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.*

♦

14.1.2 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.*

♦

14.1.3 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 14.1

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:

$$a_{n+1} - 5a_n = 0.$$

♦

14.1.4 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.*

$$a_{n+k} + c_{k-1}(n)a_{n+(k-1)} + c_{k-2}(n)a_{n+(k-2)} + \cdots + c_2(n)a_{n+2} + c_1(n)a_{n+1} + c_0(n)a_n = h(n).$$

♦♦♦

14.2 Soluciones

Como ya vimos en 13.2.2, 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 14.2

¿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:

$$\begin{array}{llllllll} n=1. & a_3 = 4a_2 - 4a_1 & = & 4a_2 - 8 & & & & \\ n=2. & a_4 = 4a_3 - 4a_2 & = & 4(4a_2 - 8) - 4a_2 & = & 12a_2 - 32 & & \\ n=3. & a_5 = 4a_4 - 4a_3 & = & 4(12a_2 - 32) - 4(4a_2 - 8) & = & 32a_2 - 96 & & \\ n=4. & a_6 = 4a_5 - 4a_4 & = & 4(32a_2 - 96) - 4(12a_2 - 32) & = & 80a_2 - 256 & & \\ \vdots & \vdots & & \vdots & & \vdots & & \end{array}$$

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 para cada valor de a_2 que tomáramos tendríamos una solución diferente. 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:

$$\{0, 1, 1, 2, 3, 5, 8, 13, 21, 34, \ldots\ldots, \}$$

♦

14.2.1 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 $n = k + 1$,

$$\begin{array}{rcccccccc} a_{k+(k+1)} & = & h(k+1) & - & c_{k-1}(k+1)a_{k+k} & - & c_{k-2}(k)a_{k+(k-1)} & - & \cdots\cdots \\ & & & - & c_2(k+1)a_{k+3} & - & c_1(k+1)a_{k+2} & - & c_0(k)a_{k+1} \end{array}$$

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,

$$\begin{array}{rcccccc} a_{k+(p+1)} & = & h(p+1) & - & c_{k-1}(p+1)a_{k+p} & - & c_{k-2}(p+1)a_{k+(p-1)} \\ & - & \cdots\cdots\cdots\cdots & - & c_2(p+1)a_{k+[p-(k-3)]} & - & c_1(p+1)a_{k+[p-(k-2)]} \\ & - & c_0(p+1)a_{k+[p-(k-1)]} & & & & \\ & = & h(p+1) & - & c_{k-1}(p+1)a_{k+p} & - & c_{k-2}(p+1)a_{k+(p-1)} \\ & - & \cdots\cdots\cdots\cdots & - & c_2(p+1)a_{p+3} & - & c_1(p+1)a_{p+2} \\ & - & c_0(p+1)a_{p+1} & & & & \end{array}$$

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 14.1 Obsérvese que el teorema anterior puede modificarse con facilidad para aplicarlo a situaciones en las que las condiciones iniciales estén dadas por k valores 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.

♦♦♦

14.3 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.

14.3.1 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,

$$\{r_n\} \text{ y } \{s_n\} \text{ son soluciones} \Longrightarrow \{\alpha_1 r_n + \alpha_2 s_n\} \text{ con } \alpha_1 \text{ y } \alpha_2 \text{ reales, también lo es.}$$

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

$$\begin{array}{ccccccc} \alpha_1 r_{n+k} & + & \alpha_2 s_{n+k} & + & c_{k-1}(n)\left(\alpha_1 r_{n+(k-1)} + \alpha_2 s_{n+(k-1)}\right) & + & \cdots \\ & + & c_1(n)\left(\alpha_1 r_{n+1} + \alpha_2 s_{n+1}\right) & + & c_0(n)\left(\alpha_1 r_n + \alpha_2 s_n\right) & = & 0 \end{array}$$

para cada $n \in \mathbb{Z}^+$. Por lo tanto, la sucesión

$$\alpha_1 \{r_n\} + \alpha_2 \{s_n\} = \{\alpha_1 r_n + \alpha_2 s_n\}$$

también es una solución de la ecuación.

♦

14.3.2 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 15

Recurrencias Lineales Homogéneas

15.1 Primer Orden con Coeficientes Constantes

15.1.1 Solución General

Las ecuaciones de recurrencia lineales homogéneas de primer orden y con coeficientes constantes,

$$a_{n+1} = c_0 a_n,\ n \geqslant 1$$

son las más simples. Obtendremos su solución utilizando la iteración.

Demostración.

$$\begin{array}{lllllll} a_2 &=& c_0 a_1 & & & & \\ a_3 &=& c_0 a_2 &=& c_0 c_0 a_1 &=& c_0^2 a_1 \\ a_4 &=& c_0 a_3 &=& c_0 c_0^2 a_1 &=& c_0^3 a_1 \\ a_5 &=& c_0 a_4 &=& c_0 c_0^3 a_1 &=& c_0^4 a_1 \\ \vdots & & \vdots & & \vdots & & \vdots \end{array}$$

luego podemos inferir que la sucesión $\{a_n\}$ tal que $a_n = c_0^{n-1} a_1,\ \forall n \geqslant 1$ es solución de la ecuación. Probaremos, por inducción, que en efecto lo es.

- Para $n = 2$,
$$a_2 = c_0 a_1 = c_0^{2-1} a_1$$
es decir, se cumple.
- Supongamos que es cierto para $n = p$, o sea, $a_p = c_0^{p-1} a_1$.
- Veamos que también lo es para $n = p + 1$. En efecto,
$$a_{p+1} = c_0 a_p = c_0 c_0^{p-1} a_1 = c_0^p a_1$$
por lo tanto,
$$a_n = c_0^{n-1} a_1,\ \forall n \in \mathbb{Z}^+$$

Así pues, la sucesión $\{a_n\}$ tal que $a_n = c_0^{n-1} a_1,\ \forall n \in \mathbb{Z}^+$ es solución de la ecuación. Obsérvese que esta solución no es única ya que para cada valor que demos a a_1 obtendremos una solución.

♦

15.1.2 Solución única

Según vimos en 14.2.1 para que la ecuación tenga solución única necesitamos una condición inicial. Tomando como tal $a_1 = \alpha$, tendremos

$$\begin{aligned} a_1 &= \alpha \\ a_{n+1} &= c_0 a_n,\ n \geqslant 1 \end{aligned}$$

y la solución única será la sucesión $\{a_n\}$ tal que $a_n = c_0^{n-1}\alpha$.

Una de las estrategias más utilizadas para resolver ecuaciones de recurrencia es encontrar, primero la solución general y luego utilizar las condiciones iniciales para resolver las constantes arbitrarias que aparecen en ella.

♦

Ejemplo 15.1

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

$$\begin{aligned} a^1 &= a \\ a^{n+1} &= a \cdot a^n,\ n \geqslant 1 \end{aligned}$$

En este caso, la ecuación de recurrencia se utiliza para definir el significado de a^n. Así, si escribimos

$$\begin{aligned} a_1 &= a \\ a_{n+1} &= a \cdot a_n,\ n \geqslant 1 \end{aligned}$$

estaremos en el caso planteado en 15.1.1 con $\alpha = a$ y $c_0 = a$. La solución sería, por tanto, la sucesión $\{a_n\}$ tal que $a_n = a \cdot a^{n-1} = a^n$.

♦

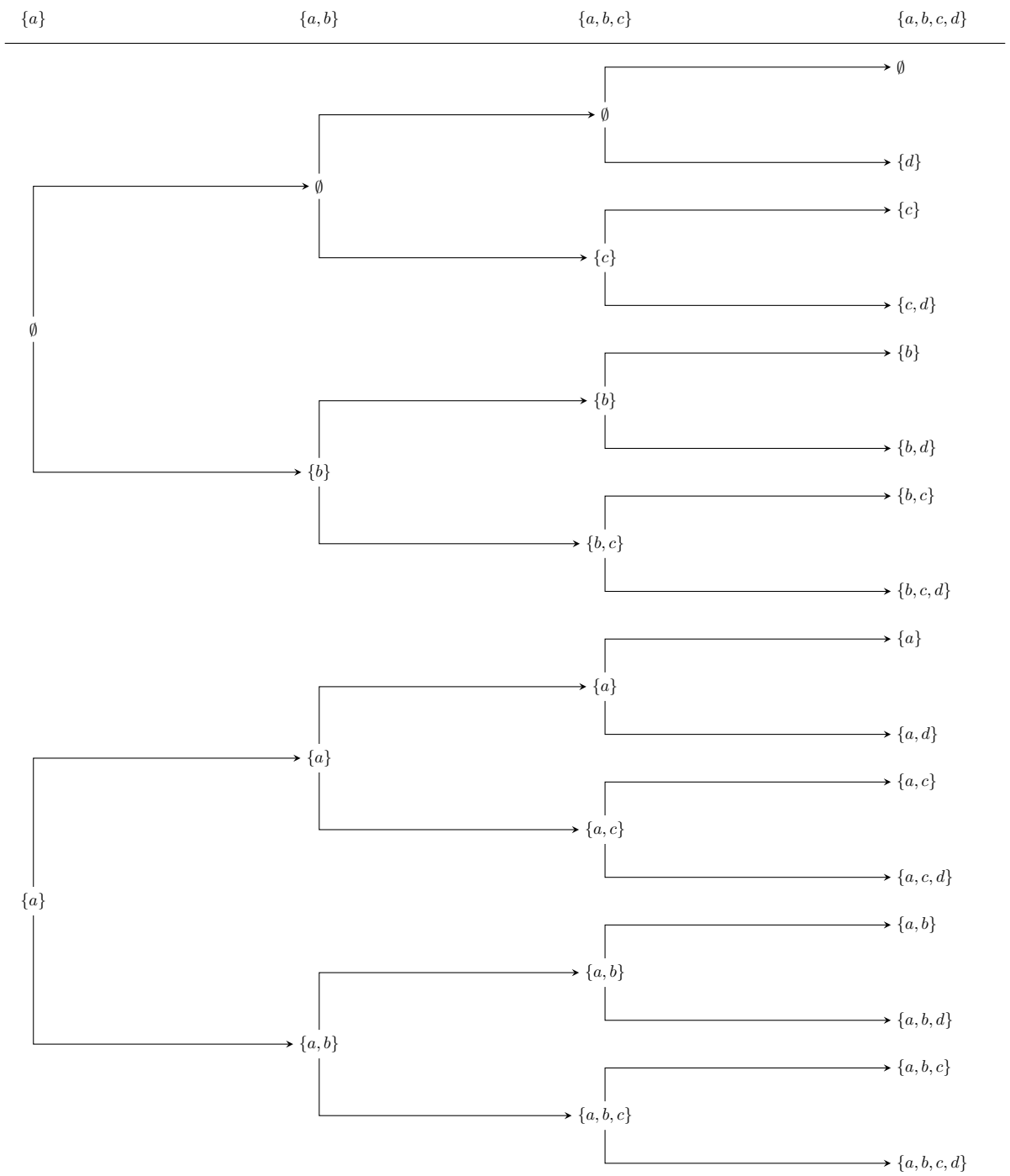
Ejemplo 15.2

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 apreciarse, 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 15.1.1, la solución general sería la sucesión $\{a_n\}$ tal que,

$$a_n = 2^{n-1}a_1, \ \forall n$$

y aplicando la condición inicial,

$$\left.\begin{array}{rcl} a_1 & = & 2 \\ a_n & = & 2^{n-1}a_1 \end{array}\right\} \implies a_n = 2^{n-1}2 \implies a_n = 2^n$$

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 15.3

Resolver la ecuación de recurrencia,

$$\begin{array}{rcl} a_2 & = & 144 \\ a_{n+1} & = & 6a_n,\ n \geqslant 1 \end{array}$$

Solución.

La ecuación propuesta es lineal homogénea de primer orden con coeficientes constantes. En este caso no conocemos el valor de a_1 pero su cálculo es fácil. En efecto,

$$a_{n+1} = 6a_n \implies a_2 = 6a_1 \implies a_1 = \frac{a_2}{6} = \frac{144}{6} = 24$$

y tendríamos

$$\begin{array}{rcl} a_1 & = & 24 \\ a_{n+1} & = & 6a_n,\ n \geqslant 1 \end{array}$$

cuya solución general, como ya sabemos, es la sucesión $\{a_n\}$ tal que $a_n = 6^{n-1}a_1$. Entonces

$$\left.\begin{array}{rcl} a_n & = & 6^{n-1}a_1 \\ a_1 & = & 24 \end{array}\right\} \implies a_n = 6^{n-1}24 \implies a_n = 4 \cdot 6^n$$

es solución de la ecuación propuesta y además, por 15.1.2, es única.

♦

Ejemplo 15.4

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 15.1.1,

$$a_n = 1,006^{n-1}a_1$$

y como la condición inicial es $a_1 = 5000$,

$$\left.\begin{aligned} a_n &= 1,006^{n-1}a_1 \\ a_1 &= 5000 \end{aligned}\right\} \implies a_n = 5000 \cdot 1,006^{n-1}$$

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:

$$a_{13} = 5000 \cdot 1,006^{12} = 5372,12 \text{ Euros.}$$

♦♦♦

15.2 Segundo orden con Coeficientes Constantes

Según 14.1.4, una ecuación de este tipo puede escribirse en la forma

$$a_{n+2} + c_1a_{n+1} + c_0a_n = 0$$

sin más que hacer $k = 2$ en su forma general.

Por ejemplo, consideremos la ecuación

$$a_{n+2} + a_{n+1} - 2a_n = 0,\ n \geqslant 1$$

despejando a_{n+2}, tendremos

$$a_{n+2} = -a_{n+1} + 2a_n,\ n \geqslant 1$$

Entonces,

$$\begin{array}{lllllll} a_3 &=& -a_2 + 2a_1 & & & & \\ a_4 &=& -a_3 + 2a_2 &=& -(-a_2 + 2a_1) + 2a_2 &=& -2a_1 + 3a_2 \\ a_5 &=& -a_4 + 2a_3 &=& -(-2a_1 + 3a_2) + 2(-a_2 + 2a_1) &=& 6a_1 - 5a_2 \\ a_6 &=& -a_5 + 2a_4 &=& -(6a_1 - 5a_2) + 2(-2a_1 + 3a_2) &=& -10a_1 + 11a_2 \\ \vdots & & \vdots & & \vdots & & \vdots \\ \vdots & & \vdots & & \vdots & & \vdots \end{array}$$

y aunque continuáramos iterando 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 $a_n = a_1c_0^{n-1}$, 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 otra "buena conjetura" llamada *método de las raíces características* que, efectivamente, nos ofrece una solución general. Comenzaremos con un caso particular para, posteriormente, buscar una generalización.

Ejemplo 15.5

Resolver la ecuación de recurrencia

$$a_{n+2} = 2a_n - a_{n+1},\ n \geqslant 1$$

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 misma, 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 $a_n = (-2)^n$,

$$\begin{aligned} 2a_n - a_{n+1} &= 2(-2)^n - (-2)^{n+1} \\ &= (-2)^n(2 - (-2)) \\ &= 4(-2)^n \\ &= (-2)^2(-2)^n \\ &= (-2)^{n+2} \\ &= a_{n+2} \end{aligned}$$

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* (14.3.1), podemos concluir que la sucesión $\{a_n\}$ tal que

$$a_n = \alpha_1(-2)^n + \alpha_2 \cdot 1^n = \alpha_1(-2)^n + \alpha_2$$

también es solución para cualquier par de constantes reales α_1 y α_2. Tenemos, pues, la solución general de la ecuación propuesta y para obtener una solución única, necesitaremos dos condiciones iniciales que nos permitan calcular α_1 y α_2.

15.3 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.

15.3.1 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.

♦

15.3.2 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 15.6

Resolver la ecuación de recurrencia,

$$a_{n+2} - 4a_{n+1} + 4a_n = 0,\ n \geqslant 0$$

Solución.

Su ecuación característica (15.3.2) es:

$$\lambda^2 - 4\lambda + 4 = 0.$$

Entonces,

$$\begin{aligned} \lambda^2 - 4\lambda + 4 = 0 \quad &\Longrightarrow \quad \lambda = \frac{\lambda \pm \sqrt{16 - 4 \cdot 1 \cdot 4}}{2} \\ &\Longrightarrow \quad \lambda = \frac{4}{2} \\ &\Longrightarrow \quad \lambda = 2 \end{aligned}$$

es decir, la ecuación característica tiene una raíz doble ($\lambda = 2$). Por el teorema 15.3.1, las sucesiones $\{2^n\}$ y $\{2^n\}$ son, ambas, solución de la ecuación. Por el *principio de superposición* (14.3.1), 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* (14.3.1), 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.

15.3.3 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 15.7

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.

La ecuación propuesta escrita en su forma general es,

$$\begin{aligned} a_1 &= 1 \\ a_2 &= 1 \\ a_{n+2} - a_{n+1} - a_n &= 0 \end{aligned}$$

o sea, es lineal, homogénea, de segundo orden y con coeficientes constantes.

◊ Obtención de la solución general.

Por 15.3.3, si λ es raíz de su ecuación característica con multiplicidad m, entonces las sucesiones $\{a_n\}$ tales que

$$a_n = n^q\lambda^n,\ 0 \leqslant q \leqslant m-1$$

son, todas, soluciones de la ecuación.

⁜ Ecuación característica.

$$\begin{aligned} \lambda^2 - \lambda - 1 = 0 &\implies \lambda = \frac{1 \pm \sqrt{1+4}}{2} \\ &\implies \lambda = \frac{1 \pm \sqrt{5}}{2} \\ &\implies \begin{cases} \lambda_1 = \dfrac{1+\sqrt{5}}{2} \\ \lambda_2 = \dfrac{1-\sqrt{5}}{2}. \end{cases} \end{aligned}$$

Es decir, la ecuación característica tiene dos soluciones, ambas con multiplicidad $m = 1$.

⁕ Soluciones.

Por tanto, las sucesiones

$$\left\{n^0\lambda_1^n\right\} = \left\{\left(\frac{1+\sqrt{5}}{2}\right)^n\right\}$$

y

$$\left\{n^0\lambda_2^n\right\} = \left\{\left(\frac{1-\sqrt{5}}{2}\right)^n\right\}$$

son, ambas, solución de la ecuación propuesta.

⁕ Solución general.

Por el *Principio de Superposición*, 14.3.1, la solución general será

$$\{a_n\} = \alpha_1\left\{\left(\frac{1+\sqrt{5}}{2}\right)^n\right\} + \alpha_2\left\{\left(\frac{1-\sqrt{5}}{2}\right)^n\right\} = \left\{\alpha_1\left(\frac{1+\sqrt{5}}{2}\right)^n + \alpha_2\left(\frac{1-\sqrt{5}}{2}\right)^n\right\},\ \forall\alpha_1,\alpha_2\in\mathbb{R}$$

◊ Obtención de la solución única.

Finalmente, como contamos con dos condiciones iniciales, podremos hallar una solución única para la ecuación dada.

$$\begin{aligned} a_1 &= 1 \\ a_2 &= 1 \\ a_n &= \alpha_1\left(\frac{1+\sqrt{5}}{2}\right)^n + \alpha_2\left(\frac{1-\sqrt{5}}{2}\right)^n \end{aligned}$$

⁕ Cálculo de los coeficientes de la solución general.

$$\left.\begin{aligned} a_1 = 1 &\Longrightarrow \alpha_1\left(\frac{1+\sqrt{5}}{2}\right) + \alpha_2\left(\frac{1-\sqrt{5}}{2}\right) = 1 \\ a_1 = 1 &\Longrightarrow \alpha_1\left(\frac{1+\sqrt{5}}{2}\right)^2 + \alpha_2\left(\frac{1-\sqrt{5}}{2}\right)^2 = 1 \end{aligned}\right\} \Longrightarrow \left\{\begin{aligned} &\alpha_1\left(1+\sqrt{5}\right) + \alpha_2\left(1-\sqrt{5}\right) = 2 \\ &\alpha_1\left(1+\sqrt{5}\right)^2 + \alpha_2\left(1-\sqrt{5}\right)^2 = 4 \end{aligned}\right.$$

Luego,

$$\left.\begin{aligned} \alpha_1\left(1+\sqrt{5}\right) + \alpha_2\left(1-\sqrt{5}\right) &= 2 \\ -\alpha_2\left(1-\sqrt{5}\right) &= \frac{1-\sqrt{5}}{\sqrt{5}} \end{aligned}\right\} \Longrightarrow \left\{\begin{aligned} \alpha_1\left(1+\sqrt{5}\right) &= \frac{1+\sqrt{5}}{\sqrt{5}} \\ -\alpha_2\left(1-\sqrt{5}\right) &= \frac{1-\sqrt{5}}{\sqrt{5}} \end{aligned}\right.$$

$$\Longrightarrow \left\{\begin{aligned} \alpha_1 &= \frac{\sqrt{5}}{5} \\ \alpha_2 &= -\frac{\sqrt{5}}{5} \end{aligned}\right.$$

⁕ Solución única.

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 14.2.1, la única solución de la ecuación.

♦

Ejemplo 15.8

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 propuesta escrita en su forma general es,

$$\begin{aligned} a_1 &= 2 \\ a_2 &= 3 \\ a_{n+2} - 6a_{n+1} - 9a_n &= 0 \end{aligned}$$

o sea, es lineal, homogénea, de segundo orden y con coeficientes constantes.

♢ Obtención de la solución general.

Por 15.3.3, si λ es raíz de su ecuación característica con multiplicidad m, entonces las sucesiones $\{a_n\}$ tales que

$$a_n = n^q \lambda^n,\ 0 \leqslant q \leqslant m-1$$

son, todas, soluciones de la ecuación.

- ⁜ Ecuación característica.

$$\lambda^2 - 6\lambda + 9 = 0 \implies \lambda = \frac{6 \pm \sqrt{36-36}}{2} \implies \begin{cases} \lambda_1 = 3 \\ \lambda_2 = 3 \end{cases}$$

  Es decir, la ecuación característica tiene una solución, $\lambda = 3$, con multiplicidad $m = 2$.

- ⁜ Soluciones.

  Por tanto, las sucesiones

$$\left\{n^0 \lambda_1^n\right\} = \{3^n\}$$

  y

$$\left\{n^1 \lambda_2^n\right\} = \{n3^n\}$$

  son, ambas, solución de la ecuación propuesta.

- ⁜ Solución general.

  Por el *Principio de Superposición*, 14.3.1, la solución general será

$$\{a_n\} = \alpha_1 \{3^n\} + \alpha_2 \{n3^n\} = \{\alpha_1 3^n + n\alpha_2 3^n\} = \left\{(3\alpha_1 + 3n\alpha_2)\, 3^{n-1}\right\}\ \forall \alpha_1, \alpha_2 \in \mathbb{R}$$

♢ Obtención de la solución única.

Finalmente, como contamos con dos condiciones iniciales, podremos hallar una solución única para la ecuación dada.

$$\begin{aligned} a_1 &= 2 \\ a_2 &= 3 \\ a_n &= (3\alpha_1 + 3n\alpha_2)\, 3^{n-1} \end{aligned}$$

⁕ Cálculo de los coeficientes de la solución general.

$$\left.\begin{array}{lll} a_1 = 2 & \Longrightarrow & 3\alpha_1 + 3\alpha_2 = 2 \\ a_2 = 3 & \Longrightarrow & (3\alpha_1 + 6\alpha_2)\,3 = 3 \end{array}\right\} \Longrightarrow \left\{\begin{array}{rcrcl} 3\alpha_1 & + & 3\alpha_2 & = & 2 \\ 3\alpha_1 & + & 6\alpha_2 & = & 1 \end{array}\right.$$

$$\Longrightarrow \left\{\begin{array}{rcrcl} 3\alpha_1 & + & 3\alpha_2 & = & 2 \\ & & 3\alpha_2 & = & -1 \end{array}\right.$$

$$\Longrightarrow \left\{\begin{array}{rcr} 3\alpha_1 & = & 3 \\ 3\alpha_2 & = & -1 \end{array}\right.$$

⁕ Solución única.

Por lo tanto, la sucesión $\{a_n\}$ tal que

$$a_n = (3-n)\,3^{n-1};\ n \geqslant 1$$

es, por el teorema 14.2.1, la única solución de la ecuación.

♦

Ejemplo 15.9

Resolver la ecuación de recurrencia

$$a_{n+3} = 2a_{n+2} + a_{n+1} - 2a_n,\ n \geqslant 1$$

con las condiciones iniciales $a_1 = 7,\ a_2 = 15,\ a_3 = 25$.

Solución.

La ecuación escrita en su forma general es

$$a_{n+3} - 2a_{n+2} - a_{n+1} + 2a_n = 0$$

o sea, es lineal, de tercer orden y con coeficientes constantes.

◊ Obtención de la solución general.

Por 15.3.3, si λ es raíz de su ecuación característica con multiplicidad m, entonces las sucesiones $\{a_n\}$ tales que

$$a_n = n^q\lambda^n,\ 0 \leqslant q \leqslant m-1$$

son, todas, soluciones de la ecuación.

⁕ Ecuación característica.

$$\lambda^3 - 2\lambda^2 - \lambda + 2 = 0 \Longrightarrow \left\{\begin{array}{rcr} \lambda_1 & = & -1 \\ \lambda_2 & = & 1 \\ \lambda_3 & = & 2 \end{array}\right.$$

Es decir, tiene tres soluciones cada una de ellas con multiplicidad 1.

⁕ Soluciones.

Por lo tanto, las sucesiones,

$$\begin{array}{rcl} \{n^0\lambda_1^n\} & = & \{(-1)^n\} \\ \{n^0\lambda_2^n\} & = & \{1\} \\ \{n^0\lambda_3^n\} & = & \{2^n\} \end{array}$$

son, todas, soluciones de la ecuación propuesta.

⁕ Solución general.

Por el *Principio de Superposición*, 14.3.1, la solución general será la sucesión $\{a_n\}$ tal que

$$a_n = \alpha_1 (-1)^n + \alpha_2 + \alpha_3 2^n,\ \forall \alpha_1, \alpha_2, \alpha_3 \in \mathbb{R}$$

◊ Obtención de la solución única.

Como disponemos de tres condiciones iniciales, podremos calcular los coeficientes de la solución general y de esta forma obtener una solución única para las condiciones iniciales dadas.

⁕ Cálculo de los coeficientes de la solución general.

De $a_1 = 7$, $a_2 = 15$ y $a_3 = 25$ se sigue

$$\left.\begin{array}{rcrcrcr} - & \alpha_1 & + & \alpha_2 & + & 2\alpha_3 & = & 7 \\ & \alpha_1 & + & \alpha_2 & + & 4\alpha_3 & = & 15 \\ - & \alpha_1 & + & \alpha_2 & + & 8\alpha_3 & = & 25 \end{array}\right\} \Longrightarrow \left\{\begin{array}{rcl} \alpha_1 & = & 1 \\ \alpha_2 & = & 2 \\ \alpha_3 & = & 3 \end{array}\right.$$

⁕ Solución única para las condiciones iniciales dadas.

Por lo tanto, la sucesión $\{a_n\}$ tal que

$$a_n = (-1)^n + 2 + 3 \cdot 2^n,\ n \geqslant 1$$

es, por el teorema 14.2.1, la solución única de la ecuación propuesta.

♦

Ejemplo 15.10

Resolver la ecuación de recurrencia

$$a_{n+3} = -2a_{n+2} + 4a_{n+1} + 8a_n,\ n \geqslant 1$$

con las condiciones iniciales $a_1 = 2,\ a_2 = 0,\ a_3 = 24$.

Solución.

La ecuación escrita en su forma general es

$$a_{n+3} + 2a_{n+2} - 4a_{n+1} - 8a_n = 0$$

o sea, es lineal, de tercer orden y con coeficientes constantes.

◊ Obtención de la solución general.

Por 15.3.3, si λ es raíz de su ecuación característica con multiplicidad m, entonces las sucesiones $\{a_n\}$ tales que

$$a_n = n^q \lambda^n,\ 0 \leqslant q \leqslant m - 1$$

son, todas, soluciones de la ecuación.

⁕ Ecuación característica.

$$\lambda^3 + 2\lambda^2 - 4\lambda - 8 = 0 \Longrightarrow \left\{\begin{array}{rcl} \lambda_1 & = & -2 \\ \lambda_2 & = & -2 \\ \lambda_3 & = & 2 \end{array}\right.$$

Es decir, tiene tres soluciones, una de ellas con multiplicidad 2 y la otra con multiplicidad 1.

⁕ Soluciones.

Por lo tanto, las sucesiones,

$$\begin{aligned}\left\{n^0\lambda_1^n\right\} &= \left\{(-2)^n\right\}\\ \left\{n^1\lambda_2^n\right\} &= \left\{n\,(-2)^n\right\}\\ \left\{n^0\lambda_3^n\right\} &= \left\{2^n\right\}\end{aligned}$$

son, todas, soluciones de la ecuación propuesta.

⁕ Solución general.

Por el *Principio de Superposición*, 14.3.1, la solución general será la sucesión $\{a_n\}$ tal que

$$a_n = \alpha_1\,(-2)^n + \alpha_2 n\,(-2)^n + \alpha_3 2^n,\ \forall\alpha_1,\alpha_2,\alpha_3\in\mathbb{R}$$

♢ Obtención de la solución única.

Como disponemos de tres condiciones iniciales, podremos calcular los coeficientes de la solución general y de esta forma obtener una solución única para las condiciones iniciales dadas.

⁕ Cálculo de los coeficientes de la solución general.

De $a_1 = 2$, $a_2 = 0$ y $a_3 = 24$ se sigue

$$\left.\begin{array}{rcrcrcr} - & 2\alpha_1 & - & 2\alpha_2 & + & 2\alpha_3 & = & 2\\ & 4\alpha_1 & + & 8\alpha_2 & + & 4\alpha_3 & = & 0\\ - & 8\alpha_1 & - & 24\alpha_2 & + & 8\alpha_3 & = & 24 \end{array}\right\} \Longrightarrow \left\{\begin{array}{rcr} \alpha_1 & = & 1\\ \alpha_2 & = & -1\\ \alpha_3 & = & 1\end{array}\right.$$

⁕ Solución única para las condiciones iniciales dadas.

Por lo tanto, la sucesión $\{a_n\}$ tal que

$$a_n = (-2)^n - n\,(-2)^n + 2^n,\ n\geqslant 1$$

es, por el teorema 14.2.1, la solución única de la ecuación propuesta.

♦

Ejemplo 15.11

Resolver la ecuación de recurrencia

$$a_{n+3} = 6a_{n+2} - 12a_{n+1} + 8a_n,\ n\geqslant 1$$

con las condiciones iniciales $a_1 = -4$, $a_2 = -4$, $a_3 = 16$.

Solución.

La ecuación escrita en su forma general es

$$a_{n+3} - 6a_{n+2} + 12a_{n+1} - 8a_n = 0$$

o sea, es lineal, de tercer orden y con coeficientes constantes.

♢ Obtención de la solución general.

Por 15.3.3, si λ es raíz de su ecuación característica con multiplicidad m, entonces las sucesiones $\{a_n\}$ tales que

$$a_n = n^q\lambda^n,\ 0\leqslant q\leqslant m-1$$

son, todas, soluciones de la ecuación.

⁕ Ecuación característica.

$$\lambda^3 - 6\lambda^2 + 12\lambda - 8 = 0 \Longrightarrow \left\{ \begin{array}{rcl} \lambda_1 & = & 2 \\ \lambda_2 & = & 2 \\ \lambda_3 & = & 2 \end{array} \right.$$

Es decir, tiene una solución con multiplicidad 3.

⁕ Soluciones.

Por lo tanto, las sucesiones,

$$\begin{array}{rcl} \{n^0\lambda_1^n\} & = & \{2^n\} \\ \{n^1\lambda_2^n\} & = & \{n2^n\} \\ \{n^2\lambda_3^n\} & = & \{n^22^n\} \end{array}$$

son, todas, soluciones de la ecuación propuesta.

⁕ Solución general.

Por el *Principio de Superposición*, 14.3.1, la solución general será la sucesión $\{a_n\}$ tal que

$$a_n = \alpha_1 2^n + \alpha_2 n2^n + \alpha_3 n^2 2^n,\ \forall \alpha_1, \alpha_2, \alpha_3 \in \mathbb{R}$$

◊ Obtención de la solución única.

Como disponemos de tres condiciones iniciales, podremos calcular los coeficientes de la solución general y de esta forma obtener una solución única para las condiciones iniciales dadas.

⁕ Cálculo de los coeficientes de la solución general.

De $a_1 = -4$, $a_2 = -4$ y $a_3 = 16$ se sigue

$$\left. \begin{array}{rcrcrcr} 2\alpha_1 & + & 2\alpha_2 & + & 2\alpha_3 & = & -4 \\ 4\alpha_1 & + & 8\alpha_2 & + & 16\alpha_3 & = & -4 \\ 8\alpha_1 & + & 24\alpha_2 & + & 72\alpha_3 & = & 16 \end{array} \right\} \Longrightarrow \left\{ \begin{array}{rcr} \alpha_1 & = & -1 \\ \alpha_2 & = & -2 \\ \alpha_3 & = & 1 \end{array} \right.$$

⁕ Solución única para las condiciones iniciales dadas.

Por lo tanto, la sucesión $\{a_n\}$ tal que

$$a_n = -2^n - 2n2^n + n^2 2^n,\ n \geqslant 1$$

es, por el teorema 14.2.1, la solución única de la ecuación propuesta.

♦

Ejemplo 15.12

Resolver la ecuación de recurrencia

$$a_{n+4} = 5a_{n+2} - 4a_n,\ n \geqslant 1$$

con las condiciones iniciales $a_1 = 9$, $a_2 = 3$, $a_3 = 27$, $a_4 = 15$.

Solución.

La ecuación escrita en su forma general es

$$a_{n+4} - 5a_{n+2} + 4a_n = 0$$

o sea, es lineal, de cuarto orden y con coeficientes constantes.

◊ Obtención de la solución general.

Por 15.3.3, si λ es raíz de su ecuación característica con multiplicidad m, entonces las sucesiones $\{a_n\}$ tales que

$$a_n = n^q \lambda^n,\ 0 \leqslant q \leqslant m-1$$

son, todas, soluciones de la ecuación.

⁕ Ecuación característica.

$$\lambda^4 - 5\lambda^2 + 4 = 0 \Longrightarrow \left\{ \begin{array}{rcr} \lambda_1 & = & -2 \\ \lambda_2 & = & -1 \\ \lambda_3 & = & 1 \\ \lambda_4 & = & 2 \end{array} \right.$$

Es decir, tiene cuatro soluciones con multiplicidad 1 cada una de ellas.

⁕ Soluciones.

Por lo tanto, las sucesiones,

$$\begin{array}{rcl} \{n^0 \lambda_1^n\} & = & \{(-2)^n\} \\ \{n^0 \lambda_2^n\} & = & \{(-1)^n\} \\ \{n^0 \lambda_3^n\} & = & \{1\} \\ \{n^0 \lambda_3^n\} & = & \{2^n\} \end{array}$$

son, todas, soluciones de la ecuación propuesta.

⁕ Solución general.

Por el *Principio de Superposición*, 14.3.1, la solución general será la sucesión $\{a_n\}$ tal que

$$a_n = \alpha_1 (-2)^n + \alpha_2 (-1)^n + \alpha_3 + \alpha_4 2^n,\ \forall \alpha_1, \alpha_2, \alpha_3, \alpha_4 \in \mathbb{R}$$

◊ Obtención de la solución única.

Como disponemos de cuatro condiciones iniciales, podremos calcular los coeficientes de la solución general y de esta forma obtener una solución única para las condiciones iniciales dadas.

⁕ Cálculo de los coeficientes de la solución general.

De $a_1 = 9$, $a_2 = 3$, $a_3 = 27$ y $a_4 = 15$ se sigue

$$\left. \begin{array}{rcrcrcrcr} - & 2\alpha_1 & - & \alpha_2 & + & \alpha_3 & + & 2\alpha_4 & = & 9 \\ & 4\alpha_1 & + & \alpha_2 & + & \alpha_3 & + & 4\alpha_4 & = & 3 \\ - & 8\alpha_1 & - & \alpha_2 & + & \alpha_3 & + & 8\alpha_4 & = & 27 \\ & 16\alpha_1 & + & \alpha_2 & + & \alpha_3 & + & 16\alpha_4 & = & 15 \end{array} \right\} \Longrightarrow \left\{ \begin{array}{rcr} \alpha_1 & = & -1 \\ \alpha_2 & = & -2 \\ \alpha_3 & = & 1 \\ \alpha_4 & = & 2 \end{array} \right.$$

⁕ Solución única para las condiciones iniciales dadas.

Por lo tanto, la sucesión $\{a_n\}$ tal que

$$a_n = -(-2)^n - 2(-1)^n + 1 + 2^{n+1},\ n \geqslant 1$$

es, por el teorema 14.2.1, la solución única de la ecuación propuesta.

♦

Ejemplo 15.13

Resolver la ecuación de recurrencia

$$a_{n+4} = 4a_{n+3} - 3a_{n+2} - 4a_{n+1} + 4a_n,\ n \geqslant 1$$

con las condiciones iniciales $a_1 = 3,\ a_2 = 21,\ a_3 = 53,\ a_4 = 145.$

Solución.

La ecuación escrita en su forma general es

$$a_{n+4} - 4a_{n+3} + 3a_{n+2} + 4a_{n+1} - 4a_n = 0$$

o sea, es lineal, de cuarto orden y con coeficientes constantes.

◊ Obtención de la solución general.

Por 15.3.3, si λ es raíz de su ecuación característica con multiplicidad m, entonces las sucesiones $\{a_n\}$ tales que

$$a_n = n^q\lambda^n,\ 0 \leqslant q \leqslant m-1$$

son, todas, soluciones de la ecuación.

- Ecuación característica.

$$\lambda^4 - 4\lambda^3 + 3\lambda^2 + 4\lambda - 4 = 0 \Longrightarrow \begin{cases} \lambda_1 &= -1 \\ \lambda_2 &= 1 \\ \lambda_3 &= 2 \\ \lambda_4 &= 2 \end{cases}$$

  Es decir, tiene una solución con multiplicidad 2 y dos soluciones con multiplicidad 1 cada una de ellas.

- Soluciones.

  Por lo tanto, las sucesiones,

$$\begin{aligned} \{n^0\lambda_1^n\} &= \{(-1)^n\} \\ \{n^0\lambda_2^n\} &= \{1\} \\ \{n^0\lambda_3^n\} &= \{2^n\} \\ \{n^1\lambda_3^n\} &= \{n2^n\} \end{aligned}$$

  son, todas, soluciones de la ecuación propuesta.

- Solución general.

  Por el *Principio de Superposición*, 14.3.1, la solución general será la sucesión $\{a_n\}$ tal que

$$a_n = \alpha_1(-1)^n + \alpha_2 + \alpha_3 2^n + \alpha_4 n2^n,\ \forall \alpha_1, \alpha_2, \alpha_3, \alpha_4 \in \mathbb{R}$$

◊ Obtención de la solución única.

Como disponemos de cuatro condiciones iniciales, podremos calcular los coeficientes de la solución general y de esta forma obtener una solución única para las condiciones iniciales dadas.

⁕ Cálculo de los coeficientes de la solución general.

De $a_1 = 3$, $a_2 = 21$, $a_3 = 53$ y $a_4 = 145$ se sigue

$$\left.\begin{array}{rrrrrrrrrrr} - & \alpha_1 & + & \alpha_2 & + & 2\alpha_3 & + & 2\alpha_4 & = & 3 \\ & \alpha_1 & + & \alpha_2 & + & 4\alpha_3 & + & 8\alpha_4 & = & 21 \\ - & \alpha_1 & + & \alpha_2 & + & 8\alpha_3 & + & 24\alpha_4 & = & 53 \\ & \alpha_1 & + & \alpha_2 & + & 16\alpha_3 & + & 64\alpha_4 & = & 145 \end{array}\right\} \Longrightarrow \left\{\begin{array}{rcr} \alpha_1 & = & 2 \\ \alpha_2 & = & -1 \\ \alpha_3 & = & 1 \\ \alpha_4 & = & 2 \end{array}\right.$$

⁕ Solución única para las condiciones iniciales dadas.

Por lo tanto, la sucesión $\{a_n\}$ tal que

$$a_n = 2\,(-1)^n \; - \; + 2^n + n2^{n+1},\ n \geqslant 1$$

es, por el teorema 14.2.1, la solución única de la ecuación propuesta.

♦

Ejemplo 15.14

Resolver la ecuación de recurrencia

$$a_{n+4} = 2a_{n+3} + 3a_{n+2} - 4a_{n+1} - 4a_n,\ n \geqslant 1$$

con las condiciones iniciales $a_1 = 4$, $a_2 = 30$, $a_3 = 56$, $a_4 = 170$.

Solución.

La ecuación escrita en su forma general es

$$a_{n+4} - 2a_{n+3} - 3a_{n+2} + 4a_{n+1} + 4a_n = 0$$

o sea, es lineal, de cuarto orden y con coeficientes constantes.

◊ Obtención de la solución general.

Por 15.3.3, si λ es raíz de su ecuación característica con multiplicidad m, entonces las sucesiones $\{a_n\}$ tales que

$$a_n = n^q\lambda^n,\ 0 \leqslant q \leqslant m-1$$

son, todas, soluciones de la ecuación.

⁕ Ecuación característica.

$$\lambda^4 - 2\lambda^3 - 3\lambda^2 + 4\lambda + 4 = 0 \Longrightarrow \left\{\begin{array}{rcr} \lambda_1 & = & -1 \\ \lambda_2 & = & -1 \\ \lambda_3 & = & 2 \\ \lambda_4 & = & 2 \end{array}\right.$$

Es decir, tiene dos soluciones con multiplicidad 2 cada una de ellas.

⁕ Soluciones.

Por lo tanto, las sucesiones,

$$\begin{aligned}\left\{n^0\lambda_1^n\right\} &= \left\{(-1)^n\right\}\\ \left\{n^1\lambda_2^n\right\} &= \left\{n\,(-1)^n\right\}\\ \left\{n^0\lambda_3^n\right\} &= \left\{2^n\right\}\\ \left\{n^1\lambda_3^n\right\} &= \left\{n2^n\right\}\end{aligned}$$

son, todas, soluciones de la ecuación propuesta.

⁕ Solución general.

Por el *Principio de Superposición*, 14.3.1, la solución general será la sucesión $\{a_n\}$ tal que

$$a_n = \alpha_1\,(-1)^n + \alpha_2 n\,(-1)^n + \alpha_3 2^n + \alpha_4 n2^n,\ \forall\alpha_1,\alpha_2,\alpha_3,\alpha_4 \in \mathbb{R}$$

◊ Obtención de la solución única.

Como disponemos de cuatro condiciones iniciales, podremos calcular los coeficientes de la solución general y de esta forma obtener una solución única para las condiciones iniciales dadas.

⁕ Cálculo de los coeficientes de la solución general.

De $a_1 = 4$, $a_2 = 30$, $a_3 = 56$ y $a_4 = 170$ se sigue

$$\left.\begin{array}{rcrcrcrcr} -&\alpha_1&-&\alpha_2&+&2\alpha_3&+&2\alpha_4&=&4\\ &\alpha_1&+&2\alpha_2&+&4\alpha_3&+&8\alpha_4&=&30\\ -&\alpha_1&-&3\alpha_2&+&8\alpha_3&+&24\alpha_4&=&56\\ &\alpha_1&+&4\alpha_2&+&16\alpha_3&+&64\alpha_4&=&170 \end{array}\right\} \Longrightarrow \left\{\begin{array}{rcl}\alpha_1&=&2\\ \alpha_2&=&2\\ \alpha_3&=&2\\ \alpha_4&=&2\end{array}\right.$$

⁕ Solución única para las condiciones iniciales dadas.

Por lo tanto, la sucesión $\{a_n\}$ tal que

$$a_n = 2\,(-1)^n + 2n\,(-1)^n + 2^{n+1} + n2^{n+1},\ n \geqslant 1$$

es, por el teorema 14.2.1, la solución única de la ecuación propuesta.

♦

Ejemplo 15.15

Resolver la ecuación de recurrencia

$$a_{n+4} = 4a_{n+3} - 16a_{n+1} + 16a_n,\ n \geqslant 1$$

con las condiciones iniciales $a_1 = -4$, $a_2 = -8$, $a_3 = -64$, $a_4 = -192$.

Solución.

La ecuación escrita en su forma general es

$$a_{n+4} - 4a_{n+3} + 16a_{n+1} - 16a_n = 0$$

o sea, es lineal, de cuarto orden y con coeficientes constantes.

◊ Obtención de la solución general.

Por 15.3.3, si λ es raíz de su ecuación característica con multiplicidad m, entonces las sucesiones $\{a_n\}$ tales que

$$a_n = n^q\lambda^n,\ 0 \leqslant q \leqslant m-1$$

son, todas, soluciones de la ecuación.

⁕ Ecuación característica.

$$\lambda^4 - 4\lambda^3 + 16\lambda - 16 = 0 \Longrightarrow \left\{ \begin{array}{rcr} \lambda_1 & = & -2 \\ \lambda_2 & = & 2 \\ \lambda_3 & = & 2 \\ \lambda_4 & = & 2 \end{array} \right.$$

Es decir, tiene una solución con multiplicidad 1 y otra con multiplicidad 3.

⁕ Soluciones.

Por lo tanto, las sucesiones,

$$\begin{array}{rcl} \{n^0\lambda_1^n\} & = & \{(-2)^n\} \\ \{n^0\lambda_2^n\} & = & \{2^n\} \\ \{n^1\lambda_3^n\} & = & \{n2^n\} \\ \{n^2\lambda_3^n\} & = & \{n^22^n\} \end{array}$$

son, todas, soluciones de la ecuación propuesta.

⁕ Solución general.

Por el *Principio de Superposición*, 14.3.1, la solución general será la sucesión $\{a_n\}$ tal que

$$a_n = \alpha_1 (-2)^n + \alpha_2 2^n + \alpha_3 n2^n + \alpha_4 n^2 2^n, \ \forall \alpha_1, \alpha_2, \alpha_3, \alpha_4 \in \mathbb{R}$$

♢ Obtención de la solución única.

Como disponemos de cuatro condiciones iniciales, podremos calcular los coeficientes de la solución general y de esta forma obtener una solución única para las condiciones iniciales dadas.

⁕ Cálculo de los coeficientes de la solución general.

De $a_1 = -4$, $a_2 = -8$, $a_3 = -64$ y $a_4 = -192$ se sigue

$$\left. \begin{array}{rcrcrcrcr} -2\alpha_1 & + & 2\alpha_2 & + & 2\alpha_3 & + & 2\alpha_4 & = & -4 \\ 4\alpha_1 & + & 4\alpha_2 & + & 8\alpha_3 & + & 16\alpha_4 & = & -8 \\ -8\alpha_1 & + & 8\alpha_2 & + & 24\alpha_3 & + & 72\alpha_4 & = & -64 \\ 16\alpha_1 & + & 16\alpha_2 & + & 64\alpha_3 & + & 256\alpha_4 & = & -192 \end{array} \right\} \Longrightarrow \left\{ \begin{array}{rcr} \alpha_1 & = & 1 \\ \alpha_2 & = & -1 \\ \alpha_3 & = & 1 \\ \alpha_4 & = & -1 \end{array} \right.$$

⁕ Solución única para las condiciones iniciales dadas.

Por lo tanto, la sucesión $\{a_n\}$ tal que

$$a_n = (-2)^n - 2^n + n2^n - n^2 2^n, \ n \geqslant 1$$

es, por el teorema 14.2.1, la solución única de la ecuación propuesta.

♦

Ejemplo 15.16

Resolver la ecuación de recurrencia

$$a_{n+4} = 12a_{n+3} - 54a_{n+2} + 108a_{n+1} - 81a_n,\ n \geqslant 1$$

con las condiciones iniciales $a_1 = 6,\ a_2 = 0,\ a_3 = -270,\ a_4 = -2754.$

Solución.

La ecuación escrita en su forma general es

$$a_{n+4} - 12a_{n+3} + 54a_{n+2} - 108a_{n+1} + 81a_n = 0$$

o sea, es lineal, de cuarto orden y con coeficientes constantes.

◊ Obtención de la solución general.

Por 15.3.3, si λ es raíz de su ecuación característica con multiplicidad m, entonces las sucesiones $\{a_n\}$ tales que

$$a_n = n^q\lambda^n,\ 0 \leqslant q \leqslant m-1$$

son, todas, soluciones de la ecuación.

- Ecuación característica.

$$\lambda^4 - 12\lambda^3 + 54\lambda^2 - 108\lambda + 81 = 0 \Longrightarrow \begin{cases} \lambda_1 &= 3 \\ \lambda_2 &= 3 \\ \lambda_3 &= 3 \\ \lambda_4 &= 3 \end{cases}$$

  Es decir, tiene una solución con multiplicidad 4.

- Soluciones.

  Por lo tanto, las sucesiones,

$$\begin{aligned} \{n^0\lambda_1^n\} &= \{3^n\} \\ \{n^1\lambda_2^n\} &= \{n3^n\} \\ \{n^2\lambda_3^n\} &= \{n^23^n\} \\ \{n^3\lambda_3^n\} &= \{n^33^n\} \end{aligned}$$

  son, todas, soluciones de la ecuación propuesta.

- Solución general.

  Por el *Principio de Superposición*, 14.3.1, la solución general será la sucesión $\{a_n\}$ tal que

$$a_n = \alpha_1 3^n + \alpha_2 n3^n + \alpha_3 n^2 3^n + \alpha_4 n^3 3^n,\ \forall \alpha_1, \alpha_2, \alpha_3, \alpha_4 \in \mathbb{R}$$

◊ Obtención de la solución única.

Como disponemos de cuatro condiciones iniciales, podremos calcular los coeficientes de la solución general y de esta forma obtener una solución única para las condiciones iniciales dadas.

⁕ Cálculo de los coeficientes de la solución general.

De $a_1 = 6$, $a_2 = 0$, $a_3 = -270$ y $a_4 = -2754$ se sigue

$$\left.\begin{array}{rcrcrcrcr} 3\alpha_1 & + & 3\alpha_2 & + & 3\alpha_3 & + & 3\alpha_4 & = & 6 \\ 9\alpha_1 & + & 18\alpha_2 & + & 36\alpha_3 & + & 72\alpha_4 & = & 0 \\ 27\alpha_1 & + & 81\alpha_2 & + & 243\alpha_3 & + & 729\alpha_4 & = & -270 \\ 81\alpha_1 & + & 324\alpha_2 & + & 1296\alpha_3 & + & 5184\alpha_4 & = & -2754 \end{array}\right\} \Longrightarrow \left\{\begin{array}{rcr} \alpha_1 & = & 2 \\ \alpha_2 & = & -1 \\ \alpha_3 & = & 2 \\ \alpha_4 & = & -1 \end{array}\right.$$

⁕ Solución única para las condiciones iniciales dadas.

Por lo tanto, la sucesión $\{a_n\}$ tal que

$$a_n = 2 \cdot 3^n - n3^n + 2n^2 3^n - n^3 3^n, \ n \geqslant 1$$

es, por el teorema 14.2.1, la solución única de la ecuación propuesta.

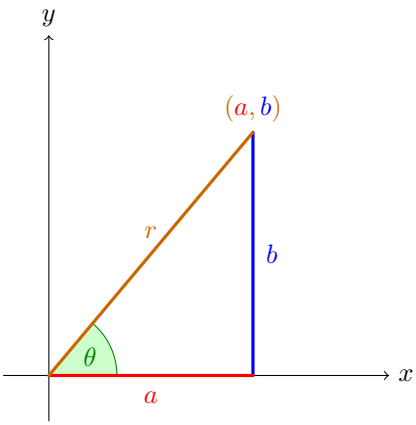
♦

Tenemos, pues, una técnica para calcular la solución de la ecuación de recurrencia lineal homogénea de orden k con coeficientes constantes. 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.

15.3.4 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,

$$c = r\,(\cos\theta + i\operatorname{sen}\theta)$$

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,

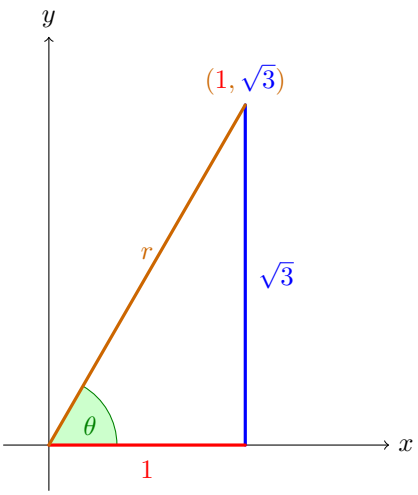
$$\begin{aligned} c = r\,(\cos\theta + i\operatorname{sen}\theta) \quad &\Longrightarrow \quad c^n = r^n\,(\cos\theta + i\operatorname{sen}\theta)^n \\ &\Longrightarrow \quad c^n = r^n\,(\cos n\theta + i\operatorname{sen} n\theta)\,, \ n \geqslant 0 \end{aligned}$$

♦

Ejemplo 15.17

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

$$\text{tag}\theta = \frac{\sqrt{3}}{1} = \sqrt{3} \implies \theta = \frac{\pi}{3}.$$

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 15.18

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,

$$\begin{aligned}
\lambda^2 - 2\lambda + 2 = 0 &\implies \lambda = \frac{2 \pm \sqrt{4 - 4 \cdot 2}}{2} \\
&\implies \lambda = \frac{2 \pm \sqrt{-4}}{2} \\
&\implies \lambda = \frac{2 \pm 2\sqrt{-1}}{2} \\
&\implies \lambda = 1 \pm i \\
&\implies \left\{ \begin{array}{rcl} \lambda & = & 1+i \\ \text{ó} & & \\ \lambda & = & 1-i \end{array} \right.
\end{aligned}$$

Por el teorema 15.3.3, las sucesiones $\{(1+i)^n\}$ y $\{(1-i)^n\}$ son, ambas, solución de la ecuación. Por el *principio de superposición* (14.3.1), 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,

$$\left.\begin{array}{rcl} a_1 & = & 2 \\ a_2 & = & 2 \\ a_n & = & \left(\sqrt{2}\right)^n\left(\beta_1\cos\frac{n\pi}{4} + \beta_2\,\text{sen}\,\frac{n\pi}{4}\right) \end{array}\right\}$$

de aquí que,

$$\left.\begin{array}{rcl}\sqrt{2}\left(\beta_1\cos\dfrac{\pi}{4}+\beta_2\,\text{sen}\,\dfrac{\pi}{4}\right) & = & 2\\ \left(\sqrt{2}\right)^2\left(\beta_1\cos\dfrac{2\pi}{4}+\beta_2\,\text{sen}\,\dfrac{2\pi}{4}\right) & = & 2\end{array}\right\} \Longrightarrow \left\{\begin{array}{rcrcl}\beta_1 & + & \beta_2 & = & 2\\ & & 2\beta_2 & = & 2\end{array}\right.$$

$$\Longrightarrow \left\{\begin{array}{rcl}\beta_1 & = & 1\\ \beta_2 & = & 1\end{array}\right.$$

y, consecuentemente, la sucesión $\{a_n\}$ tal que

$$a_n=\left(\sqrt{2}\right)^n\left(\cos\frac{n\pi}{4}+\text{sen}\,\frac{n\pi}{4}\right),\ n\geqslant 1$$

es la única solución de la ecuación propuesta.

♦♦♦

Lección 16

Recurrencias Lineales No Homogéneas

16.1 Introducción

16.1.1 Binomio de Newton

El Binomio de Newton se utiliza para calcular las potencias de un binomio.

$$(a+b)^n = \left(\begin{array}{c} n \\ 0 \end{array}\right) a^n + \left(\begin{array}{c} n \\ 1 \end{array}\right) a^{n-1}b + \left(\begin{array}{c} n \\ 2 \end{array}\right) a^{n-2}b^2 + \cdots + \left(\begin{array}{c} n \\ n-1 \end{array}\right) ab^{n-1} + \left(\begin{array}{c} n \\ n \end{array}\right) b^n$$

Cuando uno de los términos del binomio es negativo, se alternan los signos más y menos empezando por el signo más.

En cada uno de los sumandos los exponentes de a van decreciendo desde n hasta cero, en tanto que los exponentes de b crecen desde cero hasta n. La suma de los exponentes de a y b en cada uno de los términos es siempre igual a n.

Los coeficientes,

$$\left(\begin{array}{c} n \\ k \end{array}\right), \ k = 0, 1, ..., n$$

del binomio se pueden calcular fácilmente utilizando el Triángulo de Pascal o de Tartaglia.

♦

16.1.2 Triángulo de Pascal

$n=0$									1									
$n=1$								1			1							
$n=2$							1		2		1							
$n=3$						1		3		3		1						
$n=4$					1		4		6		4		1					
$n=5$				1		5		10		10		5		1				
$n=6$			1		6		15		20		15		6		1			
$n=7$		1		7		21		35		35		21		7		1		
$n=8$	1		8		28		56		70		56		28		8		1	
$n=9$	1	9		36		84		126		126		84		36		9		1

El triángulo se puede construir de forma muy sencilla. Los números de los extremos son siempre iguales a 1 y en el resto de los casos, cada número es igual a la suma de los dos números que tiene encima.

$$(a+b)^0 = 1$$
$$(a+b)^1 = 1a + 1b$$
$$(a+b)^2 = 1a^2 + 2ab + 1b^2$$
$$(a+b)^3 = 1a^3 + 3a^2b + 3ab^2 + 1b^3$$
$$(a+b)^4 = 1a^4 + 4a^3b + 6a^2b^2 + 4ab^3 + 1b^4$$
$$(a+b)^5 = 1a^5 + 5a^4b + 10a^3b^2 + 10a^2b^3 + 5ab^4 + 1b^5$$
$$(a+b)^6 = 1a^6 + 6a^5b + 15a^4b^2 + 20a^3b^3 + 15a^2b^4 + 6ab^5 + 1b^6$$
$$(a+b)^7 = 1a^7 + 7a^6b + 21a^5b^2 + 35a^4b^3 + 35a^3b^4 + 21a^2b^5 + 7ab^6 + 1b^7$$
$$(a+b)^8 = 1a^8 + 8a^7b + 28a^6b^2 + 56a^5b^3 + 70a^4b^4 + 56a^3b^5 + 28a^2b^6 + 8ab^7 + 1b^8$$
$$(a+b)^9 = 1a^9 + 9a^8b + 36a^7b^2 + 84a^6b^3 + 126a^5b^4 + 126a^4b^5 + 84a^3b^6 + 36a^2b^7 + 9ab^8 + 1b^9$$

♦

Ejemplo 16.1

Calcular el coeficiente de n^5 en el desarrollo de $(n+4)^8$ por el Binomio de Newton.

Solución.

Como n está elevado a 5 y la suma de los exponentes ha de ser, en este caso, igual a 8, el 4 deberá estar elevado a 3, es decir el término será $n^5 4^3$. El coeficiente, según el Binomio de Newton, será el número combinatorio,

$$\binom{8}{3}$$

y ahora podemos utilizar el Triángulo de Pascal para calcularlo. Bastaría buscar en la fila $n=8$ contando desde la izquierda a partir de cero y obtendríamos que es 56, es decir,

$$\binom{8}{3} = 56$$

El término en el que n está elevado a 5 en el desarrollo de $(n+4)^8$ sería, por tanto,

$$56n^5 4^3 = 56 \cdot 64n^5 = 3584n^5$$

y el coeficiente que buscábamos será 3584.

♦♦♦

16.2 Generalidades

16.2.1 Forma General

Según 14.1.4, una ecuación de recurrencia lineal, no homogénea, de orden k y con coeficientes constantes puede escribirse en su forma general, como

$$a_{n+k} + c_{k-1}a_{n+(k-1)} + c_{k-2}a_{n+(k-2)} + \cdots + c_2 a_{n+2} + c_1 a_{n+1} + c_0 a_n = h(n).$$

A la ecuación,

$$a_{n+k} + c_{k-1}a_{n+(k-1)} + c_{k-2}a_{n+(k-2)} + \cdots + c_2 a_{n+2} + c_1 a_{n+1} + c_0 a_n = 0.$$

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 la ecuación no homogénea, podemos calcular cualquier otra solución sin más que añadir una solución de la ecuación reducida a la solución encontrada.

16.2.2 Teorema

Sea la ecuación de recurrencia lineal, no homogénea, de orden k y con coeficientes constantes:

$$a_{n+k} + c_{k-1}a_{n+(k-1)} + c_{k-2}a_{n+(k-2)} + \cdots + c_2 a_{n+2} + c_1 a_{n+1} + c_0 a_n = h(n).$$

Si la sucesión $\{a_n^p\}$ es una solución particular de la ecuación dada y la sucesión $\{a_n^h\}$ 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,

$$a_{n+k} + c_{k-1}a_{n+(k-1)} + c_{k-2}a_{n+(k-2)} + \cdots + c_2 a_{n+2} + c_1 a_{n+1} + c_0 a_n = h(n)$$

y como $\{a_n^p\}$ es, por hipótesis, una solución de la ecuación,

$$a^p_{n+k} + c_{k-1}a^p_{n+(k-1)} + c_{k-2}a^p_{n+(k-2)} + \cdots + c_2 a^p_{n+2} + c_1 a^p_{n+1} + c_0 a^p_n = h(n)$$

y restando ambas ecuaciones,

$$\begin{array}{ccccccccccc} a_{n+k} & - & a^p_{n+k} & + & c_{k-1}\left(a_{n+(k-1)} - a^p_{n+(k-1)}\right) & + & c_{k-2}\left(a_{n+(k-2)} - a^p_{n+(k-2)}\right) & + & & & \\ & & & + & \cdots\cdots\cdots\cdots\cdots\cdots & + & c_0\left(a_n - a_n^p\right) & & = & 0 \end{array}$$

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, $\{a_n^p\}$, para la ecuación propuesta y éstas dependerán de la forma que tenga la función $h(n)$.

16.3 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,

$$h(n) = r^n\left(p_0 + p_1n + p_2n^2 + \cdots + p_tn^t\right)$$

podemos considerar 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 $\{a_n^p\}$ 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 $\{a_n^p\}$ 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 16.2

Resolver la ecuación de recurrencia

$$a_{n+1} = 2a_n + 1,\ n \geqslant 1$$

con la condición inicial $a_1 = 1$.

Solución.

La ecuación escrita en su forma general es

$$a_{n+1} - 2a_n = 1$$

o sea, es lineal, no homogénea, de orden 1 y con coeficientes constantes.

Por 16.2.2 la solución general de esta ecuación será la sucesión $\{a_n\}$ tal que

$$a_n = a_n^h + a_n^p$$

donde la sucesión $\{a_n^h\}$ es la solución general de la ecuación homogénea asociada y $\{a_n^p\}$ es una solución particular de la ecuación dada.

◊ Obtención de la solución general de la ecuación homogénea asociada.

Por 15.3.3, si λ es raíz de su ecuación característica con multiplicidad m, entonces las sucesiones $\{a_n\}$ tales que

$$a_n = n^q \lambda^n,\ 0 \leqslant q \leqslant m-1$$

son, todas, soluciones de la ecuación.

- ⁜ Ecuación característica.

  $$\lambda - 2 = 0 \Longrightarrow \lambda = 2$$

  Es decir, tiene una única solución que, obviamente, tiene multiplicidad $m = 1$.

- ⁜ Solución.

  Por lo tanto, la sucesión,

  $$\{n^0 \lambda^n\} \quad = \quad \{2^n\}$$

  es solución de la ecuación homogénea asociada.

- ⁜ Solución general.

  Por el *Principio de Superposición*, 14.3.1, la solución general será la sucesión $\{a_n^h\}$ tal que

  $$a_n^h = \alpha 2^n,\ \forall \alpha \in \mathbb{R}$$

◊ Obtención de una solución particular de la ecuación no homogénea propuesta.

$$a_{n+1} - 2a_n = 1$$

El término independiente,

$$h(n) = 1$$

es de la forma r^n por p_0, polinomio de grado cero,

$$h(n) = r^n p_0$$

donde $r = 1$ y $p_0 = 1$.

Como $r = 1$ no es raíz de la ecuación característica de la homogénea asociada, estaríamos en el primer caso del *Método de los Coeficientes Indeterminados*, 16.3, y la solución que buscamos sería, por tanto, la sucesión $\{a_n^p\}$ tal que

$$a_n^p = r^n A_0$$

En nuestro caso,

$$a_n^p = A_0$$

- ⁜ Cálculo de A_0.

  Como $\{a_n^p\}$ es solución de la ecuación propuesta, a_n^p deberá verificarla, es decir,

  $$a_{n+1}^p - 2a_n^p = 1 \Longrightarrow A_0 - 2A_0 = 1 \Longrightarrow A_0 = -1$$

⁕ Solución particular.

Por lo tanto, la sucesión $\{a_n^p\}$ tal que

$$a_n^p = -1$$

es una solución particular de la ecuación propuesta.

◊ Solución general.

Por 16.2.2, la sucesión $\{a_n\}$ tal que

$$a_n = \alpha 2^n - 1$$

será la solución general de nuestra ecuación.

◊ Obtención de solución única.

Como disponemos de una condición inicial, podremos calcular los coeficientes de la solución general y de esta forma obtener una solución única para dicha condición.

⁕ Cálculo de los coeficientes de la solución general.

$$a_1 = 1 \Longrightarrow \alpha 2^1 - 1 = 1 \Longrightarrow 2\alpha - 1 = 1 \Longrightarrow \alpha = 1$$

⁕ Solución única.

Por lo tanto, la sucesión $\{a_n\}$ tal que

$$a_n = 2^n - 1,\ n \geqslant 1$$

es solución única de la ecuación propuesta para la condición inicial dada.

♦

Ejemplo 16.3

Resolver la ecuación de recurrencia

$$a_{n+1} = -a_n + (-1)^{n+1},\ n \geqslant 1$$

con la condición inicial $a_1 = -3$.

Solución.

La ecuación escrita en su forma general es

$$a_{n+1} + a_n = (-1)^{n+1}$$

o sea, es lineal, no homogénea, de orden 1 y con coeficientes constantes.

Por 16.2.2 la solución general de esta ecuación será la sucesión $\{a_n\}$ tal que

$$a_n = a_n^h + a_n^p$$

donde la sucesión $\{a_n^h\}$ es la solución general de la ecuación homogénea asociada y $\{a_n^p\}$ es una solución particular de la ecuación dada.

◊ Obtención de la solución general de la ecuación homogénea asociada.

Por 15.3.3, si λ es raíz de su ecuación característica con multiplicidad m, entonces las sucesiones $\{a_n\}$ tales que

$$a_n = n^q \lambda^n,\ 0 \leqslant q \leqslant m-1$$

son, todas, soluciones de la ecuación.

⁕ Ecuación característica.

$$\lambda + 1 = 0 \Longrightarrow \lambda = -1$$

Es decir, tiene una única solución que, obviamente, tiene multiplicidad $m = 1$.

⁕ Solución.

Por lo tanto, la sucesión,

$$\left\{n^0 \lambda^n\right\} \quad = \quad \left\{(-1)^n\right\}$$

es solución de la ecuación homogénea asociada.

⁕ Solución general.

Por el *Principio de Superposición*, 14.3.1, la solución general será la sucesión $\left\{a_n^h\right\}$ tal que

$$a_n^h = \alpha\,(-1)^n\,,\ \forall \alpha \in \mathbb{R}$$

◊ Obtención de una solución particular de la ecuación no homogénea propuesta.

$$a_{n+1} + a_n = \ (-1)^{n+1}$$

El término independiente,

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

es de la forma r^n por p_0, polinomio de grado cero,

$$h(n) = r^n p_0$$

donde $r = -1$ y $p_0 = -1$.

Como $r = -1$ es raíz de la ecuación característica de la homogénea asociada, estaríamos en el segundo caso del *Método de los Coeficientes Indeterminados*, 16.3, y la solución que buscamos sería, por tanto, la sucesión $\{a_n^p\}$ tal que

$$a_n^p = n^m r^n A_0$$

En nuestro caso,

$$a_n^p = n\,(-1)^n\,A_0$$

⁕ Cálculo de A_0.

Como $\{a_n^p\}$ es solución de la ecuación propuesta, a_n^p deberá verificarla, es decir,

$$\begin{aligned}
a_{n+1}^p + a_n^p = (-1)^n(-1) \quad &\Longrightarrow \quad (n+1)(-1)^{n+1}A_0 + n(-1)^n A_0 = (-1)^n(-1) \\
&\Longrightarrow \quad (n+1)(-1)^n(-A_0) + n(-1)^n A_0 = (-1)^n(-1) \\
&\Longrightarrow \quad (n+1)(-A_0) + nA_0 = -1 \\
&\Longrightarrow \quad (-n-1+n)A_0 = -1 \\
&\Longrightarrow \quad A_0 = 1
\end{aligned}$$

⁕ Solución particular.

Por lo tanto, la sucesión $\{a_n^p\}$ tal que

$$a_n^p = n(-1)^n$$

es una solución particular de la ecuación propuesta.

◊ Solución general.

Por 16.2.2, la sucesión $\{a_n\}$ tal que

$$a_n = \alpha\,(-1)^n + n\,(-1)^n$$

será la solución general de nuestra ecuación.

◊ Obtención de solución única.

Como disponemos de una condición inicial, podremos calcular los coeficientes de la solución general y de esta forma obtener una solución única para dicha condición.

- ⁕ Cálculo de los coeficientes de la solución general.

$$a_1 = -3 \Longrightarrow \alpha(-1) + 1(-1) = -3 \Longrightarrow -\alpha - 1 = -3 \Longrightarrow \alpha = 2$$

- ⁕ Solución única.

  Por lo tanto, la sucesión $\{a_n\}$ tal que

$$a_n = 2\,(-1)^n + n\,(-1)^n,\ n \geqslant 1$$

  es solución única de la ecuación propuesta para la condición inicial dada.

♦

Ejemplo 16.4

Resolver la ecuación de recurrencia

$$a_{n+1} = -2a_n + (-2)^{n+1}\,(4n+3),\ n \geqslant 1$$

con la condición inicial $a_1 = -12$.

Solución.

La ecuación escrita en su forma general es

$$a_{n+1} + 2a_n = (-2)^{n+1}\,(4n+3)$$

o sea, es lineal, no homogénea, de orden 1 y con coeficientes constantes.

Por 16.2.2 la solución general de esta ecuación será la sucesión $\{a_n\}$ tal que

$$a_n = a_n^h + a_n^p$$

donde la sucesión $\{a_n^h\}$ es la solución general de la ecuación homogénea asociada y $\{a_n^p\}$ es una solución particular de la ecuación dada.

◊ Obtención de la solución general de la ecuación homogénea asociada.

Por 15.3.3, si λ es raíz de su ecuación característica con multiplicidad m, entonces las sucesiones $\{a_n\}$ tales que

$$a_n = n^q\lambda^n,\ 0 \leqslant q \leqslant m-1$$

son, todas, soluciones de la ecuación.

⁕ Ecuación característica.

$$\lambda + 2 = 0 \Longrightarrow \lambda = -2$$

Es decir, tiene una única solución que, obviamente, tiene multiplicidad $m = 1$.

⁕ Solución.

Por lo tanto, la sucesión,

$$\left\{n^0\lambda^n\right\} \quad = \quad \{(-2)^n\}$$

es solución de la ecuación homogénea asociada.

⁕ Solución general.

Por el *Principio de Superposición*, 14.3.1, la solución general será la sucesión $\left\{a_n^h\right\}$ tal que

$$a_n^h = \alpha\,(-2)^n\,,\ \forall\alpha \in \mathbb{R}$$

◊ Obtención de una solución particular de la ecuación no homogénea propuesta.

$$a_{n+1} + 2a_n = \ (-2)^{n+1}\,(4n+3)$$

El término independiente,

$$h(n) = \ (-2)^{n+1}\,(4n+3) = (-2)^n\,(-8n-6)$$

es de la forma r^n por p_0, polinomio de grado 1,

$$h(n) = r^n\,(p_1 n + p_0)$$

donde $r = -2$ y $p_0 = -6$ y $p_1 = -8$.

Como $r = -2$ es raíz de la ecuación característica de la homogénea asociada, estaríamos en el segundo caso del *Método de los Coeficientes Indeterminados*, 16.3, y la solución que buscamos sería, por tanto, la sucesión $\{a_n^p\}$ tal que

$$a_n^p = n^m r^n\,(A_0 + A_1 n)$$

En nuestro caso,

$$a_n^p = n\,(-2)^n\,(A_0 + A_1 n)$$

⁕ Cálculo de A_0 y A_1.

Como $\{a_n^p\}$ es solución de la ecuación propuesta, a_n^p deberá verificarla, es decir,

$$a_{n+1}^p + 2a_n^p = (-2)^n\,(-8n-6)$$

luego,

$$(n+1)(-2)^{n+1}\,[A_0 + A_1(n+1)] + 2n(-2)^n\,(A_0 + A_1 n) = (-2)^n\,(-8n-6)$$

y simplificando,

$$-2(n+1)\,[A_0 + A_1(n+1)] + 2n\,(A_0 + A_1 n) = -8n - 6$$

– El término independiente del primer miembro es

$$-2A_0 - 2A_1$$

y deberá ser igual al término independiente del segundo miembro, es decir,

$$-2A_0 - 2A_1 = -6$$

– El coeficiente del término en n del primer miembro es $-4A_1$ y deberá ser igual al coeficiente del término en n del segundo miembro, o sea,

$$-4A_1 = -8$$

Tendremos, pues, el sistema de ecuaciones,

$$\left.\begin{array}{rcrcrcl} - & 2A_0 & - & 2A_1 & = & -6 \\ & & - & 4A_1 & = & -8 \end{array}\right\} \Longrightarrow \left\{\begin{array}{rcl} A_0 & = & 1 \\ A_1 & = & 2 \end{array}\right.$$

⁕ Solución particular.

Por lo tanto, la sucesión $\{a_n^p\}$ tal que

$$a_n^p = n(-2)^n(2n+1)$$

es una solución particular de la ecuación propuesta.

◊ Solución general.

Por 16.2.2, la sucesión $\{a_n\}$ tal que

$$a_n = \alpha\,(-2)^n + n\,(-2)^n\,(2n+1)$$

será la solución general de nuestra ecuación.

◊ Obtención de solución única.

Como disponemos de una condición inicial, podremos calcular los coeficientes de la solución general y de esta forma obtener una solución única para dicha condición.

⁕ Cálculo de los coeficientes de la solución general.

$$a_1 = -12 \Longrightarrow \alpha(-2) + 3(-2) = -12 \Longrightarrow -2\alpha - 6 = -12 \Longrightarrow \alpha = 3$$

⁕ Solución única.

Por lo tanto, la sucesión $\{a_n\}$ tal que

$$a_n = 3\,(-2)^n + n\,(-2)^n\,(2n+1)\,,\ n \geqslant 1$$

es solución única de la ecuación propuesta para la condición inicial dada.

♦

Ejemplo 16.5

Resolver la ecuación de recurrencia

$$a_{n+1} = -3a_n + (-3)^{n+1}\left(3n^2+7n+4\right),\ n \geqslant 1$$

con la condición inicial $a_1 = -15$.

Solución.

La ecuación escrita en su forma general es

$$a_{n+1} + 3a_n = (-3)^{n+1}\left(3n^2+7n+4\right)$$

o sea, es lineal, no homogénea, de orden 1 y con coeficientes constantes.

Por 16.2.2 la solución general de esta ecuación será la sucesión $\{a_n\}$ tal que

$$a_n = a_n^h + a_n^p$$

donde la sucesión $\left\{a_n^h\right\}$ es la solución general de la ecuación homogénea asociada y $\{a_n^p\}$ es una solución particular de la ecuación dada.

♢ Obtención de la solución general de la ecuación homogénea asociada.

Por 15.3.3, si λ es raíz de su ecuación característica con multiplicidad m, entonces las sucesiones $\{a_n\}$ tales que

$$a_n = n^q \lambda^n,\ 0 \leqslant q \leqslant m-1$$

son, todas, soluciones de la ecuación.

⁕ Ecuación característica.

$$\lambda + 3 = 0 \Longrightarrow \lambda = -3$$

Es decir, tiene una única solución que, obviamente, tiene multiplicidad $m = 1$.

⁕ Solución.

Por lo tanto, la sucesión,

$$\left\{n^0 \lambda^n\right\} \quad = \quad \{(-3)^n\}$$

es solución de la ecuación homogénea asociada.

⁕ Solución general.

Por el *Principio de Superposición*, 14.3.1, la solución general será la sucesión $\left\{a_n^h\right\}$ tal que

$$a_n^h = \alpha\,(-3)^n\,,\ \forall \alpha \in \mathbb{R}$$

♢ Obtención de una solución particular de la ecuación no homogénea propuesta.

$$a_{n+1} + 3a_n = \ (-3)^{n+1}\left(3n^2 + 7n + 4\right)$$

El término independiente,

$$h(n) = \ (-3)^{n+1}\left(3n^2 + 7n + 4\right) = (-3)^n\left(-9n^2 - 21n - 12\right)$$

es de la forma r^n por un polinomio de grado 2,

$$h(n) = r^n\left(p_2 n^2 + p_1 n + p_0\right)$$

donde $r = -3$ y $p_0 = -12$, $p_1 = -21$ y $p_2 = -9$. Como $r = -3$ es raíz de la ecuación característica de la homogénea asociada, estaríamos en el segundo caso del *Método de los Coeficientes Indeterminados*, 16.3, y la solución que buscamos sería, por tanto, la sucesión $\{a_n^p\}$ tal que

$$a_n^p = n^m r^n\left(A_0 + A_1 n + A_2 n^2\right)$$

En nuestro caso,

$$a_n^p = n(-3)^n\left(A_0 + A_1 n + A_2 n^2\right)$$

⁕ Cálculo de A_0, A_1 y A_2.

Como $\{a_n^p\}$ es solución de la ecuación propuesta, a_n^p deberá verificarla, es decir,

$$a_{n+1}^p + 3a_n^p = (-3)^n\left(-9n^2 - 21n - 12\right)$$

luego,

$$\begin{aligned} & (n+1)(-3)^{n+1}\left[A_0+A_1(n+1)+A_2(n+1)^2\right] \\ + \quad & 3n(-3)^n\left(A_0+A_1n+A_2n^2\right) \\ = \quad & (-3)^n\left(-9n^2-21n-12\right) \end{aligned}$$

y simplificando,

$$\begin{aligned} - \quad & 3(n+1)\left[A_0+A_1(n+1)+A_2(n+1)^2\right] \\ + \quad & 3n\left(A_0+A_1n+A_2n^2\right) \\ = \quad & -9n^2-21n-12 \end{aligned}$$

es decir,

$$\begin{aligned} - \quad & 3A_0(n+1)-3A_1(n+1)^2-3A_2(n+1)^3 \\ + \quad & 3A_0n+3A_1n^2+3A_2n^3 \\ = \quad & -9n^2-21n-12 \end{aligned}$$

Para calcular las potencias de n en el primer miembro, utilizaremos el Binomio de Newton, (16.1.1), y el Triángulo de Pascal, (16.1.2), para obtener los coeficientes del Binomio.

$$\begin{array}{ccccccccc} 0 & & & & 1 & & & & \\ 1 & & & 1 & & 1 & & & \\ 2 & & 1 & & 2 & & 1 & & \\ 3 & 1 & & 3 & & 3 & & 1 & \end{array}$$

- El término independiente de $n+1$ es $n^0\cdot 1^1\cdot 1=1$.
- El término independiente de $(n+1)^2$ es $n^0\cdot 1^2\cdot 1=1$.
- El término independiente de $(n+1)^3$ es $n^0\cdot 1^3\cdot 1=1$.

Por lo tanto, el término independiente del primer miembro será:

$$-3A_0-3A_1-3A_2$$

y deberá ser igual al término independiente del segundo miembro, es decir,

$$-3A_0-3A_1-3A_2=-12$$

Obtendremos, ahora, los términos en n.

- El término en n de $n+1$ es $n^1\cdot 1^0\cdot 1=1n$.
- El término en n de $(n+1)^2$ es $n^1\cdot 1^1\cdot 2=2n$.
- El término en n de $(n+1)^3$ es $n^1\cdot 1^2\cdot 3=3n$.

El coeficiente del término en n del primer miembro será, por tanto,

$$-3A_0\cdot 1-3A_1\cdot 2-3A_2\cdot 3+3A_0=-6A_1-9A_2$$

y deberá ser igual al coeficiente de n en el segundo miembro, es decir,

$$-6A_1-9A_2=-21$$

Procediendo de manera idéntica, calcularemos el coeficiente del término en n^2 del primer miembro y lo igualamos con su correspondiente del segundo.

- El término en n^2 de $(n+1)^2$ es $n^2\cdot 1^0\cdot 1=1n^2$.
- El término en n^2 de $(n+1)^3$ es $n^2\cdot 1^1\cdot 3=3n^2$.

Es decir,

$$-3A_1 \cdot 1 - 3A_2 \cdot 3 + 3A_1 = -9 \Longrightarrow -9A_2 = -9$$

Tendremos, pues, el sistema de ecuaciones,

$$\left.\begin{array}{rrrrrrrrr} - & 3A_0 & - & 3A_1 & - & 3A_2 & = & -12 \\ & & - & 6A_1 & - & 9A_2 & = & -21 \\ & & & & - & 9A_2 & = & -9 \end{array}\right\} \Longrightarrow \left\{\begin{array}{rcl} A_0 & = & 1 \\ A_1 & = & 2 \\ A_2 & = & 1 \end{array}\right.$$

✳ Solución particular.

Por lo tanto, la sucesión $\{a_n^p\}$ tal que

$$a_n^p = n\,(-3)^n\left(n^2+2n+1\right)$$

es una solución particular de la ecuación propuesta.

◊ Solución general.

Por 16.2.2, la sucesión $\{a_n\}$ tal que

$$a_n = \alpha\,(-3)^n + n\,(-3)^n\left(n^2+2n+1\right)$$

será la solución general de nuestra ecuación.

◊ Obtención de solución única.

Como disponemos de una condición inicial, podremos calcular los coeficientes de la solución general y de esta forma obtener una solución única para dicha condición.

✳ Cálculo de los coeficientes de la solución general.

$$a_1 = -15 \Longrightarrow \alpha(-3) + 4(-3) = -15 \Longrightarrow -3\alpha - 12 = -15 \Longrightarrow \alpha = 1$$

✳ Solución única.

Por lo tanto, la sucesión $\{a_n\}$ tal que

$$a_n = (-3)^n + n\,(-3)^n\left(n^2+2n+1\right),\ n \geqslant 1$$

es solución única de la ecuación propuesta para la condición inicial dada.

♦

Ejemplo 16.6

Resolver la ecuación de recurrencia

$$a_{n+1} = -a_n + (-1)^{n+1}\left(4n^3+9n^2+9n+4\right),\ n \geqslant 1$$

con la condición inicial $a_1 = -7$.

Solución.

La ecuación escrita en su forma general es

$$a_{n+1} + a_n = (-1)^{n+1}\left(4n^3+9n^2+9n+4\right)$$

o sea, es lineal, no homogénea, de orden 1 y con coeficientes constantes.

Por 16.2.2 la solución general de esta ecuación será la sucesión $\{a_n\}$ tal que

$$a_n = a_n^h + a_n^p$$

donde la sucesión $\left\{a_n^h\right\}$ es la solución general de la ecuación homogénea asociada y $\{a_n^p\}$ es una solución particular de la ecuación dada.

◊ Obtención de la solución general de la ecuación homogénea asociada.

Por 15.3.3, si λ es raíz de su ecuación característica con multiplicidad m, entonces las sucesiones $\{a_n\}$ tales que

$$a_n = n^q\lambda^n,\ 0 \leqslant q \leqslant m-1$$

son, todas, soluciones de la ecuación.

- ⁕ Ecuación característica.

  $$\lambda + 1 = 0 \Longrightarrow \lambda = -1$$

  Es decir, tiene una única solución que, obviamente, tiene multiplicidad $m = 1$.

- ⁕ Solución.

  Por lo tanto, la sucesión,

  $$\left\{n^0\lambda^n\right\} \quad = \quad \{(-1)^n\}$$

  es solución de la ecuación homogénea asociada.

- ⁕ Solución general.

  Por el *Principio de Superposición*, 14.3.1, la solución general será la sucesión $\left\{a_n^h\right\}$ tal que

  $$a_n^h = \alpha\,(-1)^n\,,\ \forall\alpha \in \mathbb{R}$$

◊ Obtención de una solución particular de la ecuación no homogénea propuesta.

$$a_{n+1} + a_n = \ (-1)^{n+1}\left(4n^3 + 9n^2 + 9n + 4\right)$$

El término independiente,

$$h(n) = \ (-1)^{n+1}\left(4n^3 + 9n^2 + 9n + 4\right) = (-1)^n\left(-4n^3 - 9n^2 - 9n - 4\right)$$

es de la forma r^n por un polinomio de grado 3,

$$h(n) = r^n\left(p_3n^3 + p_2n^2 + p_1n + p_0\right)$$

donde $r = -1$ y $p_0 = -4$, $p_1 = -9$, $p_2 = -9$ y $p_3 = -4$. Como $r = -1$ es raíz de la ecuación característica de la homogénea asociada, estaríamos en el segundo caso del *Método de los Coeficientes Indeterminados*, 16.3, y la solución que buscamos sería, por tanto, la sucesión $\{a_n^p\}$ tal que

$$a_n^p = n^m r^n\left(A_0 + A_1n + A_2n^2 + A_3n^3\right)$$

En nuestro caso,

$$a_n^p = n(-1)^n\left(A_0 + A_1n + A_2n^2 + A_3n^3\right)$$

⁂ Cálculo de A_0, A_1, A_2 y A_3.

Como $\{a_n^p\}$ es solución de la ecuación propuesta, a_n^p deberá verificarla, es decir,

$$a_{n+1}^p + a_n^p = (-1)^n \left(-4n^3 - 9n^2 - 9n - 4\right)$$

luego,

$$\begin{aligned} & (n+1)(-1)^{n+1}\left[A_0 + A_1(n+1) + A_2(n+1)^2 + A_3(n+1)^3\right] \\ + \;& n(-1)^n\left(A_0 + A_1 n + A_2 n^2 + A_3 n^3\right) \\ = \;& (-1)^n\left(-4n^3 - 9n^2 - 9n - 4\right) \end{aligned}$$

y simplificando,

$$\begin{aligned} - \;& (n+1)\left[A_0 + A_1(n+1) + A_2(n+1)^2 + A_3(n+1)^3\right] \\ + \;& n\left(A_0 + A_1 n + A_2 n^2 + A_3 n^3\right) \\ = \;& -4n^3 - 9n^2 - 9n - 4 \end{aligned}$$

es decir,

$$\begin{aligned} - \;& A_0(n+1) - A_1(n+1)^2 - A_2(n+1)^3 - A_3(n+1)^4 \\ + \;& A_0 n + A_1 n^2 + A_2 n^3 + A_3 n^4 \\ = \;& -4n^3 - 9n^2 - 9n - 4 \end{aligned}$$

Para calcular las potencias de n en el primer miembro, utilizaremos el Binomio de Newton, (16.1.1), y el Triángulo de Pascal, (16.1.2), para obtener los coeficientes del Binomio.

$$\begin{array}{ccccccccc} 0 & & & & 1 & & & & \\ 1 & & & 1 & & 1 & & & \\ 2 & & 1 & & 2 & & 1 & & \\ 3 & & 1 & & 3 & & 3 & & 1 \\ 4 & 1 & & 4 & & 6 & & 4 & & 1 \end{array}$$

- El término independiente de $n+1$ es $n^0 \cdot 1^1 \cdot 1 = 1$.
- El término independiente de $(n+1)^2$ es $n^0 \cdot 1^2 \cdot 1 = 1$.
- El término independiente de $(n+1)^3$ es $n^0 \cdot 1^3 \cdot 1 = 1$.
- El término independiente de $(n+1)^4$ es $n^0 \cdot 1^4 \cdot 1 = 1$.

Por lo tanto, el término independiente del primer miembro será:

$$-3A_0 - 3A_1 - 3A_2$$

y deberá ser igual al término independiente del segundo miembro, es decir,

$$-3A_0 - 3A_1 - 3A_2 = -4$$

Veamos, ahora, los términos en n.

- El término en n de $n+1$ es $n^1 \cdot 1^0 \cdot 1 = 1n$.
- El término en n de $(n+1)^2$ es $n^1 \cdot 1^1 \cdot 2 = 2n$.
- El término en n de $(n+1)^3$ es $n^1 \cdot 1^2 \cdot 1 = 3n$.
- El término en n de $(n+1)^4$ es $n^1 \cdot 1^3 \cdot 4 = 4n$.

El coeficiente del término en n del primer miembro será, por tanto,

$$-A_0 \cdot 1 - A_1 \cdot 2 - A_2 \cdot 3 - A_3 \cdot 4 + A_0 = -2A_1 - 3A_2 - 4A_3$$

y deberá ser igual al coeficiente del término en n del segundo miembro, o sea,

$$-2A_1 - 3A_2 - 4A_3 = -9$$

Procederemos de forma idéntica para calcular los términos en n^2 del primer miembro.

- El término en n^2 de $(n+1)^2$ es $n^2 \cdot 1^0 \cdot 1 = 1n^2$.
- El término en n^2 de $(n+1)^3$ es $n^2 \cdot 1^1 \cdot 3 = 3n^2$.
- El término en n^2 de $(n+1)^4$ es $n^2 \cdot 1^2 \cdot 6 = 6n^2$.

Tenemos, por tanto, que el coeficiente de n^2 en el primer miembro es:

$$-A_1 \cdot 1 - A_2 \cdot 3 - A_3 \cdot 6 + A_1 = -3A_2 - 6A_3$$

e igualando a su correspondiente en el segundo miembro,

$$-3A_2 - 6A_3 = -9$$

Finalmente, calculamos el coeficiente del término en n^3 del primer miembro y lo igualamos al término en n^3 del segundo.

- El término en n^3 de $(n+1)^3$ es $n^3 \cdot 1^0 \cdot 1 = 1n^3$.
- El término en n^3 de $(n+1)^4$ es $n^3 \cdot 1^1 \cdot 4 = 4n^3$.

Es decir,

$$-A_2 \cdot 1 - A_3 \cdot 4 + A_2 = -4 \Longrightarrow -4A_3 = -4$$

Tendremos, pues, el sistema de ecuaciones,

$$\left.\begin{array}{rrrrrrrrr} - & A_0 & - & A_1 & - & A_2 & - & A_3 & = & -4 \\ & & - & 2A_1 & - & 3A_2 & - & 4A_3 & = & -9 \\ & & & & - & 3A_2 & - & 6A_3 & = & -9 \\ & & & & & & - & 4A_3 & = & -4 \end{array}\right\} \Longrightarrow \left\{\begin{array}{rcl} A_0 & = & 1 \\ A_1 & = & 1 \\ A_2 & = & 1 \\ A_3 & = & 1 \end{array}\right.$$

⁕ Solución particular.

Por lo tanto, la sucesión $\{a_n^p\}$ tal que

$$a_n^p = n\,(-1)^n\left(n^3 + n^2 + n + 1\right)$$

es una solución particular de la ecuación propuesta.

◊ Solución general.

Por 16.2.2, la sucesión $\{a_n\}$ tal que

$$a_n = \alpha\,(-1)^n + n\,(-1)^n\left(n^3 + n^2 + n + 1\right)$$

será la solución general de nuestra ecuación.

◊ Obtención de solución única.

Como disponemos de una condición inicial, podremos calcular los coeficientes de la solución general y de esta forma obtener una solución única para dicha condición.

⁕ Cálculo de los coeficientes de la solución general.

$$a_1 = -7 \Longrightarrow \alpha(-1) + 4(-1) = -7 \Longrightarrow -\alpha - 4 = -7 \Longrightarrow \alpha = 3$$

⁕ Solución única.

Por lo tanto, la sucesión $\{a_n\}$ tal que

$$a_n = 3\,(-1)^n + n\,(-1)^n\left(n^3 + n^2 + n + 1\right),\ n \geqslant 1$$

es solución única de la ecuación propuesta para la condición inicial dada.

♦

Ejemplo 16.7

Resolver la ecuación de recurrencia

$$a_{n+2} = a_n - 2\,(-1)^{n+1}\,(2n+3)\,,\ n \geqslant 1$$

con las condiciones iniciales $a_1 = -1,\ a_2 = 9$.

Solución.

La ecuación escrita en su forma general es

$$a_{n+2} - a_n = -2\,(-1)^{n+1}\,(2n+3)$$

o sea, es lineal, no homogénea, de orden 2 y con coeficientes constantes.

Por 16.2.2 la solución general de esta ecuación será la sucesión $\{a_n\}$ tal que

$$a_n = a_n^h + a_n^p$$

donde la sucesión $\left\{a_n^h\right\}$ es la solución general de la ecuación homogénea asociada y $\{a_n^p\}$ es una solución particular de la ecuación dada.

◊ Obtención de la solución general de la ecuación homogénea asociada.

Por 15.3.3, si λ es raíz de su ecuación característica con multiplicidad m, entonces las sucesiones $\{a_n\}$ tales que

$$a_n = n^q\lambda^n,\ 0 \leqslant q \leqslant m-1$$

son, todas, soluciones de la ecuación.

- Ecuación característica.

$$\lambda^2 - 1 = 0 \Longrightarrow \begin{cases} \lambda_1 &= -1 \\ \lambda_2 &= 1 \end{cases}$$

  Es decir, tiene dos soluciones con multiplicidad $m = 1$ cada una de ellas.

- Solución.

  Por lo tanto, las sucesiones,

$$\begin{aligned} \left\{n^0\lambda_1^n\right\} &= \left\{(-1)^n\right\} \\ \left\{n^0\lambda_2^n\right\} &= \{1\} \end{aligned}$$

  son, ambas, soluciones de la ecuación homogénea asociada.

- Solución general.

  Por el *Principio de Superposición*, 14.3.1, la solución general será la sucesión $\left\{a_n^h\right\}$ tal que

$$a_n^h = \alpha_1\,(-1)^n + \alpha_2,\ \forall\alpha \in \mathbb{R}$$

◊ Obtención de una solución particular de la ecuación no homogénea propuesta.

$$a_{n+2} - a_n = -2\,(-1)^{n+1}\,(2n+3)$$

El término independiente,

$$h(n) = -2\,(-1)^{n+1}\,(2n+3) = (-1)^n\,(4n+6)$$

es de la forma r^n por un polinomio de grado 1,

$$h(n) = r^n\,(p_1 n + p_0)$$

donde $r = -1$ y $p_0 = 6$ y $p_1 = 4$. Como $r = -1$ es raíz de la ecuación característica de la homogénea asociada, estaríamos en el segundo caso del *Método de los Coeficientes Indeterminados*, 16.3, y la solución que buscamos sería, por tanto, la sucesión $\{a_n^p\}$ tal que

$$a_n^p = n^m r^n \left(A_0 + A_1 n\right)$$

En nuestro caso,

$$a_n^p = n(-1)^n \left(A_0 + A_1 n\right)$$

⁕ Cálculo de A_0 y A_1.

Como $\{a_n^p\}$ es solución de la ecuación propuesta, a_n^p deberá verificarla, es decir,

$$a_{n+2}^p - a_n^p = (-1)^n \left(4n + 6\right)$$

luego,

$$(n+2)(-1)^{n+2}\left[A_0 + A_1(n+2)\right] - n(-1)^n \left(A_0 + A_1 n\right) = (-1)^n \left(4n + 6\right)$$

y simplificando,

$$(n+2)\left[A_0 + A_1(n+2)\right] - n\left(A_0 + A_1 n\right) = 4n + 6$$

es decir,

$$A_0(n+2) + A_1(n+2)^2 - A_0 n - A_1 n^2 = 4n + 6$$

– El término independiente del primer miembro es

$$2A_0 + 4A_1$$

y deberá ser igual al término independiente del segundo miembro, es decir,

$$2A_0 + 4A_1 = 6$$

– El coeficiente del término en n del primer miembro es $4A_1$, luego,

$$4A_1 = 4$$

Tendremos, pues, el sistema de ecuaciones,

$$\left.\begin{array}{rcrcl} 2A_0 & + & 4A_1 & = & 6 \\ & + & 4A_1 & = & 4 \end{array}\right\} \Longrightarrow \left\{\begin{array}{rcl} A_0 & = & 1 \\ A_1 & = & 1 \end{array}\right.$$

⁕ Solución particular.

Por lo tanto, la sucesión $\{a_n^p\}$ tal que

$$a_n^p = n\left(-1\right)^n \left(n + 1\right)$$

es una solución particular de la ecuación propuesta.

◊ Solución general.

Por 16.2.2, la sucesión $\{a_n\}$ tal que

$$a_n = \alpha_1 \left(-1\right)^n + \alpha_2 + n\left(-1\right)^n \left(n + 1\right)$$

será la solución general de nuestra ecuación.

◊ Obtención de solución única.

Como disponemos de dos condiciones iniciales, podremos calcular los coeficientes de la solución general y de esta forma obtener una solución única para dicha condición.

⁕ Cálculo de los coeficientes de la solución general.

De $a_1 = -1$ y $a_2 = 9$ se sigue

$$\left.\begin{array}{rcrcrcr} - & \alpha_1 & + & \alpha_2 & - & 2 & = & -1 \\ & \alpha_1 & + & \alpha_2 & + & 6 & = & 9 \end{array}\right\} \Longrightarrow \left\{\begin{array}{rcl} \alpha_1 & = & 1 \\ \alpha_2 & = & 2 \end{array}\right.$$

⁕ Solución única.

Por lo tanto, la sucesión $\{a_n\}$ tal que

$$a_n = (-1)^n + 2 + n\,(-1)^n\,(n+1)\,,\ n \geqslant 1$$

es solución única de la ecuación propuesta para la condición inicial dada.

♦

Ejemplo 16.8

Resolver la ecuación de recurrencia

$$a_{n+2} = -6a_{n+1} - 9a_n + 4\,(-3)^{n+3}\left(n^2+n\right),\ n \geqslant 1$$

con las condiciones iniciales $a_1 = -15,\ a_2 = 81$.

Solución.

La ecuación escrita en su forma general es

$$a_{n+2} + 6a_{n+1} + 9a_n = 4\,(-3)^{n+3}\left(n^2+n\right)$$

o sea, es lineal, no homogénea, de orden 2 y con coeficientes constantes.

Por 16.2.2 la solución general de esta ecuación será la sucesión $\{a_n\}$ tal que

$$a_n = a_n^h + a_n^p$$

donde la sucesión $\left\{a_n^h\right\}$ es la solución general de la ecuación homogénea asociada y $\{a_n^p\}$ es una solución particular de la ecuación dada.

◊ Obtención de la solución general de la ecuación homogénea asociada.

Por 15.3.3, si λ es raíz de su ecuación característica con multiplicidad m, entonces las sucesiones $\{a_n\}$ tales que

$$a_n = n^q\lambda^n,\ 0 \leqslant q \leqslant m-1$$

son, todas, soluciones de la ecuación.

⁕ Ecuación característica.

$$\lambda^2 + 6\lambda + 9 = 0 \Longrightarrow \left\{\begin{array}{rcl} \lambda_1 & = & -3 \\ \lambda_2 & = & -3 \end{array}\right.$$

Es decir, tiene una solución con multiplicidad $m = 2$.

⁕ Solución.

Por lo tanto, las sucesiones,

$$\begin{array}{rcl} \left\{n^0\lambda_1^n\right\} & = & \left\{(-3)^n\right\} \\ \left\{n^1\lambda_2^n\right\} & = & \left\{n\,(-3)^n\right\} \end{array}$$

son, ambas, soluciones de la ecuación homogénea asociada.

⁕ Solución general.

Por el *Principio de Superposición*, 14.3.1, la solución general será la sucesión $\left\{a_n^h\right\}$ tal que

$$a_n^h = \alpha_1 (-3)^n + \alpha_2 n (-3)^n\,,\ \forall \alpha \in \mathbb{R}$$

◊ Obtención de una solución particular de la ecuación no homogénea propuesta.

$$a_{n+2} + 6a_{n+1} + 9a_n = 4(-3)^{n+3}\left(n^2+n\right)$$

El término independiente,

$$h(n) = 4(-3)^{n+3}\left(n^2+n\right) = (-3)^n\left(-108n^2-108n\right)$$

es de la forma r^n por un polinomio de grado 2,

$$h(n) = r^n\left(p_2n^2+p_1n+p_0\right)$$

donde $r=-3$ y $p_0=0$, $p_1=-108$ y $p_2=-108$. Como $r=-3$ es raíz de la ecuación característica de la homogénea asociada, estaríamos en el segundo caso del *Método de los Coeficientes Indeterminados*, 16.3, y la solución que buscamos sería, por tanto, la sucesión $\{a_n^p\}$ tal que

$$a_n^p = n^m r^n\left(A_0+A_1n+A_2n^2\right)$$

En nuestro caso,

$$a_n^p = n^2(-3)^n\left(A_0+A_1n+A_2n^2\right)$$

⁕ Cálculo de A_0, A_1 y A_2.

Como $\{a_n^p\}$ es solución de la ecuación propuesta, a_n^p deberá verificarla, es decir,

$$a_{n+2}^p + 6a_{n+1}^p + 9a_n^p = (-3)^n\left(-108n^2-108n\right)$$

luego,

$$\begin{aligned}
& (n+2)^2(-3)^{n+2}\left[A_0+A_1(n+2)+A_2(n+2)^2\right] \\
+\ & 6(n+1)^2(-3)^{n+1}\left[A_0+A_1(n+1)+A_2(n+1)^2\right] \\
+\ & 9n^2(-3)^n\left(A_0+A_1n+A_2n^2\right) \\
=\ & (-3)^n\left(-108n^2-108n\right)
\end{aligned}$$

y simplificando,

$$\begin{aligned}
& 9(n+2)^2\left[A_0+A_1(n+2)+A_2(n+2)^2\right] \\
-\ & 18(n+1)^2\left[A_0+A_1(n+1)+A_2(n+1)^2\right] \\
+\ & 9n^2\left(A_0+A_1n+A_2n^2\right) \\
=\ & -108n^2-108n
\end{aligned}$$

es decir,

$$\begin{aligned}
& 9A_0(n+2)^2+9A_1(n+2)^3+9A_2(n+2)^4 \\
& -18A_0(n+1)^2-18A_1(n+1)^3-18A_2(n+1)^4 \\
& +9A_0n^2+9A_1n^3+9A_2n^4 \\
& =-108n^2-108n
\end{aligned}$$

Para calcular los coeficientes de las potencias de n en el primer miembro, utilizaremos el Binomio de Newton, (16.1.1), y el Triángulo de Pascal, (16.1.2), para obtener los coeficientes del mismo.

$$\begin{array}{ccccccccc}
0 & & & & 1 & & & & \\
1 & & & 1 & & 1 & & & \\
2 & & 1 & & 2 & & 1 & & \\
3 & & 1 & & 3 & & 3 & & 1 \\
4 & 1 & & 4 & & 6 & & 4 & & 1
\end{array}$$

- El término independiente de $(n+2)^2$ es $n^0 \cdot 2^2 \cdot 1 = 4$.
- El término independiente de $(n+2)^3$ es $n^0 \cdot 2^3 \cdot 1 = 8$.
- El término independiente de $(n+2)^4$ es $n^0 \cdot 2^4 \cdot 1 = 16$.
- El término independiente de $(n+1)^2$ es $n^0 \cdot 1^2 \cdot 1 = 1$.
- El término independiente de $(n+1)^3$ es $n^0 \cdot 1^3 \cdot 1 = 1$.
- El término independiente de $(n+1)^4$ es $n^0 \cdot 1^4 \cdot 1 = 1$.

Por lo tanto, el término independiente del primer miembro será:

$$\begin{array}{rlrlrl} & 9A_0 \cdot 4 & + & 9A_1 \cdot 8 & + & 9A_2 \cdot 16 \\ - & 18A_0 \cdot 1 & - & 18A_1 \cdot 1 & - & 18A_2 \cdot 1 \\ = & 18A_0 & + & 54A_1 & + & 126A_2 \end{array}$$

Igualándolo a cero, término independiente del segundo miembro, tendremos:

$$18A_0 + 54A_1 + 126A_2 = 0$$

Veamos como son los términos en n.

- El término en n de $(n+2)^2$ es $n^1 \cdot 2^1 \cdot 2 = 4n$.
- El término en n de $(n+2)^3$ es $n^1 \cdot 2^2 \cdot 3 = 12n$.
- El término en n de $(n+2)^4$ es $n^1 \cdot 2^3 \cdot 4 = 32n$.
- El término en n de $(n+1)^2$ es $n^1 \cdot 1^1 \cdot 2 = 2n$.
- El término en n de $(n+1)^3$ es $n^1 \cdot 1^2 \cdot 3 = 3n$.
- El término en n de $(n+1)^4$ es $n^1 \cdot 1^3 \cdot 4 = 4n$.

El coeficiente del término en n del primer miembro será, por tanto,

$$\begin{array}{rlrlrl} & 9A_0 \cdot 4 & + & 9A_1 \cdot 12 & + & 9A_2 \cdot 32 \\ - & 18A_0 \cdot 2 & - & 18A_1 \cdot 3 & - & 18A_2 \cdot 4 \\ = & & & 54A_1 & + & 216A_2 \end{array}$$

e igualando al coeficiente del término en n del segundo miembro,

$$54A_1 + 216A_2 = -108$$

Finalmente, veamos los términos en n^2.

- El término en n^2 de $(n+2)^2$ es $n^2 \cdot 2^0 \cdot 1 = 1n^2$.
- El término en n^2 de $(n+2)^3$ es $n^2 \cdot 2^1 \cdot 3 = 6n^2$.
- El término en n^2 de $(n+2)^4$ es $n^2 \cdot 2^2 \cdot 6 = 24n^2$.
- El término en n^2 de $(n+1)^2$ es $n^2 \cdot 1^0 \cdot 1 = 1n^2$.
- El término en n^2 de $(n+1)^3$ es $n^2 \cdot 1^1 \cdot 3 = 3n^2$.
- El término en n^2 de $(n+1)^4$ es $n^2 \cdot 1^2 \cdot 6 = 6n^2$.

Luego, el coeficiente del término en n^2 del primer miembro es:

$$\begin{array}{rlrlrl} & 9A_0 \cdot 1 & + & 9A_1 \cdot 6 & + & 9A_2 \cdot 24 \\ - & 18A_0 \cdot 1 & - & 18A_1 \cdot 3 & - & 18A_2 \cdot 6 \\ + & 9A_0 & & & & \\ = & & & & & 108A_2 \end{array}$$

y si igualamos al coeficiente del término en n^2 del segundo miembro,

$$108A_2 = -108$$

Tendremos, pues, el sistema de ecuaciones,

$$\left.\begin{array}{rcrcrcr} 18A_0 & + & 54A_1 & + & 126A_2 & = & 0 \\ & + & 54A_1 & + & 216A_2 & = & -108 \\ & & & + & 108A_2 & = & -108 \end{array}\right\} \Longrightarrow \left\{\begin{array}{rcr} A_0 & = & 1 \\ A_1 & = & 2 \\ A_2 & = & -1 \end{array}\right.$$

⁕ Solución particular.

Por lo tanto, la sucesión $\{a_n^p\}$ tal que

$$a_n^p = n^2\,(-3)^n\left(-n^2+2n+1\right)$$

es una solución particular de la ecuación propuesta.

◊ Solución general.

Por 16.2.2, la sucesión $\{a_n\}$ tal que

$$a_n = \alpha_1\,(-3)^n + \alpha_2 n\,(-3)^n + n^2\,(-3)^n\left(-n^2+2n+1\right)$$

será la solución general de nuestra ecuación.

◊ Obtención de solución única.

Como disponemos de dos condiciones iniciales, podremos calcular los coeficientes de la solución general y de esta forma obtener una solución única para dicha condición.

⁕ Cálculo de los coeficientes de la solución general.

De $a_1 = -15$ y $a_2 = 81$ se sigue

$$\left.\begin{array}{rcrcrcr} - & 3\alpha_1 & - & 3\alpha_2 & - & 6 & = & -15 \\ & 9\alpha_1 & + & 18\alpha_2 & + & 36 & = & 81 \end{array}\right\} \Longrightarrow \left\{\begin{array}{rcr} \alpha_1 & = & 1 \\ \alpha_2 & = & 2 \end{array}\right.$$

⁕ Solución única.

Por lo tanto, la sucesión $\{a_n\}$ tal que

$$a_n = (-3)^n + 2n\,(-3)^n + n^2\,(-3)^n\left(-n^2+2n+1\right),\ n \geqslant 1$$

es solución única de la ecuación propuesta para la condición inicial dada.

♦

Ejemplo 16.9

Resolver la ecuación de recurrencia

$$a_{n+2} = -4a_{n+1} - 4a_n - (-2)^{n+4}\left(10n^3+33n^2+38n+15\right),\ n \geqslant 1$$

con las condiciones iniciales $a_1 = -4$, $a_2 = -228$.

Solución.

La ecuación escrita en su forma general es

$$a_{n+2} + 4a_{n+1} + 4a_n = -(-2)^{n+4}\left(10n^3 + 33n^2 + 38n + 15\right)$$

o sea, es lineal, no homogénea, de orden 2 y con coeficientes constantes.

Por 16.2.2 la solución general de esta ecuación será la sucesión $\{a_n\}$ tal que

$$a_n = a_n^h + a_n^p$$

donde la sucesión $\left\{a_n^h\right\}$ es la solución general de la ecuación homogénea asociada y $\{a_n^p\}$ es una solución particular de la ecuación dada.

◊ Obtención de la solución general de la ecuación homogénea asociada.

Por 15.3.3, si λ es raíz de su ecuación característica con multiplicidad m, entonces las sucesiones $\{a_n\}$ tales que

$$a_n = n^q\lambda^n,\ 0 \leqslant q \leqslant m-1$$

son, todas, soluciones de la ecuación.

- ⁕ Ecuación característica.

$$\lambda^2 + 4\lambda + 4 = 0 \Longrightarrow \begin{cases} \lambda_1 &= -2 \\ \lambda_2 &= -2 \end{cases}$$

  Es decir, tiene una solución con multiplicidad $m = 2$.

- ⁕ Solución.

  Por lo tanto, las sucesiones,

$$\begin{aligned} \left\{n^0\lambda_1^n\right\} &= \left\{(-2)^n\right\} \\ \left\{n^1\lambda_2^n\right\} &= \left\{n\,(-2)^n\right\} \end{aligned}$$

  son, ambas, soluciones de la ecuación homogénea asociada.

- ⁕ Solución general.

  Por el *Principio de Superposición*, 14.3.1, la solución general será la sucesión $\left\{a_n^h\right\}$ tal que

$$a_n^h = \alpha_1(-2)^n + \alpha_2 n(-2)^n,\ \forall\alpha \in \mathbb{R}$$

◊ Obtención de una solución particular de la ecuación no homogénea propuesta.

$$a_{n+2} + 4a_{n+1} + 4a_n = -(-2)^{n+4}\left(10n^3 + 33n^2 + 38n + 15\right)$$

El término independiente,

$$h(n) = -(-2)^{n+4}\left(10n^3 + 33n^2 + 38n + 15\right) = (-2)^n\left(-160n^3 - 528n^2 - 608n - 240\right)$$

es de la forma r^n por un polinomio de grado 3,

$$h(n) = r^n\left(p_3n^3 + p_2n^2 + p_1n + p_0\right)$$

donde $r = -2$ y $p_0 = -240$, $p_1 = -608$, $p_2 = -528$ y $p_3 = -160$. Como $r = -2$ es raíz de la ecuación característica de la homogénea asociada, estaríamos en el segundo caso del *Método de los Coeficientes Indeterminados*, 16.3, y la solución que buscamos sería, por tanto, la sucesión $\{a_n^p\}$ tal que

$$a_n^p = n^m r^n\left(A_0 + A_1n + A_2n^2 + A_3n^3\right)$$

En nuestro caso,

$$a_n^p = n^2(-2)^n\left(A_0 + A_1n + A_2n^2 + A_3n^3\right)$$

⁂ Cálculo de A_0, A_1, A_2 y A_3.

Como $\{a_n^p\}$ es solución de la ecuación propuesta, a_n^p deberá verificarla, es decir,

$$a_{n+2}^p + 4a_{n+1}^p + 4a_n^p = (-2)^n\left(-160n^3 - 528n^2 - 608n - 240\right)$$

luego,

$$\begin{aligned}
& (n+2)^2(-2)^{n+2}\left[A_0 + A_1(n+2) + A_2(n+2)^2 + A_3(n+2)^3\right] \\
+\ & 4(n+1)^2(-2)^{n+1}\left[A_0 + A_1(n+1) + A_2(n+1)^2 + A_3(n+1)^3\right] \\
+\ & 4n^2(-2)^n\left(A_0 + A_1 n + A_2 n^2 + A_3 n^3\right) \\
=\ & (-2)^n\left(-160n^3 - 528n^2 - 608n - 240\right)
\end{aligned}$$

y simplificando,

$$\begin{aligned}
& 4(n+2)^2\left[A_0 + A_1(n+2) + A_2(n+2)^2 + A_3(n+2)^3\right] \\
-\ & 8(n+1)^2\left[A_0 + A_1(n+1) + A_2(n+1)^2 + A_3(n+1)^3\right] \\
+\ & 4n^2\left(A_0 + A_1 n + A_2 n^2 + A_3 n^3\right) \\
=\ & -160n^3 - 528n^2 - 608n - 240
\end{aligned}$$

es decir,

$$\begin{aligned}
& 4A_0(n+2)^2 + 4A_1(n+2)^3 + 4A_2(n+2)^4 + 4A_3(n+2)^5 \\
-\ & 8A_0(n+1)^2 - 8A_1(n+1)^3 - 8A_2(n+1)^4 - 8A_3(n+1)^5 \\
+\ & 4A_0n^2 + 4A_1n^3 + 4A_2n^4 + 4A_3n^5 \\
=\ & -160n^3 - 528n^2 - 608n - 240
\end{aligned}$$

Para calcular los coeficientes de las potencias de n en el primer miembro, utilizaremos el Binomio de Newton, (16.1.1), y el Triángulo de Pascal, (16.1.2), para obtener los coeficientes del mismo.

$$\begin{array}{lccccccccccc}
0 & & & & & & 1 & & & & & \\
1 & & & & & 1 & & 1 & & & & \\
2 & & & & 1 & & 2 & & 1 & & & \\
3 & & & 1 & & 3 & & 3 & & 1 & & \\
4 & & 1 & & 4 & & 6 & & 4 & & 1 & \\
5 & 1 & & 5 & & 10 & & 10 & & 5 & & 1
\end{array}$$

- El término independiente de $(n+2)^2$ es $n^0 \cdot 2^2 \cdot 1 = 4$.
- El término independiente de $(n+2)^3$ es $n^0 \cdot 2^3 \cdot 1 = 8$.
- El término independiente de $(n+2)^4$ es $n^0 \cdot 2^4 \cdot 1 = 16$.
- El término independiente de $(n+2)^5$ es $n^0 \cdot 2^5 \cdot 1 = 32$.
- El término independiente de $(n+1)^2$ es $n^0 \cdot 1^2 \cdot 1 = 1$.
- El término independiente de $(n+1)^3$ es $n^0 \cdot 1^3 \cdot 1 = 1$.
- El término independiente de $(n+1)^4$ es $n^0 \cdot 1^4 \cdot 1 = 1$.
- El término independiente de $(n+1)^5$ es $n^0 \cdot 1^5 \cdot 1 = 1$.

Por lo tanto, el término independiente del primer miembro será:

$$\begin{array}{rccccccc}
& 4A_0 \cdot 4 & + & 4A_1 \cdot 8 & + & 4A_2 \cdot 16 & + & 4A_3 \cdot 32 \\
- & 8A_0 \cdot 1 & - & 8A_1 \cdot 1 & - & 8A_2 \cdot 1 & - & 8A_3 \cdot 1 \\
= & 8A_0 & + & 24A_1 & + & 56A_2 & + & 120A_3
\end{array}$$

Igualándolo a -240, término independiente del segundo miembro, tendremos:

$$8A_0 + 24A_1 + 56A_2 + 120A_3 = -240$$

- El término en n de $(n+2)^2$ es $n^1 \cdot 2^1 \cdot 2 = 4n$.
- El término en n de $(n+2)^3$ es $n^1 \cdot 2^2 \cdot 3 = 12n$.
- El término en n de $(n+2)^4$ es $n^1 \cdot 2^3 \cdot 4 = 32n$.
- El término en n de $(n+2)^5$ es $n^1 \cdot 2^4 \cdot 5 = 80n$.
- El término en n de $(n+1)^2$ es $n^1 \cdot 1^1 \cdot 2 = 2n$.
- El término en n de $(n+1)^3$ es $n^1 \cdot 1^2 \cdot 3 = 3n$.
- El término en n de $(n+1)^4$ es $n^1 \cdot 1^3 \cdot 4 = 4n$.
- El término en n de $(n+1)^5$ es $n^1 \cdot 1^4 \cdot 5 = 5n$.

El coeficiente del término en n del primer miembro será, por tanto,

$$\begin{array}{rrrrrrrr} & 4A_0 \cdot 4 & + & 4A_1 \cdot 12 & + & 4A_2 \cdot 32 & + & 4A_3 \cdot 80 \\ - & 8A_0 \cdot 2 & - & 8A_1 \cdot 3 & - & 8A_2 \cdot 4 & - & 8A_3 \cdot 5 \\ = & & & 24A_1 & + & 96A_2 & + & 280A_3 \end{array}$$

e igualando al coeficiente del término en n del segundo miembro,

$$24A_1 + 96A_2 + 280A_3 = -608$$

Veamos, ahora, los términos en n^2.

- El término en n^2 de $(n+2)^2$ es $n^2 \cdot 2^0 \cdot 1 = 1n^2$.
- El término en n^2 de $(n+2)^3$ es $n^2 \cdot 2^1 \cdot 3 = 6n^2$.
- El término en n^2 de $(n+2)^4$ es $n^2 \cdot 2^2 \cdot 6 = 24n^2$.
- El término en n^2 de $(n+2)^5$ es $n^2 \cdot 2^3 \cdot 10 = 80n^2$.
- El término en n^2 de $(n+1)^2$ es $n^2 \cdot 1^0 \cdot 1 = 1n^2$.
- El término en n^2 de $(n+1)^3$ es $n^2 \cdot 1^1 \cdot 3 = 3n^2$.
- El término en n^2 de $(n+1)^4$ es $n^2 \cdot 1^2 \cdot 6 = 6n^2$.
- El término en n^2 de $(n+1)^5$ es $n^2 \cdot 1^3 \cdot 10 = 10n^2$.

Luego, el coeficiente del término en n^2 del primer miembro es:

$$\begin{array}{rrrrrrrr} & 4A_0 \cdot 1 & + & 4A_1 \cdot 6 & + & 4A_2 \cdot 24 & + & 4A_3 \cdot 80 \\ - & 8A_0 \cdot 1 & - & 8A_1 \cdot 3 & - & 8A_2 \cdot 6 & - & 8A_3 \cdot 10 \\ + & 4A_0 & & & & & & \\ = & & & & & 48A_2 & + & 240A_3 \end{array}$$

y si igualamos al coeficiente del término en n^2 del segundo miembro,

$$48A_2 + 240A_3 = -528$$

Finalmente, calcularemos el coeficiente del término en n^3 en el primer miembro.

- El término en n^3 de $(n+2)^3$ es $n^3 \cdot 2^0 \cdot 1 = 1n^3$.
- El término en n^3 de $(n+2)^4$ es $n^3 \cdot 2^1 \cdot 4 = 8n^3$.
- El término en n^3 de $(n+2)^5$ es $n^3 \cdot 2^2 \cdot 10 = 40n^3$.
- El término en n^3 de $(n+1)^3$ es $n^3 \cdot 1^0 \cdot 1 = 1n^3$.
- El término en n^3 de $(n+1)^4$ es $n^3 \cdot 1^1 \cdot 4 = 4n^3$.
- El término en n^3 de $(n+1)^5$ es $n^3 \cdot 1^2 \cdot 10 = 10n^3$.

Luego, el coeficiente del término en n^3 del primer miembro será:

$$\begin{array}{rrrrrrrrr} + & 4A_1 \cdot 1 & + & 4A_2 \cdot 8 & + & 4A_3 \cdot 40 \\ - & 8A_1 \cdot 1 & - & 8A_2 \cdot 4 & - & 8A_3 \cdot 10 \\ + & 4A_1 & & & & \\ = & & & & & 80A_3 \end{array}$$

y si igualamos al coeficiente del término en n^3 del segundo miembro,

$$80A_3 = -160$$

Tendremos, pues, el sistema de ecuaciones,

$$\left.\begin{array}{rrrrrrrrrrr} 8A_0 & + & 24A_1 & + & 56A_2 & + & 120A_3 & = & -240 \\ & + & 24A_1 & + & 96A_2 & + & 280A_3 & = & -608 \\ & & & + & 48A_2 & + & 240A_3 & = & -528 \\ & & & & & + & 80A_3 & = & -160 \end{array}\right\} \Longrightarrow \left\{\begin{array}{rcr} A_0 & = & 1 \\ A_1 & = & 2 \\ A_2 & = & -1 \\ A_3 & = & -2 \end{array}\right.$$

⁕ Solución particular.

Por lo tanto, la sucesión $\{a_n^p\}$ tal que

$$a_n^p = n^2 (-2)^n \left(-2n^3 - n^2 + 2n + 1\right)$$

es una solución particular de la ecuación propuesta.

◊ Solución general.

Por 16.2.2, la sucesión $\{a_n\}$ tal que

$$a_n = \alpha_1 (-2)^n + \alpha_2 n (-2)^n + n^2 (-2)^n \left(-2n^3 - n^2 + 2n + 1\right)$$

será la solución general de nuestra ecuación.

◊ Obtención de solución única.

Como disponemos de dos condiciones iniciales, podremos calcular los coeficientes de la solución general y de esta forma obtener una solución única para dicha condición.

⁕ Cálculo de los coeficientes de la solución general.

De $a_1 = -4$ y $a_2 = -228$ se sigue

$$\left.\begin{array}{rrrrrrr} - & 2\alpha_1 & - & 2\alpha_2 & 0 & = & -4 \\ & 4\alpha_1 & + & 8\alpha_2 & - 240 & = & -228 \end{array}\right\} \Longrightarrow \left\{\begin{array}{rcr} \alpha_1 & = & 1 \\ \alpha_2 & = & 1 \end{array}\right.$$

⁕ Solución única.

Por lo tanto, la sucesión $\{a_n\}$ tal que

$$a_n = (-2)^n + n (-2)^n + n^2 (-2)^n \left(-2n^3 - n^2 + 2n + 1\right), \ n \geqslant 1$$

es solución única de la ecuación propuesta para la condición inicial dada.

♦♦♦