Apuntes de Matemática Discreta

Francisco José González Gutiérrez

28 de Noviembre de 2015

Contenido

Unidad Temática I

Lógica Matemática

Lección 1

Lógica de Proposiciones

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

Arthur Conan Doyle. Un Estudio en Escarlata. 1887

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

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

1.1 Proposiciones y Tablas de Verdad

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

1.1.1 Proposición

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

■

Ejemplo 1.1

Las siguientes afirmaciones son proposiciones.

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

(b) 6 es un número primo.

(c) $3 + 2 = 6$

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

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

■

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

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

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

■

Ejemplo 1.2

Las siguientes afirmaciones no son proposiciones.

(a) $x + y > 5$

(b) ¿Te vas?

(c) Compra cinco manzanas y cuatro peras.

(d) $x = 2$

Solución

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

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

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

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

■

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

1.1.2 Valor de verdad

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

■

Ejemplo 1.3

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

(a) p: Existe Premio Nobel de informática.

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

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

(d) s: Cinco más siete es grande.

Solución

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

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

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

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

■

1.1.3 Variables de enunciado

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

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

■

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

1.1.4 Proposiciones simples

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

1.1.5 Proposición compuesta

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

Ejemplo 1.4

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

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

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

■

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

■

1.1.6 Tablas de verdad

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

Ejemplo 1.5

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

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

■

1.2 Conexión entre Proposiciones

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

1.2.1 Conjunción

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

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

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

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

■

1.2.2 Disyunción

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

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

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

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

■

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

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

1.2.3 Disyunción exclusiva

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

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

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

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

■

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

■

1.2.4 Negación

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

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

p	$\neg p$
V	F
F	V

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

■

Ejemplo 1.6

Estudiar la veracidad o falsedad de las siguientes proposiciones:

p_1: El Pentium es un microprocesador.

p_2: Es falso que el Pentium sea un microprocesador.

p_3: El Pentium no es un microprocesador.

p_4: $2 + 2 = 5$

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

Solución

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

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

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

■

Ejemplo 1.7

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

Solución

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

■

1.2.5 Tautologías y contradicciones

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

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

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

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

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

■

Ejemplo 1.8

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

Solución

Lo resolveremos escribiendo una tabla de verdad. En efecto,

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

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

■

1.2.6 Proposición condicional

Dadas dos proposiciones p y q, a la proposición compuesta

"si p, entonces q"

se le llama "proposición condicional" y se nota por

$$p \longrightarrow q$$

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

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

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

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

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

■

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

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

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

1.– Antecedente y consecuente verdaderos.

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

"*Si como mucho, entonces engordo*"

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

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

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

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

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

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

2.– Antecedente verdadero y consecuente falso.

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

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

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

3.– Antecedente falso y consecuente verdadero.

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

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

"p es una condición suficiente para q"

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

"*Si estudio mucho, entonces me canso*"

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

4.– Antecedente y consecuente falsos.

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

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

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

■

Ejemplo 1.9

Dadas las proposiciones:

p: El número a es par.

q: Los resultados salen en pantalla.

r: Los resultados se imprimen.

Enunciar las formulaciones equivalentes de las siguientes proposiciones.

(a) $q \longrightarrow p$.

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

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

Solución

(a) $q \longrightarrow p$.

Formulaciones equivalentes de $q \longrightarrow p$

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

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

Formulaciones equivalentes de $\neg q \longrightarrow r$

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

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

Formulaciones equivalentes de $r \longrightarrow (p \vee q)$

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

■

Ejemplo 1.10

Sean las proposiciones

p : Está lloviendo.

q : Iré a la playa.

r : Tengo tiempo.

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

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

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

(a.3) No está lloviendo.

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

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

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

(b.2) $r \wedge q$

(b.3) $r \longrightarrow q$

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

Solución

(a) Escribimos en forma simbólica las afirmaciones propuestas.

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

(a.2) $q \longrightarrow r$

(a.3) $\neg p$

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

(b) Escribimos en forma de afirmaciones las proposiciones.

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

(b.2) Tengo tiempo e iré a la playa.

(b.3) Iré a la playa si tengo tiempo.

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

■

1.2.7 Proposición recíproca

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

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

■

1.2.8 Proposición contrarrecíproca

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

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

■

Ejemplo 1.11

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

(a) Si llueve, no voy.

(b) Me quedaré, sólo si tú te vas.

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

Solución

(a) Si llueve, no voy.

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

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

(b) Me quedaré sólo si te vas.

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

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

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

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

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

■

1.2.9 Proposición bicondicional

Dadas dos proposiciones p y q, a la proposición compuesta

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

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

Si p, entonces q

siendo una formulación equivalente,

Una condición necesaria para p es q

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

Si q, entonces p

siendo una formulación equivalente,

Una condición suficiente para p es q

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

Una condición necesaria y suficiente para p es q

■

Ejemplo 1.12

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

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

puede expresarse simbólicamente como

$$p \longleftrightarrow q$$

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

Observemos lo siguiente: La proposición anterior afirma dos cosas

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

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

Consecuentemente, una forma alternativa de formular la proposición dada es

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

es decir,

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

■

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

Ejemplo 1.13

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

Solución

Construimos su tabla de verdad,

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

■

Ejemplo 1.14

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

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

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

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

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

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

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

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

Solución

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

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

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

Luego es una *contingencia*.

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

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

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

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

  o

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

luego la proposición es una *contingencia*.

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

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

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

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

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

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

una *tabla de verdad abreviada* será

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

y la proposición es una *tautología*.

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

Seguiremos un camino análogo al utilizado en el apartado anterior.

- Si la hipótesis, $p \wedge q$, es verdadera, la conclusión, p, no puede ser falsa.

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

  En efecto, si p es falsa, de nuevo por el valor de verdad de la conjunción, $p \wedge q$ es falsa.

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

Una *tabla de verdad abreviada* sería:

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

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

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

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

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

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

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

- Si la hipótesis, $(p \longrightarrow q) \vee (r \longrightarrow s)$, es verdadera, la conclusión, $(p \wedge r) \longrightarrow (q \vee s)$, no puede ser falsa.

  Efectivamente, si $(p \longrightarrow q) \vee (r \longrightarrow s)$ es verdad, entonces, por el valor de verdad de la disyunción, uno de los dos condicionales, $p \longrightarrow q$ o $r \longrightarrow s$, al menos, ha de ser verdadero. Pues bien,

  si $p \longrightarrow q$ es verdad, entonces p es falso o q es verdad.

  Si p es falso, $p \wedge r$ también lo será y, por lo tanto, $(p \wedge r) \longrightarrow (q \vee s)$ será verdadera independientemente de los valores de verdad de r, q y s.

  Si q es verdad, $q \vee s$ también será verdad y, consecuentemente, $(p \wedge r) \longrightarrow (q \vee s)$ será verdadera independientemente de los valores de verdad de p, r y s.

  Si $r \longrightarrow s$ es verdad, entonces r es falso o s es verdad.

  Si r es falso, $p \wedge r$ también lo será y, por lo tanto, $(p \wedge r) \longrightarrow (q \vee s)$ será verdadera independientemente de los valores de verdad de p, q y s.

  Si s es verdad, $q \vee s$ también será verdad y, consecuentemente, $(p \wedge r) \longrightarrow (q \vee s)$ será verdadera independientemente de los valores de verdad de p, q y r.
- Si la conclusión, $(p \wedge r) \longrightarrow (q \vee s)$ es falsa, la hipótesis, $(p \longrightarrow q) \vee (r \longrightarrow s)$, no puede ser verdadera.

  En efecto, si la conclusión, $[(p \wedge r) \longrightarrow (q \vee s)]$ es falsa, entonces $(p \wedge r)$ es verdad y $(q \vee s)$ es falsa de donde se sigue que p y r son, ambas, verdad y q y s son, ambas, falsas. Por lo tanto, por el valor de verdad del condicional, (1.2.6), $p \longrightarrow q$ es falsa y $r \longrightarrow s$, también, de aquí que la disyunción de las dos, $(p \longrightarrow q) \vee (r \longrightarrow s)$, sea falsa.

Haremos una tabla de verdad que recoja únicamente estos casos.

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

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

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

■

1.3 Implicación

Estudiamos en este apartado la implicación lógica entre dos proposiciones.

1.3.1 Implicación lógica

Sean P y Q dos proposiciones cualesquiera. Diremos que P implica lógicamente Q, y escribiremos $P \Longrightarrow Q$, si 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, probando que la veracidad de q se sigue de la veracidad de $p \wedge (p \longrightarrow q)$.

Solución

Probaremos, de acuerdo con la definición dada en el punto anterior, que el condicional $[p \wedge (p \longrightarrow q)] \longrightarrow q$ es unta 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, (1.2.6), 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 la definición (1.3.1) hay implicación lógica, es decir,

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

y la demostración termina.

■

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

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

■

1.3.2 Implicaciones lógicas más comunes

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

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

■

Ejemplo 1.17

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

Solución

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

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

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, (1.2.6), si $P \longrightarrow Q$ es verdad, entonces P es falsa o Q verdadera. Tendremos, pues, dos opciones:

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

En 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

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

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. $\neg (P \vee Q) \Longrightarrow (\neg P \wedge \neg Q)$.
   Probaremos que el condicional $\neg (P \vee Q) \longrightarrow (\neg P \wedge \neg Q)$ nunca puede ser falso, para lo cual veremos que la única opción de falsedad de un condicional (hipótesis verdadera y conclusión falsa) no puede darse.

En efecto, si $\neg(P \vee Q)$ es verdad, entonces por 1.2.4, $P \vee Q$ es falso, luego por 1.2.2, P y Q serán, ambas, falsas, de aquí que, de nuevo por 1.2.4, $\neg P$ y $\neg Q$ sean, las dos, verdaderas y, consecuentemente, $\neg P \wedge \neg Q$ es verdad (por 1.2.1).

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 verdad luego, por 1.2.4, 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

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

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

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

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

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

es una tautología. En efecto,

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

(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 1.2.4, $P \wedge Q$ es falso, luego por 1.2.2, una de las dos proposiciones, P o Q, al menos, ha de ser falsa, de aquí que, de nuevo por 1.2.4, una de las dos, $\neg P$ o $\neg Q$, ha de ser verdad y, consecuentemente, $\neg P \vee \neg Q$ es verdadera (por 1.2.2).
   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 1.2.4, al menos una de las dos, P o Q tiene que ser falsa y por 1.2.1 $P \wedge Q$ es falsa y, consecuentemente, $\neg(P \wedge Q)$ es verdad.
   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. Sabemos la única posibilidad de que un condicional sea falso es que sea verdad la hipótesis y la conclusión falsa. Veamos que esta situación no es posible.

  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,

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

■

Ejemplo 1.24

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

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

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

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

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

Nota 1.8 Obsérvese que esto significa que si el razonamiento es válido, entonces el condicional,

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

nunca es falso, es decir es una tautología.

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

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

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

■

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 Veamos que la veracidad de la conclusión se sigue de la veracidad de la hipótesis.

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.

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

■

1.5.3 Demostración por Contradicción o Reducción al Absurdo

Este método de demostración de la validez de un razonamiento se basa en la equivalencia lógica conocida como "Reducción al absurdo" (1.4.3),

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

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

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

es una tautología.

En efecto, si la hipótesis,

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

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

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

o lo que es igual,

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

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

Partiendo, pues, de la veracidad de

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

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

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

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

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

será, también, una tautología. Bastaría aplicar la equivalencia lógica conocida como "*reducción al absurdo*", (1.4.3), y tendríamos que

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

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

■

1.5.4 Demostración por la Contrarrecíproca

Este método de demostración de la validez de un razonamiento se basa en la equivalencia lógica conocida como "Contrarrecíproca" (1.4.3),

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

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:

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

Solución

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

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

es una tautología.

Lo haremos de varias formas.

1 Aplicando directamente la definición de implicación lógica.

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

- p es falsa y $q \longleftrightarrow \neg r$ verdadera. En este caso, la conclusión $p \longrightarrow \neg r$ es verdadera, independientemente del valor de verdad que tenga r.
- q es verdadera y $q \longleftrightarrow \neg r$ también. En tal caso, $\neg r$ ha de ser verdad y, consecuentemente, $p \longrightarrow \neg r$ es verdadera sin importar el valor de verdad de p.

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

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

es una tautología y el razonamiento es válido.

Probemos ahora lo mismo pero partiendo de la falsedad de la conclusión.

En efecto, si la conclusión, $p \longrightarrow \neg r$, es falsa, entonces p es verdad y $\neg r$ es falso y el valor de verdad de $p \longrightarrow q$ y $q \longleftrightarrow \neg r$ dependerá del valor de verdad que tenga q. Habrá pues dos opciones:

- q es verdad. En tal caso, $p \longrightarrow q$ será verdad y $q \longleftrightarrow \neg r$ falso.
- q es falso. En este caso, $p \longrightarrow q$ será falso y $q \longleftrightarrow \neg r$ verdad.

Por lo tanto y en ambos casos, la hipótesis, $(p \longrightarrow q) \wedge (p \longleftrightarrow \neg r)$, es falsa.

La tabla de verdad siguiente refleja los pasos que hemos dado.

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

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

Consecuentemente, el condicional,

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

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

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

Probaremos que

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

es una tautología.

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

$p \longrightarrow q$ es verdad.

$q \longleftrightarrow \neg r$ es verdad.

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

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

Partiendo de la veracidad de

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

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

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

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

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

también será una tautología. Aplicamos la equivalencia lógica conocida como "*reducción al absurdo*", (1.4.3), y

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

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

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

Veamos que

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

es tautología.

Utilizando las equivalencias lógicas correspondientes,

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

y

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

Probaremos, pues, que

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

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

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

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

es decir,

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

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

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

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

Finalmente, escribimos el razonamiento con palabras,

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

■

Ejemplo 1.29

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 la veracidad de la conclusión se sigue de la veracidad de la hipótesis.

1 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.

Probaremos que

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

es una tautología.

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

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

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

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

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

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

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

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

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

también lo será.

Aplicamos "*reducción al absurdo*", (1.4.3), y

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

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

4 Demostración por la contrarrecíproca.

Probaremos que

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

es una tautología.

Utilizando las equivalencias lógicas correspondientes,

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

Probaremos, pues, que

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

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,

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

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

Solución

Sean:

p : Florinda está en una fiesta.

q : Florinda está haciendo los ejercicios de Lógica.

r : Florinda aprueba lógica.

La hipótesis será:

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

Pues bien,

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

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 la propiedad p o que algunos la tienen.

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

En castellano también ocurren situaciones similares, por ejemplo,

Ella es alta y rubia.

Él vive en el campo.

Ella, él y el campo se utilizan como variables,

x es alta y rubia.

x vive en y

2.1.1 Predicado

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

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

■

Ejemplo 2.1

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

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

■

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

■

2.1.2 Universo del discurso

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

■

Ejemplo 2.2

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

■

2.1.3 Predicados y Proposiciones

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

■

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

Ejemplo 2.3

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

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

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

■

2.2 Cuantificadores

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

2.2.1 Cuantificador universal

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

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

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

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

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

■

Ejemplo 2.4

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

Solución

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

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

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

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

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

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

o

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

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

■

Ejemplo 2.5

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

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

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

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

Transcribir las siguientes proposiciones a notación lógica.

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

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

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

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

Solución

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

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

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

la cual, utilizando los predicados del enunciado, se escribiría

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

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

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

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

y utilizando los predicados,

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

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

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

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

y con los predicados,

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

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

Utilizando el cuantificador universal, $\forall$,

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

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

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

■

2.2.2 Valor de verdad del cuantificador universal

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

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

■

Ejemplo 2.6

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

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

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

Solución

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

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

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

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

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

$$a < b$$

es decir,

$$a < a + 1$$

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

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

es una proposición verdadera.

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

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

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

Aplicando de nuevo, 2.2.2, la proposición

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

es falsa.

■

2.2.3 Cuantificador existencial

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

"existe un x tal que $p(x)$"

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

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

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

■

Ejemplo 2.7

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

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

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

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

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

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

Solución

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

La forma equivalente pedida es

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

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

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

la cual puede interpretarse como

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

que por la asociatividad de $\wedge$ equivale a

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

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

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

la cual equivale a

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

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

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

es decir,

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

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

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

la cual equivale a la proposición

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

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

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

es decir,

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

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

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

que es equivalente a la proposición,

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

■

2.2.4 Valor de verdad del cuantificador existencial

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

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

Ejemplo 2.8

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

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

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

Solución

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

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

$$\exists n : n = 5$$

es verdadera.

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

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

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

$$\exists n : n + 1$$

es una proposición falsa.

■

2.2.5 Valores de verdad. Resumen

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

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

■

Ejemplo 2.9

Estudiar el valor de verdad de las siguientes proposiciones:

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

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

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

Solución

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

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

Primero escribimos la proposición en lenguaje simbólico,

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

y ahora estudiamos su valor de verdad.

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

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

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

Cuantificamos la proposición,

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

y estudiamos su valor de verdad.

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

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

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

Escribiendo la proposición en notación simbólica,

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

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

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

■

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

Ejemplo 2.10

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

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

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

Solución

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

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

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

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

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

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

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

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

■

Ejemplo 2.11

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

$p(x) : x \geqslant 0$

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

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

Estudiar el valor de verdad de las siguientes proposiciones:

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

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

Solución

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

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

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

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

es decir,

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

o sea,

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

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

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

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

$$a = 2$$

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

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

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

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

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

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

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

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

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

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

■

2.3 Cálculo de Predicados

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

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

Ejemplo 2.12

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

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

$q(n)$: n es par.

$r(n)$: n es impar.

$s(n)$: n es primo.

Expresar en notación lógica las siguientes afirmaciones:

(a) Existe un entero par.

(b) Todo número entero es par o impar.

(c) Todos los números primos son no negativos.

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

(e) No todos los enteros son pares.

(f) No todos los primos son impares.

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

Solución

(a) Existe un entero par.

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

(b) Todo número entero es par o impar.

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

(c) Todos los números primos son no negativos.

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

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

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

(e) No todos los enteros son pares.

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

(f) No todos los primos son impares.

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

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

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

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

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

2.3.1 Leyes de De Morgan generalizadas

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

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

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

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

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

Demostración

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

■

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

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

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

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

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

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

es decir,

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

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

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

o sea,

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

que es la tercera ley de De Morgan.

■

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

Por ejemplo, podemos utilizarlas para negar la proposición

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

En efecto,

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

■

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

2.3.2 Regla general

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

■

2.3.3 Proposiciones al alcance de un cuantificador

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

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

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

4. $\forall x, [p(x) \wedge q] \iff [\forall x, p(x)] \wedge q$

Demostración

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Si ahora negamos ambos miembros,

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

aplicamos las leyes de De Morgan en el segundo miembro

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

y las leyes de De Morgan generalizadas,

$$\exists x : \neg \left[\neg (p(x) \vee \neg q \right] \iff [\exists x : \neg \neg p(x)] \wedge q$$

es decir,

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

y, consecuentemente,

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

4.– $\forall x, [p(x) \wedge q] \iff [\forall x, p(x)] \wedge q$.

Lo haremos utilizando el mismo método que en el apartado anterior, aunque partiremos de la equivalencia probada en 2. En efecto,

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

y al ser esto cierto para cualquier predicado $p(x)$ y cualquier proposición q también lo será para sus negaciones, es decir,

$$\exists x : [\neg p(x) \vee \neg q] \iff [\exists x : \neg p(x)] \vee \neg q$$

y si negamos ambos miembros,

$$\neg \exists x : [\neg p(x) \vee \neg q] \iff \neg \left([\exists x : \neg p(x)] \vee \neg q \right)$$

aplicamos De Morgan al segundo,

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

las Leyes de De Morgan generalizadas,

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

y, nuevamente, De Morgan,

$$\forall x, [\neg \neg p(x) \wedge \neg \neg q] \iff [\forall x, p(x)] \wedge q$$

obtendremos,

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

■

2.3.4 Asociatividad

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

Demostración

Sea $\mathscr{U}$ un universo del discurso cualquiera y $p(x), q(x)$ dos predicados arbitrarios, siendo x cualquier elemento de $\mathscr{U}$

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

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

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

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

   $\Longrightarrow$) $[\exists x : p(x)] \vee [\exists x : q(x)] \Longrightarrow \exists x : [p(x) \vee q(x)]$.
   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*"

■

2.3.5 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, siendo x cualquier elemento de $\mathscr{U}$

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.

   Veamos que, sin embargo, no se da la equivalencia lógica como en el apartado anterior, es decir, el recíproco no es cierto o lo que es igual,

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

   En efecto, si la proposición $[\exists x : p(x)] \wedge [\exists x : q(x)]$ es verdad, entonces $[\exists x : p(x)]$ es verdad y $[\exists x : q(x)]$ también lo es. Ahora bien,

   - si $\exists x : p(x)$ es verdad, entonces existe, al menos, un valor de x, digamos a, en $\mathscr{U}$ que transforma al predicado $p(x)$ en una proposición, $p(a)$, verdadera.
   - Si $\exists x : q(x)$ es verdad, entonces existe, al menos, un valor de x, digamos b, en $\mathscr{U}$ que transforma al predicado $q(x)$ en una proposición, $q(b)$, verdadera.

   Pero el hecho de que $p(a)$ sea verdadera no significa que $q(a)$ lo sea, es decir no sabemos que valor de verdad tiene $p(a) \wedge q(a)$ y lo mismo pasaría con $p(b) \wedge q(b)$. Por lo tanto, no podemos asegurar que exista, al menos, un valor de x, sea a o sea b, en $\mathscr{U}$ que haga que el predicado $p(x) \wedge q(x)$ se transforme en una proposición verdadera, de aquí que no podemos deducir nada sobre el valor de verdad de la proposición $\exists x : [p(x) \wedge q(x)]$ y, consecuentemente, no haya implicación lógica.

   Veamos un contraejemplo que pone de manifiesto lo que decimos. Supongamos que $\mathscr{U}$ es el conjunto de los números enteros y sean los predicados,

   $p(x) : x \textit{ es un número par}$
   $q(x) : x \textit{ es un número impar}$

   Entonces, la proposición,

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

   significaría que existe, al menos, un número entero que es par y también existe, al menos, un entero que es impar, lo cual, evidentemente, es verdad. Por otra parte, la proposición,

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

   significa que hay, al menos, un número entero que es, al mismo tiempo, par e impar, lo cual es falso. Por lo tanto, la veracidad de la conclusión no se sigue de la veracidad de la hipótesis y no habría, consecuentemente, implicación lógica, es decir,

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

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 2.13

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, $\mathscr{U}$, y un predicado cualquiera, $p(x)$, siendo x cualquiera de $\mathscr{U}$.

Supongamos que el predicado $p(x)$ se transforma en proposición verdadera para, al menos, un elemento de $\mathscr{U}$ y que también existe, al menos, un elemento diferente del anterior para el que $\neg p(x)$ se transforma, asimismo, en una proposición verdadera, es decir, $\exists x : p(x)$ es verdad y $\exists x : \neg p(x)$ también lo es. Por el valor de verdad de la conjunción, tendremos que

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

es verdad.

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 2.14

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.

Supongamos que $\mathscr{U}$ es el conjunto de los números enteros 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 2.15

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

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

Solución

Veamos, primero, que $\neg\forall x, (p(x) \longrightarrow q(x)) \Longrightarrow \exists x : (p(x) \wedge \neg q(x))$.

En efecto, si $\neg\forall x, (p(x) \longrightarrow q(x))$ es verdad, entonces $\forall x, (p(x) \longrightarrow q(x))$ es falsa, lo cual significa por el valor de verdad del cuantificador universal que hay, al menos, un valor de x en $\mathscr{U}$ que transforma el predicado $p(x) \longrightarrow q(x)$ en una proposición falsa. A este valor concreto lo llamaremos a, es decir, $p(a) \longrightarrow q(a)$ es una proposición falsa. Entonces, por el valor de verdad del condicional, $p(a)$ será verdadera y $q(a)$ falsa, es decir, $\neg q(a)$ verdadera y, por lo tanto, $p(a) \wedge \neg q(a)$ será verdadera.

Hemos encontrado, pues, un valor de x en $\mathscr{U}$ que transforma el predicado $p(x) \wedge \neg q(x)$ en una proposición verdadera y eso significa, por el valor de verdad del cuantificador existencial, que $\exists x : (p(x) \wedge \neg q(x))$ es verdad.

Recíprocamente, si $\exists x : (p(x) \wedge \neg q(x))$ es verdad, entonces, por el valor de verdad del cuantificador existencial, hay, al menos, un valor de x en $\mathscr{U}$ que transforma el predicado $p(x) \wedge \neg q(x)$ en una proposición verdadera. A ese valor concreto de x lo llamaremos a, es decir, la proposición $p(a) \wedge \neg q(a)$ es verdad, de aquí que por el valor de verdad de la conjunción, $p(a)$ sea verdad $\neg q(a)$ también, es decir, $p(a)$ es verdad y $q(a)$ falsa, luego el valor de verdad del condicional asegura que la proposición $p(a) \longrightarrow q(a)$ es falsa.

Por lo tanto, hemos encontrado, al menos, un valor de x en el universo del discurso, $\mathscr{U}$, que transforma el predicado $p(x) \longrightarrow q(x)$ en una proposición falsa, es decir, la proposición $\forall x, (p(x) \longrightarrow q(x))$ es falsa y, consecuentemente, su negación, $\neg\forall x, (p(x) \longrightarrow q(x))$, será verdadera.

■

2.4 Razonamientos y Cuantificadores

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

Ejemplo 2.16

Estudiar, en el universo de todos los alumnos de la Universidad de Cádiz, la validez del siguiente razonamiento.

> Todos los alumnos de Informática estudian Matemática Discreta.
> Florinda es alumna de Informática.
> Por lo tanto, Florinda estudia Matemática Discreta.

Solución

Sean

> $p(x)$: x es alumno de Informática.
> $q(x)$: x estudia Matemática Discreta.

y llamemos f a Florinda.

El razonamiento en forma simbólica sería:

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

Comprobaremos si es válido de varias formas.

1 De acuerdo con la definición de razonamiento válido, comprobaremos que la veracidad de la conclusión se deduce de la veracidad de la hipótesis.

En efecto, si la hipótesis, $[\forall x, (p(x) \longrightarrow q(x)) \wedge p(f)]$, es verdad, entonces, por el *valor de verdad de la conjunción*, las proposiciones $\forall x, (p(x) \longrightarrow q(x))$ y $p(f)$ serán, ambas, verdaderas.

Pues bien, si $\forall x, (p(x) \longrightarrow q(x))$ es verdad, por el *valor de verdad del cuantificador universal*, el condicional $p(x) \longrightarrow q(x)$ se transformará en una proposición verdadera para todos y cada uno de los elementos del universo y, en particular, será verdad para Florinda. Así pues, tendremos que la proposición $p(f) \longrightarrow q(f)$ es verdad y, como $p(f)$ es verdad, el *valor de verdad del condicional* asegura que $q(f)$ también tiene que serlo. La veracidad de la conclusión se sigue, pues, de la veracidad de la hipótesis, luego por la definición de *implicación lógica*,

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

y, consecuentemente, el razonamiento es válido.

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

En efecto, supongamos que, $(\forall x, (p(x) \longrightarrow q(x))) \wedge p(f) \wedge \neg q(f)$ es verdad. Por el valor de verdad de la conjunción,

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

La veracidad de $\forall x, (p(x) \longrightarrow q(x))$ significa, por el valor de verdad del cuantificador universal, que el predicado $p(x) \longrightarrow q(x)$ se transforma en una proposición verdadera para cada x de $\mathscr{U}$, por lo tanto, y en particular, $p(f) \longrightarrow q(f)$ es verdad.

Pues bien, si $p(f) \longrightarrow q(f)$ es verdad y $q(f)$ es falsa, por el valor de verdad del condicional, $p(f)$ ha de ser falsa y su negación $\neg p(f)$ será verdadera con lo cual, al ser $p(f)$ verdadera, tendremos que $p(f) \wedge \neg p(f)$ es verdad.

De la veracidad de $(\forall x, (p(x) \longrightarrow q(x))) \wedge p(f) \wedge \neg q(f)$ hemos deducido la veracidad de $p(f) \wedge \neg p(f)$, luego el condicional

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

es una tautología y, al ser $p(f) \wedge \neg p(f) \Longleftrightarrow C$, esto significa que la proposición

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

también lo es. Aplicamos "*reducción al absurdo*", (1.4.3), y

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

es tautología y, consecuentemente, el razonamiento es válido.

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

$$\begin{aligned}
[(\forall x, (p(x) \longrightarrow q(x))) \wedge p(f)] \longrightarrow q(f) &\iff \neg q(f) \longrightarrow \neg\,[(\forall x, (p(x) \longrightarrow q(x))) \wedge p(f)] \\
&\iff \neg q(f) \longrightarrow \neg \forall x, (p(x) \longrightarrow q(x)) \vee \neg p(f) \qquad (1.4.3) \\
&\iff \neg q(f) \longrightarrow (\exists x, (p(x) \wedge \neg q(x))) \vee \neg p(f) \qquad (2.15)
\end{aligned}$$

Probaremos, pues, que esta última proposición es una tautología. En efecto, si $\neg q(f)$ es verdad, el valor de verdad de la conclusión dependerá de los distintos casos que puedan presentarse para el predicado $p(x)$.

- $p(x)$ se transforma en proposición verdadera para cada x de $\mathscr{U}$ o lo que es igual $\forall x, p(x)$ es verdad.
  En este caso, y en particular, $p(f)$ sería verdad y, al ser $\neg q(f)$ verdadera, habríamos encontrado un valor de x en $\mathscr{U}$ que transforma el predicado $p(x) \wedge \neg q(x)$ en proposición verdadera y, por el valor de verdad del cuantificador existencial, esto significa que $\exists x : p(x) \wedge \neg q(x)$ es verdad.
- $p(x)$ se transforma en proposición falsa para, al menos, un valor de x en $\mathscr{U}$ es decir, $\forall x, p(x)$ es falsa. Habría dos opciones:
  - x es Florinda. En este caso, $p(f)$ sería falsa y su negación, $\neg p(f)$, verdadera.
  - x no es Florinda. En tal caso, $p(f)$ debería ser verdadera y, al ser $\neg q(f)$ verdad, la conjunción $p(f) \wedge \neg q(f)$ también lo sería y, por lo tanto, habríamos encontrado, al menos, un valor de x en $\mathscr{U}$ que transforma $p(x) \wedge \neg q(x)$ en proposición verdadera, o sea $\exists x : (p(x) \wedge \neg q(x))$ es verdad.
- $p(x)$ se transforma en proposición verdadera para, al menos, un valor de x en $\mathscr{U}$ es decir, $\exists x : p(x)$ es verdadera. Al igual que en el caso anterior, habría dos opciones:
  - si x es Florinda, entonces $p(f)$ es verdad y, razonando como lo hicimos en el caso anterior, $\exists x : (p(x) \wedge \neg q(x))$ sería verdad.
  - Si x no es Florinda, entonces $p(f)$ ha de ser falsa y su negación, $\neg p(f)$, verdadera.
- $p(x)$ se transforma en proposición falsa para cada x de $\mathscr{U}$ o sea $\exists x : p(x)$ es falsa.
  En este caso, y en particular, $p(f)$ sería falsa y, por lo tanto, su negación, $\neg p(f)$, verdadera.

Hemos probado que en cualquier caso, al menos una de las dos proposiciones $(\exists x, (p(x) \wedge \neg q(x)))$ o $\neg p(f)$ es verdadera, luego

$$(\exists x, (p(x) \wedge \neg q(x))) \vee \neg p(f)$$

es verdadera y, consecuentemente,

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

también lo es y, por la equivalencia del principio, esto significa que

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

es una tautología y el razonamiento propuesto es válido.

■

Ejemplo 2.17

Consideremos el universo de los números enteros, elijamos un número a que no sea múltiplo de 2 y estudiemos la validez del siguiente razonamiento.

El número a no es múltiplo de 2.
Si un número es par, entonces es divisible por 2.
Si un número es divisible por 2, entonces es múltiplo de 2.
Por lo tanto, el número a no es par.

Solución

Sean

$p(x)$: x es par.
$q(x)$: x es divisible por 2.
$r(x)$: x es múltiplo de 2.

El razonamiento escrito en forma simbólica sería:

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

Al igual que en el ejercicio anterior, comprobaremos si el razonamiento es válido de varias formas.

1 De acuerdo con la definición de razonamiento válido, comprobaremos que la veracidad de la conclusión se deduce de la veracidad de la hipótesis.

En efecto, si la hipótesis, $\neg r(a) \wedge (\forall x, (p(x) \longrightarrow q(x))) \wedge (\forall x, (q(x) \longrightarrow r(x)))$, es verdad, por el *valor de verdad de la conjunción*, (1.2.1), tendremos que

- ⊛ $\neg r(a)$ es verdad.
- ⊛ $\forall x, (p(x) \longrightarrow q(x))$ es verdad.
- ⊛ $\forall x, (q(x) \longrightarrow r(x))$ es verdad.

De lo que se deduce,

- ⊛ $r(a)$ es falsa.
- ⊛ Por el *valor de verdad del cuantificador universal*, (2.2.2), el predicado $p(x) \longrightarrow q(x)$ se transforma en una proposición verdadera para todos y cada uno de los elementos del universo y, al ser a uno de ellos, la proposición $p(a) \longrightarrow q(a)$ es verdad.
- ⊛ Por el *valor de verdad del cuantificador universal*, (2.2.2), el predicado $q(x) \longrightarrow r(x)$ se transforma en una proposición verdadera para todos y cada uno de los elementos del universo y, al ser a uno de ellos, la proposición $q(a) \longrightarrow r(a)$ es verdad.

Pues bien, como $r(a)$ es falsa y $q(a) \longrightarrow r(a)$ verdad, por el *valor de verdad del condicional*, (1.2.6), $q(a)$ ha de ser falsa y, al ser verdad $p(a) \longrightarrow q(a)$, $p(a)$, por el mismo motivo, deberá ser falsa y, consecuentemente, $\neg p(a)$ es verdadera, es decir, a no es par.

Como la veracidad de la conclusión se sigue de la veracidad de la hipótesis, tendremos que el razonamiento es válido.

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

En efecto, supongamos que

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

es verdad.

Entonces, por el valor de verdad de la conjunción,

$\neg r(a)$ es verdad.

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

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

$p(a)$ es verdad.

Pues bien, si $\forall x, (p(x) \longrightarrow q(x))$ y $\forall x\, (q(x) \longrightarrow r(x))$ son verdaderas, entonces por el valor de verdad del cuantificador universal, (2.2.2), los predicados, $p(x) \longrightarrow q(x)$ y $q(x) \longrightarrow r(x)$ se transformarán en proposiciones verdaderas para cualquier elemento del universo y en particular para a, es decir, $p(a) \longrightarrow q(a)$ y $q(a) \longrightarrow r(a)$ son, ambas, verdaderas.

Además, si $p(a) \longrightarrow q(a)$ es verdad y $p(a)$ también lo es, entonces por el *valor de verdad del condicional*, (1.2.6), $q(a)$ tiene que ser verdad y, al ser verdad $q(a) \longrightarrow r(a)$, por el mismo motivo, la proposición $r(a)$ tiene que ser verdadera. Como $\neg r(a)$ es verdad, hemos llegado a que $r(a) \wedge \neg r(a)$ es verdadera, es decir,

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

es una tautología y, como $\neg r(a) \wedge r(a) \Longleftrightarrow C$, tendremos que

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

también lo es.

Aplicamos "*reducción al absurdo*", (1.4.3), y

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

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

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

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

$\Longleftrightarrow$ {Contrarrecíproca}

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

$\Longleftrightarrow$ {De Morgan}

$$p(a) \longrightarrow r(a) \vee (\neg\forall x, (p(x) \longrightarrow q(x))) \vee (\neg\forall x, (q(x) \longrightarrow r(x)))$$

$\Longleftrightarrow$ {Ejemplo 2.15}

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

Probaremos, pues, que este último condicional es una tautología.

En efecto, si $p(a)$ es verdad, tendremos dos opciones:

- $r(a)$ es verdad. Por el valor de verdad de la disyunción, la conclusión sería verdadera.
- $r(a)$ es falsa. En esta opción el valor de verdad de la conclusión dependerá de las proposiciones cuantificadas existencialmente y, al ser $p(a)$ verdadero, los valores de verdad de las mismas dependerán, a su vez, de los diferentes casos que puedan presentarse para el predicado $q(x)$.
  - $q(x)$ se transforma en proposición verdadera para cada x de $\mathscr{U}$, o sea $\forall x, q(x)$ es verdadera. En este caso, y en particular, la proposición $q(a)$ será verdadera. Como $\neg r(a)$ es verdad, la proposición $q(a) \wedge \neg r(a)$ es verdadera y esto significa que hemos encontrado, al menos, un valor de x en $\mathscr{U}$ que transforma el predicado $q(x) \wedge \neg r(x)$ en una proposición verdadera lo cual, a su vez, significa, por el valor de verdad del cuantificador existencial, que $\exists x : (q(x) \wedge \neg r(x))$, y con ella la conclusión, es verdad.
  - $q(x)$ se transforma en proposición falsa para cada x de $\mathscr{U}$, o sea $\exists x : q(x)$ es falsa.
    En tal caso, y en particular, la proposición $q(a)$ será falsa, su negación, $\neg q(a)$ verdadera y, al ser verdad $p(a)$, la conjunción $p(a) \wedge \neg q(a)$ será verdadera y esto significa que hemos encontrado, al menos, un valor de x en $\mathscr{U}$ que transforma el predicado $p(x) \wedge \neg q(x)$ en una proposición verdadera lo cual, por el valor de verdad del cuantificador existencial, quiere decir que $\exists x : (p(x) \wedge \neg q(x))$, y con ella la conclusión, es verdad.
  - $q(x)$ se transforma en proposición verdadera para, al menos, un valor de x en $\mathscr{U}$, es decir $\exists x, q(x)$ es verdad.
    En este caso, habrá, al menos, un valor de x en $\mathscr{U}$ que transforma el predicado $q(x)$ en una proposición verdadera y tendremos, por tanto, dos opciones:
    - si $x = a$, entonces $q(a)$ es verdadera y estaríamos en el primer caso.
    - Si $x \neq a$, entonces $q(a)$ debería ser falsa y estaríamos en el segundo caso.
  - $q(x)$ se transforma en proposición falsa para, al menos, un valor de x en $\mathscr{U}$, es decir $\forall x, q(x)$ es falsa.
    En este caso, habrá, al menos, un valor de x en $\mathscr{U}$ que transforma el predicado $q(x)$ en una proposición falsa y tendremos, por tanto, dos opciones:
    - si $x = a$, entonces $q(a)$ es falsa y estaríamos en el segundo caso.

– Si $x \neq a$, entonces $q(a)$ debería ser verdadera y estaríamos en el primer caso.

Por lo tanto, y en cualquier caso, la conclusión es verdad, es decir la proposición

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

es una tautología lo cual, por las equivalencias del principio, equivale a decir que

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

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

■

Nota 2.5 En los ejemplos anteriores, hemos deducido conclusiones particulares partiendo de premisas o hipótesis generales. Sin embargo, en la inmensa mayoría de los teoremas matemáticos hay que llegar a conclusiones generales. Por ejemplo, tendremos que probar que $p(x)$ es verdad para todos los valores de un cierto universo del discurso, es decir probar que $\forall x, p(x)$ es verdad, para lo cual habrá que establecer la veracidad de la proposición $p(a)$ para cada elemento a del universo y, como ya hemos comentado anteriormente, en la mayor parte de los universos esto no es factible. Lo que haremos para solventar esta cuestión es probar que $p(a)$ es verdad pero no para el caso en que a sea un elemento particular y concreto sino para el caso en que a denote un elemento arbitrario o genérico del universo.

■

Ejemplo 2.18

Estudiar, en el universo de los estudiantes de la Universidad de Cádiz, la validez del siguiente razonamiento:

Todos los alumnos de Informática estudian Lógica Matemática.
Todos los alumnos que estudian Lógica, saben analizar la validez de un razonamiento.
Por lo tanto, todos los alumnos de informática saben analizar la validez de un razonamiento.

Solución

Sean los predicados,

$p(x) : x$ es alumno de Informática.

$q(x) : x$ estudia Lógica Matemática.

$r(x) : x$ sabe analizar la validez de un razonamiento.

El razonamiento escrito en forma simbólica sería:

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

Comprobaremos su validez por varios métodos.

1 Comprobaremos que la veracidad de la conclusión se deduce de la veracidad de la hipótesis.

En efecto, si la proposición $(\forall x, (p(x) \longrightarrow q(x))) \wedge (\forall x, (q(x) \longrightarrow r(x)))$ es verdadera, entonces por el *valor de verdad de la conjunción*, $\forall x, (p(x) \longrightarrow q(x))$ será verdadera y $\forall x, (q(x) \longrightarrow r(x))$ también.

Pues bien, si $\forall x, (p(x) \longrightarrow q(x))$ es verdad, entonces por el *valor de verdad del cuantificador universal*, el predicado $p(x) \longrightarrow q(x)$ se transforma en una proposición verdadera para todos y cada uno de los valores de x en $\mathscr{U}$. En cada una de dichas proposiciones, y por el valor de verdad del condicional, la hipótesis es falsa o la conclusión es verdadera y habrá, por tanto, dos opciones:

- Todas las hipótesis son falsas, es decir el predicado $p(x)$ se transforma en proposición falsa para cada x de $\mathscr{U}$ o lo que es igual $\exists x : p(x)$ es falso.

  En tal caso, el predicado $p(x) \longrightarrow r(x)$ se transformará en proposición verdadera para todos los x, sin importar lo que ocurra con $r(x)$ y, por lo tanto, por el valor de verdad del cuantificador universal, $\forall x, (p(x) \longrightarrow r(x))$ es verdad.
- Las conclusiones, todas, son verdaderas, o sea $q(x)$ se transforma en proposición verdadera para cada x de $\mathscr{U}$, es decir, $\forall x, q(x)$ es verdad.

  En este caso y teniendo en cuenta que $\forall x, (q(x) \longrightarrow r(x))$ es verdad, el predicado $r(x)$ deberá transformarse en una proposición verdadera para todos los x de $\mathscr{U}$ y, por lo tanto, $p(x) \longrightarrow r(x)$ se transforma en verdadera para todos y cada uno de los valores de x en $\mathscr{U}$ lo cual significa, por el valor de verdad del cuantificador universal, que $\forall x, (p(x) \longrightarrow r(x))$ es verdad.

La veracidad de la conclusión se sigue de la veracidad de la hipótesis, luego,

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

y, por tanto, el condicional,

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

es una tautología, es decir, el razonamiento propuesto es válido.

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

Supongamos

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

es verdad. Por el valor de verdad de la conjunción,

- $\forall x, (p(x) \longrightarrow q(x))$ es verdad.
- $\forall x, (q(x) \longrightarrow r(x))$ es verdad.
- $\neg\forall x, (p(x) \longrightarrow r(x))$ es verdad, es decir, $\forall x, (p(x) \longrightarrow r(x))$ 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, es decir, $\neg q(a)$ es verdad y, consecuentemente, $q(a) \wedge \neg q(a)$ es verdad. Hemos encontrado, pues, un valor de x en $\mathscr{U}$ que transforma el predicado $q(x) \wedge \neg q(x)$ en una proposición verdadera, es decir, $\exists x : (q(x) \wedge \neg q(x))$ es verdad.

Como de la veracidad de $(\forall x,(p(x)\longrightarrow q(x)))\wedge(\forall x,(q(x)\longrightarrow r(x)))\wedge\neg\forall x,(p(x)\longrightarrow r(x))$ hemos llegado a la de $\exists x:(q(x)\wedge\neg q(x))$, tendremos que

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

es una tautología.

Ahora bien, el predicado $q(x)\wedge\neg q(x)$ se transforma en una proposición falsa para todos y cada uno de los valores de x en $\mathscr{U}$, por lo tanto, $\exists x:(q(x)\wedge\neg q(x))$ es, siempre, falsa, es decir

$$\exists x:(q(x)\wedge\neg q(x))\Longleftrightarrow C$$

luego,

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

es una tautología.

Aplicamos "*reducción al absurdo*", (1.4.3), y

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

también es una tautología siendo, por tanto, válido el razonamiento propuesto.

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 2.15 , equivale a probar que

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

es una tautología.

En efecto, si $\exists x:(p(x)\wedge\neg r(x))$ es verdad, entonces existirá, al menos, un valor de x en $\mathscr{U}$ que transforma el predicado $p(x)\wedge\neg r(x)$ en una proposición verdadera. Si a ese valor concreto lo llamamos a, tendremos que la proposición $p(a)\wedge\neg r(a)$ es verdadera luego, por el valor de verdad de la conjunción, $p(a)$ es verdad y $\neg r(a)$ también.

El valor de verdad de la conclusión dependerá, por tanto, de las distintas opciones que puedan presentarse para el predicado $q(x)$ y tendremos, por tanto, cuatro opciones:

- $q(x)$ se transforma en proposición verdadera para cada x de $\mathscr{U}$, es decir, $\forall x,q(x)$ es verdad.
  En este caso, y en particular, $q(a)$ será verdadera y como $\neg r(a)$ es verdad, la proposición $q(a)\wedge\neg r(a)$ será verdadera.
- $q(x)$ se transforma en proposición falsa para cada x de $\mathscr{U}$, es decir, $\exists x,q(x)$ es falsa.
  En tal caso, y en particular, $q(a)$ será falsa, o sea, $\neg q(a)$ es verdad y como $p(a)$ es verdad, la proposición $p(a)\wedge\neg q(a)$ será verdadera.
- $q(x)$ se transforma en proposición verdadera para, al menos, un valor de x en $\mathscr{U}$, o sea, $\exists x:q(x)$ es verdad.
  En este caso, habrá dos opciones:
  - si el valor de x encontrado es a, entonces $q(a)$ sería verdadera y estaríamos en el primer caso.
  - Si el valor de x que hemos encontrado no es a, entonces $q(a)$ ha de ser falsa y estaríamos en el segundo caso.

⁕ $q(x)$ se transforma en proposición falsa para, al menos, un valor de x en $\mathscr{U}$, o sea, $\forall x : q(x)$ es falsa.

En tal caso, habría dos opciones:

– si el valor de x encontrado es a, entonces $q(a)$ sería falsa, $\neg q(a)$ verdadera y estaríamos en el segundo caso.
– Si el valor de x que hemos encontrado no es a, entonces $q(a)$ tiene que ser verdadera y estaríamos en el primer caso.

Por lo tanto, y en cualquier caso, siempre existe, al menos, un valor de x en $\mathscr{U}$ que transforma el predicado $p(x) \wedge \neg q(x)$ o el $q(x) \wedge \neg r(x)$ en una proposición verdadera y, por lo tanto, por el valor de verdad del cuantificador existencial, (2.2.4), $\exists x : (p(x) \wedge \neg q(x))$ o $\exists x : (q(x) \wedge \neg r(x))$ son verdaderas lo cual significa, por el valor de verdad de la disyunción, (1.2.2), que la conclusión es verdadera, luego el condicional es una tautología y, consecuentemente, el razonamiento propuesto es válido.

■

Ejemplo 2.19

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,

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

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

el razonamiento propuesto escrito en lenguaje lógico sería:

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

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

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

o lo que es igual, aplicando las leyes de De Morgan generalizadas, que

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

es verdad. Entonces, por el valor de verdad de la conjunción,

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

Pues bien, si la proposición $\forall x, (p(x) \longrightarrow \neg q(x))$ es verdadera, entonces el predicado $p(x) \longrightarrow \neg q(x)$ se convertirá en proposición verdadera para cada x de $\mathscr{U}$ y, al ser $\forall x, p(x)$ verdadera, el predicado $p(x)$ también. Consecuentemente, el valor de verdad del condicional asegura que el predicado $\neg q(x)$ ha de convertirse en proposición verdadera para cada x de $\mathscr{U}$, es decir, $\forall x, \neg q(x)$ es una proposición verdadera. Tendremos, pues, que $(\exists x : q(x)) \wedge (\forall x, \neg q(x))$ es verdad y, por tanto,

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

es una tautología.

Ahora bien, por las leyes de De Morgan generalizadas,

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

por lo tanto,

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

y tendríamos que

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

es una tautología.

Aplicamos "*contradicción*", (1.4.3), y

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

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

■

Unidad Temática II

Teoría de Números

Lección 3

Divisibilidad. Algoritmo de la División

Dios hizo los enteros, el resto es obra del hombre... Todos los resultados de la más profunda investigación matemática deben ser expresables en la sencilla forma de las propiedades de los enteros.

Leopold Kronecker (1823-1891)

3.1 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 $12 = 2 \cdot 6$.

3.1.1 Definición

Sean a y b dos números enteros tales que $a \neq 0$. Diremos que "a" divide a "b" o "a" es divisor de "b" si existe un número entero q tal que $b = a \cdot q$. Suele notarse $a|b$, es decir,

$$a|b \Longleftrightarrow \exists q \in \mathbb{Z} : b = aq$$

■

Nota 3.1 Observemos lo siguiente:

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

y también,

$$\begin{aligned} a \text{ es divisor de } b &\iff b = aq;\ q \in \mathbb{Z} \\ &\iff \frac{b}{a} = q;\ q \in \mathbb{Z} \\ &\iff \frac{b}{a} \in \mathbb{Z} \\ &\iff b \text{ es divisible por } a \end{aligned}$$

luego las expresiones "a divide a b", "a es divisor de b", "b es múltiplo de a" y "b es divisible por a" significan, todas, lo mismo y se notan $a\,|b$.

■

Ejemplo 3.1

(a) 2 divide a 6 ya que $6 = 2 \cdot 3$, con $3 \in \mathbb{Z}$.

(b) 5 divide a -45 ya que $-45 = 5(-9)$, con $-9 \in \mathbb{Z}$.

(c) -4 divide a 64 ya que $64 = (-4)(-16)$, con $-16 \in \mathbb{Z}$.

(d) -7 divide a -21 ya que $-21 = (-7)3$, con $3 \in \mathbb{Z}$.

(e) 3 no divide a 5 ya que no existe ningún número entero q tal que $5 = 3 \cdot q$.

■

Obsérvese que la definición de divisibilidad nos permite hablar de división en $\mathbb{Z}$ sin ir a $\mathbb{Q}$.

Nota 3.2 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.

■

3.1.2 Propiedades

Sean a, b y c tres números enteros, siendo a y b distintos de cero. Se verifica:

(i) El 1 es divisor de cualquier número entero.

(ii) El 0 es múltiplo de cualquier número entero.

(iii) Si "a" divide a "b" y "b" divide a "a", entonces $a = \pm b$.

(iv) Si "a" divide a "b" y "b" divide a "c", entonces "a" divide a "c".

(v) Si "a" divide a "b" y "a" divide a "c", entonces "a" divide a $pb+qc$, cualesquiera que sean p y q, enteros. (A la expresión $pb + qc$ se le llama combinación lineal de b y c con coeficientes enteros).

Demostración

(i) Sea a cualquier número entero distinto de cero. Entonces,

$$a = 1 \cdot a, \text{con } a \in \mathbb{Z}$$

luego, $1 \,|a\,.$

(ii) Sea a cualquier número entero. Entonces,

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

luego, $a \,|0$

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

Recordemos que si n es cualquier entero,

$$|n| = \begin{cases} n, \text{ si } n \geqslant 0 \\ -n, \text{ si } n < 0 \end{cases}$$

entonces,

$$|a| = |b| \iff \begin{cases} a = b, \text{ si } a \geqslant 0,\ b \geqslant 0 \\ a = -b, \text{ si } a \geqslant 0,\ b < 0 \\ -a = b, \text{ si } a < 0,\ b \geqslant 0 \\ -a = -b, \text{ si } a < 0,\ b < 0 \end{cases}$$

$$\iff \begin{cases} a = b \\ \text{o} \\ a = -b \end{cases}$$

Pues bien, veamos que $a\,|b$ y $b\,|a \implies |a| = |b|, \forall a, b \in \mathbb{Z} \setminus \{0\}$ En efecto,

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

y al ser $b \neq 0$ y no tener $\mathbb{Z}$ divisores de cero, se sigue que

$$1 - q_1q_2 = 0 \implies q_1q_2 = 1 \implies \begin{cases} q_1 = q_2 = 1 \\ \text{o} \\ q_1 = q_2 = -1 \end{cases}$$

luego,

$$\left.\begin{array}{l} \left.\begin{array}{l} b = aq_1 \\ a = bq_2 \\ q_1 = q_2 = 1 \end{array}\right\} \implies a = b \\ \text{o} \\ \left.\begin{array}{l} b = aq_1 \\ a = bq_2 \\ q_1 = q_2 = -1 \end{array}\right\} \implies a = -b \end{array}\right\} \implies |a| = |b|$$

Recíprocamente, veamos ahora que $|a| = |b| \implies a\,|b$ y $b\,|a$

En efecto,

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

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

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

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

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

■

Ejemplo 3.2

Probar que si un entero divide a otros dos, entonces divide a su suma y también a su diferencia.

Solución

En efecto, sean a, b y c tres enteros cualesquiera, siendo $a \neq 0$. Entonces,

$$\left.\begin{array}{l} a\,|b \\ \text{y} \\ a\,|c \end{array}\right\} \Longrightarrow \quad a|pb + qc,\ \forall p, q \in \mathbb{Z} \quad \{3.1.2\ (v)\}$$

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

■

Ejemplo 3.3

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

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

(b) $ac\,|bc$ si, y sólo si $a\,|b$.

Solución

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

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

(b) $ac\,|bc$ si, y sólo si $a\,|b$.

"Sólo si." En efecto, supongamos que $ac\,|bc$. Entonces, existirá un entero q tal que

$$bc = acq \Longrightarrow (b - aq)c = 0$$

pero $c \neq 0$ y $\mathbb{Z}$ no tiene divisores de cero, luego

$$b - aq = 0 \Longleftrightarrow b = aq, \text{ con } q \in \mathbb{Z}$$

es decir,

$$a\,|b$$

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

■

Ejemplo 3.4

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

Solución

Aplicando el resultado obtenido en el ejemplo 3.2 ,

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

■

Ejemplo 3.5

Probar que la suma de los cuadrados de dos enteros positivos e impares es múltiplo de 2 pero no de 4.

Solución

Sean a y b dos enteros positivos e impares cualesquiera.

⁕ Veamos que $a^2 + b^2$ es múltiplo de 2. En efecto,

$$\left.\begin{array}{l} a \in \mathbb{Z}^+ \\ a \text{ impar} \end{array}\right\} \Longrightarrow a = 2p+1, \text{ con } p \in \mathbb{Z}_0^+$$

$$\left.\begin{array}{l} b \in \mathbb{Z}^+ \\ b \text{ impar} \end{array}\right\} \Longrightarrow b = 2q+1, \text{ con } q \in \mathbb{Z}_0^+$$

Entonces,

$$\begin{aligned} a^2 + b^2 &= (2p+1)^2 + (2q+1)^2 \\ &= 4p^2 + 4p + 1 + 4q^2 + 4q + 1 \\ &= 2(2p^2 + 2q^2 + 2p + 2q + 1), \text{siendo } 2p^2 + 2q^2 + 2p + 2q + 1 \in \mathbb{Z}^+ \end{aligned}$$

luego,

$$2\,|a^2 + b^2$$

es decir, $a^2 + b^2$ es múltiplo de 2.

⁕ Comprobemos ahora que a^2+b^2 no es múltiplo de 4. En efecto, supongamos que lo contrario es cierto, es decir, a^2+b^2 es múltiplo de 4, o sea,

$$4\,|\,a^2+b^2$$

Pues bien, tenemos que

$$\begin{aligned} a^2+b^2=4p^2+4p+1+4q^2+4q+1 \implies & a^2+b^2-2=4(p^2+p+q^2+q), \\ & \text{con } p^2+p+q^2+q\in\mathbb{Z}^+ \\ \implies & 4\,|\,a^2+b^2-2\,. \end{aligned}$$

Así pues,

$$\left.\begin{array}{l} 4\,|\,a^2+b^2 \\ \text{y} \\ 4\,|\,(a^2+b^2)-2 \end{array}\right\} \overset{(3.2)}{\implies} 4\,|\,(a^2+b^2)-\big[(a^2+b^2)-2\big] \implies 4\,|2$$

lo cual, obviamente, es falso y, por tanto, la suposición hecha no es cierta. Consecuentemente,

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

■

3.2 Algoritmo de la División

Estableceremos en este apartado el algoritmo de la división de dos números, comprobando que el cociente y el resto de la división son únicos.

3.2.1 Existencia y Unicidad de Cociente y Resto

Si a y b son dos números enteros con $b>0$, entonces existen otros dos números, q y r, enteros y únicos, tales que $a=bq+r$, con $0\leqslant r<b$. A los números a, b, q y r se les suele llamar, respectivamente, dividendo, divisor, cociente y resto.

Demostración

Existencia de q y r.

Sean a y b dos números enteros cualesquiera con $b>0$. Encontraremos otros dos números enteros q y r que cumplan las condiciones exigidas, es decir, tales que $a=bq+r$ y $0\leqslant r<b$. En efecto,

$$\left.\begin{array}{l} a=bq+r \\ \text{y} \\ 0\leqslant r<b \end{array}\right\} \implies \left.\begin{array}{l} r=a-bq \\ \text{y} \\ 0\leqslant r<b \end{array}\right\}$$

$$\begin{aligned} \implies & 0\leqslant a-bq<b \\ \implies & bq\leqslant a<b+bq \\ \implies & bq\leqslant a<b(q+1) \end{aligned}$$

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,

$$\left.\begin{array}{rcl} b\,|q_1 - q_2| & = & |r_2 - r_1| \\ \text{y} & & \\ |r_2 - r_1| & < & b \end{array}\right\} \implies b\,|q_1 - q_2| < b$$

$$\begin{aligned} &\implies b\,|q_1 - q_2| - b < 0 \\ &\implies b\,(|q_1 - q_2| - 1) < 0 \\ &\overset{b>0}{\implies} |q_1 - q_2| - 1 < 0 \\ &\implies |q_1 - q_2| < 1 \\ &\overset{q_1 - q_2 \in \mathbb{Z}}{\implies} |q_1 - q_2| = 0 \\ &\implies q_1 = q_2 \end{aligned}$$

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.

■

3.2.2 Corolario

Si a y b son enteros, con $b \neq 0$, entonces existen otros dos números, q y r, enteros y únicos, tales que $a = bq + r$, donde $0 \leqslant r < |b|$.

Demostración

Si $b > 0$, entonces se cumplen las hipótesis del teorema anterior, luego se verifica el corolario.

Si $b < 0$, entonces $-b > 0$ y aplicando el teorema anterior, existirán dos enteros q_1 y r, únicos, tales que

$$a = (-b)q_1 + r, \text{ con } 0 \leqslant r < -b$$

de aquí que

$$a = b(-q_1) + r, \text{ con } 0 \leqslant r < -b = |b|$$

tomando $q = -q_1$, tendremos que

$$a = bq + r, \text{ con } 0 \leqslant r < |b|$$

siendo q y r únicos, ya que q_1 y r lo eran.

■

Ejemplo 3.6

1. Sean $a = 9$ y $b = 2$.
   El mayor múltiplo de 2 menor o igual que 9 es $2 \cdot 4$, luego tomando $q = 4$ y $r = 9 - 2 \cdot 4 = 1$, tendremos que
   $$9 = 2 \cdot 4 + 1, \text{ con } 0 \leqslant 1 < 2$$
2. Sean $a = 2$ y $b = 5$.
   El mayor múltiplo de 5 menor o igual que 2 es $5 \cdot 0$, luego si $q = 0$ y $r = 2 - 5 \cdot 0 = 2$, se sigue que
   $$2 = 5 \cdot 0 + 2, \text{ con } 0 \leqslant 2 < 5$$
3. Sean $a = -17$ y $b = 10$.
   El mayor múltiplo de 10 menor o igual que -17 es $10 \cdot (-2)$, luego tomando $q = -2$ y $r = -17 - 10 \cdot (-2) = 3$, tendremos que
   $$-17 = 10(-2) + 3, \text{ con } 0 \leqslant 3 < 10$$
4. Sean $a = -10$ y $b = 17$.
   El mayor múltiplo de 17 menor o igual que -10 es $17(-1)$, luego si tomamos $q = -1$ y $r = -10 - 17(-1) = 7$, resulta que
   $$-10 = 17(-1) + 7, \text{ con } 0 \leqslant 7 < 17$$
5. Sean $a = 61$ y $b = -7$.
   El mayor múltiplo de -7 menor o igual que 61 es $(-7)(-8)$, así pues si tomamos $q = -8$ y $r = 61 - (-7)(-8) = 61 - 56 = 5$, tendremos que
   $$61 = (-7)(-8) + 5, \text{ con } 0 \leqslant 5 < |-7| = 7$$
6. Sean $a = 7$ y $b = -61$.
   El mayor múltiplo de -61 menor o igual que 7 es $(-61) \cdot 0$, por tanto tomando $q = 0$ y $r = 7 - (-61) \cdot 0 = 7$, resulta
   $$7 = (-61) \cdot 0 + 7, \text{ con } 0 \leqslant 7 < |-61| = 61$$
7. Sean $a = -21$ y $b = -15$.
   El mayor múltiplo de -15 menor o igual que -21 es $(-15)(-2)$. Tomando $q = -2$ y $r = -21 - (-15)(-2) = 9$, resulta
   $$-21 = (-15)(-2) + 9, \text{ con } 0 \leqslant 9 < |-15| = 15$$
8. Sean $a = -15$ y $b = -21$.
   El mayor múltiplo de -21 menor o igual que -15 es $(-21) \cdot 1$, así pues, si tomamos $q = 1$ y $r = -15 - (-21) \cdot 1 = 6$, tendremos
   $$-15 = (-21) \cdot 1 + 6, \text{ con } 0 \leqslant 6 < |-21| = 21$$

■

Ejemplo 3.7

Demuéstrese que el cuadrado de cualquier número impar puede escribirse en la forma

(a) $4k+1$

(b) $8k+1$

Solución

En efecto, sea a cualquier número entero.

(a) Por el teorema de existencia y unicidad de cociente y resto, pueden encontrarse dos números enteros q y r, únicos, tales que
$$a = 2q + r, \text{ con } 0 \leqslant r < 2$$
es decir, $a = 2q + r$, con $r = 0$ ó $r = 1$. Pues bien,

Si $r = 0$, entonces $a = 2q$, es decir a es par.
Si $r = 1$, entonces $a = 2q + 1$, es decir a es impar, y
$$a^2 = (2q+1)^2 = 4q^2 + 4q + 1 = 4(q^2+q) + 1 = 4k + 1, \text{ con } k = q^2 + q \in \mathbb{Z}$$

(b) En el apartado anterior teníamos que
$$a^2 = 4(q^2+q) + 1, \text{ con } q \in \mathbb{Z}$$
o lo que es igual
$$a^2 = 4q(q+1) + 1, \text{ con } q \in \mathbb{Z}.$$
Pues bien, $q(q+1)$ es par ya que uno de los dos, q o $q+1$ será par, luego $q(q+1)$ puede escribirse en la forma $2k$, con k entero. De aquí que
$$a^2 = 4q(q+1) + 1 = 4 \cdot 2k + 1 = 8k + 1, \text{ con } k \in \mathbb{Z}.$$

■

Ejemplo 3.8

Demuéstrese que si un número entero es a la vez un cuadrado y un cubo, entonces puede escribirse en la forma $7k$ ó $7k+1$.

Solución

Sea n cualquier número entero. Entonces, si ha de ser a la vez un cuadrado y un cubo, quiere decir que pueden encontrarse a y b enteros, tales que
$$n = a^2 = b^3$$
Por el teorema 3.2.1, 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 3.2.1, $k_1 = k_2$ y $r_1^2 = r_2^3$. Los diferentes valores que pueden tomar r_1^2 y r_2^3 serán, $0, 1, 4, 9, 16, 25$ y 36 para r_1^2 y $0, 1, 8, 27, 64, 125$ y 216 para r_2^3 y las únicas opciones en las que coinciden es cuando r_1 y r_2 son los dos 0 ó los dos 1. O sea,

$$a^2 = b^3 \Longleftrightarrow a^2 \text{ y } b^3 \text{ son de la forma } 7k \text{ ó } 7k + 1$$

Por tanto,

$$n \text{ es cuadrado y cubo} \Longrightarrow n = 7k \text{ ó } n = 7k + 1$$

■

Ejemplo 3.9

Demostrar que

(a) El cuadrado de cualquier número entero es de la forma $3k$ ó $3k + 1$.

(b) El cubo de cualquier número entero es de la forma $9k$, $9k + 1$ ó $9k + 8$.

Solución

Sea a un entero cualquiera. Entonces, por 3.2.1, existen q y r tales que

$$a = 3q + r, \text{ con } 0 \leqslant r < 3$$

(a) El cuadrado de a es

$$a = 3q + r \Longrightarrow a^2 = (3q + r)^2 = 3(3q^2 + 2qr) + r^2 = 3k_1 + r^2, \text{ con } k_1 = 3q^2 + 2qr$$

Pues bien,

$$\text{Para } r = 0, \ a^2 = 3k, \text{ con } k = k_1$$
$$\text{Para } r = 1, \ a^2 = 3k + 1, \text{ con } k = k_1$$
$$\text{Para } r = 2, \ a^2 = 3k_1 + 4 = 3(k_1 + 1) + 1 = 3k + 1, \text{ con } k = k_1 + 1$$

(b) Veamos ahora como es el cubo de a.

$$\begin{aligned} a = 3q + r &\Longrightarrow a^3 = (3q + r)^3 \\ &\Longrightarrow a^3 = 27q^3 + 27q^2r + 27qr + r^3 \\ &\Longrightarrow a^3 = 9(3q^3 + 3q^2r + 3qr) + r^3 \\ &\Longrightarrow a^3 = 9k + r^3, \text{ con } k = 3q^3 + 3q^2r + 3qr \in \mathbb{Z}. \end{aligned}$$

Entonces,

$$\text{Para } r = 0, \ a^3 = 9k$$
$$\text{Para } r = 1, \ a^3 = 9k + 1$$
$$\text{Para } r = 2, \ a^3 = 9k + 8$$

■

Ejemplo 3.10

Probar que el producto de tres enteros consecutivos es múltiplo de 6.

Solución

Sea a cualquier número entero. El producto de tres enteros consecutivos, siendo a uno de ellos, presenta las siguientes opciones:

$a(a+1)(a+2)$

$(a-1)a(a+1)$

$(a-2)(a-1)a$

Por el teorema de existencia y unicidad de cociente y resto, (3.2.1), existirán q_1 y r, enteros y únicos tales que

$$a = 2q_1 + r,\ 0 \leqslant r < 2$$

y habrá, por tanto, dos opciones:

1 $a = 2q_1$.

En este caso,

$$\begin{array}{rcccl} a(a+1)(a+2) & = & 2q_1(a+1)(a+2) & = & 2q_2, \text{ siendo } q_2 = q_1(a+1)(a+2) \in \mathbb{Z} \\ (a-1)a(a+1) & = & (a-1)2q_1(a+1) & = & 2q_2, \text{ siendo } q_2 = (a-1)q_1(a+1) \in \mathbb{Z} \\ (a-2)(a-1)a & = & (a-2)(a-1)2q_1 & = & 2q_2, \text{ siendo } q_2 = (a-2)(a-1)q_1 \in \mathbb{Z} \end{array}$$

2 $a = 2q_1 + 1$

En tal caso,

$$\begin{array}{rcl} a(a+1)(a+2) & = & (2q_1+1)(2q_1+2)(a+2) \\ & = & 2(2q_1+1)(q_1+1)(a+2) \\ & = & 2q_2, \text{ siendo } q_2 = (2q_1+1)(q_1+1)(a+2) \in \mathbb{Z} \\ (a-1)a(a+1) & = & 2q_1(2q_1+1)(a+1) \\ & = & 2q_2, \text{ siendo } q_2 = q_1(2q_1+1)(a+1) \in \mathbb{Z} \\ (a-2)(a-1)a & = & (a-2)2q_1(2q_1+1) \\ & = & 2q_2, \text{ siendo } q_2 = (a-2)q_1(2q_1+1) \in \mathbb{Z} \end{array}$$

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, (3.2.1), existirán q_1 y r, enteros y únicos tales que

$$a = 3q_1 + r,\ 0 \leqslant r < 3$$

y tendremos, por tanto, tres opciones:

1 $a = 3q_1$.

En este caso,

$$\begin{aligned} a(a+1)(a+2) &= 3q_1(a+1)(a+2) &&= 3q_3, \text{ siendo } q_3 = q_1(a+1)(a+2) \in \mathbb{Z} \\ (a-1)a(a+1) &= (a-1)3q_1(a+1) &&= 3q_3, \text{ siendo } q_3 = (a-1)q_1(a+1) \in \mathbb{Z} \\ (a-2)(a-1)a &= (a-2)(a-1)3q_1 &&= 3q_3, \text{ siendo } q_3 = (a-2)(a-1)q_1 \in \mathbb{Z} \end{aligned}$$

2 $a = 3q_1 + 1$.

En este caso, tendremos,

$$\begin{aligned} a(a+1)(a+2) &= (3q_1+1)(a+1)(3q_1+3) \\ &= 3(3q_1+1)(a+1)(q_1+1) \\ &= 3q_3, \text{ siendo } q_3 = (3q_1+1)(a+1)(q_1+1) \in \mathbb{Z} \\ (a-1)a(a+1) &= 3q_1(3q_1+1)(a+1) \\ &= 3q_3, \text{ siendo } q_3 = q_1(3q_1+1)(a+1) \in \mathbb{Z} \\ (a-2)(a-1)a &= (a-2)3q_1(3q_1+1) \\ &= 3q_3, \text{ siendo } q_3 = (a-2)q_1(3q_1+1) \in \mathbb{Z} \end{aligned}$$

3 $a = 3q_1 + 2$.

En tal caso,

$$\begin{aligned} a(a+1)(a+2) &= (3q_1+2)(3q_1+3)(a+2) \\ &= 3(3q_1+2)(q_1+1)(a+2) = 3q_3, \text{ siendo } q_3 = (3q_1+2)(q_1+1)(a+2) \in \mathbb{Z} \\ (a-1)a(a+1) &= (a-1)(3q_1+2)(3q_1+3) \\ &= 3(a-1)(3q_1+2)(q_1+1) \\ &= 3q_3, \text{ siendo } q_3 = (a-1)(3q_1+2)(q_1+1)) \in \mathbb{Z} \\ (a-2)(a-1)a &= 3q_1(a-1)(3q_1+1) \\ &= 3q_3, \text{ siendo } q_3 = q_1(a-1)(3q_1+1) \in \mathbb{Z} \end{aligned}$$

Por lo tanto, y en cualquier caso, el producto de tres enteros consecutivos es, siempre, múltiplo de 3.

Pues bien, teniendo en cuenta que si un número es múltiplo de otros dos, entonces ha de ser múltiplo del mínimo común múltiplo de ambos,

$$\left.\begin{array}{l} a(a+1)(a+2) = 2q_2 \\ \text{y} \\ a(a+1)(a+2) = 3q_3 \end{array}\right\} \implies a(a+1)(a+2) = \text{m.c.m}(2,3)\cdot q \implies a(a+1)(a+2) = 6q,\ q \in \mathbb{Z}$$

$$\left.\begin{array}{l} (a-1)a(a+1) = 2q_2 \\ \text{y} \\ (a-1)a(a+1) = 3q_3 \end{array}\right\} \implies (a-1)a(a+1) = \text{m.c.m}(2,3)\cdot q \implies (a-1)a(a+1) = 6q,\ q \in \mathbb{Z}$$

$$\left.\begin{array}{l} (a-1)(a-2)a = 2q_2 \\ \text{y} \\ (a-1)(a-2)a = 3q_3 \end{array}\right\} \implies (a-1)(a-2)a = \text{m.c.m}(2,3)\cdot q \implies (a-1)(a-2)a = 6q,\ q \in \mathbb{Z}$$

Es decir, el producto de tres enteros consecutivos es múltiplo de 6.

■

Ejemplo 3.11

Probar que si a es un número entero, entonces $\dfrac{a(a+1)(2a+1)}{6}$ también lo es.

Solución

En efecto,

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

y según el ejemplo anterior, existirán q_1 y q_2, enteros tales que

$$\left.\begin{array}{l} (a-1)a(a+1)=6q_1 \\ \text{y} \\ a(a+1)(a+2)=6q_2 \end{array}\right\} \implies (a-1)a(a+1)+a(a+1)(a+2)=6(q_1+q_2)=6q,\ q=q_1+q_2\in\mathbb{Z}$$

Por lo tanto,

$$\frac{a(a+1)(2a+1)}{6}=\frac{(a-1)a(a+1)+a(a+1)(a+2)}{6}=\frac{6q}{6}=q,\ \text{siendo } q\in\mathbb{Z}$$

■

3.3 Sistemas de Numeración

Consideremos, por ejemplo, el entero positivo 7345. Normalmente leemos "siete mil trescientos cuarenta y cinco" y, dado que es lo habitual, entendemos que está escrito en el sistema decimal de numeración o en "base 10".

También sabemos que la última cifra, leyendo el número de derecha a izquierda, es la de las unidades, la siguiente es la cifra de las decenas, la que sigue de las centenas, y así sucesivamente. Observemos lo siguiente:

$$7345 = 5 + 40 + 300 + 7000$$

y si escribimos los números de la derecha como potencias de diez, tendremos

$$7345 = 5\cdot 10^0 + 4\cdot 10^1 + 3\cdot 10^2 + 7\cdot 10^3$$

y esto mismo puede hacerse con cualquier número entero positivo escrito en forma decimal, es decir si tal número es $a_k a_{k-1}\cdots a_2 a_1 a_0$, entonces

$$a_k a_{k-1}\cdots a_2 a_1 a_0 = a_0\cdot 10^0 + a_1\cdot 10^1 + a_2\cdot 10^2 + \cdots + a_{k-1}\cdot 10^{k-1} + a_k\cdot 10^k = \sum_{i=0}^{k} a_i 10^i$$

y esta forma de escribir el número se conoce como "representación polinómica" del mismo tomando como base el número 10.

Normalmente, se dice que a_0 es una unidad de primer orden, a_1 de segundo orden, a_2 de tercero y, en general, diremos que a_k es una unidad de orden $k+1$.

Consideramos ahora el número 35 y lo escribimos en la forma

$$35 = 1 \cdot 2^0 + 1 \cdot 2^1 + 0 \cdot 2^2 + 0 \cdot 2^3 + 0 \cdot 2^4 + 1 \cdot 2^5.$$

En tal caso tendríamos una "representación polinómica" del número 35 tomando como base el número 2.

Nada nos impide utilizar otro número como base para la representación polinómica del número 35. Por ejemplo, si tomamos el 3, tendríamos

$$35 = 2 \cdot 3^0 + 2 \cdot 3^1 + 0 \cdot 3^2 + 1 \cdot 3^3$$

y si tomáramos el 8,

$$35 = 3 \cdot 8^0 + 4 \cdot 8^1$$

El siguiente teorema matiza y aclara estas ideas.

3.3.1 Descomposición Polinómica de un Número

Dados dos números enteros positivos n y b (con $b \geqslant 2$) pueden encontrarse $k+1$ enteros no negativos, a_k, únicos, tales que

$$n = \sum_{i=0}^{k} a_i b^i$$

con $i \geqslant 0,\ 0 \leqslant a_i < b;\ i = 0, 1, \ldots, k$, siendo $a_k \neq 0$.

Demostración

En efecto, dados n y b, por 3.2.1, existirán q_1 y a_0, únicos, tales que

$$n = bq_1 + a_0,\ \text{con}\ 0 \leqslant a_0 < b \ \text{y}\ q_1 < n.$$

Obtenido q_1 y aplicando de nuevo el *algoritmo de la división*, pueden encontrarse q_2 y a_1, únicos, tales que

$$q_1 = bq_2 + a_1 \ \text{con}\ 0 \leqslant a_1 < b,\ \text{y}\ q_2 < q_1.$$

Reiterando el proceso,

$$q_2 = bq_3 + a_2 \ \text{con}\ 0 \leqslant a_2 < b,\ \text{y}\ q_3 < q_2$$
$$q_3 = bq_4 + a_3 \ \text{con}\ 0 \leqslant a_3 < b,\ \text{y}\ q_4 < q_3$$

y así sucesivamente.

Tendremos una sucesión de enteros positivos,

$$n, q_1, q_2, q_3, q_4, \ldots$$

tal que

$$n > q_1 > q_2 > q_3 > q_4 > \cdots$$

y que por el *principio del buen orden*, tiene un primer elemento q_k tal que

$$q_k = b \cdot 0 + a_k,\ \text{con}\ 0 \leqslant a_k < b$$

y a_k ha de ser distinto de cero ya que de lo contrario q_k sería cero, lo cual es imposible ya que es un entero positivo.

Pues bien, sustituyendo el valor de q_1 en n,

$$\left.\begin{array}{l} n = q_1 b + a_0 \\ q_1 = q_2 b + a_1 \end{array}\right\} \Longrightarrow n = (q_2 b + a_1)\, b + a_0 = q_2 b^2 + a_1 b + a_0$$

y sustituyendo en este resultado el valor de q_2,

$$\left.\begin{array}{l} n = q_2 b^2 + a_1 b + a_0 \\ q_2 = q_3 b + a_2 \end{array}\right\} \Longrightarrow n = (q_3 b + a_2)\, b^2 + a_1 b + a_0 = q_3 b^3 + a_2 b^2 + a_1 b + a_0.$$

Repitiendo el proceso para q_3,

$$\left.\begin{array}{l} n = q_3 b^3 + a_2 b^2 + a_1 b + a_0 \\ q_3 = q_4 b + a_3 \end{array}\right\} \begin{array}{ll} \Longrightarrow & n = (q_4 b + a_3)\, b^3 + a_2 b^2 + a_1 b + a_0 \\ \Longrightarrow & n = q_4 b^4 + a_3 b^3 + a_2 b^2 + a_1 b + a_0. \end{array}$$

Y siguiendo hasta q_k,

$$\left.\begin{array}{l} n = q_k b + \cdots + a_2 b^2 + a_1 b + a_0 \\ q_k = a_k \end{array}\right\} \Longrightarrow n = a_k b^k + \cdots + a_2 b^2 + a_1 b + a_0$$

donde por 3.2.1, los coeficientes a_k son únicos, $0 \leqslant a_i < b,\ i = 0, 1, \ldots, k$ y, como ya hemos visto, $a_k \neq 0$.

La expresión obtenida es la *descomposición polinómica* de n en la base b y se escribe $a_0 a_1 a_2 \cdots a_{k_{(b}}$.

■

Ejemplo 3.12

Escribir en forma decimal el número $1243_{(5}$.

Solución

Bastaría escribir la representación polinómica del número.

$$1243_{(5} = 3 + 4 \cdot 5 + 2 \cdot 5^2 + 1 \cdot 5^3 = 3 + 20 + 50 + 125 = 198$$

■

En el ejemplo siguiente veremos como puede utilizarse el teorema 3.2.1 para hacer lo contrario, es decir escribir la representación de números enteros en bases distintas de la decimal.

Ejemplo 3.13

Escribir el número 5346 en base 7.

Solución

El número dado en base 7 será:

$$5346 = a_k a_{k-1} a_{k-2} \cdots a_2 a_1 a_{0_{(7}}$$

y utilizando la representación polinómica del número,

$$\begin{aligned} 5346 &= a_k \cdot 7^k + a_{k-1} \cdot 7^{k-1} + a_{k-2} \cdot 7^{k-2} + \cdots + a_2 \cdot 7^2 + a_1 \cdot 7 + a_0 \\ &= 7\left(a_k \cdot 7^{k-1} + a_{k-1} \cdot 7^{k-2} + a_{k-2} \cdot 7^{k-3} + \cdots + a_2 \cdot 7 + a_1\right) + a_0. \end{aligned} \tag{3.1}$$

Por otra parte, por el 3.2.1,

$$5346 = 7 \cdot 763 + 5 \tag{3.2}$$

y por la unicidad del cociente y resto, de (3.1) y (3.2), se sigue que

$$\begin{aligned} a_0 &= 5 \\ \text{y} & \\ 763 &= a_k \cdot 7^{k-1} + a_{k-1} \cdot 7^{k-2} + a_{k-2} \cdot 7^{k-3} + \cdots + a_2 \cdot 7 + a_1. \end{aligned}$$

Entonces,

$$\begin{aligned} 763 &= a_k \cdot 7^{k-1} + a_{k-1} \cdot 7^{k-2} + \cdots + a_3 \cdot 7^2 + a_2 \cdot 7 + a_1 \\ &= 7\left(a_k \cdot 7^{k-2} + a_{k-1} \cdot 7^{k-3} + \cdots + a_3 \cdot 7 + a_2\right) + a_1. \end{aligned} \tag{3.3}$$

y por 3.2.1,

$$763 = 7 \cdot 109 + 0 \tag{3.4}$$

y, de nuevo, por la unicidad del cociente y el resto, de (3.3) y (3.3), tendremos que

$$\begin{aligned} a_1 &= 0 \\ \text{y} & \\ 109 &= a_k \cdot 7^{k-2} + a_{k-1} \cdot 7^{k-3} + \cdots + a_4 \cdot 7^2 + a_3 \cdot 7 + a_2. \end{aligned}$$

Repitiendo el proceso,

$$\begin{aligned} 109 &= 7\left(a_k \cdot 7^{k-3} + a_{k-1} \cdot 7^{k-4} + \cdots + a_4 \cdot 7 + a_3\right) + a_2 \\ \text{y} & \\ 109 &= 7 \cdot 15 + 4 \end{aligned}$$

luego,

$$\begin{aligned} a_2 &= 4 \\ \text{y} & \\ 15 &= a_k \cdot 7^{k-3} + a_{k-1} \cdot 7^{k-4} + \cdots + a_5 \cdot 7^2 + a_4 \cdot 7 + a_3. \end{aligned}$$

Repetimos de nuevo, y

$$\begin{aligned} 15 &= 7\left(a_k \cdot 7^{k-4} + a_{k-1} \cdot 7^{k-5} + \cdots + a_5 \cdot 7 + a_4\right) + a_3 \\ \text{y} & \\ 15 &= 7 \cdot 2 + 1 \end{aligned}$$

luego,

$$\begin{aligned} a_3 &= 1 \\ \text{y} & \\ 2 &= a_k \cdot 7^{k-4} + a_{k-1} \cdot 7^{k-5} + \cdots + a_6 \cdot 7^2 + a_5 \cdot 7 + a_4. \end{aligned}$$

Por última vez,

$$2 = 7\left(a_k \cdot 7^{k-5} + a_{k-1} \cdot 7^{k-6} + \cdots + a_6 \cdot 7 + a_5\right) + a_4$$

y

$$2 = 7 \cdot 0 + 2$$

luego,

$$a_4 = 2$$

y

$$0 = a_k \cdot 7^{k-5} + a_{k-1} \cdot 7^{k-6} + \cdots + a_6 \cdot 7 + a_5.$$

A partir de aquí todos los restos son cero, el proceso termina, y

$$5346 = 2 \cdot 7^4 + 1 \cdot 7^3 + 4 \cdot 7^2 + 0 \cdot 7 + 5 = 21405_{(7}.$$

En la práctica, este proceso de divisiones sucesivas suele hacerse en la forma

5346	7			
44	763	7		
26	06	109	7	
5	63	39	15	7
	0	4	1	2

y

$$5346 = 21405_{(7}$$

■

Nota 3.3 El sistema de numeración en base 2 o sistema binario es de vital importancia en la informática. Los únicos dígitos que pueden utilizarse son los *bits* 0 y 1.

Con los dígitos 0 y 1, el número de números de cuatro cifras que pueden construirse es

$$VR_{2,4} = 2^4 = 16$$

luego utilizando cuatro posiciones, con los *bits* 0 y 1 podemos representar 16 números enteros. La representación binaria de los dieciséis primeros números enteros es

0	0000
1	0001
2	0010
3	0011
4	0100
5	0101
6	0110
7	0111
8	1000
9	1001
10	1010
11	1011
12	1100
13	1101
14	1110
15	1111

Los ordenadores utilizan, normalmente, grupos de ocho dígitos (*octetos* o *bytes*) para almacenar información. Obsérvese que el número de octetos que pueden construirse con los dígitos 0 y 1 es

$$VR_{2,8} = 2^8 = 256$$

lo cual equivale a decir que puede almacenarse cualquier número entero entre 0 y 255 en formato binario.

Otro sistema de numeración muy utilizado en la informática es el de base 16 o hexadecimal. Además de los dígitos del 0 al 9, usaremos A, B, C, D, E y F para los números 10, 11, 12, 13, 14 y 15, respectivamente.

En la primera y tercera columna de la tabla siguiente recogemos la expresión binaria y hexadecimal de los enteros entre el 0 y el 15.

Binario	Decimal	Hexadecimal
0000	0	0
0001	1	1
0010	2	2
0011	3	3
0100	4	4
0101	5	5
0110	6	6
0111	7	7
1000	8	8
1001	9	9
1010	10	A
1011	11	B
1100	12	C
1110	13	D
1110	14	E
1111	15	F

■

3.3.2 Representación Hexadecimal de un Octeto

Para escribir un octeto (número de ocho bits en binario) en forma hexadecimal, podemos escribirlo en base diez y, posteriormente, hallar su representación hexadecimal. Veremos un método para obtenerla directamente.

Según hemos visto, con los dígitos 0 y 1, podemos escribir un total de 256 octetos. La primera cuestión es saber cuantos dígitos hexadecimales tiene un octeto. En efecto, si x es dicho número, y a cada octeto le corresponde un número en hexadecimal y, dado que pueden escribirse un total de $VR_{16,x}$ números hexadecimales con x dígitos, tendremos que

$$VR_{16,x} = VR_{2,8}$$

de aquí que

$$16^x = 2^8 \Longrightarrow 2^{4x} = 2^8 \Longrightarrow 4x = 8 \Longrightarrow x = 2$$

luego a cada octeto le corresponde un número hexadecimal de dos cifras.

Pues bien, sea N un número cualquiera y sean

$$\begin{aligned} N &= a_7a_6a_5a_4a_3a_2a_1a_{0_{(2}} \\ \text{y} & \\ N &= b_1b_{0_{(16}} \end{aligned}$$

sus representaciones respectivas en binario (con ocho bits) y en hexadecimal. Entonces,

$$\begin{aligned} N &= a_0 + a_1 \cdot 2 + a_2 \cdot 2^2 + a_3 \cdot 2^3 + a_4 \cdot 2^4 + a_5 \cdot 2^5 + a_6 \cdot 2^6 + a_7 \cdot 2^7 \\ \text{y} & \\ N &= b_0 + b_1 \cdot 16 \end{aligned}$$

es decir,

$$\begin{aligned} N &= a_0 + a_1 \cdot 2 + a_2 \cdot 2^2 + a_3 \cdot 2^3 + 16(a_4 + a_5 \cdot 2 + a_6 \cdot 2^2 + a_7 \cdot 2^3) \\ \text{y} & \\ N &= b_0 + b_1 \cdot 16 \end{aligned}$$

y como el cociente y el resto de dividir N entre 16 son únicos, (3.2.1),

$$\begin{aligned} b_0 &= a_0 + a_1 \cdot 2 + a_2 \cdot 2^2 + a_3 \cdot 2^3 \\ \text{y} & \\ b_1 &= a_4 + a_5 \cdot 2 + a_6 \cdot 2^2 + a_7 \cdot 2^3 \end{aligned}$$

es decir,

$$\begin{aligned} b_{0_{(16}} &= a_3a_2a_1a_{0_{(2}} \\ \text{y} & \\ b_{1(16} &= a_7a_6a_5a_{4_{(2}} \end{aligned}$$

Así pues, para convertir un entero binario de ocho bits a base 16, basta descomponerlo en dos bloques de cuatro bits y representar cada uno de ellos en hexadecimal.

■

Ejemplo 3.14

Obtener la representación hexadecimal del número 01111100.

Solución

Descomponemos el número en dos de cuatro bits y, según la tabla anterior,

0111	1100
7	C

luego

$$01111100_{(2} = 7C_{(16}$$

■

3.3.3 Representación Binaria de un hexadecimal

Veamos ahora como puede escribirse directamente en binario un número hexadecimal de cuatro dígitos.

El número de representaciones hexadecimales con cuatro dígitos será $VR_{16,4}$. Si, al igual que en el apartado anterior, a cada uno de ellos le hacemos corresponder su representación en binario y x es el número de bits que tiene dicha representación, tendremos que

$$VR_{2,x} = VR_{16,4}$$

de aquí que

$$2^x = 16^4 \Longrightarrow 2^x = 2^{16} \Longrightarrow x = 16$$

es decir cada número de cuatro dígitos hexadecimales puede representarse por 16 dígitos binarios (dos octetos).

Pues bien, sea N un entero arbitrario y sean

$$\begin{aligned} N &= a_3a_2a_1a_{0_{(16}} \\ \text{y} & \\ N &= b_{15}b_{14}b_{13}b_{12}b_{11}b_{10}b_9b_8b_7b_6b_5b_4b_3b_2b_1b_{0_{(2}} \end{aligned}$$

sus representaciones en hexadecimal con 4 dígitos y en binario con 16 bits, respectivamente. Entonces,

$$\begin{aligned} N &= a_0 + a_1 \cdot 16 + a_2 \cdot 16^2 + a_3 \cdot 16^3 \\ \text{y} & \\ N &= b_0 + b_1 \cdot 2 + b_2 \cdot 2^2 + b_3 \cdot 2^3 + b_4 \cdot 2^4 + b_5 \cdot 2^5 + b_6 \cdot 2^6 + b_7 \cdot 2^7 + b_8 \cdot 2^8 + b_9 \cdot 2^9 + \\ & \quad b_{10} \cdot 2^{10} + b_{11} \cdot 2^{11} + b_{12} \cdot 2^{12} + b_{13} \cdot 2^{13} + b_{14} \cdot 2^{14} + b_{15} \cdot 2^{15} \end{aligned}$$

o sea,

$$\begin{aligned} N &= a_0 + a_1 \cdot 16 + a_2 \cdot 16^2 + a_3 \cdot 16^3 \\ \text{y} & \\ N &= b_0 + b_1 \cdot 2 + b_2 \cdot 2^2 + b_3 \cdot 2^3 \\ &+ 16\left(b_4 + b_5 \cdot 2 + b_6 \cdot 2^2 + b_7 \cdot 2^3\right) \\ &+ 16^2\left(b_8 + b_9 \cdot 2 + b_{10} \cdot 2^2 + b_{11} \cdot 2^3\right) \\ &+ 16^3\left(b_{12} + b_{13} \cdot 2 + b_{14} \cdot 2^2 + b_{15} \cdot 2^3\right) \end{aligned}$$

y como la descomposición polinómica de un número en una base dada es única,

$$\begin{aligned} a_0 &= b_0 + b_1 \cdot 2 + b_2 \cdot 2^2 + b_3 \cdot 2^3 \\ a_1 &= b_4 + b_5 \cdot 2 + b_6 \cdot 2^2 + b_7 \cdot 2^3 \\ a_2 &= b_8 + b_9 \cdot 2 + b_{10} \cdot 2^2 + b_{11} \cdot 2^3 \\ a_3 &= b_{12} + b_{13} \cdot 2 + b_{14} \cdot 2^2 + b_{15} \cdot 2^3 \end{aligned}$$

es decir,

$$\begin{aligned} a_{0_{(16}} &= b_3b_1b_2b_{0_{(2}} \\ a_{1_{(16}} &= b_7b_6b_5b_{4_{(2}} \\ a_{2_{(16}} &= b_{11}b_{10}b_9b_{8_{(2}} \\ a_{3_{(16}} &= b_{15}b_{14}b_{13}b_{12_{(2}} \end{aligned}$$

Así pues, para convertir un número hexadecimal de cuatro dígitos a binario, basta obtener la representación binaria con cuatro dígitos de cada uno de los símbolos hexadecimales.

■

Ejemplo 3.15

Obtener la representación binaria del número hexadecimal $A8B3$.

Solución

Según la tabla,

A	8	B	3
1010	1000	1011	0011

luego,

$$A8B3_{(16} = 1010100010110011_{(2}$$

■

3.4 Criterios de Divisibilidad

Ejemplo 3.16

Demostrar que un número entero positivo es divisible por 2 si, y sólo si lo es su última cifra.

Solución

Sea $n \in \mathbb{Z}^+$, cualquiera y sea

$$n = a_k 10^k + a_{k-1}10^{k-1} + \cdots + a_2 10^2 + a_1 10 + a_0 = \sum_{i=0}^{k} a_i 10^i$$

su representación decimal. Entonces,

$$\begin{aligned} 2\,|10 \quad &\Longrightarrow \quad 2\,|10^i \ ; \ i = 1, 2, \ldots, k \\ &\Longrightarrow \quad 2\,|a_i 10^i \ ; \ i = 1, 2, \ldots, k \\ &\Longrightarrow \quad 2\,\left|\sum_{i=1}^{k} a_i 10^i \right. \\ &\Longrightarrow \quad 2\,|n - a_0 \ . \end{aligned}$$

"Sólo si". En efecto, supongamos que n es divisible por 2. Entonces,

$$\left.\begin{array}{l} 2\,|n \\ 2\,|n - a_0 \end{array}\right\} \Longrightarrow 2\,|n - (n - a_0) \Longrightarrow 2\,|a_0$$

"Si". En efecto, supongamos ahora que la última cifra de n es divisible por 2, es decir $2\,|a_0$. Entonces

$$\left.\begin{array}{l} 2\,|a_0 \\ 2\,|n - a_0 \end{array}\right\} \Longrightarrow 2\,|a_0 + n - a_0 \Longrightarrow 2\,|n$$

Así pues,

un número entero positivo es divisible por 2 *si, y sólo si su última cifra es* 2 *o múltiplo de* 2.

■

3.4.1 Criterio General de Divisibilidad

Sea n un entero positivo, sea $\sum_{i=1}^{k} a_i 10^i$ su representación decimal, y sean r_i los restos de la división de 10^i por $p \geqslant 2$, $i = 1, 2, \ldots, k$. Entonces,

$$n \text{ es divisible por } p \text{ si, y sólo si lo es } \sum_{i=1}^{k} a_i r_i.$$

Demostración

Sea $p \geqslant 2$. Por el teorema 3.2.1, existirán q_i y r_i, $i = 1, 2, \ldots, k$ tales que

$$\begin{aligned} 10^0 &= q_0 p + r_0 \\ 10 &= q_1 p + r_1 \\ 10^2 &= q_2 p + r_2 \\ \ldots &\quad \ldots\ldots\ldots \\ 10^k &= q_k p + r_k \end{aligned}$$

es decir, $10^i = q_i p + r_i$, $i = 0, 1, \ldots, k$ donde $q_0 = 0$ y $r_0 = 1$. Entonces,

$$10^i - r_i = q_i p$$

luego,

$$p \,|10^i - r_i \ , \ i = 0, 1, 2, \ldots, k$$

de aquí que

$$p \,|a_i \left(10^i - r_i\right) \ , \ i = 0, 1, 2, \ldots, k$$

y, por lo tanto,

$$p \left| \sum_{i=0}^{k} a_i \left(10^i - r_i\right) \right.$$

luego,

$$p \left| \left(\sum_{i=0}^{k} a_i 10^i - \sum_{i=0}^{k} a_i r_i \right) \right.$$

es decir,

$$p \left| \left(n - \sum_{i=0}^{k} a_i r_i \right) \right.$$

"Sólo si". En efecto, si $p \,|n$, entonces,

$$\left.\begin{array}{l} p \,|n \\ \text{y} \\ p \left| \left(n - \sum_{i=0}^{k} a_i r_i \right) \right. \end{array}\right\} \Longrightarrow p \left| n - \left(n - \sum_{i=0}^{k} a_i r_i \right) \right. \Longrightarrow p \left| \sum_{i=0}^{k} a_i r_i \right.$$

"Si". En efecto, si $p \left| \sum_{i=0}^{k} a_i r_i \right.$, entonces,

$$\left.\begin{array}{l} p \left| \sum_{i=0}^{k} a_i r_i \right. \\ \text{y} \\ p \left| \left(n - \sum_{i=0}^{k} a_i r_i \right) \right. \end{array}\right\} \Longrightarrow p \left| \left(\sum_{i=0}^{k} a_i r_i + n - \sum_{i=0}^{k} a_i r_i \right) \right. \Longrightarrow p \,|n$$

■

Veamos de nuevo el ejemplo 3.16 .

Ejemplo 3.17

Demostrar que un número entero positivo es divisible por 2 si, y sólo si lo es su última cifra.

Solución

Sea $n \in \mathbb{Z}^+$, cualquiera, sea

$$n = a_k 10^k + a_{k-1} 10^{k-1} + \cdots + a_2 10^2 + a_1 10 + a_0 = \sum_{i=0}^{k} a_i 10^i$$

su representación decimal y sean r_i los restos de dividir 10^i entre 2 para $i = 0, 1, 2, \ldots, k$. Entonces,

$$r_0 = 1$$

y

$$r_i = 0, \ i = 1, 2, \ldots, k$$

de aquí que

$$\sum_{i=1}^{k} a_i r^i = a_0$$

luego por el criterio anterior,

"n sea divisible por 2 si, y sólo si lo es su última cifra"

■

Ejemplo 3.18

Obtener una condición necesaria y suficiente para que un número entero positivo sea divisible por 3.

Solución

Sea $n \in \mathbb{Z}^+$, cualquiera, sea

$$n = a_k 10^k + a_{k-1} 10^{k-1} + \cdots + a_2 10^2 + a_1 10 + a_0 = \sum_{i=0}^{k} a_i 10^i$$

su representación decimal y sean r_i los restos de dividir 10^i entre 3 para $i = 0, 1, 2, \ldots, k$. Por 3.2.1, existirá un entero positivo q tal que

$$10 = 3q + 1$$

luego,

$$10^i = (3q+1)^i$$

y desarrollando por el *teorema del binomio*,

$$\begin{aligned} 10^i &= (3q+1)^i \\ &= \sum_{k=0}^{i} \binom{i}{k} (3q)^k \\ &= 1 + \sum_{k=1}^{i} \binom{i}{k} 3^k q^k \\ &= 1 + 3\left[\sum_{k=1}^{i} \binom{i}{k} 3^{k-1} q^k\right] \\ &\quad \left\{\text{Tomando } q_i = \sum_{k=1}^{i} \binom{i}{k} 3^{k-1} q^k\right\} \\ &= 3q_i + 1, \ q_i \in \mathbb{Z} \end{aligned}$$

es decir, los restos, r_i, de dividir 10^i entre 3 para $i = 0, 1, 2, \ldots, k$ son siempre iguales a 1, luego

$$\sum_{i=1}^{k} a_i r_i = \sum_{i=1}^{k} a_i$$

de aquí que por el *criterio general de divisibilidad*, (3.4.1), n es divisible por 3 si, y sólo si lo es la suma de sus cifras, o lo que es igual

> *"Una condición necesaria y suficiente para que un entero positivo sea divisible por* 3 *es que la suma de sus cifras sea múltiplo de* 3*".*

■

Ejemplo 3.19

Obtener un criterio de divisibilidad por 4.

Solución

Sea $n \in \mathbb{Z}^+$, cualquiera, sea

$$n = a_k 10^k + a_{k-1} 10^{k-1} + \cdots + a_2 10^2 + a_1 10 + a_0 = \sum_{i=0}^{k} a_i 10^i$$

su representación decimal y sean r_i los restos de dividir 10^i entre 4 para $i = 0, 1, 2, \ldots, k$. Entonces, $r_0 = 1$ y $r_1 = 2$, y si tenemos en cuenta que

$$4 \,|100 \ , \text{ es decir, } \ 4 \,\big|10^2$$

tendremos que

$$4 \left| 10^{i-2} \cdot 10^2 \right. , \ i = 2, 3, \ldots, k$$

es decir,

$$4 \left| 10^i \right. , \ i = 2, 3, \ldots, k$$

luego,

$$r_i = 0, \ i = 2, 3, \ldots, k$$

de aquí que

$$\sum_{i=0}^{k} a_i r_i = a_0 + 2a_1$$

es decir,

> *"n es divisible por 4 si, y sólo si lo es la suma de la cifra de las unidades más dos veces la cifra de las decenas".*

■

Ejemplo 3.20

Obtener un criterio de divisibilidad por 5.

Solución

Sea $n \in \mathbb{Z}^+$, cualquiera, sea

$$n = a_k 10^k + a_{k-1} 10^{k-1} + \cdots + a_2 10^2 + a_1 10 + a_0 = \sum_{i=0}^{k} a_i 10^i$$

su representación decimal y sean r_i los restos de dividir 10^i entre 5 para $i = 0, 1, 2, \ldots, k$. Entonces,

$$r_0 = 1$$

y

$$r_i = 0, \ i = 1, 2, \ldots, k$$

de aquí que

$$\sum_{i=1}^{k} a_i r^i = a_0$$

luego por el criterio general de divisibilidad,

"n sea divisible por 5 si, y sólo si lo es su última cifra"

■

Ejemplo 3.21

Obtener un criterio de divisibilidad por 8.

Solución

Sea $n \in \mathbb{Z}^+$, cualquiera, y sea

$$n = a_k 10^k + a_{k-1} 10^{k-1} + \cdots + a_2 10^2 + a_1 10 + a_0 = \sum_{i=0}^{k} a_i 10^i$$

su representación polinómica en base decimal.

Si r_i son los restos de dividir 10^i entre 8 para $i = 0, 1, 2 \ldots, k$, entonces $r_0 = 1$, $r_1 = 2$ y $r_2 = 4$ y teniendo en cuenta que

$$8|1000, \text{ es decir, } 8 \left| 10^3 \right.$$

tendremos que

$$8 \left| 10^{i-3} 10^3 \right. , \ i = 3, 4, \ldots, k$$

o sea,

$$8 \left| 10^i \right. , \ i = 3, 4, \ldots, k$$

de aquí que

$$r_i = 0, \ i = 3, 4, \ldots, k$$

y, consecuentemente,

$$\sum_{i=0}^{k} a_i r_i = a_0 + 2a_1 + 4a_2.$$

Aplicando el criterio general de divisibilidad,

> *"n es divisible por* 8 *si, y sólo lo es la suma de las cifras de sus unidades más dos veces la cifra de sus decenas más cuatro veces la cifra de sus centenas"*

■

3.5 Máximo Común Divisor

Siguiendo con la operación de división que desarrollamos anteriormente, centraremos ahora nuestra atención en los divisores comunes de un número finito de números enteros.

3.5.1 Definición

Dados los números enteros positivos a_1, a_2, a_3, ..., a_n, llamaremos máximo común divisor de todos ellos al ínfimo del conjunto $\{a_1, a_2, a_3, \ldots, a_n\}$ ordenado con la relación de orden parcial de divisibilidad. Lo notaremos m.c.d.$(a_1, a_2, a_3, \ldots, a_n)$

Ejemplo 3.22

Calcular, aplicando directamente la definición anterior,

$$\text{m.c.d. } (72, 108, 144, 216, 324, 288, 432, 648, 972, 864, 1296, 1944, 2592, 3888)$$

Solución

Según la definición de máximo común divisor de varios números, tendremos que calcular el Ínfimo del conjunto

$$A = \{72, 108, 144, 216, 324, 288, 432, 648, 972, 864, 1296, 1944, 2592, 3888\}$$

ordenado con la relación de orden de divisibilidad, es decir, si a y b son cualesquiera de A,

$$a \text{ es anterior a } b \text{ siempre y cuando } a \text{ divida a } b$$

o sea,

$$a \preccurlyeq b \iff a|b$$

Recordemos que el ínfimo de A es el máximo del conjunto de sus cotas inferiores ordenado por la relación anterior. Vamos a calcular, pues, los elementos característicos de este conjunto.

Elementos Minimales. Por definición, un elemento m de A será minimal de A, respecto de la relación $\preccurlyeq$, si no hay en A elemento alguno que sea estrictamente anterior a él, es decir,

$$m \text{ es minimal de } A \iff \nexists x \in A : x \prec m$$

o lo que es igual,

$$m \text{ es minimal de } A \iff \nexists x \in A : x \preccurlyeq m \text{ y } x \neq m$$

y esto significa, teniendo en cuenta que la relación $\preccurlyeq$ es la de divisibilidad,

$$m \text{ es minimal de } A \iff \nexists x \in A : x \text{ divida a } m \text{ y } x \neq m$$

es decir,

$$m \text{ es minimal de } A \iff m \text{ no tiene en } A \text{ divisores distintos del propio } m.$$

Consecuentemente,

$$m \text{ es minimal de } A \iff m = 72 \text{ ó } m = 108$$

Obsérvese que al haber dos minimales no puede haber mínimo, ya que éste, caso de existir, ha de ser único y coincidir con el minimal.

Cotas Inferiores. Un elemento $i \in \mathbb{Z}^+$ es cota inferior de A, subconjunto de $\mathbb{Z}^+$, si es anterior a todos los elementos de A, o sea,

$$i \in \mathbb{Z}^+ \text{ es cota inferior de } A \subseteq \mathbb{Z}^+ \iff \forall x \, (x \in A \Longrightarrow i \preccurlyeq x)$$

es decir,

$$i \in \mathbb{Z}^+ \text{ es cota inferior de } A \subseteq \mathbb{Z}^+ \iff \forall x \, (x \in A \Longrightarrow i \text{ divide a } x)$$

Así pues,

$$i \in \mathbb{Z}^+ \text{ es cota inferior de } A \subseteq \mathbb{Z}^+ \iff i \text{ divide a todos los elementos de } A$$

y bastaría con que i dividiese a los minimales de A ya que por transitividad esto significaría que divide a todos los elementos de A. Por lo tanto,

$$i \in \mathbb{Z}^+ \text{ es cota inferior de } A \subseteq \mathbb{Z}^+ \iff i \text{ divide a los elementos minimales de } A.$$

Así pues,

$$\begin{aligned} i \in \mathbb{Z}^+ \text{ es cota inferior de } A \subseteq \mathbb{Z}^+ &\iff i \text{ divide a 72 y 108} \\ &\iff \begin{cases} i \text{ es divisor de 72} \\ \text{e} \\ i \text{ es divisor de 108} \end{cases} \\ &\iff \begin{cases} i \in \{1,2,4,8,3,6,12,24,9,18,36,72\} \\ \text{e} \\ i \in \{1,2,4,3,6,12,9,18,36,27,54,108\} \end{cases} \\ &\iff i \in \{1,2,4,3,6,12,9,18,36\} \end{aligned}$$

luego, si llamamos C_i al conjunto de las cotas inferiores, tendremos que

$$C_i = \{1,2,3,4,6,9,12,18,36\}$$

Ínfimo. Un elemento d de $\mathbb{Z}^+$ se dice que es el ínfimo de A, subconjunto de $\mathbb{Z}^+$, si es el máximo del conjunto de las cotas inferiores. Entonces,

$$d \in \mathbb{Z}^+ \text{ es el ínfimo de } A \subseteq \mathbb{Z}^+ \iff d \text{ es el máximo de } C_i$$

luego,

$$d \in \mathbb{Z}^+ \text{ es el ínfimo de } A \subseteq \mathbb{Z}^+ \iff d \text{ es posterior a todos los elementos de } C_i$$

o lo que es igual,

$$d \in \mathbb{Z}^+ \text{ es el ínfimo de } A \subseteq \mathbb{Z}^+ \iff d \text{ es múltiplo todos los elementos de } C_i.$$

Consecuentemente,

$$d \in \mathbb{Z}^+ \text{ es el ínfimo de } A \subseteq \mathbb{Z}^+ \iff d = 36.$$

Así pues, y según la definición de máximo común divisor,

$$\text{m.c.d.}\,(72,108,144,216,324,288,432,648,972,864,1296,1944,2592,3888) = 36$$

■

3.5.2 Proposición

Dados los números enteros a_1, a_2, a_3, …, a_n, se verifica:

$$m.c.d.\,(a_1,a_2,a_3,\ldots,a_n) = m.c.d.\,(a_1, m.c.d.\,(a_2,a_3,\ldots,a_n))$$

Demostración

Sea $d = \text{m.c.d.}\,(a_1,a_2,a_3,\ldots,a_n)$ y $d' = \text{m.c.d.}\,(a_1, \text{m.c.d.}\,(a_2,a_3,\ldots,a_n))$. Entonces, por definición

$$d = \text{m.c.d.}\,(a_1,a_2,a_3,\ldots,a_n) \implies d = \text{Ínf}\,\{a_1,a_2,a_3,\ldots,a_n\}$$

por lo tanto d será anterior (divisor) a todos los números, es decir,

$$d\,|a_1 \text{ y } d\,|a_2 \text{ y } d\,|a_3 \text{ y } \cdots \text{ y } d\,|a_n\,.$$

Pero si d es anterior (divisor) a varios números, entonces, por definición de ínfimo, será anterior (divisor) al ínfimo de todos ellos, es decir,

$$d \,|a_1 \ \text{ y } d \,\big|\text{Ínf}\,\{a_2, a_3, \ldots, a_n\}\ .$$

Nuevamente, por la definición de máximo común divisor,

$$d \,|a_1 \ \text{ y } d \,|\text{m.c.d.}\,(a_2, a_3, \ldots, a_n)$$

y, otra vez, por definición de ínfimo,

$$d \,\big|\text{Ínf}\,\{a_1, \text{m.c.d.}\,(a_2, a_3, \ldots, a_n)\}$$

y, finalizando, con la de máximo común divisor,

$$d \,|\text{m.c.d.}\,(a_1, \text{m.c.d.}\,(a_2, a_3, \ldots, a_n))$$

es decir,

$$d \,|d'$$

Por otra parte, por definición,

$$d' = \text{m.c.d.}\,(a_1, \text{m.c.d.}\,(a_2, a_3, \ldots, a_n)) \Longrightarrow d' = \text{Ínf}\,\{a_1, \text{m.c.d.}\,(a_2, a_3, \ldots, a_n)\}$$

y por ser d' el ínfimo de dos números, deberá ser anterior (divisor) a ambos, o sea,

$$d' \,|a_1 \ \text{ y } d' \,|\text{m.c.d.}\,(a_2, a_3, \ldots, a_n)$$

luego, por definición,

$$d' \,|a_1 \ \text{ y } d' \,\big|\text{Ínf}\,\{a_2, a_3, \ldots, a_n\}$$

y al ser d' anterior (divisor) al ínfimo de $a_2, a_3, \ldots, a_n$, tendrá que ser anterior (divisor) a todos ellos, es decir,

$$d' \,|a_1 \ \text{ y } d' \,|a_2 \ \text{ y } d' \,|a_3 \ \text{ y } \cdots \text{ y } d' \,|a_n$$

por tanto, d' ha de ser anterior (divisor) al ínfimo de todos,

$$d' \,\big|\text{Ínf}\,\{a_1, a_2, a_3, \ldots, a_n\}$$

y, nuevamente, por la definición de máximo común divisor,

$$d' \,|\text{m.c.d.}\,(a_1, a_2, a_3, \ldots, a_n)$$

es decir,

$$d' \,|d$$

Pues bien, como $d \,|d' \ \text{ y } d' \,|d$, por la antisimetría de la relación de divisibilidad, $d = d'$, es decir,

$$\text{m.c.d.}\,(a_1, a_2, a_3, \ldots, a_n) = \text{m.c.d.}\,(a_1, \text{m.c.d.}\,(a_2, a_3, \ldots, a_n))$$

■

Ejemplo 3.23

Calcular,

$$\text{m.c.d.}\,(576, 864, 1296, 1944)$$

aplicando la proposición anterior.

Solución

Aplicando reiteradamente la proposición anterior,

$$\begin{aligned}
\text{m.c.d.}\,(576, 864, 1296, 1944) &= \text{m.c.d.}\,(576, \text{m.c.d.}\,(864, 1296, 1944)) \\
&= \text{m.c.d.}\,(576, \text{m.c.d.}\,(864, \text{m.c.d.}\,(1296, 1944))) \\
&= \text{m.c.d.}\,(576, \text{m.c.d.}\,(864, 648)) \\
&= \text{m.c.d.}\,(576, 216) \\
&= 72
\end{aligned}$$

■

3.5.3 Máximo común divisor de dos números

Sean a y b dos números enteros. El entero $d > 0$ es el máximo común divisor de a y b si es divisor de ambos y cualquier otro divisor de a y b es, también, divisor de d.

$$d = m.c.d.(a, b) \iff \begin{cases} 1. \quad d|a \quad y \quad d|b \\ \quad y \\ 2. \quad c|a \quad y \quad c|b \implies c|d \end{cases}$$

Nota 3.4 Obsérvese que si llamamos D_a y D_b a los conjuntos formados por los divisores de a y b, respectivamente, las condiciones 1. y 2. pueden escribirse, también, de la forma siguiente:

$$\begin{aligned}
d = \text{m.c.d.}\,(a, b) &\iff \begin{cases} 1. \quad d \in D_a \quad \text{y} \quad d \in D_b \\ \quad \text{y} \\ 2. \quad c \in D_a \quad \text{y} \quad c \in D_b \implies c|d \end{cases} \\
&\iff \begin{cases} 1. \quad d \in (D_a \cap D_b) \\ \quad \text{y} \\ 2. \quad c \in (D_a \cap D_b) \implies c|d \end{cases} \\
&\iff d = \text{Máx}\,(D_a \cap D_b)
\end{aligned}$$

es decir, d es el máximo del conjunto de los divisores comunes a a y a b.

■

3.5.4 Propiedades

Sean a y b enteros distintos de cero. Se verifica:

(i) $m.c.d.\,(a, 0) = |a|$

(ii) $m.c.d.\,(a, b) = m.c.d.\,(|a|, |b|)$

Demostración

(i) En efecto, sea a cualquier entero distinto de cero. Según hemos visto en la nota 3.4,

$$\text{m.c.d.}\,(a,0) = \text{Máx}\,(D_a \cap D_0)$$

Pues bien, como todos los enteros son múltiplos de 0 ((ii) de 3.1.2), podemos considerar que todos los enteros dividen a 0. Entonces,

$$D_a \cap D_0 = D_a \cap \mathbb{Z} = D_a$$

y al ser el máximo común divisor mayor que cero, tendremos

$$\text{m.c.d.}(a,0) \quad = \quad \text{Máx}\,(D_a) \quad = \quad \left\{ \begin{array}{ll} a & \text{si, } a>0 \\ \text{y} & \\ -a & \text{si, } a<0 \end{array} \right\} \quad = \quad |a|$$

(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 presentarse. 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 $b>0$.

$$\begin{array}{lll} d_1 = \text{m.c.d.}(a,b) & \Longrightarrow & d_1\,|a \ \text{ y } d_1\,|b \\ & \Longrightarrow & d_1\,||a| \ \text{ y } d_1\,||b| \qquad \{|a|=a,\ |b|=b\} \\ & \Longrightarrow & d_1\,|\text{m.c.d.}\,(|a|\,,|b|) \\ & \Longrightarrow & d_1\,|d_2 \end{array}$$

Por otra parte,

$$\begin{array}{lll} d_2 = \text{m.c.d.}\,(|a|\,,|b|) & \Longrightarrow & d_2\,||a| \ \text{ y } d_2\,||b| \\ & \Longrightarrow & d_2\,|a \ \text{ y } d_2\,|b \qquad \{|a|=a,\ |b|=b\} \\ & \Longrightarrow & d_2\,|\text{m.c.d.}(a,b) \\ & \Longrightarrow & d_2\,|d_1 \end{array}$$

Por la propiedad (iii) de 3.1.2) y teniendo en cuenta que $d_1>0$ y $d_2>0$,

$$\left. \begin{array}{l} d_1\,|d_2 \\ \text{y} \\ d_2\,|d_1 \end{array} \right\} \Longrightarrow d_1 = d_2$$

$\boxed{2}$ $a>0$ y $b<0$.

$$\begin{array}{lll} d_1 = \text{m.c.d.}(a,b) & \Longrightarrow & d_1\,|a \ \text{ y } d_1\,|b \\ & \Longrightarrow & d_1\,|a \ \text{ y } d_1\,|-b \qquad \{(v) \text{ de } 3.1.2\} \\ & \Longrightarrow & d_1\,||a| \ \text{ y } d_1\,||b| \qquad \{|a|=a,\ |b|=-b\} \\ & \Longrightarrow & d_1\,|\text{m.c.d.}\,(|a|\,,|b|) \\ & \Longrightarrow & d_1\,|d_2 \end{array}$$

Por otra parte,

$$\begin{aligned} d_2 = \text{m.c.d.}\left(|a|,|b|\right) &\Longrightarrow d_2 \,||a| \text{ y } d_2 \,||b| \\ &\Longrightarrow d_2 \,|a \text{ y } d_2 \,|-b \quad \{|a| = a,\ |b| = -b\} \\ &\Longrightarrow d_2 \,|a \text{ y } d_2 \,|b \quad \{(v) \text{ de } 3.1.2\} \\ &\Longrightarrow d_2 \,|\text{m.c.d.}(a,b) \\ &\Longrightarrow d_2 \,|d_1 \end{aligned}$$

Por la propiedad (iii) de 3.1.2) y teniendo en cuenta que $d_1 > 0$ y $d_2 > 0$,

$$\left.\begin{array}{l} d_1 \,|d_2 \\ \text{y} \\ d_2 \,|d_1 \end{array}\right\} \Longrightarrow d_1 = d_2$$

3 $a < 0$ y $b > 0$. Se demuestra de forma análoga a los anteriores.

4 $a < 0$ y $b < 0$. Se demuestra de forma análoga a los 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,

$$\text{m.c.d.}(-a,b) = \text{m.c.d.}(a,-b) = \text{m.c.d.}(-a,-b) = \text{m.c.d.}(a,b)$$

■

3.5.5 Existencia y Unicidad del Máximo Común Divisor

Dados dos números enteros a y b distintos de cero, existe un único entero d que es el máximo común divisor de ambos

Demostración

Supondremos que a y b son enteros positivos, ya que según hemos visto en la nota de las propiedades del máximo común divisor, si uno de los dos, o ambos, fuera negativo, el máximo común divisor sería el mismo.

Existencia. Sea C el conjunto de todas las combinaciones lineales positivas con coeficientes enteros que puedan formarse con a y b, es decir,

$$C = \left\{ma + nb \in \mathbb{Z}^+ : m,n \in \mathbb{Z}\right\}$$

⊛ C no es vacío. En efecto,

$$|a| = \begin{cases} a = 1 \cdot a + 0 \cdot b, \text{ si } a \geqslant 0 \\ -a = -1 \cdot a + 0 \cdot b, \text{ si } a < 0 \end{cases}$$

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, $d|a$.
   Con un razonamiento idéntico se prueba que $d|b$.
2. d es el máximo de los divisores comunes a a y b.
   En efecto, si el entero c es otro divisor de a y b, entonces por (v) de las propiedades de la divisibilidad (3.1.2), dividirá a cualquier combinación lineal con coeficientes enteros de a y b, luego, $c\,|sa + tb$ es decir, $c|d$.

De 1. y 2. se sigue que $d = \text{m.c.d.}(a, b)$.

Unicidad. En efecto, supongamos que el máximo común divisor de a y b no fuese único.

En tal caso habría, al menos, otro entero d' que también sería máximo común divisor de a y b. Entonces,

$$d \text{ es el máximo de los divisores comunes a } a \text{ y } b.$$

y

$$d' \text{ es un divisor común de } a \text{ y } b$$

por lo tanto,

$$d'\,|d$$

Por otra parte,

$$d' \text{ es el máximo de los divisores comunes a } a \text{ y } b.$$

y

$$d \text{ es un divisor común de } a \text{ y } b$$

por lo tanto,

$$d\,|d'$$

Así pues, tenemos que

$$d'\,|d \quad \text{y} \quad d\,|d'$$

aplicamos (iii) de las propiedades de la divisibilidad (3.1.2) y,

$$d = d'$$

ya que, por definición, tanto d como d' son mayores que cero.

■

3.5.6 Corolario

Si d es el máximo común divisor de a y b, entonces d es el menor entero positivo que puede escribirse como combinación lineal de a y b con coeficientes enteros.

$$d = m.c.d.(a,b) \Longrightarrow \exists p, q \in \mathbb{Z} : d = pa + qb$$

Demostración

Se sigue directamente del teorema anterior.

■

Nota 3.5 ¿Será cierto el recíproco?. Es decir, si $d > 0$ puede escribirse como combinación lineal con coeficientes enteros de dos números dados a y b, ¿será $d = \text{m.c.d.}(a,b)$?

Veamos que, en general, no tiene porque serlo. En efecto,

$$6 = 2 \cdot 27 + (-3) \cdot 16$$

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.

■

3.5.7 Proposición

Si d es el menor entero positivo que puede escribirse como combinación lineal con coeficientes enteros de dos enteros dados a y b y es divisor común de ambos, entonces d es el máximo común divisor de a y de b.

Demostración

En efecto, supongamos que

$$d = pa + qb, \text{ con } p, q \in \mathbb{Z}$$

y

$$d|a \text{ y } d|b$$

Entonces,

1 d es divisor de a y de b. Directamente de la hipótesis.

2 d es el máximo. En efecto, sea c otro de los divisores comunes de a y b. Entonces,

$$\left.\begin{array}{l} c|a \\ \text{y} \\ c|b \end{array}\right\} \Longrightarrow c|pa+qb, \text{ con } p \text{ y } q \text{ enteros} \Longrightarrow c|d.$$

Por lo tanto, $d = \text{m.c.d.}(a,b)$.

■

Veamos ahora como un corolario a la proposición anterior que en el caso de que el máximo común divisor de a y b sea 1, se verifica el recíproco sin necesidad de añadirle ninguna hipótesis al número d.

3.5.8 Corolario

Si a y b son dos enteros distintos de cero, entonces m.c.d. $(a,b)=1$ si, y sólo si existen dos números enteros p y q tales que $pa+qb=1$.

Demostración

"Sólo si." Si m.c.d. $(a,b)=1$, entonces por el corolario 3.5.6, pueden encontrarse dos números enteros p y q tales que $pa+qb=1$.

"Si." Sean p y q dos números enteros tales que $pa+qb=1$. Como 1 es divisor de cualquier número entero, $1|a$ y $1|b$. Aplicamos la proposición anterior y m.c.d. $(a,b)=1$.

■

Ejemplo 3.24

Demuéstrese que si m.c.d. $(a,b)=1$ y m.c.d. $(a,c)=1$, entonces m.c.d. $(a,bc)=1$.

Solución

Aplicando el corolario anterior, tendremos

$$\text{m.c.d. } (a,b)=1 \iff \exists p_1,q_1\in\mathbb{Z} : p_1a+q_1b=1$$
$$\text{m.c.d. } (a,c)=1 \iff \exists p_2,q_2\in\mathbb{Z} : p_2a+q_2c=1$$

y multiplicando término a término, se sigue que

$$(p_1a+q_1b)(p_2a+q_2c)=1 \iff (p_1p_2a+p_1q_2c+p_2q_1b)a+(q_1q_2)bc=1$$

con $p_1p_2a+p_1q_2c+p_2q_1b$ y q_1q_2 enteros. Aplicamos de nuevo el corolario anterior, y

$$\text{m.c.d. } (a,bc)=1$$

■

3.5.9 Más Propiedades

Sean a y b dos números enteros. Se verifica:

(i) Si m.c.d. $(a,b)=d$, entonces m.c.d. $\left(\frac{a}{d},\frac{b}{d}\right)=1$.

(ii) m.c.d. $(ka,kb)=k\cdot$ m.c.d. (a,b), $\forall k\in\mathbb{Z}^+$.

Demostración

(i) Si m.c.d. $(a,b)=d$, entonces m.c.d. $\left(\frac{a}{d},\frac{b}{d}\right)=1$

En efecto,

$$\begin{aligned} d=\text{m.c.d.}(a,b) &\implies \exists p,q\in\mathbb{Z}: pa+qb=d && \{\text{Corolario 3.5.6}\}\\ &\iff \exists p,q\in\mathbb{Z}: p\frac{a}{d}+q\frac{b}{d}=1 &&\\ &\iff \text{m.c.d.}\left(\frac{a}{d},\frac{b}{d}\right)=1 && \{\text{Corolario 3.5.8}\}\end{aligned}$$

(ii) m.c.d. $(ka,kb)=k\text{m.c.d.}\,(a,b)\,,\ \forall k\in\mathbb{Z}^+$

En efecto, supongamos que m.c.d. $(a,b)=d$. Entonces,

$$d=\text{m.c.d.}(a,b) \implies \exists p,q\in\mathbb{Z}: pa+qb=d \quad \{\text{Corolario 3.5.6}\}$$

Veamos que kd es el máximo común divisor de ka y kb.

1. kd es divisor de ka y kb.
   En efecto,
   $$d=\text{m.c.d.}\,(a,b)\Longrightarrow\begin{cases} d\,|a \implies kd\,|ka\\ \text{y}\\ d\,|b\implies kd\,|kb\end{cases}$$
2. Sea c cualquier otro divisor común de ka y kb. Entonces,
   $$\left.\begin{array}{c} c\,|ka\\ \text{y}\\ c\,|kb\end{array}\right\}\Longrightarrow c\,|pka+qkb \ \text{ con } p,q\in\mathbb{Z}\Longrightarrow c\,|k(pa+qb) \ \text{ con } p,q\in\mathbb{Z}\Longrightarrow c\,|kd$$

Luego,

$$\text{m.c.d.}\,(ka,kb)=kd=k\text{m.c.d.}\,(a,b)$$

■

Ejemplo 3.25

Demostrar que si m.c.d. $(a,b)=1$, entonces m.c.d. $(a+b,a-b)=1$ ó 2.

Solución

Sea $d=\text{m.c.d.}\,(a+b,a-b)$. Entonces,

$$\left.\begin{array}{l} d\,|a+b\\ \text{y}\\ d\,|a-b\end{array}\right\}\Longrightarrow d\,|(a+b)+(a-b)\Longrightarrow d\,|2a$$

también

$$\left.\begin{array}{l} d\,|a+b\\ \text{y}\\ d\,|a-b\end{array}\right\}\Longrightarrow d\,|(a+b)-(a-b)\Longrightarrow d\,|2b$$

y si $d\,|2a$ y $d\,|2b$, entonces d divide al máximo común divisor de $2a$ y $2b$, es decir,

$$d\,|\text{m.c.d.}\,(2a, 2b) \implies d\,|2 \cdot \text{m.c.d.}\,(a, b) \implies d\,|2$$

pero los únicos divisores positivos de 2 son 1 y 2, luego

$$d = 1 \text{ ó } d = 2$$

o sea,

$$\text{m.c.d.}\,(a + b, a - b) = 1 \text{ ó } 2$$

■

Ejemplo 3.26

Demuéstrese que $d = \text{m.c.d.}\,(a, b)$ si, y sólo si $d\,|a\,, d\,|b$ y $\text{m.c.d.}\left(\frac{a}{d}, \frac{b}{d}\right) = 1$.

Solución

"Sólo si". Esta demostración la hicimos en (i) de 3.5.9. Ahora la haremos utilizando (ii) de dicha proposición.

Si $d = \text{m.c.d.}\,(a, b)$, es obvio que $d\,|a$ y $d\,|b$, entonces $\frac{a}{d}$ y $\frac{b}{d}$ son números enteros. Escribimos,

$$a = d \cdot \frac{a}{d} \text{ y } b = d \cdot \frac{b}{d}$$

luego,

$$\begin{aligned} \text{m.c.d.}\,(a, b) = d &\implies \text{m.c.d.}\left(d \cdot \frac{a}{d}, d \cdot \frac{b}{d}\right) = d \\ &\implies d \cdot \text{m.c.d.}\left(\frac{a}{d}, \frac{b}{d}\right) = d \\ &\implies \text{m.c.d.}\left(\frac{a}{d}, \frac{b}{d}\right) = 1 \end{aligned}$$

Veamos ahora que la hipótesis de que $d\,|a$ y $d\,|b$, permite probar el recíproco también.

"Si". En efecto, como $d\,|a$ y $d\,|b$, al igual que antes, se sigue que $\frac{a}{d}$ y $\frac{b}{d}$ son números enteros, por tanto,

$$\begin{aligned} \text{m.c.d.}\,(a, b) &= \text{m.c.d.}\left(d \cdot \frac{a}{d}, d \cdot \frac{b}{d}\right) \\ &= d \cdot \text{m.c.d.}\left(\frac{a}{d}, \frac{b}{d}\right) \\ &= d \cdot 1 \\ &= d \end{aligned}$$

■

Ejemplo 3.27

Probar que si $d|a$ y $d|b$, entonces m.c.d. $\left(\frac{a}{d}, \frac{b}{d}\right) = \frac{1}{d} \cdot$ m.c.d.(a, b).

Solución

Por hipótesis $d|a$ y $d|b$ luego $\frac{a}{d}$ y $\frac{b}{d}$ son números enteros y existe m.c.d. $\left(\frac{a}{d}, \frac{b}{d}\right)$. Pues bien, aplicando (ii) de 3.5.9,

$$d \cdot \text{m.c.d.}\left(\frac{a}{d}, \frac{b}{d}\right) = \text{m.c.d.}\left(d \cdot \frac{a}{d}, d \cdot \frac{b}{d}\right) \implies d \cdot \text{m.c.d.}\left(\frac{a}{d}, \frac{b}{d}\right) = \text{m.c.d.}\,(a, b)$$

Por lo tanto,

$$\text{m.c.d.}\left(\frac{a}{d}, \frac{b}{d}\right) = \frac{1}{d} \cdot \text{m.c.d.}\,(a, b)$$

Ejemplo 3.28

Se han plantado árboles igualmente espaciados en el contorno de un campo triangular cuyos lados miden 144m., 180m. y 240m. respectivamente. Sabiendo que hay un árbol en cada vértice y que la distancia entre dos árboles consecutivos está comprendida entre 5 y 10 metros. Calcular el número de árboles plantados.

Solución

Sea d la distancia entre dos árboles consecutivos. Entonces d de ser un divisor de 144, 180 y 240 luego ha de ser divisor de su máximo común divisor.

Pues bien, calculemos el máximo común divisor de 144, 180 y 240. Los conjuntos de divisores positivos de los tres números son:

$$D_{144} = \{1, 2, 4, 8, 16, 3, 6, 12, 24, 48, 9, 18, 36, 72, 144\}$$

y

$$D_{180} = \{1, 2, 4, 3, 6, 12, 9, 18, 36, 5, 10, 20, 15, 30, 60, 45, 90, 180\}$$

y

$$D_{240} = \{1, 2, 4, 8, 16, 3, 6, 12, 24, 48, 5, 10, 20, 40, 80, 15, 30, 60, 120, 240\}$$

Por lo tanto, el conjunto de los divisores comunes a los tres números será

$$D_{144} \cap D_{180} \cap D_{240} = \{1, 2, 4, 3, 6, 12\}$$

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

$$N = \frac{144}{6} + \frac{180}{6} + \frac{240}{6} = 94$$

■

3.6 Algoritmo de Euclides

Desarrollaremos un método para calcular el máximo común divisor de dos números conocido como el *Algoritmo de Euclides*[1]. Este método es más sencillo que el de calcular todos los divisores de ambos números cuando se trata de calcular el máximo común divisor de dos números y éstos son muy grandes.

Veamos un teorema previo que sustenta teóricamente el algoritmo.

3.6.1 Teorema

El máximo común divisor del dividendo y del divisor de una división es el mismo que el máximo común divisor del divisor y el resto.

Demostración

Sean a y b dos números enteros cualesquiera con $b \neq 0$. Por el teorema de existencia y unicidad de cociente y resto, existirán dos números enteros, únicos, q y r tales que

$$a = bq + r : 0 \leqslant r < b$$

Probaremos que el máximo común divisor de a y b es el mismo que el de b y r.

En efecto, sea $d = \text{m.c.d.}\,(a, b)$. Entonces, d es un divisor común a a y a b, luego por (v) de 3.1.2,

$$d \,|a + (-q)b$$

es decir,

$$d \,|r\ .$$

Por lo tanto,

$$d \,|b \ \text{ y } d \,|r\ . \tag{3.5}$$

Veamos ahora que es el máximo de los divisores comunes de b y r. En efecto, si c es otro divisor común a b y r, nuevamente por (v) de 3.1.2,

$$c \,|bq + r$$

es decir,

$$c \,|a$$

luego,

$$c \,|a \ \text{ y } c \,|b$$

[1] Matemático griego del siglo III antes de Cristo. Se sabe que enseñaba matemáticas en Alejandría, donde fundó la escuela más célebre de la antigüedad. Es sobre todo conocido por sus *Elementos*, que continúan siendo considerados como el libro de geometría por excelencia. En el principio de esta obra, importante por su gran claridad y rigor, hay la definición de las "nociones comunes", a las que Euclides recurre casi constantemente en las páginas que siguen, y entre las cuales figura su famoso postulado. A continuación va desarrollando, en un orden lógico, los diversos teoremas. El conjunto consta de trece libros, a los que suele unirse otros dos atribuidos a Hipsicles, matemático de Alejandría que vivió probablemente en el siglo II antes de Cristo. Los cuatro primeros libros tratan de la geometría del plano y estudian las razones y las proporciones. La teoría de los números enteros es el objeto de los libros VII, VIII y IX. El libro X, más largo, y considerado también como el más perfecto de todos, está consagrado al estudio de los irracionales algebraicos más simples. La última parte trata de la geometría del espacio. Los *Cálculos*, especie de complemento de los *Elementos*, tienen una forma más analítica. Una obra perdida, la de los *Lugares de la superficie*, debía tener por objeto el estudio de las secciones planas de las superficies de revolución de segundo grado. Los textos de Proclo y de Papo nos han transmitido los *Porismas* sobre los cuales se ha discutido mucho, pero que, según Chasles, contienen en germen las tres teorías modernas de la razón anarmónica, de las divisiones homográficas y de la involución. En fin, en su *Optica*, Euclides procede como en geometría, poniendo en cabeza algunas proposiciones fundamentales, la más importante de las cuales admite la propagación de los rayos luminosos en línea recta.

y, consecuentemente, ha de dividir al máximo común divisor de a y b, es decir,

$$c \,|d\ . \tag{3.6}$$

De (3.5) y (3.6) se sigue que

$$\text{m.c.d.}\,(b,r) = d$$

y, por lo tanto,

$$\text{m.c.d.}\,(a,b) = \text{m.c.d.}\,(b,r)$$

■

3.6.2 Algoritmo de Euclides

El teorema anterior es el fundamento del algoritmo de Euclides, proceso de divisiones sucesivas que permite calcular el máximo común divisor de dos números.

Demostración

Sean a y b dos números enteros que supondremos mayores que cero y tales que $a \neq b$.

Obsérvese que al ser

$$\text{m.c.d.}\,(a,b) = \text{m.c.d.}\,(|a|\,,|b|)$$

el suponer que $a > 0$ y $b > 0$ no significa pérdida de generalidad alguna y lo mismo ocurre con suponer que $a \neq b$ ya que $\text{m.c.d.}(a,a) = a$. Como $a \neq b$, será $a > b$ ó $a < b$. Supondremos que $a > b$.

Por el teorema 3.2.1, 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 3.2.1, obtenemos q_2 y r_2 tales que
$$b = r_1q_2 + r_2 : 0 \leqslant r_2 < r_1$$
y por el teorema previo,
$$\text{m.c.d.}(b,r_1) = \text{m.c.d.}(r_1,r_2)$$
y, nuevamente, pueden ocurrir dos cosas:
  - Si $r_2 = 0$, entonces
$$\text{m.c.d.}(b,r_1) = \text{m.c.d.}(r_1,r_2) = \text{m.c.d.}(r_1,0) = r_1$$
y, consecuentemente,
$$\text{m.c.d.}(a,b) = \text{m.c.d.}(b,r_1) = \text{m.c.d.}(r_1,r_2) = r_1$$
terminando el proceso.

– Si $r_2 \neq 0$, entonces el teorema 3.2.1 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 3.29

Hallar el máximo común divisor de 1369 y 2597 y expresarlo como una combinación lineal con coeficientes enteros de ellos.

Solución

Lo haremos de forma práctica, disponiendo los cálculos en una tabla

	1	1	8	1	2	2	3	1	1	2
2597	1369	1228	141	100	41	18	5	3	2	1
1228	141	100	41	18	5	3	2	1	0	

luego,

$$\text{m.c.d.}(2597, 1369) = 1$$

Según vimos en 3.5.6,

Si $d = \text{m.c.d.}(a, b)$, entonces podemos encontrar dos enteros p y q tales que $d = pa + qb$.

Es decir, podemos escribir d como combinación lineal, con coeficientes enteros, de a y b y nuestro problema es encontrar dichos coeficientes, para lo cual utilizaremos de nuevo el Algoritmo de Euclides aunque haciendo

las "cuentas" hacia atrás.

$$\left.\begin{array}{r} 1 = 3 - 1 \cdot 2 \\ 2 = 5 - 1 \cdot 3 \end{array}\right\} \implies \begin{array}{rcl} 1 & = & 3 - 1(5 - 3 \cdot 1) \\ & = & (-1) \cdot 5 + 2 \cdot 3 \end{array}$$

$$\left.\begin{array}{r} 1 = (-1) \cdot 5 + 2 \cdot 3 \\ 3 = 18 - 3 \cdot 5 \end{array}\right\} \implies \begin{array}{rcl} 1 & = & (-1)5 + 2(18 - 3 \cdot 5) \\ & = & 2 \cdot 18 + (-7) \cdot 5 \end{array}$$

$$\left.\begin{array}{r} 1 = 2 \cdot 18 + (-7) \cdot 5 \\ 5 = 41 - 2 \cdot 18 \end{array}\right\} \implies \begin{array}{rcl} 1 & = & 2 \cdot 18 + (-7)(41 - 2 \cdot 18) \\ & = & (-7) \cdot 41 + 16 \cdot 18 \end{array}$$

$$\left.\begin{array}{r} 1 = (-7) \cdot 41 + 16 \cdot 18 \\ 18 = 100 - 2 \cdot 41 \end{array}\right\} \implies \begin{array}{rcl} 1 & = & (-7) \cdot 41 + 16(100 - 2 \cdot 41) \\ & = & 16 \cdot 100 + (-39) \cdot 41 \end{array}$$

$$\left.\begin{array}{r} 1 = 16 \cdot 100 + (-39) \cdot 41 \\ 41 = 141 - 1 \cdot 100 \end{array}\right\} \implies \begin{array}{rcl} 1 & = & 16 \cdot 100 + (-39)(141 - 1 \cdot 100) \\ & = & (-39) \cdot 141 + 55 \cdot 100 \end{array}$$

$$\left.\begin{array}{r} 1 = (-39) \cdot 141 + 55 \cdot 100 \\ 100 = 1228 - 8 \cdot 141 \end{array}\right\} \implies \begin{array}{rcl} 1 & = & (-39) \cdot 141 + 55(1228 - 8 \cdot 141) \\ & = & 55 \cdot 1228 + (-479) \cdot 141 \end{array}$$

$$\left.\begin{array}{r} 1 = 55 \cdot 1228 + (-479) \cdot 141 \\ 141 = 1369 - 1 \cdot 1228 \end{array}\right\} \implies \begin{array}{rcl} 1 & = & 55 \cdot 1228 + (-479)(1369 - 1 \cdot 1228) \\ & = & (-479) \cdot 1369 + 534 \cdot 1228 \end{array}$$

$$\left.\begin{array}{r} 1 = (-479) \cdot 1369 + 534 \cdot 1228 \\ 1228 = 2597 - 1 \cdot 1369 \end{array}\right\} \implies \begin{array}{rcl} 1 & = & (-479) \cdot 1369 + 534(2597 - 1 \cdot 1369) \\ & = & 534 \cdot 2597 + (-1013) \cdot 1369 \end{array}$$

De aquí que los coeficientes que buscábamos sean $p = 534$ y $q = -1013$ y la expresión del máximo común divisor como combinación lineal de 2597 y 1369 con esos coeficientes sea:

$$1 = 534 \cdot 2597 + (-1013) \cdot 1369$$

Obsérvese que esta expresión no es única. En efecto, para cualquier $k \in \mathbb{Z}$, tendremos

$$\begin{array}{rcl} 1 & = & 534 \cdot 2597 + (-1013) \cdot 1369 \\ & = & 534 \cdot 2597 + (-1013) \cdot 1369 + (-1369k) \cdot 2597 + (2597k) \cdot 1369 \\ & = & (534 - 1369k)2597 + (-1013 + 2597k)1369 \end{array}$$

Obsérvese también que

$$\text{m.c.d.}\,(-1369, 2597) = 1$$
$$\text{m.c.d.}\,(1369, -2597) = 1$$
$$\text{m.c.d.}\,(-1369, -2597) = 1$$

y en tales casos las combinaciones lineales con coeficientes enteros serían:

$$\begin{array}{rcl} 1 & = & 1013 \cdot (-1369) + 534 \cdot 2597 \\ 1 & = & (-1013) \cdot 1369 + (-534)(-2597) \\ 1 & = & 1013 \cdot (-1369) + (-534)(-2597) \end{array}$$

■

Ejemplo 3.30

Calcular el máximo común divisor de 231 y 1820. Expresar dicho número como una combinación lineal con coeficientes enteros de ellos dos.

Solución

	7	1	7	4
1820	231	203	28	7
203	28	7	0	

Ahora calcularemos los coeficientes de la combinación lineal siguiendo, al igual que hicimos en el ejemplo anterior, el proceso inverso.

$$\left.\begin{array}{rcrcr} 7 & = & 203 & - & 7\cdot 28 \\ 28 & = & 231 & - & 1\cdot 203 \end{array}\right\} \implies 7 = 203 - 7(231 - 1\cdot 203)$$

$$\implies 7 = (-7)\cdot 231 + 8\cdot 203$$

$$\left.\begin{array}{rcrcr} 7 & = & (-7)\cdot 231 & + & 8\cdot 203 \\ 203 & = & 1820 & - & 7\cdot 231 \end{array}\right\} \implies 7 = (-7)\cdot 231 + 8(1820 - 7\cdot 231)$$

$$\implies 7 = 8\cdot 1820 + (-63)\cdot 231$$

es decir, la combinación lineal pedida es

$$7 = 8\cdot 1820 + (-63)\cdot 231$$

■

Ejemplo 3.31

¿Cuál es el mayor número que al emplearlo como divisor de 68130 y 107275 origina los restos 27 y 49, respectivamente?

Solución

Sea a el número que buscamos. Entonces, por 3.2.1, existirán q_1 y q_2, enteros, tales que

$$\left.\begin{array}{rcrcr} 68130 & = & aq_1 & + & 27 \\ \text{y} & & & & \\ 107275 & = & aq_2 & + & 49 \end{array}\right\} \implies \left.\begin{array}{rcl} 68103 & = & aq_1, \text{ con } q_1 \in \mathbb{Z} \\ \text{y} & & \\ 107226 & = & aq_2, \text{ con } q_2 \in \mathbb{Z} \end{array}\right\}$$

$$\implies a \,|68103 \text{ y } a\,|107226$$

luego a es un divisor común a 68103 y 107226 y como tiene que ser el mayor, será

$$a = \text{m.c.d.}\,(68103, 107226)$$

y utilizando el Algoritmo de Euclides para el cálculo del máximo común divisor,

	1	1	1	1	0	1	1	6
107226	68103	39123	28980	10143	18837	10143	8694	1449
39123	28980	10143	18837	10143	8694	1449	0	

luego, $a = 1449$

■

Ejemplo 3.32

Halla dos números cuyo máximo común divisor es 7 y tales que los cocientes obtenidos en su determinación por el algoritmo de Euclides son, en orden inverso, 7, 2, 3 y 36.

Solución

Presentando los cálculos en la forma práctica que vimos antes, si los números buscados son a y b, tendremos

	36	3	2	7
a	b	r_1	r_2	r_3
r_1	r_2	r_3	0	

por tanto,

$$\text{m.c.d.}\,(a,b) = \text{m.c.d.}\,(r_3,0) = r_3$$

y como según el enunciado 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 $b = 364$.

■

3.7 Mínimo Común Múltiplo

Estudiaremos en esta sección los múltiplos comunes a un par de números enteros.

3.7.1 Definición

Dados los números enteros positivos $a_1, a_2, a_3, \ldots, a_n$, llamaremos mínimo común múltiplo de todos ellos al supremo del conjunto $\{a_1, a_2, a_3, \ldots, a_n\}$ ordenado con la relación de orden parcial de divisibilidad. Lo notaremos m.c.m.$(a_1, a_2, a_3, \ldots, a_n)$

Ejemplo 3.33

Calcular, aplicando directamente la definición anterior,

$$\text{m.c.m. } (72, 108, 144, 216, 324, 288, 432, 648, 972, 864, 1296, 1944, 2592, 3888)$$

Solución

Según la definición de mínimo común múltiplo de varios números, tendremos que calcular el Supremo del conjunto

$$A = \{72, 108, 144, 216, 324, 288, 432, 648, 972, 864, 1296, 1944, 2592, 3888\}$$

ordenado con la relación de orden de divisibilidad, es decir, si a y b son cualesquiera de A,

$$b \text{ es posterior a } a \text{ siempre y cuando } b \text{ sea múltiplo de } a$$

o sea,

$$a \preccurlyeq b \iff a|b \Longrightarrow b = a \cdot q, \text{ con } q \text{ entero.}$$

Recordemos que el supremo de A es el mínimo del conjunto de sus cotas superiores ordenado por la relación anterior. Vamos a calcular, pues, los elementos característicos de este conjunto.

Elementos Maximales. Por definición, un elemento m de A será maximal de A, respecto de la relación $\preccurlyeq$, si no hay en A elemento alguno que sea estrictamente posterior a él, es decir,

$$m \text{ es maximal de } A \iff \nexists x \in A : m \prec x$$

o lo que es igual,

$$m \text{ es maximal de } A \iff \nexists x \in A : m \preccurlyeq x \text{ y } m \neq x$$

y esto significa, teniendo en cuenta que la relación $\preccurlyeq$ es la de divisibilidad,

$$m \text{ es maximal de } A \iff \nexists x \in A : m \text{ sea múltiplo de } x \text{ y } m \neq x$$

es decir,

$$m \text{ es maximal de } A \iff m \text{ no tiene en } A \text{ múltiplos distintos del propio } m.$$

Consecuentemente,

$$m \text{ es maximal de } A \iff m = 2592 \text{ ó } m = 3888$$

Obsérvese que al haber dos maximales no puede haber máximo, ya que éste, caso de existir, ha de ser único y coincidir con el maximal.

Cotas Superiores. Un elemento $s \in \mathbb{Z}^+$ es cota superior de A, subconjunto de $\mathbb{Z}^+$, si es posterior a todos los elementos de A, o sea,

$$s \in \mathbb{Z}^+ \text{ es cota superior de } A \text{ en } \mathbb{Z}^+ \iff \forall x, (x \in A \Longrightarrow x \preccurlyeq s)$$

es decir,

$$s \in \mathbb{Z}^+ \text{ es cota superior de } A \text{ en } \mathbb{Z}^+ \iff \forall x, (x \in A \Longrightarrow s \text{ es múltiplo de } x)$$

Así pues,

$$s \in \mathbb{Z}^+ \text{ es cota superior de } A \text{ en } \mathbb{Z}^+ \iff s \text{ es múltiplo de todos los elementos de } A$$

y bastaría con que s fuese múltiplo de los maximales de A ya que por transitividad esto significaría que es múltiplo de todos los elementos de A. Por lo tanto,

$$s \in \mathbb{Z}^+ \text{ es cota superior de } A \text{ en } \mathbb{Z}^+ \iff s \text{ es múltiplo de los elementos maximales de } A.$$

Así pues,

$$s \in \mathbb{Z}^+ \text{ es cota superior de } A \subseteq \mathbb{Z}^+ \iff s \text{ es múltiplo de 2592 y 3888}$$

$$\iff \begin{cases} s \text{ es múltiplo de 2592} \\ \text{y} \\ s \text{ es múltiplo de 3888} \end{cases}$$

$$\iff \begin{cases} s \text{ es múltiplo de } 2^5 \cdot 3^3 \\ \text{y} \\ s \text{ es múltiplo de } 2^4 \cdot 3^5 \end{cases}$$

$$\iff s = 2^5 \cdot 3^5 \cdot k,\ k \in \mathbb{Z}^+$$

luego, si llamamos C_s al conjunto de las cotas inferiores, tendremos que

$$C_s = \left\{2^5 \cdot 3^5 \cdot k,\ k \in \mathbb{Z}^+\right\}$$

Supremo. Un elemento m de $\mathbb{Z}^+$ se dice que es el supremo de A, subconjunto de $\mathbb{Z}^+$, si es el mínimo del conjunto de las cotas superiores. Entonces,

$$m \in \mathbb{Z}^+ \text{ es el supremo de } A \subseteq \mathbb{Z}^+ \iff m \text{ es el mínimo de } C_s$$

luego,

$$m \in \mathbb{Z}^+ \text{ es el supremo de } A \subseteq \mathbb{Z}^+ \iff m \text{ es anterior a todos los elementos de } C_s$$

o lo que es igual,

$$m \in \mathbb{Z}^+ \text{ es el supremo de } A \subseteq \mathbb{Z}^+ \iff m \text{ es divisor de todos los elementos de } C_s.$$

Consecuentemente,

$$m \in \mathbb{Z}^+ \text{ es el supremo de } A \subseteq \mathbb{Z}^+ \iff m = 2^5 \cdot 3^5 = 7776.$$

Así pues, y según la definición de mínimo común múltiplo,

$$\text{m.c.m.}\,(72, 108, 144, 216, 324, 288, 432, 648, 972, 864, 1296, 1944, 2592, 3888) = 7776$$

■

3.7.2 Proposición

Dados los números enteros a_1, a_2, a_3, ..., a_n, se verifica:

$$\textit{m.c.m.}\,(a_1, a_2, a_3, \ldots, a_n) = \textit{m.c.m.}\,(a_1, \textit{m.c.m.}\,(a_2, a_3, \ldots, a_n))$$

Demostración

Sea $m = \text{m.c.m.}\,(a_1, a_2, a_3, \ldots, a_n)$ y $m' = \text{m.c.m.}\,(a_1, \text{m.c.m.}\,(a_2, a_3, \ldots, a_n))$. Entonces, por definición

$$m = \text{m.c.m.}\,(a_1, a_2, a_3, \ldots, a_n) \implies m = \text{Sup}\,\{a_1, a_2, a_3, \ldots, a_n\}$$

por lo tanto m será posterior (múltiplo) de todos los números, es decir,

$$a_1 \,|m \ \text{ y } a_2 \,|m \ \text{ y } a_3 \,|m \ \text{ y } \cdots \text{ y } a_n \,|m\ .$$

Pero si m es posterior (múltiplo) de varios números, entonces, por definición de supremo, será posterior (múltiplo) al supremo de todos ellos, es decir,

$$a_1 \,|m \;\text{ y } \operatorname{Sup}\{a_2, a_3, \ldots, a_n\}\,|m\ .$$

Nuevamente, por la definición de mínimo común múltiplo,

$$a_1 \,|m \;\text{ y m.c.m.}\,(a_2, a_3, \ldots, a_n)\,|m$$

y, otra vez, por definición de supremo,

$$\operatorname{Sup}\{a_1, \text{m.c.m.}\,(a_2, a_3, \ldots, a_n)\}\,|m$$

y, finalizando, con la de mínimo común múltiplo,

$$\text{m.c.m.}\,(a_1, \text{m.c.m.}\,(a_2, a_3, \ldots, a_n))\,|m$$

es decir,

$$m' \,|m$$

Por otra parte, por definición,

$$m' = \text{m.c.m.}\,(a_1, \text{m.c.m.}\,(a_2, a_3, \ldots, a_n)) \Longrightarrow m' = \operatorname{Sup}\{a_1, \text{m.c.m.}\,(a_2, a_3, \ldots, a_n)\}$$

y por ser m' el supremo de dos números, deberá ser posterior (múltiplo) de ambos, o sea,

$$a_1 \,|m' \;\text{ y m.c.m.}\,(a_2, a_3, \ldots, a_n)\,|m'$$

luego, por definición,

$$a_1 \,|m' \;\text{ y } \operatorname{Sup}\{a_2, a_3, \ldots, a_n\}\,|m'$$

y al ser m' posterior (múltiplo) del supremo de $a_2, a_3, \ldots, a_n$, tendrá que ser posterior (múltiplo) de todos ellos, es decir,

$$a_1 \,|m' \;\text{ y } a_2 \,|m' \;\text{ y } a_3 \,|m' \;\text{ y } \cdots \text{ y } a_n \,|m'$$

por tanto, m' ha de ser posterior (múltiplo) del supremo de todos,

$$\operatorname{Sup}\{a_1, a_2, a_3, \ldots, a_n\}\,|m'$$

y, nuevamente, por la definición de mínimo común múltiplo,

$$\text{m.c.m.}\,(a_1, a_2, a_3, \ldots, a_n)\,|m'$$

es decir,

$$m \,|m'$$

Pues bien, como $m \,|m' \;$ y $\; m' \,|m$, por la antisimetría de la relación de divisibilidad, $m = m'$, es decir,

$$\text{m.c.m.}\,(a_1, a_2, a_3, \ldots, a_n) = \text{m.c.m.}\,(a_1, \text{m.c.m.}\,(a_2, a_3, \ldots, a_n))$$

■

3.7.3 Mínimo común múltiplo de dos números

Sean a y b dos números enteros. El entero $m > 0$ es el mínimo común múltiplo de a y b si es múltiplo de ambos y cualquier otro múltiplo de a y b lo es, también, de m. Es decir,

$$m = m.c.m.(a,b) \iff \begin{cases} 1. \quad a|m \quad y \quad b|m \\ \quad y \\ 2. \quad a|c \quad y \quad b|c \quad \Longrightarrow \quad m|c \end{cases}$$

Nota 3.6 Obsérvese que si llamamos M_a y M_b a los conjuntos formados por los múltiplos de a y b, respectivamente, las condiciones 1. y 2. pueden escribirse, también, de la forma siguiente:

$$\begin{aligned} m = \text{m.c.m.}\,(a,b) &\iff \begin{cases} 1. \quad m \in M_a \quad \text{y} \quad m \in M_b \\ \text{y} \\ 2. \quad c \in M_a \quad \text{y} \quad c \in M_b \quad \Longrightarrow \quad m|c \end{cases} \\ &\iff \begin{cases} 1. \quad m \in (M_a \cap M_b) \\ \text{y} \\ 2. \quad c \in (M_a \cap M_b) \quad \Longrightarrow \quad m|c \end{cases} \\ &\iff m = \text{Mín}\,(M_a \cap M_b) \end{aligned}$$

es decir, m es el mínimo del conjunto de los múltiplos comunes a a y a b.

■

Ejemplo 3.34

Calcular el mínimo común múltiplo de 12 y 15.

Solución

Según la nota anterior,

$$m = \text{Mín}\,(M_{12} \cap M_{15})$$

donde M_{12} y M_{15} son los conjuntos integrados, respectivamente, por los múltiplos de 12 y de 15. Pues bien,

sea a cualquier entero. Entonces

$$
\begin{aligned}
a \in M_{12} \cap M_{15} &\iff \begin{cases} a \in M_{12} \\ \text{y} \\ a \in M_{15} \end{cases} \\
&\iff \begin{cases} \exists q_1 \in \mathbb{Z} : a = 12 \cdot q_1 \\ \text{y} \\ \exists q_2 \in \mathbb{Z}^+ : a = 15 \cdot q_2 \end{cases} \\
&\implies 12q_1 = 15q_2 \\
&\iff \frac{q_1}{q_2} = \frac{15}{12} \\
&\quad \left\{ \begin{array}{l} \text{m.c.d.}(q_1, q_2) = q \\ \text{y} \\ \text{m.c.d.}(15, 12) = 3 \end{array} \right\} \\
&\iff \frac{\frac{q_1}{q}}{\frac{q_2}{q}} = \frac{\frac{15}{3}}{\frac{12}{3}} \\
&\implies \frac{\frac{q_1}{q}}{\frac{q_2}{q}} = \frac{5}{4} \\
&\iff \begin{cases} \frac{q_1}{q} = 5 \\ \text{y} \qquad \{\text{Fracciones Irreducibles}\} \\ \frac{q_2}{q} = 4 \end{cases} \\
&\iff \begin{cases} q_1 = 5q, \ q \in \mathbb{Z}^+ \\ \text{y} \\ q_2 = 4q, \ q \in \mathbb{Z}^+ \end{cases} \\
&\implies \begin{cases} \exists q \in \mathbb{Z}^+ : a = 12 \cdot 5q \\ \text{y} \\ \exists q \in \mathbb{Z}^+ : a = 15 \cdot 4q \end{cases} \\
&\iff \exists q \in \mathbb{Z}^+ : a = 60q
\end{aligned}
$$

Como a era cualquiera, hemos probado que

$$M_{12} \cap M_{15} \subseteq \left\{ n : n = 60q, q \in \mathbb{Z}^+ \right\}$$

Veamos la inclusión contraria. En efecto,

$$\begin{aligned}
a \in \{n : n = 60q, q \in \mathbb{Z}^+\} &\iff \exists q \in \mathbb{Z}^+ : a = 60q \\
&\iff \exists q \in \mathbb{Z}^+ : \begin{cases} a = 12(5q) \\ \text{y} \\ a = 15(4q) \end{cases} \\
&\implies \begin{cases} a = 12q_1, \text{ con } q_1 = 5q \in \mathbb{Z}^+ \\ \text{y} \\ a = 15q_2, \text{ con } q_2 = 4q \in \mathbb{Z}^+ \end{cases} \\
&\iff \begin{cases} a \in M_{12} \\ \text{y} \\ a \in M_{15} \end{cases} \\
&\iff a \in M_{12} \cap M_{15}
\end{aligned}$$

Por lo tanto,

$$\left\{n : n = 60q, q \in \mathbb{Z}^+\right\} \subseteq M_{12} \cap M_{15}$$

y por la doble inclusión,

$$M_{12} \cap M_{15} = \left\{n : n = 60q, \ q \in \mathbb{Z}^+\right\}$$

y

$$m = \text{Mín}\left(M_{12} \cap M_{15}\right) = \text{Mín}\left\{n : n = 60q, \ q \in \mathbb{Z}^+\right\} = 60$$

■

3.7.4 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.$(a, b) = |ab|$.

Consideraremos, primero, el caso en que tanto a como b sean positivos. Según 3.6, m.c.m.$(a,b) =$ Mín $(M_a \cap M_b)$. Pues bien, sea c cualquier entero. Entonces,

$$
\begin{aligned}
c \in (M_a \cap M_b) &\iff \begin{cases} c \in M_a \\ \text{y} \\ c \in M_b \end{cases} \\
&\iff \begin{cases} \exists q_1 \in \mathbb{Z} : c = aq_1 \\ \text{y} \\ \exists q_2 \in \mathbb{Z} : c = bq_2 \end{cases} \\
&\implies aq_1 = bq_2 \\
&\iff \frac{q_1}{q_2} = \frac{b}{a} \\
&\qquad \left\{ \begin{array}{l} \exists q \in \mathbb{Z}^+ : \text{m.c.d.}(q_1, q_2) = q \\ \text{m.c.d.}(a,b) = 1 \end{array} \right\} \\
&\iff \frac{\frac{q_1}{q}}{\frac{q_2}{q}} = \frac{b}{a} \\
&\iff \begin{cases} \dfrac{q_1}{q} = b \\ \text{y} \qquad\qquad \{\text{Fracciones irreducibles}\} \\ \dfrac{q_2}{q} = a \end{cases} \\
&\iff \begin{cases} \exists q \in \mathbb{Z}^+ : q_1 = bq \\ \text{y} \\ \exists q \in \mathbb{Z}^+ : q_2 = aq \end{cases} \\
&\implies \begin{cases} \exists q \in \mathbb{Z}^+ : c = abq \\ \text{y} \\ \exists q \in \mathbb{Z}^+ : c = baq \end{cases} \\
&\iff c \in \{n : n = abq, q \in \mathbb{Z}^+\}
\end{aligned}
$$

De la arbitrariedad de c se sigue que

$$M_a \cap M_b \subseteq \left\{n : n = abq, q \in \mathbb{Z}^+\right\}$$

Recíprocamente,

$$\begin{aligned} c \in \{n : n = abq, q \in \mathbb{Z}^+\} &\iff \exists q \in \mathbb{Z}^+ : c = abq \\ &\iff \exists q \in \mathbb{Z}^+ : \begin{cases} c = a(bq) \\ \text{y} \\ c = b(aq) \end{cases} \\ &\implies \begin{cases} c = aq_1, \text{ con } q_1 = bq \in \mathbb{Z} \\ \text{y} \\ c = bq_2, \text{ con } q_2 = aq \in \mathbb{Z} \end{cases} \\ &\iff \begin{cases} c \in M_a \\ \text{y} \\ c \in M_b \end{cases} \\ &\iff c \in (M_a \cap M_b) \end{aligned}$$

luego,

$$\left\{n : n = abq, q \in \mathbb{Z}^+\right\} \subseteq (M_a \cap M_b)$$

y de la doble inclusión se sigue que

$$M_a \cap M_b = \left\{n : n = abq, q \in \mathbb{Z}^+\right\}$$

y, por tanto,

$$\text{m.c.m.}(a, b) = \text{Mín}\,(M_a \cap M_b) = \text{Mín}\left\{n : n = abq, q \in \mathbb{Z}^+\right\} = ab$$

Como a y b eran enteros positivos, $a = |a|$ y $b = |b|$, luego,

$$\text{m.c.m.}(a, b) = |ab|$$

Veamos que ocurre en los restantes casos.

- $a > 0$ y $b < 0$.
  En este caso, $-b > 0$ y aplicando el resultado anterior a a y $-b$, tendríamos

$$\begin{aligned} \text{m.c.m.}(a, b) &= a\,(-b) \\ &= |a|\,|b| \qquad \{|a| = a \text{ y } |b| = -b\} \\ &= |ab| \end{aligned}$$

- $a < 0$ y $b > 0$.
  En este caso, $-a > 0$ y aplicando el resultado anterior a $-a$ y b, tendríamos

$$\begin{aligned} \text{m.c.m.}(a, b) &= (-a)\,b \\ &= |a|\,|b| \qquad \{|a| = -a \text{ y } |b| = b\} \\ &= |ab| \end{aligned}$$

- $a < 0$ y $b < 0$.
  En tal caso, $-a > 0$ y $-b > 0$. Procediendo igual que en los casos anteriores,

$$\begin{aligned} \text{m.c.m.}(a, b) &= (-a)\,(-b) \\ &= |a|\,|b| \qquad \{|a| = -a \text{ y } |b| = -b\} \\ &= |ab| \end{aligned}$$

(b) $\text{m.c.m.}(ka, kb) = k \cdot \text{m.c.m.}(a, b),\ \forall k \in \mathbb{Z}^+$.

En efecto, sea $m = \text{m.c.m.}\,(a, b)$. Entonces,

1. $$m = \text{m.c.m.}\,(a, b) \Longrightarrow \begin{cases} a \,|m \Longrightarrow ka \,|km \\ \text{y} \\ b \,|m \Longrightarrow kb \,|km \end{cases}$$
   es decir, km es múltiplo común de ka y kb.
2. Veamos que km es el mínimo de los múltiplos comunes a ka y kb. En efecto, supongamos que c es otro múltiplo común de ka y kb. Entonces,
   $$ka \,|c \iff \exists q_1 \in \mathbb{Z} : c = ka \cdot q_1 \Longrightarrow \frac{c}{k} = a \cdot q_1 \iff a \left| \frac{c}{k} \right.$$
   y
   $$kb \,|c \iff \exists q_2 \in \mathbb{Z} : c = kb \cdot q_2 \Longrightarrow \frac{c}{k} = b \cdot q_2 \iff b \left| \frac{c}{k} \right.$$
   o sea, $\dfrac{c}{k}$ es un múltiplo común de a y b, luego ha de serlo también de su mínimo común múltiplo, m, luego
   $$m \left| \frac{c}{k} \right. \iff \exists q \in \mathbb{Z} : \frac{c}{k} = m \cdot q \iff c = km \cdot q \iff km \,|c$$
   y por lo tanto, c es múltiplo de km.

De 1. y 2. se sigue que

$$\text{m.c.m.}(ka, kb) = km = k \cdot \text{m.c.m.}(a, b)$$

(c) $\text{m.c.d.}(a, b) \cdot \text{m.c.m.}(a, b) = |ab|$.

En efecto, por (i) de 3.5.9, si $d = \text{m.c.d.}(a, b)$, entonces $\dfrac{a}{d}$ y $\dfrac{b}{d}$ han de ser primos entre sí, es decir, $\text{m.c.d.}\left(\dfrac{a}{d}, \dfrac{b}{d}\right) = 1$, luego por (a),

$$\text{m.c.m.}\left(\frac{a}{d}, \frac{b}{d}\right) = \left|\frac{a}{d} \cdot \frac{b}{d}\right|$$

y por (b),

$$\text{m.c.m.}(a, b) = \text{m.c.m.}\left(\frac{d \cdot a}{d}, \frac{d \cdot b}{d}\right) = d \cdot \text{m.c.m.}\left(\frac{a}{d}, \frac{b}{d}\right)$$

Pues bien,

$$\text{m.c.d.}(a, b) \cdot \text{m.c.m.}(a, b) = d \cdot d \cdot \text{m.c.m.}\left(\frac{a}{d}, \frac{b}{d}\right) = d^2 \left|\frac{a}{d} \cdot \frac{b}{d}\right| = d^2 \frac{|ab|}{d^2} = |ab|$$

■

Ejemplo 3.35

Sean a y b dos números enteros distintos de cero. Demostrar que las tres condiciones siguientes son equivalentes:

(i) $a \,|b$

(ii) $\text{m.c.d.}(a, b) = |a|$

(iii) $\text{m.c.m.}(a, b) = |b|$

Solución

$(i) \Longrightarrow (ii)$.

En efecto, $a \,|a$ y como, por hipótesis, $a \,|b$, tendremos que a es divisor común a a y a b, luego ha de dividir a su máximo común divisor, es decir,

$$a \,|\text{m.c.d.}(a,b) \ .$$

Por otro lado,

$$\text{m.c.d.}(a,b) \,|a$$

de aquí que por (iii) de 3.1.2,

$$\text{m.c.d.}(a,b) = \pm a$$

Como $\text{m.c.d.}(a,b) > 0$, tomamos,

$$\text{m.c.d.}(a,b) = \begin{cases} a, \text{ si } a > 0 \\ -a, \text{ si } a < 0 \end{cases}$$

es decir, $\text{m.c.d.}(a,b) = |a|$.

$(ii) \Longrightarrow (iii)$.

En efecto, si $\text{m.c.d.}(a,b) = |a|$, entonces aplicando (iii) de 3.7.4, 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 $\text{m.c.m.}(a,b) = |b|$, entonces $|b|$ es el mínimo de los múltiplos comunes a a y a b, es decir $|b|$ es múltiplo de a o lo que es lo mismo, a es divisor de $|b|$ y, por lo tanto, de b, es decir,

$$a \,|b$$

■

Ejemplo 3.36

Determinar el máximo común divisor y el mínimo común múltiplo de las siguientes parejas de números y expresar, en cada caso, el máximo común divisor como una combinación lineal de ellos.

(a) 2689 y 4001

(b) 7982 y 7983

Solución

(a) Hallamos el máximo común divisor de 2689 y 4001 mediante el algoritmo de Euclides.

	1	2	20	5	2	2	2
4001	2689	1312	65	12	5	2	1
1312	65	12	5	2	1	0	

luego,

$$\text{m.c.d.}\,(4001, 2689) = 1$$

y, por tanto,

$$\text{m.c.m.}\,(4001, 2689) = 4001 \cdot 2689 = 10758689$$

Expresamos ahora el máximo común divisor como una combinación lineal con coeficientes enteros de 4001 y 2689.

$$\left.\begin{array}{r} 1 = 5 - 2 \cdot 2 \\ 2 = 12 - 2 \cdot 5 \end{array}\right\} \implies \begin{array}{rcl} 1 & = & 5 - 2(12 - 2 \cdot 5) \\ & = & (-2) \cdot 12 + 5 \cdot 5 \end{array}$$

$$\left.\begin{array}{r} 1 = (-2) \cdot 12 + 5 \cdot 5 \\ 5 = 65 - 5 \cdot 12 \end{array}\right\} \implies \begin{array}{rcl} 1 & = & (-2) \cdot 12 + 5(65 - 5 \cdot 12) \\ & = & 5 \cdot 65 + (-27) \cdot 12 \end{array}$$

$$\left.\begin{array}{r} 1 = 5 \cdot 65 + (-27) \cdot 12 \\ 12 = 1312 - 20 \cdot 65 \end{array}\right\} \implies \begin{array}{rcl} 1 & = & 5 \cdot 65 + (-27)(1312 - 20 \cdot 65) \\ & = & (-27) \cdot 1312 + 545 \cdot 65 \end{array}$$

$$\left.\begin{array}{r} 1 = (-27) \cdot 1312 + 545 \cdot 65 \\ 65 = 2689 - 2 \cdot 1312 \end{array}\right\} \implies \begin{array}{rcl} 1 & = & -27 \cdot 1312 + 545(2689 - 2 \cdot 1312) \\ & = & 545 \cdot 2689 + (-1117) \cdot 1312 \end{array}$$

$$\left.\begin{array}{r} 1 = 545 \cdot 2689 + (-1117) \cdot 1312 \\ 1312 = 4001 - 1 \cdot 2689 \end{array}\right\} \implies \begin{array}{rcl} 1 & = & 545 \cdot 2689 + \\ & & (-1117)(4001 - 1 \cdot 2689) \\ & = & (-1117) \cdot 4001 + 1662 \cdot 2689 \end{array}$$

luego la combinación lineal buscada es

$$1 = (-1117) \cdot 4001 + 1662 \cdot 2689$$

(b) Al igual que en el apartado anterior, utilizamos el algoritmo de Euclides para hallar el máximo común divisor de 7982 y 7983.

	1	7982
7983	7982	1
1	0	

luego,

$$\text{m.c.d.}\,(7983, 7982)) = 1$$

y

$$\text{m.c.m.}\,(7983, 7982) = 7983 \cdot 7982 = 63720306$$

La combinación lineal buscada será, por tanto,

$$1 = 7983 + (-1) \cdot 7982$$

■

Ejemplo 3.37

Para cada $a \in \mathbb{Z}^+$, ¿Cuál es el mínimo común múltiplo y el máximo común divisor de a y $a+1$?

Solución

Obsérvese lo siguiente:

Si a es par(impar), entonces $a+1$ es impar(par), luego el único divisor común positivo que tienen es el 1, de aquí que

$$\text{m.c.d.}\,(a, a+1) = 1$$

Si empleamos el algoritmo de Euclides

	1	a
$a+1$	a	1
1	0	

o sea,

$$\text{m.c.d.}\,(a, a+1) = 1$$

De

$$\text{m.c.d.}\,(a, a+1) \cdot \text{m.c.m.}\,(a, a+1) = a(a+1)$$

se sigue que

$$\text{m.c.m.}\,(a, a+1) = a(a+1)$$

■

Ejemplo 3.38

Sean a, b y c tres números enteros positivos tales que a y b son primos entre sí. Probar que si $a\,|c$ y $b\,|c$, entonces $ab\,|c$. ¿Se verifica también si a y b no son primos entre sí?

Solución

En efecto,

$$\left.\begin{array}{l} a\,|c \iff c \text{ es múltiplo de } a \\ \text{y} \\ b\,|c \iff c \text{ es múltiplo de } b \end{array}\right\} \implies c \text{ es múltiplo del m.c.m. } (a,b)$$

$$\{\text{m.c.m. } (a,b) = ab\}$$

$$\implies c \text{ es múltiplo de } ab$$

$$\iff ab\,|c$$

Si a y b no son primos entre sí, no se verifica la proposición. Por ejemplo

$$4\,|16 \quad \text{y } 8\,|16$$

sin embargo 32 no divide a 16.

■

Ejemplo 3.39

El mínimo común múltiplo de los términos de una fracción es 340. Determinar dicha fracción sabiendo que no altera su valor si se suma 20 al numerador y 25 al denominador.

Solución

Sean a y b el numerador y del denominador de la fracción buscada y sea d el máximo común divisor de ambos números, entonces

$$\frac{a}{b} = \frac{a+20}{b+25} \iff ab + 25a = ab + 20b \iff \frac{a}{b} = \frac{20}{25}$$

Como el cociente es positivo, a y b han de ser los dos positivos o los dos negativos, luego,

$$\frac{a}{b} = \frac{20}{25} \implies \frac{|a|}{|b|} = \frac{20}{25}$$

y si dividimos numerador y denominador de ambas fracciones por su máximo común divisor, tendremos

$$\frac{\frac{|a|}{d}}{\frac{|b|}{d}} = \frac{\frac{20}{5}}{\frac{25}{5}} \implies \frac{\frac{|a|}{d}}{\frac{|b|}{d}} = \frac{4}{5} \iff \left\{\begin{array}{l} \dfrac{|a|}{d} = 4 \\ \text{y} \\ \dfrac{|b|}{d} = 5 \end{array}\right.$$

Por otra parte,

$$\text{m.c.d. } (a,b) \cdot \text{m.c.m. } (a,b) = |ab|$$

luego,

$$d \cdot 340 = |ab|$$

de aquí que

$$\frac{|a|}{d} = \frac{340}{|b|} \quad \text{y} \quad \frac{|b|}{d} = \frac{340}{|a|}$$

y comparando estas igualdades con las anteriores, tendremos

$$\left.\begin{array}{l} \dfrac{|a|}{d} = 4 \\ \text{y} \\ \dfrac{|a|}{d} = \dfrac{340}{|b|} \end{array}\right\} \implies \frac{340}{|b|} = 4 \Longrightarrow |b| = \frac{340}{4} \Longrightarrow |b| = 85 \Longrightarrow b = 85 \text{ o } b = -85$$

$$\left.\begin{array}{l} \dfrac{|b|}{d} = 5 \\ \text{y} \\ \dfrac{|b|}{d} = \dfrac{340}{|a|} \end{array}\right\} \implies \frac{340}{|a|} = 5 \Longrightarrow |a| = \frac{340}{5} \Longrightarrow |a| = 68 \Longrightarrow a = 68 \text{ o } a = -68$$

Luego las dos soluciones son $a = 68$ y $b = 85$ o $a = -68$ y $b = -85$.

■

Ejemplo 3.40

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 3.5.8, podremos encontrar dos enteros p y q tales que

$$pa + qb = 1$$

de aquí que

$$\begin{array}{lcll} pa^2 & + & qab & = a \\ \text{y} & & & \\ pab & + & qb^2 & = b \end{array}$$

Pues bien, sea d un divisor común a ab y $a+b$. Entonces,

$$\left.\begin{array}{l} d\,|ab \\ \text{y} \\ d\,|a+b \implies d\,|a\,(a+b) \end{array}\right\} \implies d\,|ab \text{ y } d\,|a\,(a+b)-ab$$

$$\implies d\,|ab \text{ y } d\,|a^2+ab-ab$$

$$\implies d\,|ab \text{ y } d\,|a^2$$

$$\implies d\,|pa^2+qab$$

$$\implies d\,|a$$

Por otro lado,

$$\left.\begin{array}{l} d\,|ab \\ \text{y} \\ d\,|a+b \implies d\,|b\,(a+b) \end{array}\right\} \implies d\,|ab \text{ y } d\,|b\,(a+b)-ab$$

$$\implies d\,|ab \text{ y } d\,|b^2+ab-ab$$

$$\implies d\,|ab \text{ y } d\,|b^2$$

$$\implies d\,|pab+qb^2$$

$$\implies d\,|b$$

Por tanto, d es un divisor común a a y b, luego será divisor del máximo común divisor de ambos, es decir,

$$d\,|\text{m.c.d.}(a,b) \implies d\,|1 \implies d=1$$

por lo tanto,

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

■

Ejemplo 3.41

Hallar dos números enteros positivos, sabiendo que su suma es 240 y su mínimo común múltiplo es 1768.

Solución

Sean a y b los números buscados y sea d su máximo común divisor. Entonces, por 3.7.4, y teniendo en cuenta que al ser ambos números positivos, $|ab|=ab$, tendremos

$$\text{m.c.d.}(a,b)\cdot\text{m.c.m.}(a,b)=ab \iff ab=1768d$$

Luego,

$$\left.\begin{array}{l} a+b=240 \\ \text{y} \\ ab=1768d \end{array}\right\}$$

Por otra parte, por el ejemplo anterior, 3.40 ,

$$\begin{aligned}
\text{m.c.d.}(a,b)=d &\implies \text{m.c.d.}\left(\frac{a}{d},\frac{b}{d}\right)=1\\
&\implies \text{m.c.d.}\left(\frac{a}{d}\cdot\frac{b}{d},\frac{a}{d}+\frac{b}{d}\right)=1\\
&\implies \text{mc.d.}\left(\frac{ab}{d^2},\frac{a+b}{d}\right)=1\\
&\implies \frac{\frac{ab}{d^2}}{\frac{a+b}{d}} \text{ es irreducible.}
\end{aligned}$$

Entonces,

$$\begin{aligned}
\frac{\frac{ab}{d^2}}{\frac{a+b}{d}}=\frac{\frac{1768}{d}}{\frac{240}{d}} &\implies \frac{\frac{ab}{d^2}}{\frac{a+b}{d}}=\frac{1768}{240}\\
&\implies \frac{\frac{ab}{d^2}}{\frac{a+b}{d}}=\frac{\frac{1768}{8}}{\frac{240}{8}} \quad \{\text{m.c.d.}(1768,240)=8\}\\
&\implies \frac{\frac{ab}{d^2}}{\frac{a+b}{d}}=\frac{221}{30}\\
&\implies \begin{cases} \frac{ab}{d^2}=221 \\ \text{y} \\ \frac{a+b}{d}=30 \end{cases} \quad \{\text{Fracciones irreducibles}\}\\
&\implies \begin{cases} \frac{a}{d}\cdot\frac{b}{d}=13\cdot 17 \\ \text{y} \\ a+b=30d \end{cases}\\
&\implies \begin{cases} \frac{a}{d}=13 \text{ y } \frac{b}{d}=17 \text{ o } \frac{a}{d}=17 \text{ y } \frac{b}{d}=13 \\ \text{y} \\ d=\frac{240}{30} \end{cases}\\
&\implies \begin{cases} a=13d \text{ y } b=17d \text{ o } a=17d \text{ y } b=13d \\ \text{y} \\ d=8 \end{cases}\\
&\implies a=104 \text{ y } b=136 \text{ o } a=136 \text{ y } b=104
\end{aligned}$$

de aquí que los números buscados sean 104 y 136.

■

Ejemplo 3.42

Determinar dos números enteros positivos sabiendo que su mínimo común múltiplo es 360 y la suma de sus cuadrados 5409.

Solución

Sean a y b los números a determinar, entonces m.c.m. $(a,b) = 360$ y $a^2 + b^2 = 5409$.

De 3.7.4 y llamando d al m.c.d.(a,b), , se sigue que

$$d \cdot \text{m.c.m.}(a,b) = ab \Longrightarrow ab = 360d$$

Por lo tanto, tendremos,

$$\left.\begin{array}{l} ab = 360d \\ a^2 + b^2 = 5409 \end{array}\right\}$$

Por otra parte, aplicando reiteradamente el ejemplo 3.24 ,

$$\text{m.c.d.}\left(\frac{a}{d}, \frac{b}{d}\right) = 1 \Longrightarrow \text{m.c.d.}\left(\frac{a^2}{d^2}, \frac{b^2}{d^2}\right) = 1$$

y utilizando el resultado del ejercicio 3.40 ,

$$\begin{array}{rcl} \text{m.c.d.}\left(\frac{a^2}{d^2}, \frac{b^2}{d^2}\right) = 1 & \Longrightarrow & \text{m.c.d.}\left(\frac{a^2b^2}{d^4}, \frac{a^2+b^2}{d^2}\right) = 1 \\ & \Longrightarrow & \text{m.c.d.}\left(\frac{360^2}{d^2}, \frac{5409}{d^2}\right) = 1 \\ & \Longrightarrow & d^2\text{m.c.d.}\left(\frac{360^2}{d^2}, \frac{5409}{d^2}\right) = d^2 \\ & \Longrightarrow & \text{m.c.d.}\left(d^2\frac{360^2}{d^2}, d^2\frac{5409}{d^2}\right) = d^2 \\ & \Longrightarrow & \text{m.c.d.}\left(360^2, 5409\right) = d^2 \\ & \Longrightarrow & d^2 = 9 \\ & \Longrightarrow & d = 3 \end{array}$$

Sustituyendo,

$$\left.\begin{array}{l} ab = 360d \\ a^2 + b^2 = 5409 \end{array}\right\} \overset{d=3}{\Longrightarrow} \left\{\begin{array}{l} ab = 1080 \\ a^2 + b^2 = 5409 \end{array}\right.$$

$$\Longrightarrow \left\{\begin{array}{l} 2ab = 2160 \\ a^2 + b^2 = 5409 \end{array}\right.$$

$$\Longrightarrow \left\{\begin{array}{l} a^2 + 2ab + b^2 = 7569 \\ a^2 - 2ab + b^2 = 3249 \end{array}\right.$$

$$\Longrightarrow \left\{\begin{array}{l} (a+b)^2 = 87^2 \\ (a-b)^2 = 57^2 \end{array}\right.$$

$$\Longrightarrow \left\{\begin{array}{l} a + b = 87 \\ a - b = 57 \end{array}\right.$$

$$\Longrightarrow \left\{\begin{array}{l} a = 72 \\ b = 15 \end{array}\right.$$

■

Lección 4

Teorema Fundamental de la Aritmética

El concepto de número primo se remonta a la antigüedad. Los griegos poseían dicho concepto, así como una larga lista de teoremas y propiedades relacionados con él. Los cuatro ejemplos siguientes aparecen en los *Elementos de Euclides*:

- Todo entero positivo distinto de 1 es un producto de números primos.
- Teorema fundamental de la Aritmética: "Todo entero positivo puede descomponerse de manera única como un producto de números primos".
- Existen infinitos números primos.
- Podemos obtener una lista de los números primos por medio del método conocido como la *Criba de Eratóstenes*.

4.1 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.

4.1.1 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.

■

4.1.2 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.

■

4.1.3 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

$\Longrightarrow$)

Lo haremos por contradicción. En efecto, supongamos que $p \in \mathbb{Z}^+$ es primo y $\exists a, b \in \mathbb{Z},\ 1 < a < p,\ 1 < b < p$ 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.

$\Longleftarrow$)

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 4.1 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 $1 < a, b < p$.

■

4.1.4 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 $\mathbb{Z}^+$. Aplicando el "principio de la buena ordenación" C tendrá mínimo o primer elemento y que llamaremos m. Pues bien,

$$\begin{aligned}
m \in C \quad &\Longrightarrow \quad \begin{cases} m \text{ es compuesto.} \\ \text{y} \\ m \text{ no tiene divisores primos.} \end{cases} \\
&\Longrightarrow \quad \begin{cases} m \text{ tiene más de 2 divisores.} \\ \text{y} \\ m \text{ no tiene divisores primos.} \end{cases} \\
&\Longrightarrow \quad \begin{cases} \text{Hay, al menos, un } m_1 \in \mathbb{Z}^+, \text{ divisor de } m \text{ y distinto de 1 y de } m. \\ \text{y} \\ m_1 \text{ no es primo.} \end{cases} \\
&\Longrightarrow \quad \text{Hay, al menos, un } m_1 \in \mathbb{Z}^+, \text{ compuesto tal que } m_1 | m \text{ y } 1 < m_1 < m.
\end{aligned}$$

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.

4.1.5 Teorema

Existen infinitos números primos.

Demostración

Supongamos lo contrario, es decir la cantidad de números primos existente es finita, pongamos, por ejemplo, que sólo hay k números primos,

$$p_1, p_2, \ldots\ldots, p_k.$$

Pues bien, sea m el producto de todos ellos más 1, es decir,

$$m = p_1 \cdot p_2 \cdot \cdots\cdots p_k + 1$$

Entonces, obviamente,

$$m > 1, \text{ y } m \neq p_i, \ i = 1, 2, \ldots, k$$

es decir es distinto de todos los primos que existen, luego no puede ser primo, de aquí que sea compuesto y, por el teorema anterior, tendrá, al menos, un divisor primo que tendrá que ser uno de los existentes, o sea, existe p_j con $j \in \{1, 2, \ldots\ldots, k\}$ tal que

$$p_j \,|m$$

y como

$$p_j \,|p_1 \cdot p_2 \cdot \cdots\cdots p_k$$

entonces dividirá a la diferencia de ambos,

$$p_j \,|m - p_1 \cdot p_2 \cdot \cdots\cdots p_k$$

luego,

$$p_j \,|1$$

de aquí que $p_j = 1$ ó $p_j = -1$ y esto es imposible ya que p_j es primo.

De la contradicción a la que hemos llegado, se sigue que la suposición hecha es falsa y, por tanto, existen infinitos números primos.

■

Ejemplo 4.1

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 $p_1 \cdot p_2 \cdot \cdots\cdots p_n + 1$ 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.

$$\begin{aligned}
a \text{ cuadrado perfecto} &\iff \sqrt{a} \in \mathbb{Z} \\
&\implies \exists q_1, r \in \mathbb{Z} : \sqrt{a} = 2q_1 + r, \text{ con } r = 0 \text{ ó } r = 1 \ (3.2.1) \\
&\iff \exists q_1, r \in \mathbb{Z} : a = (2q_1 + r)^2, \text{ con } r = 0 \text{ ó } r = 1 \\
&\iff \exists q_1, r \in \mathbb{Z} : a = 4q_1^2 + 4q_1 r + r^2, \text{ con } r = 0 \text{ ó } r = 1 \\
&\iff \exists q_1, r \in \mathbb{Z} : a = 4\left(q_1^2 + q_1 r\right) + r^2, \text{ con } r = 0 \text{ ó } r = 1 \\
&\quad \left\{\text{Tomando } q \in \mathbb{Z} \text{ tal que } q = q_1^2 + q_1 r\right\} \\
&\iff \exists q \in \mathbb{Z} : \begin{cases} a = 4q \\ \text{o} \\ a = 4q+1 \end{cases}
\end{aligned}$$

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

$$a \neq 4q \text{ y } a \neq 4q+1, \forall q \in \mathbb{Z} \Longrightarrow a \text{ no es un cuadrado perfecto} \tag{4.1}$$

Pues bien, los p_i, para $1 \leqslant i \leqslant n$, son números primos, luego todos, excepto p_1, que es 2, son impares, y como el producto de dos números impares es impar, $p_2 \cdot p_3 \cdots p_n$ es impar, luego.

$$\begin{aligned}
\exists q \in \mathbb{Z} : p_2 \cdot p_3 \cdots p_n = 2q+1 &\implies \exists q \in \mathbb{Z} : p_1 \cdot p_2 \cdot p_3 \cdots p_n + 1 = 2(2q+1) + 1 \\
&\implies \exists q \in \mathbb{Z} : p_1 \cdot p_2 \cdot p_3 \cdots p_n + 1 = 4q + 3
\end{aligned}$$

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 (4.1),

$$a = p_1 \cdot p_2 \cdot p_3 \cdots p_n + 1 \Longrightarrow a \text{ no es un cuadrado perfecto}$$

es decir ningún número entero de la forma $p_1 \cdot p_2 \cdot p_3 \cdots p_n + 1$ es un cuadrado perfecto.

■

4.2 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.

4.2.1 Teorema

Si un número entero mayor que 1 *no tiene divisores primos menores o iguales que su raíz, entonces es primo.*

Demostración

Sea a entero estrictamente mayor que 1. Utilizamos el método de demostración por la contrarrecíproca, es decir veremos que

si a no es primo, entonces existe, al menos, un divisor primo de a menor o igual que su raíz.

En efecto, si a no es primo, entonces es compuesto luego,

$$a = bc, \text{ siendo } 1 < b < a \text{ y } 1 < c < a$$

Pues bien, uno de los divisores de a, b ó c ha de ser menor o igual que la raíz de a. Es decir, $b \leqslant \sqrt{a}$ ó $c \leqslant \sqrt{a}$ ya que si no fuera así tendríamos que

$$\left.\begin{array}{l} b > \sqrt{a} \\ \text{y} \\ c > \sqrt{a} \end{array}\right\} \implies bc > \sqrt{a}\sqrt{a} \implies a > a$$

lo cual, obviamente, es imposible. Supondremos, sin pérdida de generalidad, que $b \leqslant \sqrt{a}$. Ahora puede ocurrir lo siguiente:

- Si b es primo, entonces el teorema estará demostrado ya que

$$b \text{ es divisor primo de } a \text{ y } b \leqslant \sqrt{a}$$

[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.

– Si b no es primo, entonces por la proposición 4.1.2, b tendrá, al menos, un divisor primo p. Entonces,

$$\left.\begin{array}{l} p|b \\ \text{y} \\ b|a \end{array}\right\} \implies p|a$$

luego hemos encontrado

$$p \text{ divisor primo de } a \text{ y } p \leqslant \sqrt{a}$$

es decir, el teorema estaría probado.

■

4.2.2 Eratóstenes

Veamos como se utiliza el teorema anterior para construir la criba de Eratóstenes y encontrar números primos.

Solución

Partiremos de que los enteros 2 y 3 son primos.

Sea a un número entero mayor que 1 que esté entre los cuadrados de los dos primeros números primos sin que pueda ser el segundo, es decir, $2^2 \leqslant a < 3^2$. Entonces,

$$2^2 \leqslant a < 3^2 \implies 2 \leqslant \sqrt{a} < 3$$

luego el único número primo menor o igual que $\sqrt{a}$ sería el 2. Particularizando el teorema anterior, tendríamos

si un número entero entre 4 y 8 no es múltiplo de 2, entonces es primo.

La forma de proceder en la práctica es la siguiente:

- Escribimos todos los números enteros entre 4 y 8.

4 5 6 7 8

- Tachamos los que sean múltiplos de 2.

~~4~~ 5 ~~6~~ 7 ~~8~~

- Los números que no están tachados no son múltiplos de 2, luego son primos, así que ya tenemos todos los números primos que hay entre 2 y 8.

2 3 ~~4~~ 5 ~~6~~ 7 ~~8~~

Tomemos ahora a tal que $3^2 \leqslant a < 5^2$. Entonces,

$$3^2 \leqslant a < 5^2 \implies 3 \leqslant \sqrt{a} < 5$$

luego los números primos menores o iguales que la raíz de a son 2 y 3. Particularizando, al igual que antes, el teorema anterior:

si un entero entre 9 y 24 no es múltiplo de 2 ni de 3, entonces es primo.

Procediendo, en la práctica, igual que antes

- Escribimos todos los números enteros entre 9 y 24.

9 10

11 12 13 14 15 16 17 18 19 20

21 22 23 24

- Tachamos los que sean múltiplos de 2.

9 ~~10~~

11 ~~12~~ 13 ~~14~~ 15 ~~16~~ 17 ~~18~~ 19 ~~20~~

21 ~~22~~ 23 ~~24~~

- Tachamos los que sean múltiplos de 3.

~~9~~ ~~10~~

11 ~~12~~ 13 ~~14~~ ~~15~~ ~~16~~ 17 ~~18~~ 19 ~~20~~

~~21~~ ~~22~~ 23 ~~24~~

- Los que quedan sin tachar no son múltiplos de 2 ni de 3, por lo tanto, son primos. Añadimos los que teníamos entre 2 y 8 y tendremos todos los números primos entre 2 y 24.

2 3 ~~4~~ 5 ~~6~~ 7 ~~8~~ ~~9~~ ~~10~~

11 ~~12~~ 13 ~~14~~ ~~15~~ ~~16~~ 17 ~~18~~ 19 ~~20~~

~~21~~ ~~22~~ 23 ~~24~~

Elegimos ahora a tal que $5^2 \leqslant a < 7^2$. Entonces,

$$5^2 \leqslant a < 7^2 \Longrightarrow 5 \leqslant \sqrt{a} < 7$$

luego los números primos menores o iguales que la raíz de a son 2, 3 y 5. Particularizando, de nuevo, el teorema anterior:

si un entero entre 25 y 48 no es múltiplo de 2, ni de 3, ni de 5, entonces es primo.

Procediendo, en la práctica, igual que en los casos anteriores

- Escribimos todos los números enteros entre 25 y 48.

				25	26	27	28	29	30
31	32	33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48		

- Tachamos los que sean múltiplos de 2.

				25	~~26~~	27	~~28~~	29	~~30~~
31	~~32~~	33	~~34~~	35	~~36~~	37	~~38~~	39	~~40~~
41	~~42~~	43	~~44~~	45	~~46~~	47	~~48~~		

- Tachamos los que sean múltiplos de 3.

				25	~~26~~	~~27~~	~~28~~	29	~~30~~
31	~~32~~	~~33~~	~~34~~	35	~~36~~	37	~~38~~	~~39~~	~~40~~
41	~~42~~	43	~~44~~	~~45~~	~~46~~	47	~~48~~		

- Tachamos los que sean múltiplos de 5.

				~~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, son 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~~		

El número a estará, ahora, entre 7^2 y 11^2. Pues bien,

$$7^2 \leqslant a < 11^2 \Longrightarrow 7 \leqslant \sqrt{a} < 11$$

luego los números primos menores o iguales que la raíz de a son 2, 3, 5 y 7. Particularizando, de nuevo, el teorema anterior:

> si un entero entre 49 y 120 no es múltiplo de 2, ni de 3, ni de 5, ni de 7, entonces es primo.

Procediendo, en la práctica, igual que en los casos anteriores

- Escribimos todos los números enteros entre 49 y 120.

								49	50
51	52	53	54	55	56	57	58	59	60
61	62	63	64	65	66	67	68	69	70
71	72	73	74	75	76	77	78	79	80
81	82	83	84	85	86	87	88	89	90
91	92	93	94	95	96	97	98	99	100
101	102	103	104	105	106	107	108	109	110
111	112	113	114	115	116	117	118	119	120

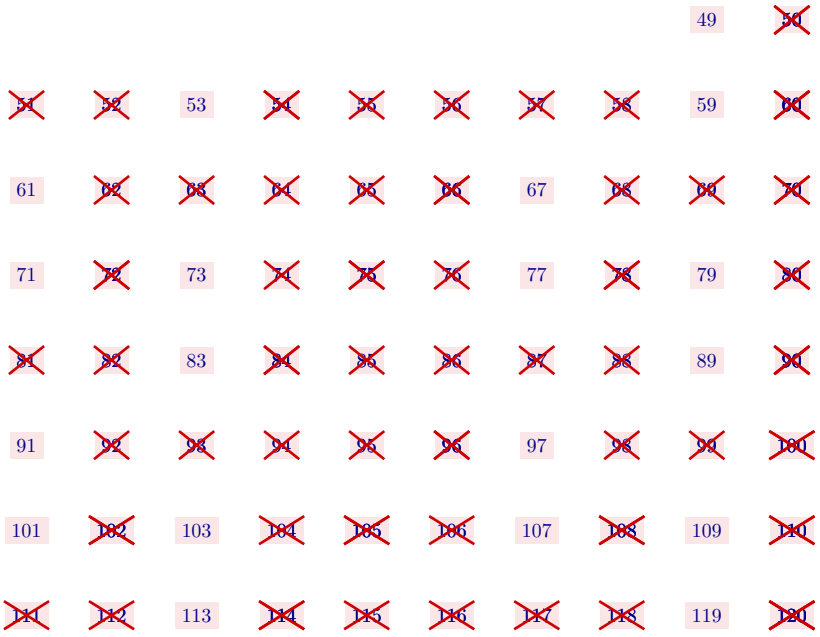
- Tachamos los que sean múltiplos de 2.

								49	~~50~~
51	~~52~~	53	~~54~~	55	~~56~~	57	~~58~~	59	~~60~~
61	~~62~~	63	~~64~~	65	~~66~~	67	~~68~~	69	~~70~~
71	~~72~~	73	~~74~~	75	~~76~~	77	~~78~~	79	~~80~~
81	~~82~~	83	~~84~~	85	~~86~~	87	~~88~~	89	~~90~~
91	~~92~~	93	~~94~~	95	~~96~~	97	~~98~~	99	~~100~~
101	~~102~~	103	~~104~~	105	~~106~~	107	~~108~~	109	~~110~~
111	~~112~~	113	~~114~~	115	~~116~~	117	~~118~~	119	~~120~~

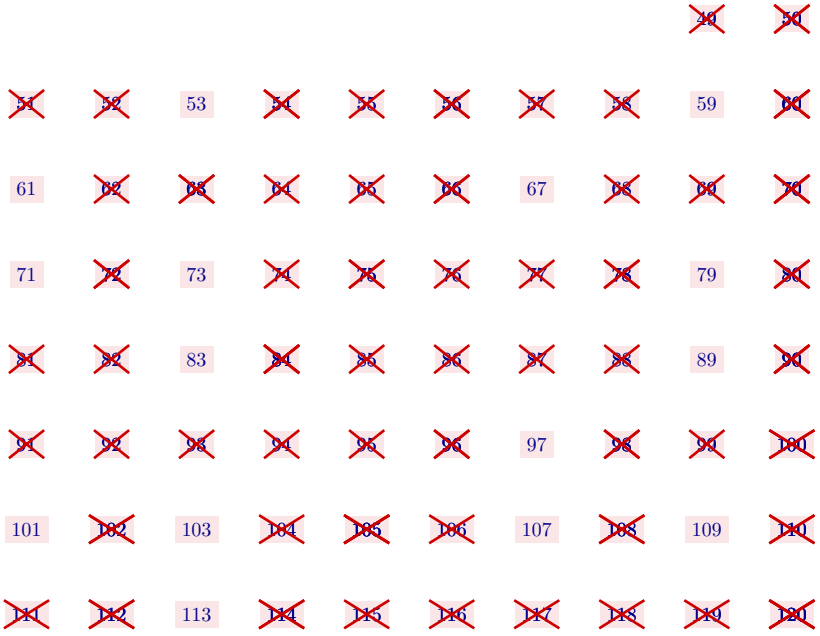
⁕ Tachamos los que sean múltiplos de 3.

								49	~~50~~
~~51~~	~~52~~	53	~~54~~	55	~~56~~	~~57~~	~~58~~	59	~~60~~
61	~~62~~	~~63~~	~~64~~	65	~~66~~	67	~~68~~	~~69~~	~~70~~
71	~~72~~	73	~~74~~	~~75~~	~~76~~	77	~~78~~	79	~~80~~
~~81~~	~~82~~	83	~~84~~	85	~~86~~	~~87~~	~~88~~	89	~~90~~
91	~~92~~	~~93~~	~~94~~	95	~~96~~	97	~~98~~	~~99~~	~~100~~
101	~~102~~	103	~~104~~	~~105~~	~~106~~	107	~~108~~	109	~~110~~
~~111~~	~~112~~	113	~~114~~	115	~~116~~	~~117~~	~~118~~	119	~~120~~

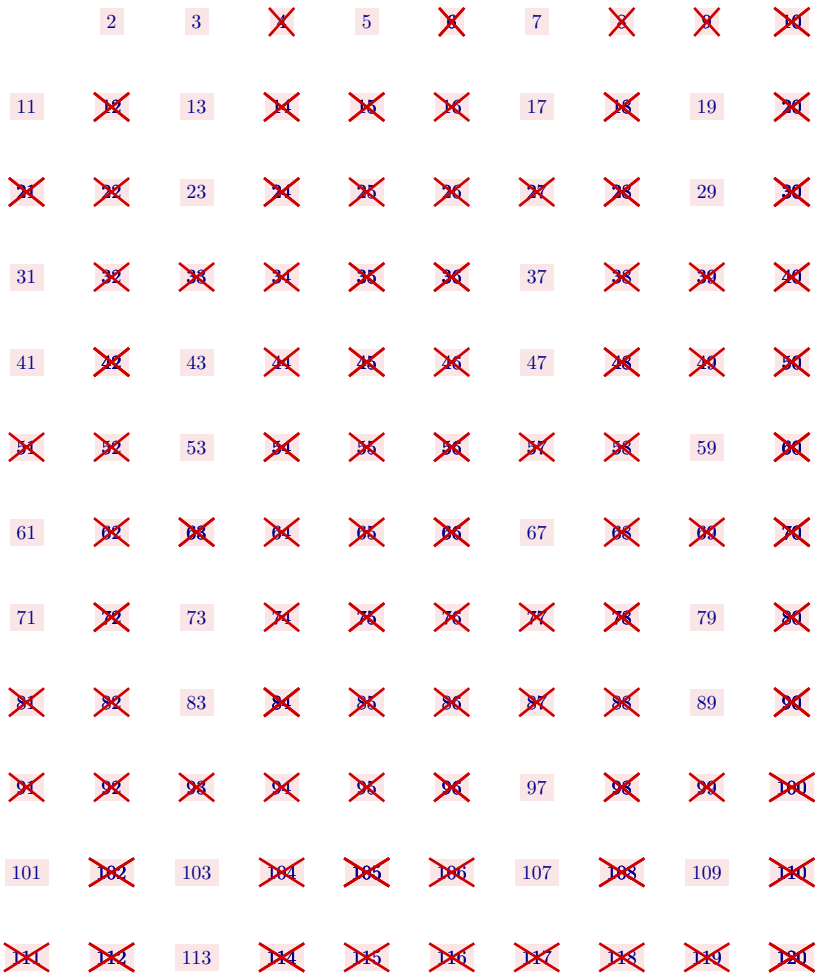
⁕ Tachamos los que sean múltiplos de 5.



⁕ 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, son primos. Añadimos los que teníamos entre 2 y 48 y tendremos todos los números primos entre 2 y 120.



Nota 4.2 Observemos lo siguiente:

(1) Para obtener los números primos entre 4 y 8 hemos eliminado, únicamente, los múltiplos de 2, luego no hay, entre 4 y 8, ningún múltiplo de 3 que no sea, también, múltiplo de 2 ya que si lo hubiera, al no haberlo tachado, sería primo y eso es imposible.

(2) Para encontrar los primos entre 9 y 24, hemos tachado los múltiplos de 2 y de 3, luego entre 9 y 24 no hay, por la misma razón que en el punto anterior, ningún múltiplo de 5 que no sea también, múltiplo de 2, de 3 ó de ambos.

De (1) y (2) se deduce que si queremos obtener los números primos entre 2 y 24 de una sola vez, bastaría con eliminar todos los múltiplos de 2, excepto el 2 y todos los de 3, excepto el 3.

Este mismo razonamiento puede ampliarse a cualquier entero a de forma que si queremos obtener todos los números primos que hay entre 2 y a, bastaría con eliminar los múltiplos de todos los números primos p, excepto el propio p, que sean menores o iguales que la raíz de a, o lo que es igual de cualquier primo p tal que $p^2 \leqslant \sqrt{a}$.

■

Ejemplo 4.2

Obtener todos los números primos que hay entre 2 y 200.

Solución

Seguiremos el procedimiento visto en la nota anterior paso a paso.

Primer paso. Escribimos todos los números entre 1 y 200.

	2	3	4	5	6	7	8	9	10
11	12	13	14	15	16	17	18	19	20
21	22	23	24	25	26	27	28	29	30
31	32	33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48	49	50
51	52	53	54	55	56	57	58	59	60
61	62	63	64	65	66	67	68	69	70
71	72	73	74	75	76	77	78	79	80
81	82	83	84	85	86	87	88	89	90
91	92	93	94	95	96	97	98	99	100
101	102	103	104	105	106	107	108	109	110
111	112	113	114	115	116	117	118	119	120
121	122	123	124	125	126	127	128	129	130
131	132	133	134	135	136	137	138	139	140
141	142	143	144	145	146	147	148	149	150
151	152	153	154	155	156	157	158	159	160
161	162	163	164	165	166	167	168	169	170
171	172	173	174	175	176	177	178	179	180
181	182	183	184	185	186	187	188	189	190
191	192	193	194	195	196	197	198	199	200

Segundo paso. $2^2 \leqslant 200$. Eliminamos, por tanto, todos los múltiplos de 2 excepto el 2.

	2	3	~~4~~	5	~~6~~	7	~~8~~	9	~~10~~
11	~~12~~	13	~~14~~	15	~~16~~	17	~~18~~	19	~~20~~
21	~~22~~	23	~~24~~	25	~~26~~	27	~~28~~	29	~~30~~
31	~~32~~	33	~~34~~	35	~~36~~	37	~~38~~	39	~~40~~
41	~~42~~	43	~~44~~	45	~~46~~	47	~~48~~	49	~~50~~
51	~~52~~	53	~~54~~	55	~~56~~	57	~~58~~	59	~~60~~
61	~~62~~	63	~~64~~	65	~~66~~	67	~~68~~	69	~~70~~
71	~~72~~	73	~~74~~	75	~~76~~	77	~~78~~	79	~~80~~
81	~~82~~	83	~~84~~	85	~~86~~	87	~~88~~	89	~~90~~
91	~~92~~	93	~~94~~	95	~~96~~	97	~~98~~	99	~~100~~
101	~~102~~	103	~~104~~	105	~~106~~	107	~~108~~	109	~~110~~
111	~~112~~	113	~~114~~	115	~~116~~	117	~~118~~	119	~~120~~
121	~~122~~	123	~~124~~	125	~~126~~	127	~~128~~	129	~~130~~
131	~~132~~	133	~~134~~	135	~~136~~	137	~~138~~	139	~~140~~
141	~~142~~	143	~~144~~	145	~~146~~	147	~~148~~	149	~~150~~
151	~~152~~	153	~~154~~	155	~~156~~	157	~~158~~	159	~~160~~
161	~~162~~	163	~~164~~	165	~~166~~	167	~~168~~	169	~~170~~
171	~~172~~	173	~~174~~	175	~~176~~	177	~~178~~	179	~~180~~
181	~~182~~	183	~~184~~	185	~~186~~	187	~~188~~	189	~~190~~
191	~~192~~	193	~~194~~	195	~~196~~	197	~~198~~	199	~~200~~

Tercer paso. $3^2 \leqslant 200$. Eliminamos, por tanto, todos los múltiplos de 3 excepto el 3.

	2	3	~~4~~	5	~~6~~	7	~~8~~	~~9~~	~~10~~
11	~~12~~	13	~~14~~	~~15~~	~~16~~	17	~~18~~	19	~~20~~
~~21~~	~~22~~	23	~~24~~	25	~~26~~	~~27~~	~~28~~	29	~~30~~
31	~~32~~	~~33~~	~~34~~	35	~~36~~	37	~~38~~	~~39~~	~~40~~
41	~~42~~	43	~~44~~	~~45~~	~~46~~	47	~~48~~	49	~~50~~
~~51~~	~~52~~	53	~~54~~	55	~~56~~	~~57~~	~~58~~	59	~~60~~
61	~~62~~	~~63~~	~~64~~	65	~~66~~	67	~~68~~	~~69~~	~~70~~
71	~~72~~	73	~~74~~	~~75~~	~~76~~	77	~~78~~	79	~~80~~
~~81~~	~~82~~	83	~~84~~	85	~~86~~	~~87~~	~~88~~	89	~~90~~
91	~~92~~	~~93~~	~~94~~	95	~~96~~	97	~~98~~	~~99~~	~~100~~
101	~~102~~	103	~~104~~	~~105~~	~~106~~	107	~~108~~	109	~~110~~
~~111~~	~~112~~	113	~~114~~	115	~~116~~	~~117~~	~~118~~	119	~~120~~
121	~~122~~	~~123~~	~~124~~	125	~~126~~	127	~~128~~	~~129~~	~~130~~
131	~~132~~	133	~~134~~	~~135~~	~~136~~	137	~~138~~	139	~~140~~
~~141~~	~~142~~	143	~~144~~	145	~~146~~	~~147~~	~~148~~	149	~~150~~
151	~~152~~	~~153~~	~~154~~	155	~~156~~	157	~~158~~	~~159~~	~~160~~
161	~~162~~	163	~~164~~	~~165~~	~~166~~	167	~~168~~	169	~~170~~
~~171~~	~~172~~	173	~~174~~	175	~~176~~	~~177~~	~~178~~	179	~~180~~
181	~~182~~	~~183~~	~~184~~	185	~~186~~	187	~~188~~	~~189~~	~~190~~
191	~~192~~	193	~~194~~	~~195~~	~~196~~	197	~~198~~	199	~~200~~

Cuarto paso. $5^2 \leqslant 200$. Eliminamos, por tanto, todos los múltiplos de 5 excepto el 5.

	2	3	~~4~~	5	~~6~~	7	~~8~~	~~9~~	~~10~~
11	~~12~~	13	~~14~~	~~15~~	~~16~~	17	~~18~~	19	~~20~~
~~21~~	~~22~~	23	~~24~~	~~25~~	~~26~~	~~27~~	~~28~~	29	~~30~~
31	~~32~~	~~33~~	~~34~~	~~35~~	~~36~~	37	~~38~~	~~39~~	~~40~~
41	~~42~~	43	~~44~~	~~45~~	~~46~~	47	~~48~~	49	~~50~~
~~51~~	~~52~~	53	~~54~~	~~55~~	~~56~~	~~57~~	~~58~~	59	~~60~~
61	~~62~~	~~63~~	~~64~~	~~65~~	~~66~~	67	~~68~~	~~69~~	~~70~~
71	~~72~~	73	~~74~~	~~75~~	~~76~~	77	~~78~~	79	~~80~~
~~81~~	~~82~~	83	~~84~~	~~85~~	~~86~~	~~87~~	~~88~~	89	~~90~~
91	~~92~~	~~93~~	~~94~~	~~95~~	~~96~~	97	~~98~~	~~99~~	~~100~~
101	~~102~~	103	~~104~~	~~105~~	~~106~~	107	~~108~~	109	~~110~~
~~111~~	~~112~~	113	~~114~~	~~115~~	~~116~~	~~117~~	~~118~~	119	~~120~~
121	~~122~~	~~123~~	~~124~~	~~125~~	~~126~~	127	~~128~~	~~129~~	~~130~~
131	~~132~~	133	~~134~~	~~135~~	~~136~~	137	~~138~~	139	~~140~~
~~141~~	~~142~~	143	~~144~~	~~145~~	~~146~~	~~147~~	~~148~~	149	~~150~~
151	~~152~~	~~153~~	~~154~~	~~155~~	~~156~~	157	~~158~~	~~159~~	~~160~~
161	~~162~~	163	~~164~~	~~165~~	~~166~~	167	~~168~~	169	~~170~~
~~171~~	~~172~~	173	~~174~~	~~175~~	~~176~~	~~177~~	~~178~~	179	~~180~~
181	~~182~~	~~183~~	~~184~~	~~185~~	~~186~~	187	~~188~~	~~189~~	~~190~~
191	~~192~~	193	~~194~~	~~195~~	~~196~~	197	~~198~~	199	~~200~~

Quinto paso. $7^2 \leqslant 200$. Eliminamos, por tanto, todos los múltiplos de 7 excepto el 7.

	2	3	~~4~~	5	~~6~~	7	~~8~~	~~9~~	~~10~~
11	~~12~~	13	~~14~~	~~15~~	~~16~~	17	~~18~~	19	~~20~~
~~21~~	~~22~~	23	~~24~~	~~25~~	~~26~~	~~27~~	~~28~~	29	~~30~~
31	~~32~~	~~33~~	~~34~~	~~35~~	~~36~~	37	~~38~~	~~39~~	~~40~~
41	~~42~~	43	~~44~~	~~45~~	~~46~~	47	~~48~~	~~49~~	~~50~~
~~51~~	~~52~~	53	~~54~~	~~55~~	~~56~~	~~57~~	~~58~~	59	~~60~~
61	~~62~~	~~63~~	~~64~~	~~65~~	~~66~~	67	~~68~~	~~69~~	~~70~~
71	~~72~~	73	~~74~~	~~75~~	~~76~~	~~77~~	~~78~~	79	~~80~~
~~81~~	~~82~~	83	~~84~~	~~85~~	~~86~~	~~87~~	~~88~~	89	~~90~~
~~91~~	~~92~~	~~93~~	~~94~~	~~95~~	~~96~~	97	~~98~~	~~99~~	~~100~~
101	~~102~~	103	~~104~~	~~105~~	~~106~~	107	~~108~~	109	~~110~~
~~111~~	~~112~~	113	~~114~~	~~115~~	~~116~~	~~117~~	~~118~~	~~119~~	~~120~~
121	~~122~~	~~123~~	~~124~~	~~125~~	~~126~~	127	~~128~~	~~129~~	~~130~~
131	~~132~~	~~133~~	~~134~~	~~135~~	~~136~~	137	~~138~~	139	~~140~~
~~141~~	~~142~~	143	~~144~~	~~145~~	~~146~~	~~147~~	~~148~~	149	~~150~~
151	~~152~~	~~153~~	~~154~~	~~155~~	~~156~~	157	~~158~~	~~159~~	~~160~~
~~161~~	~~162~~	163	~~164~~	~~165~~	~~166~~	167	~~168~~	169	~~170~~
~~171~~	~~172~~	173	~~174~~	~~175~~	~~176~~	~~177~~	~~178~~	179	~~180~~
181	~~182~~	~~183~~	~~184~~	~~185~~	~~186~~	187	~~188~~	~~189~~	~~190~~
191	~~192~~	193	~~194~~	~~195~~	~~196~~	197	~~198~~	199	~~200~~

Sexto paso. $11^2 \leqslant 200$. Eliminamos, por tanto, todos los múltiplos de 11 excepto el 11.

	2	3	~~4~~	5	~~6~~	7	~~8~~	~~9~~	~~10~~
11	~~12~~	13	~~14~~	~~15~~	~~16~~	17	~~18~~	19	~~20~~
~~21~~	~~22~~	23	~~24~~	~~25~~	~~26~~	~~27~~	~~28~~	29	~~30~~
31	~~32~~	~~33~~	~~34~~	~~35~~	~~36~~	37	~~38~~	~~39~~	~~40~~
41	~~42~~	43	~~44~~	~~45~~	~~46~~	47	~~48~~	~~49~~	~~50~~
~~51~~	~~52~~	53	~~54~~	~~55~~	~~56~~	~~57~~	~~58~~	59	~~60~~
61	~~62~~	~~63~~	~~64~~	~~65~~	~~66~~	67	~~68~~	~~69~~	~~70~~
71	~~72~~	73	~~74~~	~~75~~	~~76~~	~~77~~	~~78~~	79	~~80~~
~~81~~	~~82~~	83	~~84~~	~~85~~	~~86~~	~~87~~	~~88~~	89	~~90~~
~~91~~	~~92~~	~~93~~	~~94~~	~~95~~	~~96~~	97	~~98~~	~~99~~	~~100~~
101	~~102~~	103	~~104~~	~~105~~	~~106~~	107	~~108~~	109	~~110~~
~~111~~	~~112~~	113	~~114~~	~~115~~	~~116~~	~~117~~	~~118~~	~~119~~	~~120~~
~~121~~	~~122~~	~~123~~	~~124~~	~~125~~	~~126~~	127	~~128~~	~~129~~	~~130~~
131	~~132~~	~~133~~	~~134~~	~~135~~	~~136~~	137	~~138~~	139	~~140~~
~~141~~	~~142~~	~~143~~	~~144~~	~~145~~	~~146~~	~~147~~	~~148~~	149	~~150~~
151	~~152~~	~~153~~	~~154~~	~~155~~	~~156~~	157	~~158~~	~~159~~	~~160~~
~~161~~	~~162~~	163	~~164~~	~~165~~	~~166~~	167	~~168~~	169	~~170~~
~~171~~	~~172~~	173	~~174~~	~~175~~	~~176~~	~~177~~	~~178~~	179	~~180~~
181	~~182~~	~~183~~	~~184~~	~~185~~	~~186~~	~~187~~	~~188~~	~~189~~	~~190~~
191	~~192~~	193	~~194~~	~~195~~	~~196~~	197	~~198~~	199	~~200~~

Séptimo paso. $13^2 \leqslant 200$. Eliminamos todos los múltiplos de 13 excepto el 13.

	2	3	~~4~~	5	~~6~~	7	~~8~~	~~9~~	~~10~~
11	~~12~~	13	~~14~~	~~15~~	~~16~~	17	~~18~~	19	~~20~~
~~21~~	~~22~~	23	~~24~~	~~25~~	~~26~~	~~27~~	~~28~~	29	~~30~~
31	~~32~~	~~33~~	~~34~~	~~35~~	~~36~~	37	~~38~~	~~39~~	~~40~~
41	~~42~~	43	~~44~~	~~45~~	~~46~~	47	~~48~~	~~49~~	~~50~~
~~51~~	~~52~~	53	~~54~~	~~55~~	~~56~~	~~57~~	~~58~~	59	~~60~~
61	~~62~~	~~63~~	~~64~~	~~65~~	~~66~~	67	~~68~~	~~69~~	~~70~~
71	~~72~~	73	~~74~~	~~75~~	~~76~~	~~77~~	~~78~~	79	~~80~~
~~81~~	~~82~~	83	~~84~~	~~85~~	~~86~~	~~87~~	~~88~~	89	~~90~~
~~91~~	~~92~~	~~93~~	~~94~~	~~95~~	~~96~~	97	~~98~~	~~99~~	~~100~~
101	~~102~~	103	~~104~~	~~105~~	~~106~~	107	~~108~~	109	~~110~~
~~111~~	~~112~~	113	~~114~~	~~115~~	~~116~~	~~117~~	~~118~~	~~119~~	~~120~~
~~121~~	~~122~~	~~123~~	~~124~~	~~125~~	~~126~~	127	~~128~~	~~129~~	~~130~~
131	~~132~~	~~133~~	~~134~~	~~135~~	~~136~~	137	~~138~~	139	~~140~~
~~141~~	~~142~~	~~143~~	~~144~~	~~145~~	~~146~~	~~147~~	~~148~~	149	~~150~~
151	~~152~~	~~153~~	~~154~~	~~155~~	~~156~~	157	~~158~~	~~159~~	~~160~~
~~161~~	~~162~~	163	~~164~~	~~165~~	~~166~~	167	~~168~~	~~169~~	~~170~~
~~171~~	~~172~~	173	~~174~~	~~175~~	~~176~~	~~177~~	~~178~~	179	~~180~~
181	~~182~~	~~183~~	~~184~~	~~185~~	~~186~~	~~187~~	~~188~~	~~189~~	~~190~~
191	~~192~~	193	~~194~~	~~195~~	~~196~~	197	~~198~~	199	~~200~~

Octavo paso. $17^2 > 200$. Se acabó. Los números primos entre 1 y 200 son los que no están tachados.

■

4.3 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*".

4.3.1 Lema de Euclides

Si un número entero divide al producto de otros dos y es primo con uno de ellos, entonces divide al tercero.

Demostración

Sean a, b y c tres números enteros cualesquiera. Probaremos que

$$a\,|bc \text{ y m.c.d.}(a,b) = 1 \Longrightarrow a\,|c$$

En efecto, como m.c.d. $(a,b) = 1$, por el corolario 3.5.8, existirán dos números enteros p y q tales que

$$pa + qb = 1$$

Entonces,

$$\left.\begin{array}{l} a\,|bc \\ \text{y} \\ a\,|a \Longrightarrow a\,|ac \end{array}\right\} \Longrightarrow \quad a\,|pac + qbc \quad \Longrightarrow \quad a\,|(pa+qb)\,c \quad \Longrightarrow \quad a\,|c$$

■

4.3.2 Corolario

Una condición necesaria y suficiente para que un número entero mayor que 1 *sea primo es que si divide a un producto de dos enteros, entonces ha de dividir a uno de los dos.*

Demostración

La condición es *necesaria*.

Veamos que si p es cualquier entero mayor que 1,

$$p \text{ es primo} \Longrightarrow \forall n_1, n_2 \in \mathbb{Z}\,(p\,|n_1 n_2 \Longrightarrow p\,|n_1 \text{ o } p\,|n_2\,)$$

Supongamos que p es primo y que a y b son dos enteros cualesquiera. Probaremos que

$$p \text{ es primo} \Longrightarrow (p\,|ab \Longrightarrow p\,|a \text{ o } p\,|b\,)$$

o lo que es igual,

$$p \text{ es primo y } p\,|ab \Longrightarrow p\,|a \text{ o } p\,|b$$

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,

$$\left.\begin{array}{l} \text{m.c.d.}(a,p)=1 \\ \text{y} \\ p\,|ab \end{array}\right\} \Longrightarrow p\,|b$$

Si p no fuera divisor de b, siguiendo un proceso análogo llegaríamos a que $p\,|a$

La condición es *suficiente*.

Sea p cualquier entero mayor que 1, veamos que

$$\forall n_1, n_2 \in \mathbb{Z}\,(p\,|n_1 n_2 \Longrightarrow p\,|n_1 \text{ ó } p\,|n_2\,) \Longrightarrow p \text{ es primo}$$

probando el contrarrecíproco.

En efecto, supongamos que p no es primo. Entonces, por 4.1.3,

$$p \text{ no es primo} \Longleftrightarrow \exists a, b \in \mathbb{Z} : 1 < a < p \text{ y } 1 < b < p : p = ab \Longrightarrow p\,|ab$$

Además, p no puede dividir a a ni a b, ya que

- si p divide a a, entonces
$$p\,|a \Longrightarrow p\,|a \text{ y } a\,|p \Longrightarrow p = a$$
lo cual es imposible ya que $a \neq p$.
- si p divide a b, entonces
$$p\,|b \Longrightarrow p\,|b \text{ y } b\,|p \Longrightarrow p = b$$
lo cual es imposible ya que $b \neq p$.

luego, si p no es primo, hemos encontrado dos enteros a y b tales que p divide a ab y no divide a a ni a b.

■

4.3.3 Corolario

Si un número primo divide al producto de varios números enteros, entonces ha de dividir, al menos, a uno de ellos.

Demostración

Sea p cualquier número primo, probaremos que

$$p|a_1 \cdot a_2 \cdot a_3 \cdot \cdots \cdot a_n \Longrightarrow \exists a_i : p|a_i,\ 1 \leqslant i \leqslant n$$

En efecto, supongamos que

$$p\,|a_1 \cdot a_2 \cdot a_3 \cdot \cdots \cdot a_n$$

entonces,

$$p\,|a_1 \cdot (a_2 \cdot a_3 \cdot \cdots \cdot a_n)$$

y aplicando el corolario anterior

$$p\,|a_1 \text{ ó } p\,|a_2 \cdot a_3 \cdot \cdots \cdot a_n$$

– Si $p\,|a_1$, el corolario está demostrado, de lo contrario

$$p\,|a_2 \cdot a_3 \cdot \cdots \cdot a_n$$

luego,

$$p\,|a_2 \cdot (a_3 \cdot \cdots \cdot a_n)$$

y, nuevamente por el corolario anterior,

$$p\,|a_2 \;\text{ ó }\; p\,|a_3 \cdot a_4 \cdot \cdots \cdot a_n$$

– Si $p\,|a_2$, el corolario está demostrado, de lo contrario

$$p\,|a_3 \cdot a_4 \cdot \cdots \cdot a_n$$

luego,

$$p\,|a_3 \cdot (a_4 \cdot \cdots \cdot a_n)$$

Repitiendo el proceso un número finito de veces, encontraremos, al menos, un a_i, $1 \leqslant i \leqslant n$, tal que $p\,|a_i$.

■

Ejemplo 4.3

Demostrar que si $p, q_1, q_2, \ldots, q_r$ son primos y $p\,|q_1 \cdot q_2 \cdots q_r$, entonces existe algún $i = 1, 2, \ldots, r$ tal que $p = q_i$

Solución

En efecto, por el corolario 4.3.3 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 4.4

Demostrar que el número $\sqrt{2}$ es irracional.

Solución

Si $\sqrt{2}$ fuese racional, entonces podría expresarse como un cociente de dos enteros a y b primos entre sí (fracción irreducible), es decir,

$$\sqrt{2} = \frac{a}{b} : \text{m.c.d.}\,(a, b) = 1$$

Pues bien, elevando al cuadrado ambos miembros de esta igualdad, resulta:

$$\sqrt{2} = \frac{a}{b} \Longrightarrow 2 = \frac{a^2}{b^2} \Longrightarrow a^2 = 2b^2 \Longrightarrow 2\,|a \cdot a$$

luego por el corolario 4.3.3

$$2\,|a$$

y, consecuentemente, existe un entero q tal que

$$a = 2q$$

entonces,

$$a = 2q \Longrightarrow a^2 = 4q^2 \Longrightarrow 2b^2 = 4q^2 \Longrightarrow b^2 = 2q^2 \Longrightarrow 2 \,|b^2 \Longrightarrow 2 \,|b \cdot b$$

y, nuevamente por el corolario 4.3.3, se sigue que

$$2 \,|b$$

Así pues, 2 es un divisor común de a y b, lo cual es una contradicción ya que estos dos números son primos entre sí, luego la suposición hecha es falsa y $\sqrt{2}$ es irracional.

■

Ejemplo 4.5

Demostrar que la $\sqrt[3]{5}$ es un número irracional.

Solución

En efecto, supongamos que no lo fuese, entonces existirán dos números enteros a y b primos entre sí tales que

$$\sqrt[3]{5} = \frac{a}{b}$$

elevando al cubo ambos miembros de la igualdad, tendremos

$$5 = \frac{a^3}{b^3} \Longrightarrow a^3 = 5b^3 \Longrightarrow 5 \,|a^3$$

de donde se sigue, al ser 5 un número primo, que

$$5 \,|a$$

luego existe un número entero q tal que

$$a = 5q \Longrightarrow a^3 = 5^3q^3 \Longrightarrow 5b^3 = 5^3q^3 \Longrightarrow b^3 = 5^2q^3 \Longrightarrow 5 \,|b^3$$

por tanto,

$$5 \,|b$$

Concluimos, pues, que 5 es un divisor común de a y de b, lo cual contradice el hecho de que estos dos números sean primos entre sí, luego la suposición hecha es falsa y $\sqrt[3]{5}$ es un número irracional.

■

Ejemplo 4.6

Probar que si a no es la k-ésima potencia de ningún número entero, entonces $\sqrt[k]{a}$ es irracional cualesquiera que sean a y k enteros positivos.

Solución

Sean a y k enteros positivos cumpliendo las condiciones del enunciado y supongamos que $\sqrt[k]{a}$ es un número racional.

Entonces, podrá expresarse como un cociente de dos números enteros primos entre sí, es decir, existirán b y c de $\mathbb{Z}$, tales que

$$\sqrt[k]{a} = \frac{b}{c}, \text{ con m.c.d. } (b, c) = 1$$

elevando a k ambos miembros de esta igualdad, resulta

$$\sqrt[k]{a} = \frac{b}{c} \Longrightarrow a = \frac{b^k}{c^k} \Longrightarrow b^k = a \cdot c^k \Longrightarrow a \,|b^k \ .$$

Si

$$a = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \cdots \cdot p_t^{\alpha_t}$$

es la descomposición de a en factores primos, ha de existir un i entre 1 y t tal que α_i no sea múltiplo de k ya que por hipótesis a no es la k-ésima potencia de un número entero.

Pues bien, como $a \,|b^k$, b^k ha de tener todos los factores primos de a con exponentes iguales o mayores, luego tendremos que

$$p_i^{\alpha_i} \,|b^k$$

y p_i debe aparecer en la descomposición en factores primos de b, luego

$$a = p_i^s q$$

donde q y p_i son primos entre sí y $\alpha_i < k \cdot s$ ya que como vimos anteriormente, α_i no es múltiplo de k, por tanto,

$$b^k = p_i^{ks} \cdot q^k$$

Así pues,

$$\begin{aligned} ac^k = b^k \quad &\Longrightarrow \quad p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \cdots \cdot p_t^{\alpha_t} \cdot b^k = p_i^{ks} \cdot q^k \\ &\Longrightarrow \quad p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \cdots \cdot p_{i-1}^{\alpha_i - 1} p_{i+1}^{\alpha_i + 1} \cdot \cdots \cdot p_t^{\alpha_t} \cdot b^k = p_i^{ks - \alpha_i} \cdot q^k \end{aligned}$$

luego,

$$p_i \,|p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \cdots \cdot p_{i-1}^{\alpha_i - 1} p_{i+1}^{\alpha_i + 1} \cdot \cdots \cdot p_t^{\alpha_t} \cdot b^k$$

y como p_i no divide a $p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \cdots \cdot p_t^{\alpha_t}$, entonces

$$p_i \,|c^k$$

y al ser p_i un número primo, se sigue que

$$p_i \,|c$$

y como

$$p_i \,|b$$

tendremos que $p_i \neq 1$ es un divisor común de b y c lo cual contradice el hecho de que b y c sean primos entre sí, por tanto la suposición hecha es falsa y $\sqrt[k]{a}$ es irracional.

■

4.3.4 Teorema Fundamental de la Aritmética

Cualquier número entero mayor que 1 *puede escribirse de manera única, salvo el orden, como un producto de números primos.*

Demostración

Sea a un número entero mayor que 1. Probaremos, primero, que a puede escribirse como un producto de números primos y, posteriormente, veremos que esa descomposición es, salvo en el orden de los factores, única.

⁂ *Descomposición.*

- Si a es primo, consideramos el número como un producto de un sólo factor y el teorema está demostrado.
- Si a no es primo, entonces es compuesto, y la proposición 4.1.4 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 4.1.4 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,

$$\begin{aligned} a = p_1(p_2 p_3 \cdots p_k) &\implies p_1 \,|a \\ &\implies p_1 \,|q_1 q_2 q_3 \cdots q_r \\ &\implies p_1 \,|q_j \text{ para algún } j \text{ entre 1 y } r. \text{ \{Corolario 4.3.3\}} \\ &\implies p_1 = q_j, \text{ ya que } q_j \text{ es primo y } p_1 \neq 1. \end{aligned}$$

Podemos suponer que $j = 1$. Si no lo fuese bastaría con cambiar el orden de los factores. Tendremos, pues, que $p_1 = q_1$ y

$$p_1 p_2 p_3 \cdots p_k = p_1 q_2 q_3 \cdots q_r$$

de donde, al ser $p_1 \neq 0$, se sigue que

$$p_2 p_3 \cdots p_k = q_2 q_3 \cdots q_r$$

Sea ahora

$$a_1 = p_2 p_3 \cdots p_k$$

y

$$a_1 = q_2 q_3 \cdots q_r.$$

Entonces $a_1 < a$, y

$$\begin{aligned} a_1 = p_2(p_3 p_4 \cdots p_k) &\implies p_2 \,|a_1 \\ &\implies p_2 \,|q_2 q_3 q_4 \cdots q_r \\ &\implies p_2 \,|q_j \text{ para algún } j \text{ entre 2 y } r. \text{ \{Corolario 4.3.3\}} \\ &\implies p_2 = q_j, \text{ ya que } q_j \text{ es primo y } p_2 \neq 1. \end{aligned}$$

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,

$$p_2 p_3 \cdots p_k = p_2 q_3 \cdots q_r$$

y, al ser $p_2 \neq 0$, tendremos que

$$p_3 p_4 \cdots p_k = q_3 q_4 \cdots q_r$$

y llamando

$$a_2 = p_3 p_4 \cdots p_k$$

y

$$a_2 = q_3 q_4 \cdots q_r.$$

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

$$a_{k-1} = q_k q_{k+1} \cdots q_r.$$

siendo $a_{k-1} < a_{k-2} < \cdots < a_2 < a_1 < a$. Entonces,

$$\begin{aligned} a_{k-1} = p_k &\implies p_k \,|a_{k-1} \\ &\implies p_k \,|q_k q_{k+1} q_{k+2} \cdots q_r \\ &\implies p_k \,|q_j \text{ para algún } j \text{ entre } k \text{ y } r. \text{ \{Corolario 4.3.3\}} \\ &\implies p_k = q_j, \text{ ya que } q_j \text{ es primo y } p_k \neq 1 \end{aligned}$$

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, pues, la descomposición única.

■

4.3.5 Corolario

Sea a un número entero tal que $|a| > 1$, entonces a tiene una factorización única de la forma:

$$a = \pm p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$$

siendo $k \geqslant 1$, los p_k primos distintos con $p_1 < p_2 < \cdots < p_k$ y $\alpha_i \geqslant 1$ para $1 \leqslant i \leqslant k$.

Demostración

Si $|a| > 1$, entonces $a > 1$ ó $a < -1$. Pues bien,

- Si $a > 1$, por el *Teorema fundamental de la aritmética*, a puede descomponerse en factores primos. Agrupamos todos los primos iguales a p_1 en el factor $p_1^{\alpha_1}$, hacemos igual con p_2, p_3, y así sucesivamente hasta p_k, obteniendo así la descomposición pedida.
- Si $a < -1$, entonces $-a > 1$ aplicamos el razonamiento anterior a $-a$ y

$$-a = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k} \Longrightarrow a = -p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$$

■

Ejemplo 4.7

Descomponer en factores primos el número 720.

Solución

Obtendremos una descomposición del tipo anterior.

- Empezamos buscando el divisor más pequeño de 720.
  Como
  $$720 = 2 \cdot 360$$
  dicho divisor es, obviamente, el 2.
- Hacemos lo mismo con el 360.
  Dado que
  $$360 = 2 \cdot 180$$
  el divisor más pequeño de 360 es 2.
- Repetimos el proceso sucesivamente, y

$$\begin{aligned} 180 &= 2 \cdot 90 \\ 90 &= 2 \cdot 45 \\ 45 &= 3 \cdot 15 \\ 15 &= 3 \cdot 5 \\ 5 &= 1 \cdot 5 \end{aligned}$$

Ahora bastaría sustituir cada igualdad en la igualdad anterior, y resultaría

$$720 = 2 \cdot 2 \cdot 2 \cdot 2 \cdot 3 \cdot 3 \cdot 5 = 2^4 \cdot 3^2 \cdot 5$$

En la práctica suelen disponerse los cálculos en la forma siguiente:

720	2
360	2
180	2
90	2
45	3
15	3
5	5
1	

Ahora sólo habrá que contar los números que hay de cada factor, y

$$720 = 2^4 \cdot 3^2 \cdot 5$$

■

4.4 Divisores de un número

4.4.1 Lema

Si a y b son dos números enteros tales que $|a| > 1$ y $|b| > 1$, entonces pueden encontrarse k números primos $p_1, p_2, \ldots, p_k$ y k números enteros $\alpha_i \geqslant 0$ y $\beta_i \geqslant 0$, $1 \leqslant i \leqslant k$ tales que

$$a = \pm p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$$

y

$$b = \pm p_1^{\beta_1} p_2^{\beta_2} \cdots p_k^{\beta_k}$$

siendo $p_1 < p_2 < \cdots < p_k$.

Demostración

La descomposición de a y b se sigue directamente del corolario 4.3.5.

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 4.8

Descomponer $a = 270$ y $b = 368$ en factores primos según el lema anterior.

Solución

$$\begin{array}{r|l} 270 & 2 \\ 135 & 3 \\ 45 & 3 \\ 15 & 3 \\ 5 & 5 \\ 1 & \end{array} \quad \Longrightarrow \quad 270 = 2 \cdot 3^3 \cdot 5$$

$$\begin{array}{r|l} 368 & 2 \\ 184 & 2 \\ 92 & 2 \\ 46 & 2 \\ 23 & 23 \\ 1 & \end{array} \quad \Longrightarrow \quad 368 = 2^4 \cdot 23$$

Ahora bastaría escribir,

$$270 = 2^2 \cdot 3^2 \cdot 5 \cdot 23^0$$
$$368 = 2^4 \cdot 3^0 \cdot 5^0 \cdot 23$$

para tener los números en la forma descrita en el lema.

■

4.4.2 Criterio General de Divisibilidad

Sean a y b dos números enteros tales que $|a|, |b| > 1$. Se verifica que a es divisible por b si, y sólo si a tiene, al menos, todos los factores primos de b con exponentes iguales o mayores.

Demostración

Sean a y b dos enteros cualesquiera de valor absoluto mayor que 1. Observemos lo siguiente:

$$\left.\begin{array}{l} |a| > 1 \\ \text{y} \\ |b| > 1 \end{array}\right\} \Longrightarrow \left\{\begin{array}{l} a > 1 \quad \text{ó} \quad a < -1 \\ \text{y} \\ b > 1 \quad \text{ó} \quad b < -1 \end{array}\right.$$

$$\Longrightarrow \left\{\begin{array}{l} 1. \quad a > 1 \quad \text{y} \quad b > 1 \\ \text{ó} \\ 2. \quad a > 1 \quad \text{y} \quad b < -1 \\ \text{ó} \\ 3. \quad a < -1 \quad \text{y} \quad b > 1 \\ \text{ó} \\ 4. \quad a < -1 \quad \text{y} \quad b < -1 \end{array}\right.$$

1. $a > 1$ y $b > 1$.

"Sólo si". En efecto, supongamos que a es divisible por b. Entonces

$$\begin{aligned} a \text{ es divisible por } b &\iff \frac{a}{b} \in \mathbb{Z} \\ &\iff \exists q \in \mathbb{Z} : \frac{a}{b} = q \\ &\iff \exists q \in \mathbb{Z} : a = b \cdot q \end{aligned}$$

Aplicamos el lema anterior (4.4.1) y podemos escribir b y q en la forma,

$$b = p_1^{\beta_1} p_2^{\beta_2} \cdots p_k^{\beta_k}, \text{con } \beta_i \geqslant 0,\ 1 \leqslant i \leqslant k \tag{4.2}$$

$$q = p_1^{\gamma_1} p_2^{\gamma_2} \cdots p_k^{\gamma_k}, \text{con } \gamma_i \geqslant 0,\ 1 \leqslant i \leqslant k$$

donde en las factorizaciones anteriores se verifica:

$\beta_i = 0$, si p_i no está en la descomposición en factores primos de q,

y

$\gamma_i = 0$, si p_i no está en la descomposición en factores primos de b

y, por lo tanto,

$$\left.\begin{array}{l} \beta_i = 0 \text{ en } b \implies \gamma_i \geqslant 1 \text{ en } q \\ \text{y} \\ \gamma_i = 0 \text{ en } q \implies \beta_i \geqslant 1 \text{ en } b \end{array}\right\} \implies \beta_i + \gamma_i \geqslant 1,\ 1 \leqslant i \leqslant k$$

Entonces,

$$a = p_1^{\beta_1+\gamma_1} p_2^{\beta_2+\gamma_2} \cdots p_k^{\beta_k+\gamma_k}, \text{con } \beta_i + \gamma_i \geqslant 1,\ 1 \leqslant i \leqslant k$$

y tomando $\alpha_i = \beta_i + \gamma_i$ para cada $i = 1, 2, \cdots, k$, tendremos

$$a = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}, \text{con } \alpha_i \geqslant 1,\ 1 \leqslant i \leqslant k$$

siendo,

$$\alpha_i = \beta_i + \gamma_i,\ \text{con } \gamma_i \geqslant 0 \Longrightarrow \alpha_i \geqslant \beta_i,\ \text{para } 1 \leqslant i \leqslant k$$

y a tiene, al menos, todos los factores primos de b ya que en la factorización (4.2) puede haber algún(os) β_i iguales a cero.

"Si". En efecto, supongamos que a tiene, al menos, todos los factores primos de b con exponentes iguales o mayores. Entonces, si la descomposición en factores primos de b (4.3.5) es:

$$b = p_1^{\beta_1} p_2^{\beta_2} \cdots p_j^{\beta_j}, \text{con } \beta_i \geqslant 0,\ 1 \leqslant i \leqslant j$$

la factorización de a debe ser:

$$a = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_j^{\alpha_j} \cdot p_{j+1}^{\alpha_{j+1}} \cdots p_k^{\alpha_k}, \text{con} \begin{cases} \alpha_i \geqslant \beta_i,\ \text{si } 1 \leqslant i \leqslant j \\ \text{y} \\ \alpha_i \geqslant 0,\ \text{si } j+1 \leqslant i \leqslant k \end{cases}$$

si ahora completamos la descomposición de b añadiendo, con exponente cero, los factores primos de a que le faltan,

$$b = p_1^{\beta_1} p_2^{\beta_2} \cdots p_j^{\beta_j} \cdot p_{j+1}^{\beta_{j+1}} \cdots p_k^{\beta_k}, \text{con} \begin{cases} \beta_i \geqslant 1,\ \text{si } 1 \leqslant i \leqslant j \\ \text{y} \\ \beta_i = 0,\ \text{si } j+1 \leqslant i \leqslant k \end{cases}$$

y finalmente, dividimos a entre b,

$$\frac{a}{b} = \frac{p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}}{p_1^{\beta_1} p_2^{\beta_2} \cdots p_k^{\beta_k}} = p_1^{\alpha_1-\beta_1} p_2^{\alpha_2-\beta_2} \cdots p_k^{\alpha_k-\beta_k}$$

y como

$$\alpha_i \geqslant \beta_i \Longrightarrow \alpha_i - \beta_i \geqslant 0,\ \text{para } 1 \leqslant i \leqslant k$$

tendremos que $\dfrac{a}{b}$ 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 $-b$.

■

4.4.3 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 4.3.5, a admite una descomposición única,

$$a = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \cdots \cdot p_k^{\alpha_k}$$

siendo $k \geqslant 1$, los p_k primos distintos con $p_1 < p_2 < \cdots < p_k$ y $\alpha_i \geqslant 1$ para $1 \leqslant i \leqslant k$. Pues bien, sea b cualquier entero distinto de cero. Entonces,

$$b \neq 0 \implies \begin{cases} 1.\ b > 0 \\ \text{ó} \\ 2.\ b < 0 \end{cases}$$

Analizaremos, también, ambos casos.

1.1 $b > 0$. Sea, pues, D_a el conjunto formado por los divisores de a. Entonces,

$$\begin{aligned} b \in D_a &\iff b \text{ es divisor de } a \\ &\iff a \text{ es divisible por } b \\ &\iff \begin{cases} a \text{ tiene en su descomposición, al menos, todos los factores} \\ \text{primos de } b \text{ con exponentes iguales o mayores.} \end{cases} \\ &\iff \begin{cases} b \text{ tiene en su descomposición, a lo sumo, todos los factores} \\ \text{primos de } a \text{ con exponentes iguales o menores.} \end{cases} \\ &\iff b = p_1^{\beta_1} \cdot p_2^{\beta_2} \cdot \cdots \cdot p_k^{\beta_k}, \text{con } 0 \leqslant \beta_i \leqslant \alpha_i,\ 1 \leqslant i \leqslant k \end{aligned}$$

y como b es entero, los β_i han de ser no negativos. Por tanto,

$$D_a = \left\{ p_1^{\beta_1} \cdot p_2^{\beta_2} \cdot \cdots \cdot p_k^{\beta_k}, \text{con } 0 \leqslant \beta_i \leqslant \alpha_i,\ 1 \leqslant i \leqslant k \right\}$$

será el conjunto de los divisores positivos de a.

1.2 $b < 0$. En este caso $-b > 0$, aplicamos a $-b$ lo que acabamos de hacer y,

$$D_a = \left\{-p_1^{\beta_1} \cdot p_2^{\beta_2} \cdot \cdots\cdots \cdot p_k^{\beta_k}, \text{con } 0 \leqslant \beta_i \leqslant \alpha_i,\ 1 \leqslant i \leqslant k\right\}$$

es el conjunto formado por los divisores negativos de a.

El conjunto de todos los divisores de a será, por tanto,

$$D_a = \left\{\pm p_1^{\beta_1} \cdot p_2^{\beta_2} \cdot \cdots\cdots \cdot p_k^{\beta_k}, \text{con } 0 \leqslant \beta_i \leqslant \alpha_i,\ 1 \leqslant i \leqslant k\right\}$$

2. $a < -1$. En este caso,

$$a < -1 \Longrightarrow -a > 1$$

aplicamos todo lo que hicimos en el caso anterior a $-a$ y tendremos:

$$D_{-a} = \left\{\pm p_1^{\beta_1} \cdot p_2^{\beta_2} \cdot \cdots\cdots \cdot p_k^{\beta_k}, \text{con } 0 \leqslant \beta_i \leqslant \alpha_i,\ 1 \leqslant i \leqslant k\right\}$$

De 1. y 2. se sigue que:

$$D_{|a|} = \left\{\pm p_1^{\beta_1} \cdot p_2^{\beta_2} \cdot \cdots\cdots \cdot p_k^{\beta_k}, \text{con } 0 \leqslant \beta_i \leqslant \alpha_i,\ 1 \leqslant i \leqslant k\right\}$$

■

4.4.4 Método para la obtención de todos los divisores de un número

Expondremos un método basado en el apartado anterior para calcular todos los divisores de cualquier entero de valor absoluto mayor que 1.

Demostración

Sea a un entero tal que $|a| > 1$. Según hemos visto en el apartado anterior,

$$D_{|a|} = \left\{\pm p_1^{\beta_1} \cdot p_2^{\beta_2} \cdot \cdots\cdots \cdot p_k^{\beta_k}, \text{con } 0 \leqslant \beta_i \leqslant \alpha_i,\ 1 \leqslant i \leqslant k\right\}$$

Calcularemos, únicamente, los divisores positivos ya que sólo hay que cambiar el signo a éstos para obtener los negativos. Haremos una tabla con todos los divisores procediendo de la forma siguiente:

- Divisores de la forma $p_1^{\beta_1} \cdot p_2^0 \cdot p_3^0 \cdot \cdots\cdots \cdot p_k^0$ con $0 \leqslant \beta_1 \leqslant \alpha_1$. Escribimos todas las potencias de p_1.

p_1^0	p_1	p_1^2	$\cdots\cdots$	$p_1^{\alpha_1}$

- Divisores de la forma $p_1^{\beta_1} \cdot p_2^{\beta_2} \cdot p_3^0 \cdot \cdots\cdots \cdot p_k^0$ con $0 \leqslant \beta_1 \leqslant \alpha_1$ y $0 \leqslant \beta_2 \leqslant \alpha_2$. Bastaría multiplicar cada uno de los anteriores por todas las potencias de p_2 a partir de p_2^1.

	p_1^0	p_1	p_1^2	$\cdots\cdots$	$p_1^{\alpha_1}$
$\times p_2$	$p_1^0 p_2$	$p_1 p_2$	$p_1^2 p_2$	$\cdots\cdots$	$p_1^{\alpha_1} p_2$
$\times p_2^2$	$p_1^0 p_2^2$	$p_1 p_2^2$	$p_1^2 p_2^2$	$\cdots\cdots$	$p_1^{\alpha_1} p_2^2$
$\times p_2^3$	$p_1^0 p_2^3$	$p_1 p_2^3$	$p_1^2 p_2^3$	$\cdots\cdots$	$p_1^{\alpha_1} p_2^3$
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots \quad \vdots$	$\vdots$
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots \quad \vdots$	$\vdots$
$\times p_2^{\alpha_2}$	$p_1^0 p_2^{\alpha_2}$	$p_1 p_2^{\alpha_2}$	$p_1^2 p_2^{\alpha_2}$	$\cdots\cdots$	$p_1^{\alpha_1} p_2^{\alpha_2}$

⁕ Divisores de la forma $p_1^{\beta_1} \cdot p_2^{\beta_2} \cdot p_3^{\beta_3} \cdot p_4^0 \cdot \cdots \cdot p_k^0$ con

$$0 \leqslant \beta_1 \leqslant \alpha_1,\ 0 \leqslant \beta_2 \leqslant \alpha_2 \text{ y } 0 \leqslant \beta_3 \leqslant \alpha_3.$$

Multiplicamos cada uno de los anteriores por todas las potencias de p_3 desde p_3^1.

	p_1^0	p_1	p_1^2	$\cdots\cdots$	$p_1^{\alpha_1}$
$\times p_2$	$p_1^0 p_2$	$p_1 p_2$	$p_1^2 p_2$	$\cdots\cdots$	$p_1^{\alpha_1} p_2$
$\times p_2^2$	$p_1^0 p_2^2$	$p_1 p_2^2$	$p_1^2 p_2^2$	$\cdots\cdots$	$p_1^{\alpha_1} p_2^2$
$\times p_2^3$	$p_1^0 p_2^3$	$p_1 p_2^3$	$p_1^2 p_2^3$	$\cdots\cdots$	$p_1^{\alpha_1} p_2^3$
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots \quad \vdots$	$\vdots$
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots \quad \vdots$	$\vdots$
$\times p_2^{\alpha_2}$	$p_1^0 p_2^{\alpha_2}$	$p_1 p_2^{\alpha_2}$	$p_1^2 p_2^{\alpha_2}$	$\cdots\cdots$	$p_1^{\alpha_1} p_2^{\alpha_2}$
$\times p_3$	$p_1^0 p_3$	$p_1 p_3$	$p_1^2 p_3$	$\cdots\cdots$	$p_1^{\alpha_1} p_3$
	$p_1^0 p_2 p_3$	$p_1 p_2 p_3$	$p_1^2 p_2 p_3$	$\cdots\cdots$	$p_1^{\alpha_1} p_2 p_3$
	$p_1^0 p_2^2 p_3$	$p_1 p_2^2 p_3$	$p_1^2 p_2^2 p_3$	$\cdots\cdots$	$p_1^{\alpha_1} p_2^2 p_3$
	$p_1^0 p_2^3 p_3$	$p_1 p_2^3 p_3$	$p_1^2 p_2^3 p_3$	$\cdots\cdots$	$p_1^{\alpha_1} p_2^3 p_3$
	$\vdots$	$\vdots$	$\vdots$	$\vdots \quad \vdots$	$\vdots$
	$\vdots$	$\vdots$	$\vdots$	$\vdots \quad \vdots$	$\vdots$
	$p_1^0 p_2^{\alpha_2} p_3$	$p_1 p_2^{\alpha_2} p_3$	$p_1^2 p_2^{\alpha_2} p_3$	$\cdots\cdots$	$p_1^{\alpha_1} p_2^{\alpha_2} p_3$
$\times p_3^2$	$p_1^0 p_3^2$	$p_1 p_3^2$	$p_1^2 p_3^2$	$\cdots\cdots$	$p_1^{\alpha_1} p_3^2$
	$p_1^0 p_2 p_3^2$	$p_1 p_2 p_3^2$	$p_1^2 p_2 p_3^2$	$\cdots\cdots$	$p_1^{\alpha_1} p_2 p_3^2$
	$p_1^0 p_2^2 p_3^2$	$p_1 p_2^2 p_3^2$	$p_1^2 p_2^2 p_3^2$	$\cdots\cdots$	$p_1^{\alpha_1} p_2^2 p_3^2$
	$p_1^0 p_2^3 p_3^2$	$p_1 p_2^3 p_3^2$	$p_1^2 p_2^3 p_3^2$	$\cdots\cdots$	$p_1^{\alpha_1} p_2^3 p_3^2$
	$\vdots$	$\vdots$	$\vdots$	$\vdots \quad \vdots$	$\vdots$
	$\vdots$	$\vdots$	$\vdots$	$\vdots \quad \vdots$	$\vdots$
	$p_1^0 p_2^{\alpha_2} p_3^2$	$p_1 p_2^{\alpha_2} p_3^2$	$p_1^2 p_2^{\alpha_2} p_3^2$	$\cdots\cdots$	$p_1^{\alpha_1} p_2^{\alpha_2} p_3^2$
	$\vdots$	$\vdots$	$\vdots$	$\vdots \quad \vdots$	$\vdots$
	$\vdots$	$\vdots$	$\vdots$	$\vdots \quad \vdots$	$\vdots$
$\times p_3^{\alpha_3}$	$p_1^0 p_3^{\alpha_3}$	$p_1 p_3^{\alpha_3}$	$p_1^2 p_3^{\alpha_3}$	$\cdots\cdots$	$p_1^{\alpha_1} p_3^{\alpha_3}$
	$p_1^0 p_2 p_3^{\alpha_3}$	$p_1 p_2 p_3^{\alpha_3}$	$p_1^2 p_2 p_3^{\alpha_3}$	$\cdots\cdots$	$p_1^{\alpha_1} p_2 p_3^{\alpha_3}$
	$p_1^0 p_2^2 p_3^{\alpha_3}$	$p_1 p_2^2 p_3^{\alpha_3}$	$p_1^2 p_2^2 p_3^{\alpha_3}$	$\cdots\cdots$	$p_1^{\alpha_1} p_2^2 p_3^{\alpha_3}$
	$p_1^0 p_2^3 p_3^{\alpha_3}$	$p_1 p_2^3 p_3^{\alpha_3}$	$p_1^2 p_2^3 p_3^{\alpha_3}$	$\cdots\cdots$	$p_1^{\alpha_1} p_2^3 p_3^{\alpha_3}$
	$\vdots$	$\vdots$	$\vdots$	$\vdots \quad \vdots$	$\vdots$
	$\vdots$	$\vdots$	$\vdots$	$\vdots \quad \vdots$	$\vdots$
	$p_1^0 p_2^{\alpha_2} p_3^{\alpha_3}$	$p_1 p_2^{\alpha_2} p_3^{\alpha_3}$	$p_1^2 p_2^{\alpha_2} p_3^{\alpha_3}$	$\cdots\cdots$	$p_1^{\alpha_1} p_2^{\alpha_2} p_3^{\alpha_3}$

⁕ Así sucesivamente hasta obtener todos los divisores de la forma

$$p_1^{\beta_1} \cdot p_2^{\beta_2} \cdot p_3^{\beta_3} \cdots p_k^{\beta_k}$$

siendo,

$$\begin{aligned} &0 \leqslant \beta_1 \leqslant \alpha_1 \\ &0 \leqslant \beta_2 \leqslant \alpha_2 \\ &0 \leqslant \beta_3 \leqslant \alpha_3 \\ &\cdots\cdots\cdots \\ &0 \leqslant \beta_k \leqslant \alpha_k \end{aligned}$$

■

Ejemplo 4.9

Calcular todos los divisores de 604800.

Solución

Descomponemos el número dado en factores primos.

$$\begin{array}{r|l} 604800 & 2 \\ 302400 & 2 \\ 151200 & 2 \\ 75600 & 2 \\ 37800 & 2 \\ 18900 & 2 \\ 9450 & 2 \\ 4725 & 3 \\ 1575 & 3 \\ 525 & 3 \\ 175 & 5 \\ 35 & 5 \\ 7 & 7 \\ 1 & \end{array} \quad \Longrightarrow \quad 604800 = 2^7 \cdot 3^3 \cdot 5^2 \cdot 7$$

Hacemos una tabla con todos los divisores de 604800 utilizando el método visto en el apartado anterior.

	1	2	4	8	16	32	64	128
$\times 3$	3	6	12	24	48	96	192	384
$\times 3^2$	9	18	36	72	144	288	576	1152
$\times 3^3$	27	54	108	216	432	864	1728	3456
$\times 5$	5	10	20	40	80	160	320	640
	15	30	60	120	240	480	960	1920
	45	90	180	360	720	1440	2880	5760
	135	270	540	1080	2160	4320	8640	17280
$\times 5^2$	25	50	100	200	400	800	1600	3200
	75	150	300	600	1200	2400	4800	9600
	225	450	900	1800	3600	7200	14400	28800
	675	1350	2700	5400	10800	21600	43200	86400
$\times 7$	7	14	28	56	112	224	448	896
	21	42	84	168	336	672	1344	2688
	63	126	252	504	1008	2016	4032	8064
	189	378	756	1512	3024	6048	12096	24192
	35	70	140	280	560	1120	2240	4480
	105	210	420	840	1680	3360	6720	13440
	315	630	1260	2520	5040	10080	20160	40320
	945	1890	3780	7560	15120	30240	60480	120960
	175	350	700	1400	2800	5600	11200	22400
	525	1050	2100	4200	8400	16800	33600	67200
	1575	3150	6300	12600	25200	50400	100800	201600
	4725	9450	18900	37800	75600	151200	302400	604800

4.4.5 Número de divisores de un número compuesto

Si a es un entero de valor absoluto mayor que 1 y $a = p_1^{\alpha_1} p_2^{\alpha_2} \cdot \cdots \cdot p_k^{\alpha_k}$ es su descomposición en factores primos, entonces el número de divisores de a es

$$N_a = (\alpha_1 + 1)(\alpha_2 + 1) \cdot \cdots \cdot (\alpha_k + 1)$$

Demostración

En efecto, según vimos en 4.4.3, 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

$$\begin{array}{|c|} \hline p_1^0 \\ \hline p_1^1 \\ \hline p_1^2 \\ \hline \vdots \\ \hline p_1^{\alpha_1} \\ \hline \end{array} \Bigg\} (\alpha_1 + 1)$$

  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:

$$\begin{array}{|c|c|} \hline p_1^0 & p_1^0 \cdot p_2^0 \\ \hline & p_1^0 \cdot p_2^1 \\ \hline & p_1^0 \cdot p_2^2 \\ \hline & \vdots \\ \hline & p_1^0 \cdot p_2^{\alpha_2} \\ \hline \end{array} \Bigg\} (\alpha_2 + 1)$$

$$\begin{array}{|c|c|} \hline p_1^1 & p_1^1 \cdot p_2^0 \\ \hline & p_1^1 \cdot p_2^1 \\ \hline & p_1^1 \cdot p_2^2 \\ \hline & \vdots \\ \hline & p_1^1 \cdot p_2^{\alpha_2} \\ \hline \end{array} \Bigg\} (\alpha_2 + 1)$$

$$\vdots$$

$$\begin{array}{|c|c|} \hline p_1^{\alpha_1} & p_1^{\alpha_1} \cdot p_2^0 \\ \hline & p_1^{\alpha_1} \cdot p_2^1 \\ \hline & p_1^{\alpha_1} \cdot p_2^2 \\ \hline & \vdots \\ \hline & p_1^{\alpha_1} \cdot p_2^{\alpha_2} \\ \hline \end{array} \Bigg\} (\alpha_2 + 1)$$

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 4.10

¿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.

■

4.4.6 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 descomposición en factores primos, entonces la suma de todos los divisores de a es

$$S_a = \frac{p_1^{\alpha_1+1}-1}{p_1-1} \cdot \frac{p_2^{\alpha_2+1}-1}{p_2-1} \cdot \frac{p_3^{\alpha_3+1}-1}{p_3-1} \cdot \cdots \cdot \frac{p_k^{\alpha_k+1}-1}{p_k-1}$$

Demostración

En efecto, según vimos en 4.4.3, 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 $p_1, p_2, p_3, \cdots, p_k$.

■

4.5 Reglas para el cálculo del máximo común divisor y el mínimo común múltiplo de dos números

Estableceremos un método alternativo al algoritmo de Euclides para el cálculo del máximo común divisor de dos números. Está basado en el Teorema Fundamental de la Aritmética.

4.5.1 Máximo común divisor

El máximo común divisor de dos números enteros es igual al producto de los factores primos comunes a ambos, elevados a los menores exponentes con que aparezcan en sus respectivas descomposiciones en factores primos.

Demostración

Sean a y b enteros cualesquiera. Recordemos que la relación de orden parcial de divisibilidad es:

$$a \preccurlyeq b \iff a \text{ es divisor de } b$$

Pues bien, por el corolario 4.3.5, tanto a como b admiten una descomposición única en factores primos y según vimos en 4.4.3,

$$a \text{ es divisor de } b \iff \left\{ \begin{array}{l} a \text{ tiene en su descomposición, a lo sumo, todos los factores} \\ \text{primos de } b \text{ con exponentes iguales o menores.} \end{array} \right.$$

Ahora bien, por el lema 4.4.1, 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 descomposición de b no aparece en la de a y $\beta_i = 0$ si el p_i de la descomposición de a no aparece en la de b. Podemos pues, escribir de nuevo la relación de divisibilidad en estos términos,

$$\begin{aligned} a \preccurlyeq b &\iff a \text{ es divisor de } b \\ &\iff \left\{ \begin{array}{l} a \text{ tiene en su factorización todos los factores} \\ \text{primos de } b \text{ con exponentes iguales o menores.} \end{array} \right. \\ &\iff \alpha_i \leqslant \beta_i, \forall i, 1 \leqslant i \leqslant k \end{aligned}$$

Supongamos que a y b son dos enteros cualesquiera de valor absoluto mayor que 1.

- Si a divide a b, entonces m.c.d.$(a, b) = a$.
- Si b divide a a, entonces m.c.d.$(a, b) = b$.

Supondremos, por tanto, que a no divide a b ni b divide a a.

Por definición de máximo común divisor,

$$\text{m.c.d.}(a, b) = \inf\{a, b\} = \max\left(C_{\inf}\left(\{a, b\}\right)\right).$$

siendo $C_{\inf}\left(\{a, b\}\right)$ el conjunto de las cotas inferiores del conjunto $\{a, b\}$ ordenado por la relación de orden parcial de divisibilidad.

Pues bien, sea c cualquiera de $\mathbb{Z}^+$. Aplicando el lema 4.4.1, podemos escribir c en la forma:

$$c = p_1^{\gamma_1} p_2^{\gamma_2} \cdot \cdots \cdot p_k^{\gamma_k}$$

Pues bien,

$$\begin{aligned} c \in C_{\inf}(\{a,b\}) &\iff c \preccurlyeq x, \forall x \in \{a,b\} \\ &\iff \begin{cases} c \preccurlyeq a \\ \text{y} \\ c \preccurlyeq b \end{cases} \\ &\iff \begin{cases} \gamma_i \leqslant \alpha_i,\ 1 \leqslant i \leqslant k \\ \text{y} \\ \gamma_i \leqslant \beta_i,\ 1 \leqslant i \leqslant k \end{cases} \\ &\iff \gamma_i \leqslant \min\{\alpha_i, \beta_i\},\ 1 \leqslant i \leqslant k \end{aligned}$$

Por lo tanto,

$$C_{\inf}(\{a,b\}) = \{p_1^{\gamma_1} p_2^{\gamma_2} \cdot \cdots \cdot p_k^{\gamma_k} : \gamma_i \leqslant \min\{\alpha_i, \beta_i\},\ 1 \leqslant i \leqslant k\}.$$

Entonces,

$$\begin{aligned} \text{m.c.d.}(a,b) &= \inf(\{a,b\}) \\ &= \max(C_{\inf}(\{a,b\})) \\ &= \max\{p_1^{\gamma_1} p_2^{\gamma_2} \cdot \cdots \cdot p_k^{\gamma_k} : \gamma_i \leqslant \min\{\alpha_i, \beta_i\},\ 1 \leqslant i \leqslant k\} \\ &= p_1^{\min\{\alpha_1,\beta_1\}} p_2^{\min\{\alpha_1,\beta_2\}} \cdot \cdots \cdot p_k^{\min\{\alpha_k,\beta_k\}} \end{aligned}$$

Ahora, para cada i entre 1 y k, puede ocurrir lo siguiente:

$$\begin{aligned} \min\{\alpha_i, \beta_i\} = 0 &\implies \begin{cases} \alpha_i = 0 \\ \text{ó} \\ \beta_i = 0 \end{cases} \\ &\implies \begin{cases} p_i \text{ no está en la descomposición} \\ \text{en factores primos de } a. \\ \text{ó} \\ p_i \text{ no está en la descomposición} \\ \text{en factores primos de } b. \end{cases} \\ &\implies \text{El factor primo } p_i \text{ no es común a } a \text{ y a } b \end{aligned}$$

ó

$$\begin{aligned} \min\{\alpha_i, \beta_i\} \neq 0 &\implies \begin{cases} \alpha_i \neq 0 \\ \text{y} \\ \beta_i \neq 0 \end{cases} \\ &\implies \begin{cases} p_i \text{ está en la descomposición en factores primos de } a. \\ \text{y} \\ p_i \text{ está en la descomposición en factores primos de } b. \end{cases} \\ &\implies \text{El factor primo } p_i \text{ es común a } a \text{ y a } b \end{aligned}$$

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 4.11

Calcular el máximo común divisor de 1548 y 18900.

Solución

Lo calcularemos siguiendo los pasos del apartado anterior.

Descomponemos ambos números en factores primos.

$$\begin{array}{r|l} 1584 & 2 \\ 792 & 2 \\ 396 & 2 \\ 198 & 2 \\ 99 & 3 \\ 33 & 3 \\ 11 & 11 \\ 1 & \end{array} \quad \Longrightarrow \quad 1584 = 2^4 \cdot 3^2 \cdot 11$$

$$\begin{array}{r|l} 18900 & 2 \\ 9450 & 2 \\ 4725 & 3 \\ 1575 & 3 \\ 525 & 3 \\ 175 & 5 \\ 35 & 5 \\ 7 & 7 \\ 1 & \end{array} \quad \Longrightarrow \quad 18900 = 2^2 \cdot 3^3 \cdot 5^2 \cdot 7$$

Completamos la descomposición en factores primos de los dos números, añadiendo a cada uno de ellos los factores primos que no tenga del otro, con exponente cero (lema 4.4.1).

$$\begin{aligned} 1584 &= 2^4 \cdot 3^2 \cdot 5^0 \cdot 7^0 \cdot 11 \\ 18900 &= 2^2 \cdot 3^3 \cdot 5^2 \cdot 7 \cdot 11^0 \end{aligned}$$

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).

■

4.5.2 Mínimo común múltiplo

El mínimo común múltiplo de dos números enteros es igual al producto de los factores primos comunes y no comunes a ambos, elevados a los mayores exponentes con que aparezcan en sus respectivas descomposiciones en factores primos.

Demostración

Sean a y b son dos enteros cualesquiera de valor absoluto mayor que 1.

Al igual que en el apartado anterior, el lema 4.4.1 nos permite 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 descomposición de b no aparece en la de a y $\beta_i = 0$ si el p_i de la descomposición de a no aparece en la de b. Podemos pues, escribir de nuevo la relación de divisibilidad en estos términos,

$$\begin{aligned} a \preccurlyeq b &\iff a \text{ es divisor de } b \\ &\iff \left\{ \begin{array}{l} a \text{ tiene en su factorización todos los factores} \\ \text{primos de } b \text{ con exponentes iguales o menores.} \end{array} \right. \\ &\iff \alpha_i \leqslant \beta_i, \forall i, 1 \leqslant i \leqslant k \end{aligned}$$

- Si a divide a b, entonces m.c.m.$(a, b) = b$.
- Si b divide a a, entonces m.c.m.$(a, b) = a$.

Supondremos, por tanto, que a no divide a b ni b divide a a.

Por definición de mínimo común múltiplo,

$$\text{m.c.m.}(a, b) = \sup\{a, b\} = \min\left(C_{\sup}\left(\{a, b\}\right)\right).$$

siendo $C_{\sup}\left(\{a, b\}\right)$ el conjunto de las cotas superiores del conjunto $\{a, b\}$ ordenado por la relación de orden parcial de divisibilidad.

Sea s cualquiera de $\mathbb{Z}^+$. Aplicando el lema 4.4.1, podemos escribir s en la forma:

$$s = p_1^{\gamma_1} p_2^{\gamma_2} \cdot \cdots \cdot p_k^{\gamma_k}$$

Pues bien,

$$\begin{aligned} s \in C_{\sup}\left(\{a, b\}\right) &\iff x \preccurlyeq s, \forall x \in \{a, b\} \\ &\iff \left\{ \begin{array}{l} a \preccurlyeq s \\ \text{y} \\ b \preccurlyeq s \end{array} \right. \\ &\iff \left\{ \begin{array}{l} \alpha_i \leqslant \gamma_i,\ 1 \leqslant i \leqslant k \\ \text{y} \\ \beta_i \leqslant \gamma_i,\ 1 \leqslant i \leqslant k \end{array} \right. \\ &\iff \gamma_i \geqslant \max\{\alpha_i, \beta_i\},\ 1 \leqslant i \leqslant k \end{aligned}$$

Luego,

$$C_{\sup}\left(\{a, b\}\right) = \{p_1^{\gamma_1} p_2^{\gamma_2} \cdot \cdots \cdot p_k^{\gamma_k} : \gamma_i \geqslant \max\{\alpha_i, \beta_i\},\ 1 \leqslant i \leqslant k\}$$

Entonces,

$$\begin{aligned} \text{m.c.m.}(a, b) &= \min\left(C_{\sup}\left(\{a, b\}\right)\right) \\ &= \min\{p_1^{\gamma_1} p_2^{\gamma_2} \cdot \cdots \cdot p_k^{\gamma_k} : \gamma_i \geqslant \max\{\alpha_i, \beta_i\},\ 1 \leqslant i \leqslant k\} \\ &= p_1^{\max\{\alpha_1, \beta_1\}} p_2^{\max\{\alpha_1, \beta_2\}} \cdot \cdots \cdot p_k^{\max\{\alpha_k, \beta_k\}} \end{aligned}$$

Ahora, para cada i entre 1 y k, puede ocurrir lo siguiente:

$$\left.\begin{array}{l}\alpha_i = 0\\ \text{y}\\ \beta_i \neq 0\end{array}\right\} \Longrightarrow \text{El factor primo } p_i \text{ no es común a } a \text{ y a } b \text{ y } \max\{\alpha_i, \beta_i\} = \beta_i$$

ó

$$\left.\begin{array}{l}\alpha_i \neq 0\\ \text{y}\\ \beta_i = 0\end{array}\right\} \Longrightarrow \text{El factor primo } p_i \text{ no es común a } a \text{ y a } b \text{ y } \max\{\alpha_i, \beta_i\} = \alpha_i$$

ó

$$\left.\begin{array}{l}\alpha_i \neq 0\\ \text{y}\\ \beta_i \neq 0\end{array}\right\} \Longrightarrow \text{El factor primo } p_i \text{ es común a } a \text{ y a } b$$

Por lo tanto, el mínimo común múltiplo de dos números es igual al productos de los factores primos comunes y no comunes a ambos elevados a sus mayores exponentes.

■

Ejemplo 4.12

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 4.4.1).

$$\begin{aligned} 1584 &= 2^4 \cdot 3^2 \cdot 5^0 \cdot 7^0 \cdot 11 \\ 18900 &= 2^2 \cdot 3^3 \cdot 5^2 \cdot 7 \cdot 11^0 \end{aligned}$$

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 4.13

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 4.3.5, 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 4.4.2 tanto a como b deberán tener en su factorización, al menos, todos los factores primos de 18 con exponentes iguales o mayores. Pues bien, como $18 = 2 \cdot 3^2$,

$$\text{m.c.d.}(a,b) = 18 \implies \begin{cases} 18 \,|a \\ \text{y} \\ 18 \,|b \end{cases} \implies \begin{cases} 2 \cdot 3^2 \,|a \\ \text{y} \\ 2 \cdot 3^2 \,|b \end{cases} \implies \begin{cases} \begin{cases} p_1 = 2 \text{ y } \alpha_1 \geqslant 1 \\ \text{y} \\ p_2 = 3 \text{ y } \alpha_2 \geqslant 2 \end{cases} \\ \text{y} \\ \begin{cases} q_1 = 2 \text{ y } \beta_1 \geqslant 1 \\ \text{y} \\ q_2 = 3 \text{ y } \beta_2 \geqslant 2 \end{cases} \end{cases}$$

Por otra parte, el número de divisores de a es 21. Entonces, utilizando el resultado de 4.4.5,

$$\begin{aligned} N_a = 21 &\implies (\alpha_1 + 1)(\alpha_2 + 1)(\alpha_3 + 1) \cdot \cdots \cdot (\alpha_k + 1) = 21 \\ &\implies \alpha_i + 1 \text{ es divisor de } 21, \text{ para } 1 \leqslant i \leqslant k \\ &\quad \left[\ 21 = 3 \cdot 7 \implies D_{21} = \{1, 3, 7, 21\}\ \right] \\ &\implies \alpha_i + 1 \in \{1, 3, 7, 21\},\ 1 \leqslant i \leqslant k \end{aligned}$$

Ahora bien,

$$\left.\begin{array}{l} \alpha_1 \geqslant 1 \implies \alpha_1 + 1 \geqslant 2 \\ \text{y} \\ \alpha_2 \geqslant 2 \implies \alpha_2 + 1 \geqslant 3 \\ \text{y} \\ \alpha_i + 1 \in \{1, 3, 7, 21\},\ 1 \leqslant i \leqslant k \end{array}\right\} \implies \begin{cases} \alpha_1 + 1 \in \{3, 7, 21\} \\ \text{y} \\ \alpha_2 + 1 \in \{3, 7, 21\} \\ \text{y} \\ \alpha_i + 1 \in \{1, 3, 7, 21\},\ 3 \leqslant i \leqslant k \end{cases}$$

Además,

$$\alpha_i + 1 \neq 21,\ 1 \leqslant i \leqslant k$$

ya que si alguno de ellos fuera igual a 21, todos los demás deberían ser iguales a 1 y eso es imposible porque $\alpha_1 + 1$ y $\alpha_2 + 1$ son, ambos, distintos de 1. Entonces,

$$\left.\begin{array}{l} \alpha_1 + 1 \in \{3, 7, 21\} \\ \text{y} \\ \alpha_2 + 1 \in \{3, 7, 21\} \\ \text{y} \\ \alpha_i + 1 \in \{1, 3, 7, 21\}\ \ 3 \leqslant i \leqslant k \\ \text{y} \\ \alpha_i + 1 \neq 21,\ 1 \leqslant i \leqslant k \end{array}\right\} \implies \left\{\begin{array}{l} \alpha_1 + 1 \in \{3, 7\} \\ \text{y} \\ \alpha_2 + 1 \in \{3, 7\} \\ \text{y} \\ \alpha_i + 1 \in \{1, 3, 7\}\ \ 3 \leqslant i \leqslant k \end{array}\right.$$

Pues bien,

$$\alpha_1 + 1 \in \{3, 7\} \implies \left\{\begin{array}{l} \alpha_1 + 1 = 3 \\ \text{ó} \\ \alpha_1 + 1 = 7 \end{array}\right.$$

Estudiemos ambos casos:

$$\left.\begin{array}{l} \alpha_1 + 1 = 3 \\ \text{y} \\ (\alpha_1 + 1)(\alpha_2 + 1)(\alpha_3 + 1) \cdots\cdots (\alpha_k + 1) = 21 \end{array}\right\} \implies \alpha_i + 1 \neq 3,\ 2 \leqslant i \leqslant k$$

y

$$\left.\begin{array}{l} \alpha_i + 1 \neq 3,\ 2 \leqslant i \leqslant k \\ \text{y} \\ \alpha_2 + 1 \in \{3, 7\} \\ \text{y} \\ \alpha_i + 1 \in \{1, 3, 7\},\ 3 \leqslant i \leqslant k \end{array}\right\} \implies \left\{\begin{array}{l} \alpha_2 + 1 = 7 \\ \text{y} \\ \alpha_i + 1 \in \{1, 7\},\ 3 \leqslant i \leqslant k \end{array}\right.$$

y

$$\left.\begin{array}{l} \alpha_2 + 1 = 7 \\ \text{y} \\ \alpha_i + 1 \in \{1, 7\},\ 3 \leqslant i \leqslant k \\ \text{y} \\ (\alpha_1 + 1)(\alpha_2 + 1)(\alpha_3 + 1) \cdots\cdots (\alpha_k + 1) = 21 \end{array}\right\} \implies \alpha_i + 1 = 1,\ 3 \leqslant i \leqslant k$$

Por lo tanto, en este caso, tenemos:

$$\begin{array}{l} \alpha_1 + 1 = 3 \\ \text{y} \\ \alpha_2 + 1 = 7 \\ \text{y} \\ \alpha_i + 1 = 1,\ 3 \leqslant i \leqslant k \end{array}$$

Veamos ahora que ocurre si $\alpha_1 + 1 = 7$.

$$\left.\begin{array}{l} \alpha_1 + 1 = 7 \\ \text{y} \\ (\alpha_1+1)(\alpha_2+1)(\alpha_3+1)\cdots\cdots(\alpha_k+1) = 21 \end{array}\right\} \implies \alpha_i + 1 \neq 7,\ 2 \leqslant i \leqslant k$$

y

$$\left.\begin{array}{l} \alpha_i + 1 \neq 7,\ 2 \leqslant i \leqslant k \\ \text{y} \\ \alpha_2 + 1 \in \{3, 7\} \\ \text{y} \\ \alpha_i + 1 \in \{1, 3, 7\},\ 3 \leqslant i \leqslant k \end{array}\right\} \implies \left\{\begin{array}{l} \alpha_2 + 1 = 3 \\ \text{y} \\ \alpha_i + 1 \in \{1, 3\},\ 3 \leqslant i \leqslant k \end{array}\right.$$

y

$$\left.\begin{array}{l} \alpha_2 + 1 = 3 \\ \text{y} \\ \alpha_i + 1 \in \{1, 3\},\ 3 \leqslant i \leqslant k \\ \text{y} \\ (\alpha_1+1)(\alpha_2+1)(\alpha_3+1)\cdots\cdots(\alpha_k+1) = 21 \end{array}\right\} \implies \alpha_i + 1 = 1,\ 3 \leqslant i \leqslant k$$

Luego,

$$\begin{array}{l} \alpha_1 + 1 = 7 \\ \text{y} \\ \alpha_2 + 1 = 3 \\ \text{y} \\ \alpha_i + 1 = 1,\ 3 \leqslant i \leqslant k \end{array}$$

Reuniendo ambos casos:

$$\left.\begin{array}{l} \alpha_1 + 1 = 3 \\ \text{y} \\ \alpha_2 + 1 = 7 \\ \text{y} \\ \alpha_i + 1 = 1,\ 3 \leqslant i \leqslant k \end{array}\right\} \implies \left.\begin{array}{l} \alpha_1 = 2 \\ \text{y} \\ \alpha_2 = 6 \\ \text{y} \\ \alpha_i = 0,\ 3 \leqslant i \leqslant k \end{array}\right\} \implies a = 2^2 \cdot 3^6$$

ó

$$\left.\begin{array}{l} \alpha_1 + 1 = 7 \\ \text{y} \\ \alpha_2 + 1 = 3 \\ \text{y} \\ \alpha_i + 1 = 1,\ 3 \leqslant i \leqslant k \end{array}\right\} \implies \left.\begin{array}{l} \alpha_1 = 6 \\ \text{y} \\ \alpha_2 = 2 \\ \text{y} \\ \alpha_i = 0,\ 3 \leqslant i \leqslant k \end{array}\right\} \implies a = 2^6 \cdot 3^2$$

Un razonamiento análogo puede hacerse para b. En efecto, el número de divisores de b es 10, luego

$$\begin{array}{rcl} N_b = 10 & \implies & (\beta_1+1)(\beta_2+1)(\beta_3+1)\cdots\cdots(\beta_m+1) = 10 \\ & \implies & \beta_j + 1 \text{ es divisor de 10, para } 1 \leqslant j \leqslant m \\ & & \left[\ 10 = 2 \cdot 5 \implies D_{10} = \{1, 2, 5, 10\}\ \right] \\ & \implies & \beta_j + 1 \in \{1, 2, 5, 10\},\ 1 \leqslant j \leqslant m \end{array}$$

Ahora bien,

$$\left.\begin{array}{l} \beta_1 \geqslant 1 \implies \beta_1 + 1 \geqslant 2 \\ \text{y} \\ \beta_2 \geqslant 2 \implies \beta_2 + 1 \geqslant 3 \\ \text{y} \\ \beta_j + 1 \in \{1, 2, 5, 10\} \;\; 1 \leqslant j \leqslant m \end{array}\right\} \implies \left\{\begin{array}{l} \beta_1 + 1 \in \{2, 5, 10\} \\ \text{y} \\ \beta_2 + 1 \in \{5, 10\} \\ \text{y} \\ \beta_j + 1 \in \{1, 2, 5, 10\}, \;\; 3 \leqslant j \leqslant m \end{array}\right.$$

además,

$$\beta_j + 1 \neq 10, \;\; 1 \leqslant j \leqslant m.$$

En efecto, si alguno de ellos fuera igual a 10, todos los demás serían iguales a 1 y eso es imposible ya que

$\beta_1 + 1$ y $\beta_2 + 1$ son, ambos, distintos de 1. Entonces,

$$\left.\begin{array}{l} \beta_1 + 1 \in \{2, 5, 10\} \\ \text{y} \\ \beta_2 + 1 \in \{5, 10\} \\ \text{y} \\ \beta_j + 1 \in \{1, 2, 5, 10\}\,,\ 3 \leqslant j \leqslant m \\ \text{y} \\ \beta_j + 1 \neq 10,\ 1 \leqslant j \leqslant m \end{array}\right\} \implies \left\{\begin{array}{l} \beta_1 + 1 \in \{2, 5\} \\ \text{y} \\ \beta_2 + 1 = 5 \\ \text{y} \\ \beta_j + 1 \in \{1, 2, 5\}\,,\ 3 \leqslant j \leqslant m \end{array}\right.$$

$$\left[\begin{array}{l} \left.\begin{array}{l} \beta_2 + 1 = 5 \\ \text{y} \\ (\beta_1 + 1)\,(\beta_2 + 1) \cdots (\beta_m + 1) = 10 \end{array}\right\} \implies \beta_j + 1 \neq 5, \text{ para cualquier } j \neq 2 \end{array}\right]$$

$$\implies \left\{\begin{array}{l} \beta_1 + 1 = 2 \\ \text{y} \\ \beta_2 + 1 = 5 \\ \text{y} \\ \beta_j + 1 \in \{1, 2\}\,,\ 3 \leqslant j \leqslant m \end{array}\right.$$

$$\left[\begin{array}{l} \left.\begin{array}{l} \beta_1 + 1 = 2 \\ \text{y} \\ \beta_2 + 1 = 5 \\ \text{y} \\ (\beta_1 + 1)\,(\beta_2 + 1)\,(\beta_3 + 1) \cdots\cdots (\beta_m + 1) = 10 \end{array}\right\} \implies \beta_j + 1 \neq 2,\ 3 \leqslant j \leqslant m \end{array}\right]$$

$$\implies \left\{\begin{array}{l} \beta_1 + 1 = 2 \\ \text{y} \\ \beta_2 + 1 = 5 \\ \text{y} \\ \beta_j + 1 = 1,\ 3 \leqslant j \leqslant m \end{array}\right.$$

$$\implies \left\{\begin{array}{l} \beta_1 = 1 \\ \text{y} \\ \beta_2 = 4 \\ \text{y} \\ \beta_j = 0,\ 3 \leqslant j \leqslant m \end{array}\right.$$

$$\implies b = 2 \cdot 3^4$$

Tenemos, pues, dos soluciones:

$$\left(a = 2^2 \cdot 3^6 \text{ ó } a = 2^6 \cdot 3^2\right) \text{ y } b = 2 \cdot 3^4 \implies \begin{cases} 1.\ a = 2^2 \cdot 3^6 \text{ y } b = 2 \cdot 3^4 \\ \text{ó} \\ 2.\ a = 2^6 \cdot 3^2 \text{ y } b = 2 \cdot 3^4 \end{cases}$$

Veamos cual de las dos es la que buscamos.

1. $a = 2^2 \cdot 3^6$ y $b = 2 \cdot 3^4$. 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 4.4.3,

   $$\text{m.c.d.}(a, b) = 2 \cdot 3^2 = 18$$

   que coincide con el dato proporcionado por el enunciado.

La solución correcta del ejercicio es, pues,

$$a = 576 \text{ y } b = 162$$

■

Ejemplo 4.14

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 tiene 8 divisores, $N_a = 8$, luego,

$$\begin{aligned} N_a = 8 &\implies (\alpha_1 + 1)(\alpha_2 + 1) = 8 \\ &\implies \alpha_1 + 1 \text{ y } \alpha_2 + 1 \text{ son, ambos, divisores de } 8 \\ &\quad \left[\ 8 = 2^3 \implies D_8 = \{1, 2, 4, 8\}\ \right] \\ &\implies \begin{cases} \alpha_1 + 1 \in \{1, 2, 4, 8\} \\ \text{y} \\ \alpha_2 + 1 \in \{1, 2, 4, 8\} \end{cases} \end{aligned}$$

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 4.4.3,

   $$D_a = \left\{ p_1^\alpha p_2^\beta : 0 \leqslant \alpha \leqslant 1 \text{ y } 0 \leqslant \beta \leqslant 3 \right\}$$

   y podemos escribirlos todos utilizando el método que vimos en 4.4.4, 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 4.4.3, tendremos que

   $$D_{320} = \left\{ 2^\gamma 3^\delta : 0 \leqslant \gamma \leqslant 6 \text{ y } 0 \leqslant \delta \leqslant 1 \right\}$$

   y por 4.4.4,

	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 4.4.3,

$$D_a=\left\{p_1^\alpha p_2^\beta : 0\leqslant \alpha\leqslant 3 \text{ y } 0\leqslant \beta\leqslant 1\right\}$$

y podemos escribirlos todos utilizando el método que vimos en 4.4.4, es decir,

	1	p_1	p_1^2	p_1^3
$\times p_2$	p_2	p_1p_2	$p_1^2p_2$	$p_1^3p_2$

Calculamos ahora la suma de todos ellos, S_a. En efecto, sumando por filas,

$$\begin{aligned} S_a &= 1+p_1+p_1^2+p_1^3+p_2+p_1p_2+p_1^2p_2+p_1^3p_2 \\ &= \left(1+p_1+p_1^2+p_1^3\right)(1+p_2) \end{aligned}$$

y, entonces,

$$S_a=320 \quad \Longrightarrow \quad \left(1+p_1+p_1^2+p_1^3\right)(1+p_2)=320$$

$$\Longrightarrow \left\{\begin{array}{l} 1+p_1+p_1^2+p_1^3 \text{ es divisor de } 320 \\ \text{y} \\ 1+p_2 \text{ es divisor de } 320 \end{array}\right.$$

y como $320 = 2^6 \cdot 5$, de nuevo por 4.4.3, 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 4.15

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:

$$\left.\begin{array}{l}\alpha_1 = 3\\ \text{y}\\ \alpha_2 = 2\\ \text{y}\\ \alpha_3 = 1\\ \text{y}\\ a = 2^{\alpha_1}5^{\alpha_2}7^{\alpha_3}\end{array}\right\} \Longrightarrow a = 2^3 5^2 7 \implies a = 1400$$

Veamos ahora la suma de todos sus divisores. Por 4.4.6,

$$S = \frac{2^{3+1}-1}{2-1}\cdot\frac{5^{2+1}-1}{5-1}\cdot\frac{7^{1+1}-1}{7-1} = 3720$$

■

Ejemplo 4.16

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,

$$a = 2^3p_2^{\alpha_2}p_3^{\alpha_3}\cdots p_k^{\alpha_k}$$

y si ninguno de los restantes factores primos es 3, entonces,

$$3a = 3\cdot 2^3p_2^{\alpha_2}p_3^{\alpha_3}\cdots p_k^{\alpha_k}$$

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,

$$\begin{aligned}
N_{3a} = 28 \quad &\Longrightarrow \quad (3+1)(\alpha_2+2)(\alpha_3+1)\cdots(\alpha_k+1) = 28\\
&\Longrightarrow \quad (\alpha_2+2)(\alpha_3+1)\cdots(\alpha_k+1) = 7\\
&\Longrightarrow \quad \begin{cases} \alpha_2+2 \text{ es divisor de } 7\\ \text{y}\\ \alpha_i+1 \text{ es divisor de } 7,\ 3 \leqslant i \leqslant k \end{cases}\\
&\Longrightarrow \quad \begin{cases} \alpha_2+2 \in \{1,7\}\\ \text{y}\\ \alpha_i+1 \in \{1,7\},\ 3 \leqslant i \leqslant k \end{cases}\\
&\qquad [\alpha_2 \geqslant 1 \Longrightarrow \alpha_2+2 \geqslant 3]\\
&\Longrightarrow \quad \begin{cases} \alpha_2+2 = 7\\ \text{y}\\ \alpha_i+1 \in \{1,7\},\ 3 \leqslant i \leqslant k \end{cases}\\
&\qquad [(\alpha_2+2)(\alpha_3+1)\cdots(\alpha_k+1) = 7]\\
&\Longrightarrow \quad \begin{cases} \alpha_2+2 = 7\\ \text{y}\\ \alpha_i+1 = 1,\ 3 \leqslant i \leqslant k \end{cases}\\
&\Longrightarrow \quad \begin{cases} \alpha_2 = 5\\ \text{y}\\ \alpha_i = 0,\ 3 \leqslant i \leqslant k \end{cases}
\end{aligned}$$

es decir el número pedido es

$$a = 2^3 \cdot 3^5 = 8 \cdot 243 = 1944.$$

Veamos ahora cuales son sus divisores. Utilizando el método 4.4.4,

	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 5

Ecuaciones Diofánticas

5.1 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.

5.1.1 Definición

Una ecuación diofántica es una ecuación lineal con coeficientes enteros y que exige soluciones también enteras.

5.2 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.

5.2.1 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

$$d = \text{m.c.d.}(a, b) \implies d|a \text{ y } d|b \implies d|ax_0 + by_0 \implies d|c$$

[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,

$$\begin{aligned} \text{m.c.d.}(a,b) = d &\implies \text{m.c.d.}\left(\frac{a}{d}, \frac{b}{d}\right) = 1 \\ &\iff \exists p, q \in \mathbb{Z} : \frac{a}{d}p + \frac{b}{d}q = 1 \\ &\implies a\frac{cp}{d} + b\frac{cq}{d} = c \end{aligned}$$

siendo $\dfrac{c}{d}$ entero ya que, por hipótesis, d es divisor de c. Ahora bastaría tomar

$$x_0 = \frac{cp}{d} \text{ e } y_0 = \frac{cq}{d}$$

y tendríamos que

$$ax_0 + by_0 = c$$

es decir los enteros x_0 e y_0 son solución de la ecuación.

La solución encontrada se llamará *solución particular* del sistema.

■

Obsérvese que este teorema además de asegurar la existencia de solución para una ecuación de este tipo, ofrece un método para calcularla. El siguiente ejemplo aclarará estas cuestiones.

Ejemplo 5.1

Encontrar una solución para la ecuación diofántica $525x + 100y = 50$

Solución

♢ Veamos si existe solución entera para la ecuación.

Calculamos el máximo común divisor de 525 y 100 mediante el algoritmo de Euclides.

	5	4
525	100	25
25	0	

es decir,

$$\text{m.c.d.}\,(525, 100) = 25$$

y como 25 divide a 50, el teorema anterior asegura la existencia de solución entera para la ecuación.

♢ Calculamos una solución para la ecuación.

Siguiendo el método indicado en la demostración del teorema, hallamos los coeficientes de la combinación lineal del máximo común divisor de 525 y 100. Bastaría seguir el algoritmo de Euclides hacia atrás.

$$25 = 1 \cdot 525 + (-5) \cdot 100$$

por tanto, los coeficientes buscados son $p = 1$ y $q = -5$ y según el citado teorema una solución para la ecuación sería

$$x_0 = \frac{cp}{d} \text{ e } y_0 = \frac{cq}{d}$$

donde c es el término independiente de la ecuación y d el máximo común divisor de los coeficientes de x e y. Consecuentemente,

$$x_0 = \frac{50 \cdot 1}{25} = 2$$

e

$$y_0 = \frac{50 \cdot (-5)}{25} = -10$$

■

5.2.2 Solución General

Sean a, b y c tres números enteros no nulos tales que el máximo común divisor de a y b divide a c. Entonces la solución general de la ecuación $ax + by = c$ es

$$x = x_0 + k \cdot \frac{b}{d}$$
$$y = y_0 - k \cdot \frac{a}{d}$$

donde x_0 e y_0 es una solución particular de la misma y k es cualquier número entero.

Demostración

Sea d el máximo común divisor de a y b. Por hipótesis d divide a c luego el teorema 5.2.1 asegura la existencia de una solución particular $x = x_0$ e $y = y_0$ para la ecuación. Entonces,

$$ax_0 + by_0 = c$$

Dividiendo ahora ambos miembros de esta ecuación por el máximo común divisor de a y b, tendremos,

$$\frac{a}{d}x_0 + \frac{b}{d}y_0 = \frac{c}{d}$$

siendo $\frac{c}{d}$ entero y $\frac{a}{d}, \frac{b}{d}$ números enteros primos entre sí, luego el máximo común divisor de ambos es 1 y como 1 divide a $\frac{c}{d}$, el teorema 5.2.1 asegura la existencia de una solución particular x_1, y_1 para esta ecuación, luego

$$\frac{a}{d}x_1 + \frac{b}{d}y_1 = \frac{c}{d}$$

Pues bien,

$$\left.\begin{array}{l} \frac{a}{d}x_1 + \frac{b}{d}y_1 = \frac{c}{d} \\ \frac{a}{d}x_0 + \frac{b}{d}y_0 = \frac{c}{d} \end{array}\right\} \implies \frac{a}{d}(x_1 - x_0) + \frac{b}{d}(y_1 - y_0) = 0$$

$$\implies \frac{a}{d}(x_1 - x_0) = \frac{b}{d}(y_0 - y_1)$$

$$\iff \frac{b}{d} \Big| \frac{a}{d}(x_1 - x_0)$$

y al ser $\frac{b}{d}$ primo con $\frac{a}{d}$, dividirá a $x_1 - x_0$, luego

$$\frac{b}{d} | x_1 - x_0 \iff \exists k \in \mathbb{Z} : x_1 - x_0 = k \cdot \frac{b}{d} \implies x_1 = x_0 + k \cdot \frac{b}{d}$$

Sustituimos el valor de $x_1 - x_0$ en $\frac{a}{d}(x_1 - x_0) + \frac{b}{d}(y_1 - y_0) = 0$ y resulta

$$\frac{a}{d} \cdot k \cdot \frac{b}{d} + \frac{b}{d}(y_1 - y_0) = 0 \implies \frac{a}{d} \cdot k + y_1 - y_0 = 0 \implies y_1 = y_0 - k \cdot \frac{a}{d}$$

Veamos, finalmente, que x_1 e y_1 es solución de la ecuación $ax + by = c$.

En efecto,

$$\begin{aligned} ax_1 + by_1 &= a\left(x_0 + k \cdot \frac{b}{d}\right) + b\left(y_0 - k \cdot \frac{a}{d}\right) \\ &= ax_0 + a \cdot k \cdot \frac{b}{d} + by_0 - b \cdot k \cdot \frac{a}{d} \\ &= ax_0 + by_0 \\ &= c \end{aligned}$$

y tomando $x = x_1$ e $y = y_1$,

$$\begin{aligned} x &= x_0 + k \cdot \frac{b}{d} \\ y &= y_0 - k \cdot \frac{a}{d} \end{aligned}$$

es solución de la ecuación $ax + by = c$ cualquiera que sea $k \in \mathbb{Z}$. La llamaremos *solución general* de dicha ecuación.

■

Nota 5.1 En el ejemplo anterior, teníamos que

$$x_0 = 2 \text{ e } y_0 = -10$$

era una solución particular para la ecuación

$$525x + 100y = 50$$

luego una solución general de la misma, será:

$$\begin{aligned} x &= 2 + k \cdot \frac{100}{25} = 2 + 4k \\ y &= -10 - k \cdot \frac{525}{25} = -10 - 21k \end{aligned}$$

siendo k cualquier número entero.

■

Ejemplo 5.2

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 5.2.1 se sigue que la ecuación propuesta admite una solución particular $x = x_0$, $y = y_0$.

♢ Calculamos esta solución particular.

Volviendo hacia atrás en el algoritmo de Euclides, tendremos

$$22 = (-8) \cdot 66 + 1 \cdot 550$$

luego,

$$x_0 = \frac{88 \cdot (-8)}{22} = -32$$
$$y_0 = \frac{88 \cdot 1}{22} = 4$$

es una *solución particular* de la ecuación.

♢ Calculemos ahora la *solución general*.

Según lo visto en el teorema 5.2.2 si una solución particular de la misma es $x_0 = -32$ e $y_0 = 4$, entonces la solución general es:

$$x = -32 + k \cdot \frac{550}{22} = -32 + 25 \cdot k$$
$$y = 4 - k \cdot \frac{66}{22} = 4 - 3k$$

siendo k cualquier número entero.

■

Ejemplo 5.3

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.

$$6 = 1 \cdot 30 + (-2) \cdot 12$$

luego entonces los coeficientes buscados son 1 y -2 y la *solución particular* de la ecuación es

$$x_0 = \frac{1200 \cdot 1}{6} = 200$$

$$y_0 = \frac{1200 \cdot (-2)}{6} = -400$$

♢ La *solución general* será:

$$x = 200 + k \cdot \frac{12}{6} = 200 + 2k$$

$$y = -400 - k \cdot \frac{30}{6} = -400 - 5k$$

siendo k cualquier número entero.

♢ Veamos, finalmente, cuantos litros se han comprado de cada tipo de leche.

Según lo visto hasta ahora, la cantidad de leche entera es

$$C_e = 200 + 2k, k \in \mathbb{Z}$$

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 5.4

Hallar los valores de $c \in \mathbb{Z}^+$, con $10 < c < 20$ para los cuales no tiene solución la ecuación diofántica $84x + 990y = c$. Determinar la solución para los restantes valores de c.

Solución

♢ La ecuación $84x + 990y = c$ admitirá solución entera si, y sólo si el máximo común divisor de 84 y 990 divide a c.

Hallamos dicho máximo común divisor por el algoritmo de Euclides.

	11	1	3	1	2
990	84	66	18	12	6
66	18	12	6	0	

luego

$$\text{m.c.d.}\,(84, 990) = 6$$

entonces,

$$84x + 990y = c \text{ tiene solución entera} \iff 6 \,|\, c \iff \exists q \in \mathbb{Z} : c = 6 \cdot q$$

y como $10 < c < 20$, tendremos que las opciones posibles para las que la ecuación tiene solución son

$$c = 12 \text{ y } c = 18$$

por tanto los valores de c para los que la ecuación no admite solución entera serán:

$$11, 13, 14, 15, 16, 17 \text{ y } 19$$

♢ Calculamos una *solución particular* para la ecuación propuesta.

Volviendo hacia atrás el cálculo hecho en el algoritmo de Euclides, tendremos

$$\left.\begin{array}{l} 6 = 18 - 1 \cdot 12 \\ 12 = 66 - 3 \cdot 18 \end{array}\right\} \implies \begin{array}{rcl} 6 & = & 18 - 1(66 - 3 \cdot 18) \\ & = & -1 \cdot 66 + 4 \cdot 18 \end{array}$$

$$\left.\begin{array}{l} 6 = -1 \cdot 66 + 4 \cdot 18 \\ 18 = 84 - 1 \cdot 66 \end{array}\right\} \implies \begin{array}{rcl} 6 & = & -1 \cdot 66 + 4(84 - 1 \cdot 66) \\ & = & 4 \cdot 84 - 5 \cdot 66 \end{array}$$

$$\left.\begin{array}{l} 6 = 4 \cdot 84 - 5 \cdot 66 \\ 66 = 990 - 11 \cdot 84 \end{array}\right\} \implies \begin{array}{rcl} 6 & = & 4 \cdot 84 - 5(990 - 11 \cdot 84) \\ & = & -5 \cdot 990 + 59 \cdot 84 \end{array}$$

luego,

$$6 = 59 \cdot 84 + (-5) \cdot 990$$

♢ Solución para $c = 12$.

– Una *solución particular* es

$$x_0 = \frac{12 \cdot 59}{6} = 118$$
$$y_0 = \frac{12 \cdot (-5)}{6} = -10$$

– La *solución general* es

$$x = 118 + k \cdot \frac{990}{6} = 118 + 165k$$
$$y = -10 - k \cdot \frac{84}{6} = -10 - 14k$$

siendo k cualquier número entero.

♢ Solución para $c = 18$.

– Una *solución particular* es

$$x_0 = \frac{18 \cdot 59}{6} = 177$$
$$y_0 = \frac{18 \cdot (-5)}{6} = -15$$

– La *solución general* es

$$x = 177 + k \cdot \frac{990}{6} = 177 + 165k$$
$$y = -15 - k \cdot \frac{84}{6} = -15 - 14k$$

siendo k cualquier número entero.

■

Ejemplo 5.5

Hallar las soluciones enteras de la ecuación

$$\sqrt{(x+y)(x-y)+(2x+2y-3)y-2(x-7)}=x+y+3$$

Solución

Elevando al cuadrado ambos miembros

$$x^2-y^2+2xy+2y^2-3y-2x+14=x^2+y^2+2xy+6x+6y+9$$

y simplificando, resulta

$$8x+9y=5$$

♢ Veamos si tiene soluciones enteras.

8 y 9 son primos entre sí, luego

$$\text{m.c.d.}\,(8,9)=1$$

y como 1 divide a 5, término independiente de la ecuación, esta tendrá soluciones enteras.

♢ Calculamos una *solución particular*

El máximo común divisor de 8 y 9 escrito en combinación lineal de ambos, es

$$1=(-1)\cdot 8+1\cdot 9$$

luego una solución particular es:

$$x_0=\frac{5\cdot(-1)}{1}=-5$$

$$y_0=\frac{5\cdot 1}{1}=5$$

♢ La *solución general*, por tanto, será

$$x=-5+9k$$

$$y=5-8k$$

siendo k cualquier número entero.

■

Ejemplo 5.6

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

$$\left.\begin{aligned}3x+2&=N\\4y+3&=N\end{aligned}\right\}$$

y restando miembro a miembro, resulta

$$3x-4y=1$$

♢ Veamos si esta ecuación tiene soluciones enteras.

Como m.c.d. $(3, 4) = 1$ y 1 divide a 1, término independiente de la ecuación, resulta que la misma admite soluciones enteras.

♢♢ *Solución particular*

$$1 = (-1) \cdot 3 + (-1)(-4)$$

luego,

$$x_0 = \frac{1 \cdot (-1)}{1} = -1$$

$$y_0 = \frac{1(-1)}{1} = -1$$

es una *solución particular* de la ecuación.

♢♢ *Solución general*

$$x = -1 + \frac{-4}{1} \cdot k = -1 - 4k$$

$$y = 1 - \frac{3}{1} \cdot k = -1 - 3k$$

siendo k cualquier número entero.

♢ Calculemos, finalmente, cuantas manzanas hay en el cesto.

$$\left.\begin{array}{l} 3x + 2 = N \\ x = -1 - 4k \end{array}\right\} \Longrightarrow 3(-1 - 4k) + 2 = N \Longrightarrow N = -12k - 1$$

y como N no puede ser 100 porque 100 es múltiplo de 4 y tampoco puede ser 110 porque da resto 2 al dividirlo entre 4,

$$100 < N < 110$$

tendremos,

$$100 < -12k - 1 < 110 \Longrightarrow \frac{101}{12} < -k < \frac{111}{12} \Longrightarrow \frac{-111}{12} < k < \frac{-101}{12} \Longrightarrow -9.25 < k < -8.42$$

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 5.7

Hallar el menor número entero positivo que dividido por 4, 7 y 11 da resto 3, y que dividido por 13 da resto 1.

Solución

Sea n el número buscado, entonces por el algoritmo de la división existen q_1, q_2 y q_3 tales que

$$\left.\begin{array}{l} n = 4q_1 + 3 \Longrightarrow n - 3 = 4q_1 \\ n = 7q_2 + 3 \Longrightarrow n - 3 = 7q_2 \\ n = 11q_3 + 3 \Longrightarrow n - 3 = 11q_3 \end{array}\right\}$$

luego

$$4\,|n-3\ ,\ 7\,|n-3\ \text{ y }11\,|n-3$$

es decir, $n-3$ es un múltiplo común a 4, 7 y 11, por tanto ha de ser múltiplo de su mínimo común múltiplo y al ser

$$\text{m.c.m.}(4,7,11) = 4\cdot 7\cdot 11 = 308$$

será

$$308\,|n-3$$

luego existirá un entero x tal que

$$n-3 = 308x$$

es decir,

$$n = 308x+3$$

Por otro lado y también por el algoritmo de la división, existirá un entero y tal que

$$n = 13y+1$$

por tanto,

$$\left.\begin{array}{l} n = 308x+3 \\ n = 13y+1 \end{array}\right\} \Longrightarrow 308x-13y = -2$$

♢ Veamos si esta ecuación admite soluciones enteras.

Calculamos el máximo común divisor de 308 y 13 por el algoritmo de Euclides.

	23	1	2	4
308	13	9	4	1
9	4	1	0	

luego

$$\text{m.c.d.}\,(308,13) = 1$$

y 1 divide a -2, término independiente de la ecuación, luego tiene soluciones enteras.

♢♢ *Solución particular*

Buscamos los coeficientes enteros de 1 expresado como combinación lineal de 308 y -13.

$$\left.\begin{array}{l} 1 = 9-2\cdot 4 \\ 4 = 13-1\cdot 9 \end{array}\right\} \Longrightarrow \begin{array}{rcl} 1 & = & 9-2(13-1\cdot 9) \\ & = & 2(-13)+3\cdot 9 \end{array}$$

$$\left.\begin{array}{l} 1 = 2(-13)+3\cdot 9 \\ 9 = 308-23\cdot 13 \end{array}\right\} \Longrightarrow \begin{array}{rcl} 1 & = & 2(-13)+3\cdot[308+23\cdot(-13)] \\ & = & 3\cdot 308+71\cdot(-13) \end{array}$$

luego

$$1 = 3\cdot 308+71\cdot(-13)$$

y una *solución particular* es:

$$x_0 = \frac{(-2)\cdot 3}{1} = -6$$

$$y_0 = \frac{(-2)\cdot 71}{1} = -142$$

♢♢ *Solución general*

$$x = -6 + k \cdot \frac{-13}{1} = -6 - 13k$$
$$y = -142 - k \cdot \frac{308}{1} = -142 - 308k$$

donde k es cualquier número entero.

♢ Calculemos, finalmente, el número pedido.

$$\left.\begin{array}{l} n = 308x + 3 \\ x = -6 - 13k \end{array}\right\} \Longrightarrow n = 308(-6 - 13k) + 3 = -1845 - 4004k$$

y al ser $n > 0$, tendremos

$$\begin{array}{rcl} -1845 - 4004k > 0 & \Longrightarrow & k < -\dfrac{1845}{4004} \\ & \Longrightarrow & k < -0.46 \\ & \Longrightarrow & k \leqslant -1 \\ & \Longleftrightarrow & \exists q \in \mathbb{Z}_0^+ : -1 = k + q \\ & \Longleftrightarrow & \exists q \in \mathbb{Z}_0^+ : k = -1 - q \end{array}$$

luego,

$$n = -1845 - 4004(-1 - q) = -1845 + 4004 + 4004q = 2159 + 4004q$$

y el número más pequeño se producirá para el menor valor que pueda tomar $q \in \mathbb{Z}_0^+$, es decir, $q = 0$. Entonces,

$$n = 2159 + 4004 \cdot 0 = 2159$$

y es el menor número entero que cumple las condiciones del enunciado.

■

Ejemplo 5.8

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:

$$\left.\begin{array}{l} x + y + z = 100 \\ 50x + 1000y + 5000z = 100000 \end{array}\right\} \Longrightarrow \left\{\begin{array}{l} z = 100 - x - y \\ 50x + 1000y + 5000z = 100000 \end{array}\right.$$
$$\Longrightarrow 50x + 1000y + 5000(100 - x - y) = 100000$$
$$\Longrightarrow 4950x + 4000y = 400000$$

♢ 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.

$$\left.\begin{array}{l} 50 = 200 + (-1)\cdot 150 \\ 150 = 950 - 4\cdot 200 \end{array}\right\} \implies 50 = 200 + (-1)\,(950 - 4\cdot 200)$$

$$\implies 50 = -1\cdot 950 + 5\cdot 200$$

$$\left.\begin{array}{l} 50 = -1\cdot 950 + 5\cdot 200 \\ 200 = 4000 - 4\cdot 950 \end{array}\right\} \implies 50 = -1\cdot 950 + 5\,(4000 - 4\cdot 950)$$

$$\implies 50 = 5\cdot 4000 + (-21)\cdot 950$$

$$\left.\begin{array}{l} 50 = 5\cdot 4000 + (-21)\cdot 950 \\ 950 = 4950 - 1\cdot 4000 \end{array}\right\} \implies 50 = 5\cdot 4000 + (-21)\,(4950 - 1\cdot 4000)$$

$$\implies 50 = -21\cdot 4950 + 26\cdot 4000$$

luego,

$$p = -21 \text{ y } q = 26$$

por tanto,

$$x_0 = \frac{400000\cdot(-21)}{50} = -168000$$

$$y_0 = \frac{400000\cdot 26}{50} = 208000$$

es una solución particular de la ecuación.

♢♢ La *solución general* será,

$$x = -168000 + k\cdot\frac{4000}{50} = 80k - 168000$$

$$y = 208000 - k\cdot\frac{4950}{50} = 208000 - 99k$$

siendo k cualquier número entero.

♢ Veamos, finalmente, cuantos animales de cada clase compró.

Teniendo en cuenta que adquirió animales de las tres clases, tendremos

$$\left.\begin{array}{l} x > 0 \implies 80k - 168000 > 0 \implies 80k > 168000 \implies k > 2100 \\ y > 0 \implies 208000 - 99k > 0 \implies 99k < 208000 \implies k < 2101.01 \end{array}\right\} \implies 2100 < k < 2101.01$$

y como k es un número entero, se sigue que $k = 2101$.

Así pues,

$$x = 80 \cdot 2101 - 168000 = 80$$
$$y = 208000 - 99 \cdot 2101 = 1$$

y al ser

$$x + y + z = 100$$

será

$$z = 100 - 80 - 1 = 19$$

por tanto compró 80 pollos, 1 conejo y 19 terneros.

■

Ejemplo 5.9

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, también, resto 7 al dividirlos por 33.

Solución

Según el *teorema de existencia y unicidad de cociente y resto*, 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 $n \in \mathbb{Z}_0^+$, tendremos que probar, por tanto,

$$\left.\begin{array}{l} n = 3x + 1 \\ \text{y} \\ n = 11y + 7 \end{array}\right\} \implies \exists q \in \mathbb{Z}_0^+ : n = 33q + 7$$

Pues bien,

$$\left.\begin{array}{l} n = 3x + 1 \\ \text{y} \\ n = 11y + 7 \end{array}\right\} \implies 3x + 1 = 11y + 7 \implies 3x - 11y = 6$$

♢ 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.

$$\left.\begin{array}{l} 1 = 3 + (-1)\cdot 2 \\ 2 = 11 - 3\cdot 3 \end{array}\right\} \implies 1 = 3 + (-1)(11 - 3\cdot 3)$$
$$\implies 1 = -1\cdot 11 + 4\cdot 3$$

es decir, $1 = 4\cdot 3 + 1(-11)$, luego,

$$x_0 = \frac{6\cdot 4}{1} = 24$$

e

$$y_0 = \frac{6\cdot 1}{1} = 6$$

♢ Obtenemos la solución general.

$$x = 24 - 11k$$

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 n sería 1, pero 1 no da resto 7 al dividirlo entre 11, luego $x > 0$. Entonces,

$$\begin{aligned} x > 0 &\implies 24 - 11k > 0 \\ &\implies -11k > -24 \\ &\implies 11k < 24 \\ &\implies k < \frac{24}{11} \\ &\implies k < 2.18 \\ &\implies k \leqslant 2 \quad \{k \text{ es entero}\} \\ &\implies \exists q \in \mathbb{Z}_0^+ : 2 = k + q \\ &\implies \exists q \in \mathbb{Z}_0^+ : k = 2 - q \\ &\implies \exists q \in \mathbb{Z}_0^+ : x = 24 - 11(2 - q) \\ &\implies \exists q \in \mathbb{Z}_0^+ : x = 11q + 2 \end{aligned}$$

y como $n = 3x + 1$,

$$\exists q \in \mathbb{Z}_0^+ : n = 3(11q + 2) + 1 \implies \exists q \in \mathbb{Z}_0^+ : n = 33q + 7.$$

Que era lo que queríamos probar.

■

Lección 6

Aritmética en $\mathbb{Z}_m$

En su obra *Disquisitiones Arithmeticae*, publicada en 1801, Gauss introdujo en las Matemáticas el concepto de congruencia. Dada la analogía que existía entre ella y la igualdad algebraica, Gauss adopto el símbolo $\equiv$, notación que aún se utiliza para la congruencia.

la relación de congruencia ha proporcionado las herramientas con las cuales se han demostrado importantes hitos de la Teoría de Números, de hecho ha sido un instrumento de vital importancia para el estudio de la divisibilidad en $\mathbb{Z}$.

Muchos problemas de Cálculo con enteros muy grandes pueden reducirse a problemas equivalentes usando enteros pequeños mediante el uso de las congruencias.

6.1 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.

6.1.1 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 $a \equiv b(\text{mód } m)$, es decir,

$$a \equiv b(\text{mód } m) \iff m|a-b$$

Ejemplo 6.1

$80 \equiv 20(\text{mód } 15)$, ya que $15|60$

$-8 \equiv 16(\text{mód } 4)$, ya que $4|-24$

$-5 \equiv -25(\text{mód } 10)$, ya que $10|20$

$12 \equiv -3(\text{mód } 5)$, ya que $5|15$

■

Ejemplo 6.2

Encontrar cinco número enteros distintos, cada uno los cuales sea congruente con 13 módulo 11.

Solución

Sea a cualquiera de los números buscados. Entonces,

$$\begin{aligned} a \equiv 13(\text{mód } 11) &\iff 11|a-13 \\ &\iff \exists q \in \mathbb{Z} : a-13 = 11q \\ &\iff \exists q \in \mathbb{Z} : a = 11q+13 \end{aligned}$$

Si ahora tomamos, por ejemplo, $q = -2,\ -1,\ 0,\ 1$ ó 2, tendremos los cinco números buscados:

$$\begin{aligned} a &= 11(-2)+13 = -9 \\ a &= 11(-1)+13 = 2 \\ a &= 11\cdot 0+13 = 13 \\ a &= 11\cdot 1+13 = 24 \\ a &= 11\cdot 2+13 = 35 \end{aligned}$$

■

6.1.2 Teorema

Sea m cualquier número entero positivo. Entonces,

(a) Cualquier número entero es congruente módulo m exactamente con uno de los enteros $0, 1, \ldots\ldots, m-1$.

(b) Dos números enteros son congruentes entre sí módulo m si, y sólo si ambos dan el mismo resto al dividirlos por m.

Demostración

(a) Probaremos que si a es un número entero cualquiera, entonces es congruente módulo m exactamente con uno de los enteros $0, 1, \ldots\ldots, m-1$.

En efecto,

$$\begin{aligned} a \in \mathbb{Z} \text{ y } m \in \mathbb{Z}^+ &\implies \text{Existen } q \text{ y } r, \text{ enteros y únicos} : a = mq+r, \text{ siendo } 0 \leqslant r < m \ \{(3.2.1)\} \\ &\iff \exists q, r \in \mathbb{Z} : a - r = mq, \text{ siendo } 0 \leqslant r < m \\ &\iff \exists r \in \mathbb{Z} : m|a-r, \text{ siendo } 0 \leqslant r < m \\ &\iff \exists r \in \mathbb{Z} : a \equiv r(\text{mód } m), \text{ siendo } 0 \leqslant r < m \\ &\iff \begin{cases} a \equiv 0(\text{mód } m) \\ \text{ó} \\ a \equiv 1(\text{mód } m) \\ \text{ó} \\ a \equiv 2(\text{mód } m) \\ \vdots \\ \text{ó} \\ a \equiv m-1(\text{mód } m) \end{cases} \end{aligned}$$

Al número r, único, lo llamaremos *menor residuo de a, módulo m.*

(b) En efecto, sean a y b dos enteros cualesquiera.

"Sólo si." En efecto, supongamos que $a \equiv b(\text{mód } m)$, entonces,

$$
\begin{aligned}
a \equiv b(\text{mód } m) &\iff m|a-b \\
&\iff \exists q \in \mathbb{Z} : a - b = mq \\
&\left\{ \begin{array}{l} \text{Por el teorema de existencia y unicidad de cociente y resto (3.2.1)} \\ \text{existirán } q_1, r_1, q_2, r_2, \text{ enteros y únicos, tales que} \\ \left\{ \begin{array}{l} a = mq_1 + r_1,\ 0 \leqslant r_1 < m \\ \text{y} \\ b = mq_2 + r_2,\ 0 \leqslant r_2 < m \end{array} \right. \end{array} \right\} \implies a - b = m(q_1 - q_2) + r_1 - r_2 \\
&\implies \left\{ \begin{array}{l} \exists q \in \mathbb{Z} : a - b = mq \\ \exists q_1, q_2, r_1, r_2 : a - b = m(q_1 - q_2) + r_1 - r_2,\ 0 \leqslant r_1 < m,\ 0 \leqslant r_2 < m \end{array} \right. \\
&\left\{ \begin{array}{l|l} 0 \leqslant r_1 < m & \\ \text{y} & \implies -m < r_1 - r_2 < m \iff 0 \leqslant |r_1 - r_2| < m \\ 0 \leqslant r_2 < m & \end{array} \right\} \\
&\implies \left\{ \begin{array}{l} \exists q \in \mathbb{Z} : a - b = mq \\ \exists q_1, q_2, r_1, r_2 : a - b = m(q_1 - q_2) + r_1 - r_2, \text{ siendo } 0 \leqslant |r_1 - r_2| < m \end{array} \right. \\
&\implies |r_1 - r_2| = 0 \ \{\text{El resto de dividir } a - b \text{ entre } m \text{ ha de ser único}\} \\
&\iff r_1 = r_2
\end{aligned}
$$

es decir, a y b dan, ambos, el mismo resto al dividirlos por m.

"Si." Recíprocamente, supongamos que a y b, dan, ambos, el mismo resto al dividirlos por m, es decir, existen q_1, q_2 y r, enteros, tales que

$$a = mq_1 + r \text{ y } b = mq_2 + r.$$

Entonces,

$$
\begin{aligned}
&\left\{ \begin{array}{l} a = mq_1 + r \\ \text{y} \\ b = mq_2 + r \end{array} \right. \implies a - b = m(q_1 - q_2) \\
&\implies \exists q \in \mathbb{Z} : a - b = mq \ \{\text{Tomando } q = q_1 - q_2\} \\
&\iff m|a-b \\
&\iff a \equiv b\,(\text{mód } m)
\end{aligned}
$$

■

Ejemplo 6.3

Demuéstrese que todo número primo mayor o igual que 5 es congruente con 1 ó con 5, módulo 6.

Solución

Probaremos que

si p es primo y $p \geqslant 5$, entonces $p \equiv 1(\text{mód } 6)$ ó $p \equiv 5(\text{mód } 6)$.

En efecto, supongamos que la proposición es falsa, es decir,

p es primo y $p \geqslant 5$ y, sin embargo, $p \not\equiv 1(\text{mód } 6)$ y $p \not\equiv 5(\text{mód } 6)$.

Entonces, por (a) del teorema anterior, $p \equiv 0(\text{mód } 6)$ ó $p \equiv 2(\text{mód } 6)$ ó $p \equiv 3(\text{mód } 6)$ ó $p \equiv 4(\text{mód } 6)$. Pues bien,

- Si $p \equiv 0(\text{mód } 6)$, entonces $6|p$ lo cual es imposible ya que p es primo.
- Si $p \equiv 2(\text{mód } 6)$, entonces

$$\left.\begin{array}{l} 6|p-2 \\ \text{y} \\ 2|6 \end{array}\right\} \Longrightarrow \left.\begin{array}{l} 2|p-2 \\ \text{y} \\ 2|2 \end{array}\right\} \Longrightarrow 2|p-2+2 \Longrightarrow 2|p$$

  y esto contradice el que p sea primo.

- Si $p \equiv 3(\text{mód } 6)$, entonces

$$\left.\begin{array}{l} 6|p-3 \\ \text{y} \\ 3|6 \end{array}\right\} \Longrightarrow \left.\begin{array}{l} 3|p-3 \\ \text{y} \\ 3|3 \end{array}\right\} \Longrightarrow 3|p-3+3 \Longrightarrow 3|p$$

  y esto contradice el que p sea primo.

- Si $p \equiv 4(\text{mód } 6)$, entonces

$$\left.\begin{array}{l} 6|p-4 \\ \text{y} \\ 2|6 \end{array}\right\} \Longrightarrow \left.\begin{array}{l} 2|p-4 \\ \text{y} \\ 2|4 \end{array}\right\} \Longrightarrow 2|p-4+4 \Longrightarrow 2|p$$

  y esto contradice el que p sea primo.

Hemos llegado, por tanto, a una contradicción y la proposición propuesta es cierta, es decir, p ha de ser congruente módulo 6 con 1 ó con 5.

■

Ejemplo 6.4

Demuéstrese que si $d|m$ y $a \equiv b(\text{mód } m)$, entonces $a \equiv b(\text{mód } d)$.

Solución

Directamente de la transitividad de la relación de divisibilidad,

$$\left.\begin{array}{l} d|m \\ a \equiv b(\text{mód } m) \Longleftrightarrow m|a-b \end{array}\right\} \Longrightarrow d|a-b \Longleftrightarrow a \equiv b(\text{mód } d)$$

■

6.2 Propiedades

Veremos a continuación algunas propiedades de las congruencias que son, con frecuencia, bastante útiles

6.2.1 Teorema

Sean a, b, c y m son tres enteros con $m > 0$. Se verifica:

(a) $a \equiv a(\text{mód } m)$.

(b) Si $a \equiv b(\text{mód } m)$, *entonces* $b \equiv a(\text{mód } m)$

(c) Si $a \equiv b(\text{mód } m)$ *y* $b \equiv c(\text{mód } m)$, *entonces* $a \equiv c(\text{mód } m)$

Demostración

Utilizaremos las propiedades de la divisibilidad (3.1.2).

(a) $a \equiv a(\text{mód } m)$
Teniendo en cuenta que $m \neq 0$,

$$m|0 \iff m|a-a \iff a \equiv a(\text{mód } m)$$

(b) Si $a \equiv b(\text{mód } m)$, entonces $b \equiv a(\text{mód } m)$. En efecto,

$$a \equiv b(\text{mód } m) \iff m|a-b \iff m|(-1)(a-b) \implies m|b-a \iff b \equiv a(\text{mód } m)$$

(c) Si $a \equiv b(\text{mód } m)$ y $b \equiv c(\text{mód } m)$, entonces $a \equiv c(\text{mód } m)$. En efecto,

$$\left.\begin{array}{l} a \equiv b(\text{mód } m) \iff m|a-b \\ \text{y} \\ b \equiv c(\text{mód } m) \iff m|b-c \end{array}\right\} \implies m|(a-b)+(b-c) \implies m|a-c \implies a \equiv c(\text{mód } m)$$

■

6.2.2 Teorema

Sean a, b, c, d, p y m, enteros con $p \neq 0$ y $m > 0$. Se verifica:

(a) si $a \equiv b(\text{mód } m)$ *y* $c \equiv d(\text{mód } m)$, *entonces* $a + c \equiv b + d(\text{mód } m)$ *y* $ac \equiv bd(\text{mód } m)$.

(b) Si $a \equiv b(\text{mód } m)$, *entonces* $pa \equiv pb(\text{mód } m)$.

(c) Si $p|a$, $p|b$, $m.c.d.(p, m) = 1$ *y* $a \equiv b(\text{mód } m)$, *entonces* $\frac{a}{p} \equiv \frac{b}{p}(\text{mód } m)$.

Demostración

Utilizaremos, al igual que en el teorema anterior, las propiedades de la divisibilidad (3.1.2)

(a) si $a \equiv b(\text{mód } m)$ y $b \equiv c(\text{mód } m)$, entonces $a+c \equiv b+d(\text{mód } m)$ y $ac \equiv bd(\text{mód } m)$.

En efecto,

$$\left.\begin{array}{l} a \equiv b(\text{mód } m) \Longleftrightarrow m|a-b \\ \text{y} \\ c \equiv d(\text{mód } m) \Longleftrightarrow m|c-d \end{array}\right\} \Longrightarrow m|(a-b)+(c-d) \Longrightarrow m|(a+c)-(b+d)$$

luego,

$$a+c \equiv b+d(\text{módm}).$$

Análogamente,

$$\left.\begin{array}{l} a \equiv b(\text{mód } m) \Longleftrightarrow m|a-b \Longrightarrow m|ac-bc \\ \text{y} \\ c \equiv d(\text{mód } m) \Longleftrightarrow m|c-d \Longrightarrow m|bc-bd \end{array}\right\} \Longrightarrow m|(ac-bc)+(bc-bd) \Longrightarrow m|ac-bd$$

por lo tanto,

$$ac \equiv bd(\text{módm}).$$

(b) Si $a \equiv b(\text{mód } m)$, entonces $pa \equiv pb(\text{mód } m)$. En efecto,

$$a \equiv b(\text{mód } m) \Longleftrightarrow m|a-b \Longrightarrow m|p(a-b) \Longrightarrow m|pa-pb \Longleftrightarrow pa \equiv pb(\text{mód } m)$$

(c) Si $p|a$, $p|b$, m.c.d.$(p,m)=1$ y $a \equiv b(\text{mód } m)$, entonces $\dfrac{a}{p} \equiv \dfrac{b}{p}(\text{mód } m)$.

En efecto,

$$\left.\begin{array}{l} \left.\begin{array}{l} p|a \\ \text{y} \\ p|b \end{array}\right\} \Longrightarrow p|a-b \\ \text{y} \\ a \equiv b(\text{mód } m) \Longleftrightarrow m|a-b \end{array}\right\} \Longrightarrow \text{m.c.m.}(p,m)|a-b \Longrightarrow pm\,|a-b \Longrightarrow \exists q \in \mathbb{Z} : a-b=pmq$$

Pues bien,

$$a-b=pmq \Longrightarrow \frac{a}{p}-\frac{b}{p}=mq \Longleftrightarrow m\left|\frac{a}{p}-\frac{b}{p}\right.$$

Consecuentemente,

$$\frac{a}{p} \equiv \frac{b}{p}(\text{mód } m)$$

■

Ejemplo 6.5

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 6.1.2 a es congruente módulo 3 con 0, 1 ó 2. Pues bien,

$$\begin{aligned}
a \equiv 0(\text{mód } 3) &\implies a^2 \equiv 0(\text{mód } 3) \ \{(6.2.2\ (a))\} \\
&\iff 3|a^2 \\
&\iff a^2 \text{ es divisible por } 3 \\
&\text{ó} \\
a \equiv 1(\text{mód } 3) &\implies a^2 \equiv 1(\text{mód } 3) \ \{(6.2.2\ (a))\} \\
&\text{ó} \\
a \equiv 2(\text{mód } 3) &\implies a^2 \equiv 4(\text{mód } 3) \ \{(6.2.2\ (a))\} \\
&\iff \begin{cases} a^2 \equiv 4(\text{mód } 3) \\ \text{y} \\ 4 \equiv 1(\text{mód } 3) \end{cases} \\
&\iff a^2 \equiv 1(\text{mód } 3) \ \{6.2.1(c)\}
\end{aligned}$$

luego a^2 es divisible por 3 o es congruente con 1 módulo 3.

■

Veamos ahora un corolario que generaliza algunos apartados del teorema anterior.

6.2.3 Corolario

Si $a_i \equiv b_i(\text{mód } m)$ para $1 \leqslant i \leqslant n$, entonces

(i) $\displaystyle\sum_{i=1}^{n} a_i \equiv \sum_{i=1}^{n} b_i(\text{mód } m)$

(ii) $\displaystyle\prod_{i=1}^{n} a_i \equiv \prod_{i=1}^{n} b_i(\text{mód } m)$

Demostración

Procederemos, en ambos casos, por inducción.

(i) $\displaystyle\sum_{i=1}^{n} a_i \equiv \sum_{i=1}^{n} b_i(\text{mód } m)$

Paso básico. Veamos que es cierto para $n = 2$. En efecto, por el teorema anterior,

$$\left.\begin{aligned} a_1 &\equiv b_1(\text{mód } m) \\ a_2 &\equiv b_2(\text{mód } m) \end{aligned}\right\} \implies a_1 + a_2 \equiv b_1 + b_2(\text{mód } m)$$

Paso inductivo. Supongamos que la proposición es cierta para $n = p$, es decir,

$$\text{si } a_i \equiv b_i(\text{mód } m),\ i = 1, 2, \ldots, p, \text{ entonces } \sum_{i=1}^{p} a_i \equiv \sum_{i=1}^{p} b_i(\text{mód } m)$$

Veamos que también se cumple para $n = p + 1$. En efecto, si

$$a_i \equiv b_i(\text{mód } m),\ i = 1, 2, \ldots, p, p+1$$

entonces por la hipótesis de inducción y por ser cierta la propiedad para $i = 2$, tendremos que

$$\left.\begin{array}{l} \displaystyle\sum_{i=1}^{p} a_i \equiv \sum_{i=1}^{p} b_i(\text{mód } m) \\ a_{p+1} \equiv b_{p+1}(\text{mód } m) \end{array}\right\} \Longrightarrow \sum_{i=1}^{p} a_i + a_{p+1} \equiv \sum_{i=1}^{p} b_i + b_{p+1}(\text{mód } m) \Longrightarrow \sum_{i=1}^{p+1} a_i \equiv \sum_{i=1}^{p+1} b_i(\text{mód } m)$$

y, consecuentemente, la proposición será cierta para todo n.

(ii) $\displaystyle\prod_{i=1}^{n} a_i \equiv \prod_{i=1}^{n} b_i(\text{mód } m)$

Basta aplicar el apartado (a) del teorema anterior y la igualdad

$$\prod_{i=1}^{p+1} a_i = \prod_{i=1}^{p} a_i \cdot a_{p+1}$$

para llegar, al igual que en el apartado anterior, al resultado.

■

Ejemplo 6.6

Demostrar que si el último dígito de un número n es t, entonces

$$n^2 \equiv t^2(\text{mód } 10)$$

Solución

En efecto, si

$$n = a_k 10^k + a_{k-1} 10^{k-1} + \cdots + a_1 10 + a_0$$

es la descomposición polinómica de n, entonces $a_0 = t$, luego

$$n = \sum_{i=1}^{k} a_i 10^i + t$$

de aquí que

$$n - t = \sum_{i=1}^{k} a_i 10^i$$

Ahora bien,

$$10 \equiv 0(\text{mód } 10)$$

luego

$$10^i \equiv 0(\text{mód } 10),\ 1 \leqslant i \leqslant k$$

y también

$$a_i 10^i \equiv 0(\text{mód } 10),\ 1 \leqslant i \leqslant k$$

de aquí que por el corolario anterior,

$$\sum_{i=1}^{k} a_i 10^i \equiv 0(\text{mód } 10).$$

Consecuentemente,

$$n - t \equiv 0(\text{mód } 10)$$

y, por lo tanto,

$$n \equiv t(\text{mód } 10)$$

de donde resulta que

$$n^2 \equiv t^2(\text{mód } 10)$$

■

Ejemplo 6.7

Demostrar que el resto de dividir 20^{4572} entre 7 es 1.

Solución

En efecto,

$$\left.\begin{array}{r} 21 \equiv 0(\text{mód } 7) \\ -1 \equiv -1(\text{mód } 7) \end{array}\right\} \Longrightarrow 20 \equiv -1(\text{mód } 7) \Longrightarrow 20^{4572} \equiv (-1)^{4572}(\text{mód } 7) \Longrightarrow 20^{4572} \equiv 1(\text{mód } 7)$$

es decir el resto es 1.

■

Ejemplo 6.8

Demostrar:

(a) Si $a \equiv b(\text{mód } m)$, entonces m.c.d.$(a, m) =$ m.c.d.(b, m).

(b) Si $a \equiv b(\text{mód } m)$, entonces $a^n \equiv b^n(\text{mód } m)$ para cualquier entero positivo n.

(c) Si $a + b \equiv c(\text{mód } m)$, entonces $a \equiv c - b(\text{mód } m)$.

(d) Si $a \equiv b(\text{mód } m)$ y $d|a$ y $d|m$, entonces $d|b$.

Solución

(a) Si $a \equiv b(\text{mód } m)$, entonces $\text{m.c.d.}(a,m) = \text{m.c.d.}(b,m)$. En efecto,

$$a \equiv b(\text{mód } m) \Longleftrightarrow m|a-b \Longleftrightarrow \exists q \in \mathbb{Z} : a-b = mq$$

Pues bien, sea $d_1 = \text{m.c.d}(a,m)$ y $d_2 = \text{m.c.d}(b,m)$. Entonces,

$$d_1 = \text{m.c.d}(a,m) \Longrightarrow \left\{ \begin{array}{l} d_1|a \\ \text{y} \\ d_1|m \Longrightarrow d_1|mq \Longrightarrow d_1|a-b \end{array} \right\} \Longrightarrow d_1|a-(a-b) \Longrightarrow d_1|b$$

Es decir, d_1 divide a b y a m, por tanto dividirá al máximo común divisor de ambos, luego

$$d_1|d_2$$

Análogamente,

$$d_2 = \text{m.c.d}(b,m) \Longrightarrow \left\{ \begin{array}{l} d_2|b \\ \text{y} \\ d_2|m \Longrightarrow d_2|mq \Longrightarrow d_2|a-b \end{array} \right\} \Longrightarrow d_2|a-b+b \Longrightarrow d_2|a$$

O sea, d_2 divide a a y a m, luego dividirá al máximo común divisor de ambos, de aquí que

$$d_2|d_1$$

Finalmente, como d_1 y d_2 son enteros positivos, por la antisimetría de la relación de divisibilidad en $\mathbb{Z}^+$, d_1 será igual a d_2, es decir,

$$\text{m.c.d.}(a,m) = \text{m.c.d.}(b,m)$$

(b) Si $a \equiv b(\text{mód } m)$, entonces $a^n \equiv b^n(\text{mód } m)$ para cualquier entero positivo n.

Basta aplicar el apartado (ii) del corolario anterior para $a_i = a,\ 1 \leqslant i \leqslant n$ y $b_i = b,\ 1 \leqslant i \leqslant n$

(c) Si $a+b \equiv c(\text{mód } m)$, entonces $a \equiv c-b(\text{mód } m)$.

En efecto,

$$a+b \equiv c(\text{mód } m) \Longleftrightarrow m|a+b-c \Longleftrightarrow m|a-(c-b) \Longleftrightarrow a \equiv c-b(\text{mód } m)$$

(d) Si $a \equiv b(\text{mód } m)$ y $d|a$ y $d|m$, entonces $d|b$.

En efecto,

$$a \equiv b(\text{mód } m) \Longleftrightarrow m|a-b$$

y como $d|m$, por la transitividad de la relación de divisibilidad, $d|a-b$. Así pues,

$$\left. \begin{array}{l} d|a \\ d|a-b \end{array} \right\} \Longrightarrow d|a-(a-b) \Longrightarrow d|b$$

■

Ejemplo 6.9

Demostrar que para cualquier entero positivo n, el número $3 \cdot 5^{2n+1} + 2^{3n+1}$ es divisible por 17.

Solución

Observemos lo siguiente:

$$\left.\begin{array}{l} 3\cdot 5^{2n+1} = 3\cdot (5^2)^n \cdot 5 = 15\cdot 25^n \\ 2^{3n+1} = (2^3)^n \cdot 2 = 2\cdot 8^n \end{array}\right\} \implies 3\cdot 5^{2n+1} + 2^{3n+1} = 15\cdot 25^n + 2\cdot 8^n$$

Por otra parte,

$$\left.\begin{array}{l} 15 \equiv -2(\text{mód } 17) \\ 25 \equiv 8(\text{mód } 17) \Longrightarrow 25^n \equiv 8^n(\text{mód } 17) \end{array}\right\} \Longrightarrow 15\cdot 25^n \equiv -2\cdot 8^n(\text{mód } 17)$$

luego,

$$15\cdot 25^n + 2\cdot 8^n \equiv 0(\text{mód } 17)$$

es decir,

$$3\cdot 5^{2n+1} + 2^{3n+1} \equiv 0(\text{mód } 17)$$

por lo tanto, el número dado es divisible por 17.

■

Ejemplo 6.10

Demostrar por inducción que el número $7^{2n} - 48n - 1$ es divisible por 2304 para cualquier entero positivo n.

Solución

Probaremos que

$$7^{2n} - 48n - 1 \equiv 0(\text{mód } 2304)$$

o lo que es igual,

$$(7^2)^n \equiv 48n + 1(\text{mód } 2304)$$

es decir,

$$49^n \equiv 48n + 1(\text{mód } 2304)$$

o sea,

$$(48+1)^n \equiv 48n + 1(\text{mód } 2304)$$

Procederemos por inducción.

- Para $n = 1$ es cierto claramente.
- Veamos si es cierto para $n = 2$. En efecto,

$$\begin{array}{rcl} (48+1)^2 = 48^2 + 2\cdot 48 + 1 & \iff & (48+1)^2 = 48\cdot 2 + 1 + 2304 \\ & \iff & (48+1)^2 - (48\cdot 2 + 1) = 2304 \\ & \iff & (48+1)^2 \equiv 48\cdot 2 + 1(\text{mód } 2304) \end{array}$$

- Supongamos que es cierto para $n = p$, es decir,

$$(48+1)^p \equiv 48p + 1(\text{mód } 2304)$$

⋊ Veamos que es cierto para $n = p + 1$. En efecto,

$$\begin{aligned} 48 + 1 &\equiv 48 + 1(\text{mód } 2304) && \{\text{Por ser cierto para } n = 1\} \\ (48 + 1)^p &\equiv 48p + 1(\text{mód } 2304) && \{\text{Por la hipótesis de inducción}\} \end{aligned}$$

luego,

$$(48 + 1)^p(48 + 1) \equiv (48p + 1)(48 + 1)(\text{mód } 2304).$$

Por otra parte,

$$(48p + 1)(48 + 1) = 2304p + 48 + 48p + 1$$

es decir,

$$(48p + 1)(48 + 1) - [48(p + 1) + 1] = 2304p$$

de aquí que

$$(48p + 1)(48 + 1) \equiv 48(p + 1) + 1(\text{mód } 2304).$$

Finalmente, por la transitividad de la relación de congruencia, de

$$\begin{aligned} (48 + 1)^p(48 + 1) &\equiv (48p + 1)(48 + 1)(\text{mód } 2304) \\ (48p + 1)(48 + 1) &\equiv 48(p + 1) + 1(\text{mód } 2304) \end{aligned}$$

se sigue que

$$(48 + 1)^{p+1} \equiv 48(p + 1) + 1(\text{mód } 2304).$$

Consecuentemente, la congruencia es cierta para cada entero positivo n, o sea,

$$(48 + 1)^n \equiv 48n + 1(\text{mód } 2304)$$

y, consecuentemente,

$$7^{2n} - 48n + 1$$

es divisible por 2304 para cualquier entero positivo n.

■

Ejemplo 6.11

Calcular el resto de dividir $9^{6n+1} + 3^{2n+1} \cdot 487^{2n} - 10$ por 730.

Solución

Observemos lo siguiente:

$$\begin{aligned} 9^{6n+1} + 3^{2n+1} \cdot 487^{2n} - 10 &= (9^3)^{2n} \cdot 9 + (3 \cdot 487)^{2n} \cdot 3 - 10 \\ &= 729^{2n} \cdot 9 + 1461^{2n} \cdot 3 - 10 \end{aligned}$$

Pues bien,

$$\begin{aligned} 729 \equiv -1(\text{mód } 730) &\implies 729^{2n} \equiv (-1)^{2n}(\text{mód } 730) \\ &\implies 729^{2n} \equiv 1(\text{mód } 730) \\ &\implies 729^{2n} \cdot 9 \equiv 9(\text{mód } 730) \\ &\iff 9^{6n+1} \equiv 9(\text{mód } 730). \end{aligned}$$

Por otra parte,

$$\begin{aligned} 1461 \equiv 1(\text{mód } 730) &\implies 1461^{2n} \equiv 1^{2n}(\text{mód } 730) \\ &\implies 1461^{2n} \equiv 1(\text{mód } 730) \\ &\implies 1461^{2n} \cdot 3 \equiv 3(\text{mód } 730) \\ &\iff 3^{2n+1} \cdot 487^{2n} \equiv 3(\text{mód } 730) \end{aligned}$$

de aquí que

$$9^{6n+1} + 3^{2n+1} \cdot 487^{2n} \equiv 12(\text{mód } 730)$$

es decir,

$$9^{6n+1} + 3^{2n+1} \cdot 487^{2n} - 10 \equiv 2(\text{mód } 730)$$

y, consecuentemente, el resto de dividir el número dado entre 730 es 2.

■

Ejemplo 6.12

Demostrar que para cualquier entero positivo n, el número $10^n(9n-1)+1$ es divisible por 9.

Solución

En efecto,

$$10 \equiv 1(\text{mód } 9) \implies 10^n \equiv 1(\text{mód } 9)$$

y

$$9n \equiv 0(\text{mód } 9) \iff 9n \equiv 1-1(\text{mód } 9) \iff 9n-1 \equiv -1(\text{mód } 9)$$

luego,

$$10^n(9n-1) \equiv -1(\text{mód } 9)$$

por lo tanto,

$$10^n(9n-1)+1 \equiv 0(\text{mód } 9)$$

y, consecuentemente, el resto de dividir el número dado entre 9 es cero.

■

6.3 Conjunto de las clases de restos módulo m

En este apartado veremos que la relación de congruencia es de equivalencia y calcularemos el conjunto cociente, al cual llamaremos $\mathbb{Z}_m$. Este conjunto será $\{[0],[1],\ldots,[m-1]\}$, donde

$$\begin{aligned} [0] &= \{n : n = mq, q \in \mathbb{Z}\} \\ [1] &= \{n : n = mq+1, q \in \mathbb{Z}\} \\ &\vdots \qquad\qquad \vdots \\ [m-1] &= \{n : n = mq+m-1, q \in \mathbb{Z}\} \end{aligned}$$

Con esta interpretación, cada elemento de $\mathbb{Z}_m$ es considerado como el conjunto de todos los enteros congruentes con un entero r tal que $0 \leqslant r \leqslant m-1$.

Esta es la razón de que la propiedad cíclica de las congruencias sea tan importante. Si contamos desde 0 a 10 en base decimal, originamos un ciclo desde 0 a 9 y volvemos al 0. Por ejemplo, el cuentakilómetros de un coche es una instrumentación física de esta propiedad. Los dígitos desde el 0 hasta el 9 se sitúan en un círculo, y cuando éste gira, tiene lugar la cuenta. Cuando un círculo pasa desde el 9 hasta el 0, el siguiente círculo a su izquierda se incrementa en 1. El cuentakilómetros vuelve a 0 de nuevo cuando el coche recorre 100.000 kms. Así pues, el cuentakilómetros es una instrumentación de $\mathbb{Z}_{100.000}$ y cada una de las ruedas de dígitos son instrumentaciones de $\mathbb{Z}_{10}$.

La informática también es bastante dependiente de esta propiedad. Por ejemplo, un byte es un número de ocho bits que varía desde 00000000 hasta 11111111; si añadimos 1 a 11111111 volvemos de nuevo a 00000000. Esta transición se registra normalmente como un desbordamiento. El hecho de contar en un ordenador, supone exactamente el mismo principio que el utilizado en el cuentakilómetros. Además, no importa lo potente que sea el mismo, siempre será una máquina finita. Así que cada esfuerzo para tratar con los números enteros es, básicamente, una aproximación de los enteros por $\mathbb{Z}_m$ para algún m lo suficientemente grande. Este hecho, combinado con la naturaleza cíclica de $\mathbb{Z}_m$, es la base para algoritmos utilizados en la generación de números aleatorios.

6.3.1 Relación de Equivalencia

Dado un entero $m > 0$, la relación de congruencia módulo m es una relación de equivalencia en el conjunto de los números enteros.

Demostración

Se sigue directamente del teorema 6.2.2.

■

6.3.2 Clases de Equivalencia

Dado un número entero cualquiera, a, su clase de equivalencia es el conjunto formado por todos los enteros que dan el mismo resto que a al dividirlos entre m.

Demostración

Sea, pues, a cualquier número entero. Hallaremos $[a]$.

Por el teorema de existencia y unicidad de cociente y resto, (3.2.1), existirán q_2 y r, enteros y únicos, tales que

$$a = mq_2 + r, \text{ siendo } 0 \leqslant r < m \tag{6.1}$$

Pues bien, si b es un entero elegido arbitrariamente, entonces,

$$\begin{aligned}
b \in [a] &\iff b \equiv a \,(\text{mód } m) \\
&\iff m|b-a \\
&\iff \exists q_1 \in \mathbb{Z} : b - a = mq_1 \\
&\iff \exists q_1 \in \mathbb{Z} : b = mq_1 + a \\
&\implies \exists q_1, q_2, r \in \mathbb{Z} : b = mq_1 + mq_2 + r, \text{ siendo } 0 \leqslant r < m \ \{(6.1)\} \\
&\iff \exists q_1, q_2, r \in \mathbb{Z} : b = m(q_1 + q_2) + r, \text{ siendo } 0 \leqslant r < m \\
&\implies \exists q, r \in \mathbb{Z} : b = mq + r, \text{ siendo } 0 \leqslant r < m \ \{\text{Tomando } q = q_1 + q_2\} \\
&\iff \exists q, r \in \mathbb{Z} : b - r = mq, \text{ siendo } 0 \leqslant r < m \\
&\iff \exists r \in \mathbb{Z} : m|b-r, \text{ siendo } 0 \leqslant r < m \\
&\iff \exists r \in \mathbb{Z} : b \equiv r \,(\text{mód } m)\,, \text{ siendo } 0 \leqslant r < m \\
&\iff \exists r \in \mathbb{Z} : b \in [r]\,, \text{ siendo } 0 \leqslant r < m
\end{aligned}$$

Como b era cualquier entero, hemos probado la veracidad de la proposición,

$$\forall n, (n \in [a] \longrightarrow \exists r \in \{0, 1, \ldots, m-1\} : n \in [r])$$

lo cual, por la definición de inclusión de conjuntos, equivale a decir que puede encontrarse, al menos, un r en $\{0, 1, \ldots, m-1\}$ tal que

$$[a] \subseteq [r]$$

Recíprocamente, supongamos que existe $r \in \{0, 1, \ldots, m-1\}$ tal que $b \in [r]$. Entonces,

$$\begin{aligned}
b \in [r] &\iff b \equiv r \,(\text{mód } m)\,, \text{ siendo } 0 \leqslant r < m \\
&\iff m|b-r, \text{ siendo } 0 \leqslant r < m \\
&\iff \exists q_1 \in \mathbb{Z} : b - r = mq_1, \text{ siendo } 0 \leqslant r < m \\
&\iff \exists q_1 \in \mathbb{Z} : b = mq_1 + r, \text{ siendo } 0 \leqslant r < m \\
&\implies \exists q_1, q_2 \in \mathbb{Z} : b = mq_1 + a - mq_2 \,\{(6.1)\} \\
&\iff \exists q_1, q_2 \in \mathbb{Z} : b = m(q_1 - q_2) + a \\
&\implies \exists q \in \mathbb{Z} : b = mq + a \ \{\text{Tomando } q = q_1 - q_2\} \\
&\iff \exists q \in \mathbb{Z} : b - a = mq \\
&\iff m|b-a \\
&\iff b \equiv a \,(\text{mód } m) \\
&\iff b \in [a]
\end{aligned}$$

De la arbitrariedad de b se sigue, nuevamente, la veracidad de la proposición,

$$\forall n, (n \in [r] \longrightarrow n \in [a])$$

para algún $r \in \{0, 1, \ldots, m-1\}$ luego por la definición de inclusión de conjuntos,

$$[r] \subseteq [a]$$

Finalmente, por la doble inclusión de conjuntos, hemos llegado a que si a es cualquier número entero, entonces,

$$\exists r \in \{0, 1, \ldots, m-1\} : [a] = [r]$$

o lo que es igual, la clase de equivalencia de a, $[a]$, es igual a la clase de su resto, r, al dividir por m, es decir,

$$\begin{array}{rcl} [a] & = & [0] \\ \text{o} & & \\ [a] & = & [1] \\ \text{o} & & \\ [a] & = & [2] \\ \text{o} & & \\ \vdots & & \vdots \\ \text{o} & & \\ [a] & = & [m-1] \end{array}$$

Solo nos falta hallar $[r]$, siendo $0 \leqslant r < m$. En efecto, si b es cualquier número entero, entonces,

$$\begin{array}{rcl} b \in [r] & \iff & b \equiv r(\text{mód } m) \\ & \iff & m|b-r \\ & \iff & \exists q \in \mathbb{Z} : b - r = mq \\ & \iff & \exists q \in \mathbb{Z} : b = mq + r \end{array}$$

y al ser b cualquiera, esto significa que la proposición

$$\forall n, (x \in [r] \longleftrightarrow x \in \{n : n = mq + r,\ 0 \leqslant r < m\})$$

es verdadera y, por lo tanto, el *axioma de extensión*, asegura que

$$[r] = \{n : n = mq + r,\ 0 \leqslant r < m\}$$

es decir, la clase de equivalencia de r, siendo $0 \leqslant r < m$ está integrada por todos los números que dan resto r al dividirlos por m. Luego,

$$\begin{array}{rcl} [0] & = & \{n : n = mq, q \in \mathbb{Z}\} \\ [1] & = & \{n : n = mq + 1, q \in \mathbb{Z}\} \\ [2] & = & \{n : n = mq + 2, q \in \mathbb{Z}\} \\ \vdots & & \vdots \\ [m-1] & = & \{n : n = mq + m - 1, q \in \mathbb{Z}\} \end{array}$$

■

6.3.3 Conjunto Cociente

Al conjunto formado por las clases de equivalencia, es decir al conjunto cociente, lo llamaremos conjunto de las clases de resto módulo m y lo notaremos por $\mathbb{Z}_m$

$$\mathbb{Z}_m = \{[0], [1], [2], \ldots, [m-1]\}$$

Demostración

Por definición de conjunto cociente,

$$\mathbb{Z}\Big/_{\equiv} = \{[n] : n \in \mathbb{Z}\}$$

Entonces, si N es cualquier subconjunto de números enteros,

$$\begin{aligned} N \in \mathbb{Z}/_{\equiv} &\iff \exists a \in \mathbb{Z} : N = [a] \\ &\iff \exists r \in \{0, 1, 2, \ldots, m-1\} : N = [r] \ (6.3.2) \\ &\iff N = [0] \ \vee \ N = [1] \ \vee \ N = [2] \ \vee \ \ldots \ \vee \ N = [m-1] \\ &\iff N = \{[0], [1], [2], \ldots, [m-1]\} \end{aligned}$$

Por lo tanto, el axioma de extensión asegura que el conjunto cociente, que a partir de ahora notaremos como $\mathbb{Z}_m$, será

$$\begin{aligned} \mathbb{Z}_m &= \{[0], [1], \ldots, [m-1]\} \\ &= \{\{n : n = mq, q \in \mathbb{Z}\}, \{n : n = mq+1, q \in \mathbb{Z}\}, \ldots, \{n : n = mq+m-1, q \in \mathbb{Z}\}\} \end{aligned}$$

y lo llamaremos *conjunto de las clases de restos módulo m.*

■

Ejemplo 6.13

En el conjunto de los números enteros se considera la relación de congruencia módulo 5. Hallar las clases de equivalencia del -22, -6, 0, 3, 5, 7, 18 y 20.

Solución

Sea a cualquier número entero. Según acabamos de ver,

$$[a] = [r], \text{ siendo } r \text{ el resto de dividir } a \text{ entre } 5.$$

Entonces,

- $-22 = 5(-5) + 3$, luego $[-22] = [3]$, es decir,
$$[-22] = \{n : n = 5q + 3, q \in \mathbb{Z}\}$$
- $-6 = 5(-2) + 4$, luego $[-6] = [4]$, es decir,
$$[-6] = \{n : n = 5q + 4, q \in \mathbb{Z}\}$$
- $0 = 5 \cdot 0 + 0$, luego
$$[0] = \{n : n = 5q, q \in \mathbb{Z}\}$$
- $3 = 5 \cdot 0 + 3$, luego
$$[3] = \{n : n = 5q + 3, q \in \mathbb{Z}\}$$
- $5 = 5 \cdot 1 + 0$, luego $[5] = [0]$, es decir,
$$[5] = \{n : n = 5q, q \in \mathbb{Z}\}$$
- $7 = 5 \cdot 1 + 2$, luego $[7] = [2]$, es decir,
$$[7] = \{n : n = 5q + 2, q \in \mathbb{Z}\}$$
- $18 = 5 \cdot 3 + 3$, luego $[18] = [3]$, es decir,
$$[18] = \{n : n = 5q + 3, q \in \mathbb{Z}\}$$
- $20 = 5 \cdot 4 + 0$, luego $[20] = [0]$, es decir,
$$[20] = \{n : n = 5q, q \in \mathbb{Z}\}$$

■

6.4 Aritmética en $\mathbb{Z}_m$

6.4.1 Suma

Dados dos enteros cualesquiera a y b, definimos la suma en $\mathbb{Z}_m$ en la forma siguiente:

$$[a] + [b] = [a + b]$$

Ejemplo 6.14

Sumar en el conjunto de las clases de restos módulo 5, $\mathbb{Z}_5$, las clases [31] y [58].

Solución

Según la definición que acabamos de ver,

$$[31] + [58] = [31 + 58] = [89]$$

y como $89 = 5 \cdot 17 + 4$, entonces $[89] = [4]$ de aquí que $[31] + [58] = [4]$.

También podíamos haber hecho lo siguiente:

$$\left.\begin{array}{rcl} 31 = 5 \cdot 6 + 1 & \Longrightarrow & [31] = [1] \\ 58 = 5 \cdot 11 + 3 & \Longrightarrow & [58] = [3] \end{array}\right\} \Longrightarrow [31] + [58] = [1] + [3] = [1 + 3] = [4]$$

■

6.4.2 Bien Definida

La suma está bien definida, es decir, no depende de los representantes que se elijan en cada clase, en el sentido de que si $[a] = [a']$ y $[b] = [b']$, entonces $[a] + [b] = [a'] + [b']$.

Demostración

En efecto,

$$\left.\begin{array}{l} [a] = [a'] \Longleftrightarrow a \equiv a' (\text{mód } m) \\ \text{y} \\ [b] = [b'] \Longleftrightarrow b \equiv b' (\text{mód } m) \end{array}\right\} \Longrightarrow a + b \equiv a' + b' (\text{mód } m) \Longrightarrow [a + b] = [a' + b'] \Longleftrightarrow [a] + [b] = [a'] + [b']$$

■

La suma en $\mathbb{Z}_m$ es asociativa y conmutativa. Veamos, a continuación, cuál es su elemento neutro.

6.4.3 Elemento Neutro para la Suma

El elemento neutro para la suma en $\mathbb{Z}_m$ es la clase $[0]$.

Demostración

Sea $[a]$ cualquiera de $\mathbb{Z}_m$ y sea $[e]$ el neutro para la suma. Entonces,

$$\begin{aligned}[e]+[a]=[a] &\iff [e+a]=[a]\\ &\iff e+a\equiv a(\text{mód } m)\\ &\iff e\equiv a-a(\text{mód } m)\\ &\iff e\equiv 0(\text{mód } m)\\ &\iff [e]=[0]\end{aligned}$$

■

6.4.4 Elemento Opuesto

Si $[a]$ es cualquiera de $\mathbb{Z}_m$, entonces su opuesto es $[-a]$

Demostración

En efecto, sea $[a']$ el opuesto de $[a]$. Entonces,

- Si $a=0$, entonces,
$$[0]+[a']=[0]\Longrightarrow [0+a']=[0]\Longrightarrow [a']=[0]$$
es decir, el opuesto a $[0]$ es él mismo.
- Si $a\neq 0$, entonces,
$$\begin{aligned}[a]+[a']=[0] &\iff [a+a']=[0]\\ &\iff a+a'\equiv 0(\text{mód } m)\\ &\iff a'\equiv -a(\text{mód } m)\\ &\iff [a']=[-a]\end{aligned}$$
Calculemos, pues, $[-a]$. Por definición de clase de equivalencia, (6.3.2), será el conjunto formado por todos los números enteros que den el mismo resto que $-a$ al dividir entre m. Pues bien, por el teorema de existencia y unicidad de cociente y resto, existirán dos enteros únicos, q y r, tales que $a=mq+r$, siendo $0<r<m$ (si r fuera cero, $[a]=[0]$). Entonces,
$$\begin{aligned}a=mq+r &\Longrightarrow -a=m\,(-q)-r\\ &\Longrightarrow -a=m\,(-q)-r+m-m\\ &\Longrightarrow -a=m\,(-q-1)+m-r\end{aligned}$$
donde,
$$0<r<m\Longrightarrow -m<-r<0\Longrightarrow 0<m-r<m$$
es decir, el resto de dividir $-a$ entre m es $m-r$ y, por tanto,
$$[-a]=[m-r]\Longrightarrow [a']=[m-r]$$

■

6.4.5 Producto

Dados dos enteros cualesquiera a y b, definimos el producto en $\mathbb{Z}_m$ en la forma siguiente:

$$[a] \cdot [b] = [a \cdot b]$$

■

6.4.6 Bien Definido

El producto está bien definido, es decir, no depende de los representantes que se elijan en cada clase, en el sentido de que si $[a] = [a']$ y $[b] = [b']$, entonces $[a] \cdot [b] = [a'] \cdot [b']$.

Demostración

En efecto,

$$\left.\begin{array}{l} [a] = [a'] \Longleftrightarrow a \equiv a'(\text{módm}) \\ \text{y} \\ [b] = [b'] \Longleftrightarrow b \equiv b'(\text{módm}) \end{array}\right\} \Longrightarrow a \cdot b \equiv a' \cdot b'(\text{módm}) \Longrightarrow [a \cdot b] = [a' \cdot b'] \Longleftrightarrow [a] \cdot [b] = [a'] \cdot [b']$$

■

El producto en $\mathbb{Z}_m$ es asociativo y conmutativo.

6.4.7 Elemento Neutro para el Producto

El elemento neutro para la multiplicación en $\mathbb{Z}_m$ es la clase $[1]$.

Demostración

En efecto, para cada $[a]$ de $\mathbb{Z}_m$, se verifica que

$$[1] \cdot [a] = [1 \cdot a] = [a]$$

■

6.4.8 Elemento Inverso

Un elemento $[a]$ de $\mathbb{Z}_m$ es invertible (admite inverso) si, y sólo si, a y m son primos entre si.

Demostración

En efecto, sea $[a]$ cualquiera de $\mathbb{Z}_m$. Entonces,

$$\begin{aligned}
[a] \text{ es invertible en } \mathbb{Z}_m &\iff \exists [a'] \in \mathbb{Z}_m : [a][a'] = [1] \\
&\iff \exists [a'] \in \mathbb{Z}_m : [aa'] = [1] \\
&\iff \exists a' \in \mathbb{Z} : aa' \equiv 1(\text{mód } m) \\
&\iff \exists a' \in \mathbb{Z} : m | aa' - 1 \\
&\iff \exists a', q \in \mathbb{Z} : aa' - 1 = mq \\
&\iff \exists a', q \in \mathbb{Z} : aa' - mq = 1 \\
&\iff \text{La ecuación diofántica } aa' - mq = 1 \text{ tiene solución} \\
&\iff \text{m.c.d.}(a, m) | 1 \\
&\iff \text{m.c.d.}(a, m) = 1 \\
&\iff a \text{ y } m \text{ son primos entre sí.}
\end{aligned}$$

Obsérvese que si a'_0 es una solución particular de la ecuación $aa' - mq = 1$, entonces la solución general será

$$a' = a'_0 - mk, \ k \in \mathbb{Z}$$

luego,

$$\begin{aligned}
a' = a'_0 - mk &\iff a' - a'_0 = m(-k), k \in \mathbb{Z} \\
&\iff m | a' - a'_0 \\
&\iff a' \equiv a'_0 (\text{mód } m) \\
&\iff [a'] = [a'_0]
\end{aligned}$$

es decir, $[a'] = [a'_0]$, donde a'_0 es una solución particular de la ecuación. El inverso de un elemento de $\mathbb{Z}_m$, caso de existir, es, por lo tanto, único.

■

Nota 6.1 Observemos lo siguiente:

$$[a] \in \mathbb{Z}_m \iff 0 \leqslant a \leqslant m - 1$$

por lo tanto,

- Si m es primo, entonces m.c.d.$(a, m) = 1$ para todo a distinto de cero, luego todos los elementos de $\mathbb{Z}_m$, excepto el cero, poseen inverso.

Podemos concluir, pues, que *una condición necesaria y suficiente para que todos los elementos de $\mathbb{Z}_m$ distintos de cero posean inverso es que m sea primo.*

■

Ejemplo 6.15

Hallar los inversos de

(a) $[2]$ en $\mathbb{Z}_{11}$

(b) $[7]$ en $\mathbb{Z}_{15}$

(c) $[7]$ en $\mathbb{Z}_{16}$

(d) $[5]$ en $\mathbb{Z}_{13}$

Solución

(a) Inverso de $[2]$ en $\mathbb{Z}_{11}$.

Como 11 es primo, todos los elementos de $\mathbb{Z}_{11}$, excepto el cero, tienen inverso. Sea, pues, x el inverso de $[2]$ en $\mathbb{Z}_{11}$. Entonces,

$$\begin{aligned} x \text{ es el inverso de } [2] \text{ en } \mathbb{Z}_{11} &\iff [2]\cdot x = [1] \text{ en } \mathbb{Z}_{11} \\ &\iff [2x] = [1] \text{ en } \mathbb{Z}_{11} \\ &\iff 2x \equiv 1 (\text{mód } 11) \text{ en } \mathbb{Z} \\ &\iff 11 | 2x-1 \text{ en } \mathbb{Z} \\ &\iff \exists y \in \mathbb{Z} : 2x - 11y = 1 \end{aligned}$$

Tenemos una ecuación diofántica del tipo $ax + by = c$ donde $a = 2$, $b = -11$ y $c = 1$.

1 Solución particular. Utilizamos el algoritmo de Euclides para obtener el máximo común divisor de 2 y -11 y los coeficientes p y q necesarios para el cálculo.

	5	2
11	2	1
1	0	

$$\Longrightarrow \quad d = \text{m.c.d.}(2,-11) = 1 \quad \Longrightarrow \quad 1 = 11 - 5\cdot 2 \quad \Longrightarrow \quad 1 = -5\cdot 2 + (-1)(-11)$$

De aquí que $p = -5$, $q = -1$ y la solución particular será, por tanto,

$$x_0 = \frac{cp}{d} \Longrightarrow x_0 = \frac{1(-5)}{1} \Longrightarrow x_0 = -5$$

2 Solución general.

$$x = x_0 + k\frac{b}{d}, k \in \mathbb{Z} \Longrightarrow x = -5 + k\frac{-11}{1} \Longrightarrow x = -5 - 11k, k \in \mathbb{Z}$$

3 Cálculo del inverso.

$$\begin{aligned} x = -5 - 11k &\iff x = 11(-k) + 5 \\ &\iff x + 5 = 11(-k) \\ &\iff 11 \,|\, x + 5 \\ &\iff x \equiv -5 \,(\text{mód } 11) \\ &\iff x = [-5] \text{ en } \mathbb{Z}_{11} \\ &\iff x = [11-5] \text{ en } \mathbb{Z}_{11} \\ &\iff x = [6] \text{ en } \mathbb{Z}_{11} \end{aligned}$$

luego el inverso de [2] en $\mathbb{Z}_{11}$ es [6].

(b) Inverso de [7] en $\mathbb{Z}_{15}$.

Como 7 y 15 son primos entre sí, 7 tendrá inverso en $\mathbb{Z}_{15}$. Pues bien,

$$\begin{aligned} x \text{ es el inverso de } [7] \text{ en } \mathbb{Z}_{15} &\iff [7x] = [1] \text{ en } \mathbb{Z}_{15} \\ &\iff 7x \equiv 1(\text{mód } 15) \text{ en } \mathbb{Z} \\ &\iff 15|7x-1 \text{ en } \mathbb{Z} \\ &\iff \exists y \in \mathbb{Z} : 7x - 15y = 1 \end{aligned}$$

Ecuación diofántica de la forma $ax + by = c$, donde $a = 7$, $b = -15$ y $c = 1$.

1 Solución particular. Obtenemos el máximo común divisor de los coeficientes, 7 y -15, mediante el algoritmo de Euclides y lo volvemos atrás para obtener los coeficientes p y q necesarios para el cálculo.

	2	7
15	7	1
1	0	

$$\implies d = \text{m.c.d.}(7,-15) = 1 \implies 1 = 15 - 2 \cdot 7 \implies 1 = -2 \cdot 7 + (-1)(-15)$$

Luego, $p = -2$, $q = -1$ y, por tanto, la solución particular de la ecuación es:

$$x_0 = \frac{cp}{d} \Longrightarrow x_0 = \frac{1(-2)}{1} \Longrightarrow x_0 = -2$$

2 Solución general.

$$x = x_0 + k\frac{b}{d}, k \in \mathbb{Z} \Longrightarrow x = -2 + k\frac{-15}{1} \Longrightarrow x = -2 - 15k, k \in \mathbb{Z}$$

3 Cálculo del inverso.

$$\begin{aligned} x = -2 - 15k &\iff x = 15(-k) - 2 \\ &\iff x - (-2) = 15(-k) \\ &\iff 15 \,|x - (-2) \\ &\iff x \equiv -2 \,(\text{mód } 15) \\ &\iff x = [-2] \\ &\iff x = [15 - 2] \\ &\iff x = [13] \end{aligned}$$

luego el inverso de [7] en $\mathbb{Z}_{15}$ es [13].

(c) Inverso de [7] en $\mathbb{Z}_{16}$.

Como 7 y 16 son primos entre sí, [7] tendrá inverso en $\mathbb{Z}_{16}$. Pues bien,

$$\begin{aligned} x \text{ es el inverso de } [7] \text{ en } \mathbb{Z}_{16} &\iff [7x] = [1] \text{ en } \mathbb{Z}_{16} \\ &\iff 7x \equiv 1(\text{mód } 16) \text{ en } \mathbb{Z} \\ &\iff 16|7x-1 \text{ en } \mathbb{Z} \\ &\iff \exists x \in \mathbb{Z} : 7x - 16y = 1 \end{aligned}$$

Tenemos, pues, una ecuación diofántica del tipo $ax + by = c$ con $a = 7$, $b = -16$ y $c = 1$

1 Solución particular. Obtenemos el máximo común divisor de los coeficientes, 7 y -16, mediante el algoritmo de Euclides y lo volvemos atrás para obtener los coeficientes p y q necesarios para el cálculo.

		2	3	2
16	7	2	1	
2	1	0		

$$\Longrightarrow \quad d = \text{m.c.d.}(7,-16) = 1 \quad \Longrightarrow \quad \begin{cases} 1 = 7 - 3 \cdot 2 \\ 2 = 16 - 2 \cdot 7 \end{cases}$$

$$\Longrightarrow \quad 1 = 7 - 3(16 - 2 \cdot 7)$$

$$\Longrightarrow \quad 1 = 7 \cdot 7 + 3(-16)$$

Por lo tanto, $p = 7$, $q = 3$ y, consecuentemente,

$$x_0 = \frac{cp}{d} \Longrightarrow x_0 = \frac{1 \cdot 7}{1} \Longrightarrow x_0 = 7$$

2 Solución general.

$$x = x_0 + k\frac{b}{d} \Longrightarrow x = 7 + k\frac{-16}{1} \Longrightarrow x = 7 - 16k$$

3 Cálculo del inverso.

$$\begin{aligned} x = 7 - 16k &\iff x = 16(-k) + 7 \\ &\iff x - 7 = 16(-k) \\ &\iff 16 \,|x - 7 \\ &\iff x \equiv 7 \,(\text{mód } 16) \\ &\iff x = [7] \end{aligned}$$

luego el inverso de [7] en $\mathbb{Z}_{16}$ es [7].

(d) Inverso de [5] en $\mathbb{Z}_{13}$.

Como 13 es primo, todos los elementos de $\mathbb{Z}_{13}$, excepto el cero, tienen inverso. Lo calcularemos utilizando un procedimiento análogo al utilizado en los apartados anteriores.

$$\begin{aligned} x \text{ es el inverso de } [5] \text{ en } \mathbb{Z}_{13} &\iff [5x] = [1] \text{ en } \mathbb{Z}_{13} \\ &\iff 5x \equiv 1(\text{mód } 13) \text{ en } \mathbb{Z} \\ &\iff 13|5x - 1 \text{ en } \mathbb{Z} \\ &\iff \exists x \in \mathbb{Z} : 5x - 13y = 1 \end{aligned}$$

Ecuación diofántica del tipo $ax + by = c$, donde $a = 5$, $b = -13$ y $c = 1$.

1 Solución particular. Obtenemos el máximo común divisor de los coeficientes, 5 y -13, mediante el algoritmo de Euclides y lo volvemos atrás para obtener los coeficientes p y q necesarios para el cálculo.

		2	1	1	2
13	5	3	2	1	
3	2	1	0		

$$\Longrightarrow \quad d = \text{m.c.d.}(5,-13) = 1$$

luego,

$$\left.\begin{array}{rcrcr} 1 &=& 3 &-& 1 \cdot 2 \\ 2 &=& 5 &-& 1 \cdot 3 \end{array}\right\} \Longrightarrow \quad 1 = 3 - 1(5 - 1 \cdot 3) = (-1) \cdot 5 + 2 \cdot 3$$

$$\left.\begin{array}{rcrcr} 1 &=& (-1) \cdot 5 &+& 2 \cdot 3 \\ 3 &=& 13 &-& 2 \cdot 5 \end{array}\right\} \Longrightarrow \quad 1 = (-1) \cdot 5 + 2(13 - 2 \cdot 5) = (-5) \cdot 5 + 2 \cdot 13$$

es decir,

$$1 = (-5)\cdot 5 + (-2)(-13) \implies p = -5 \text{ y } q = -2$$

Entonces,

$$x_0 = \frac{cp}{d} \Longrightarrow x_0 = \frac{1(-5)}{1} \Longrightarrow x_0 = -5$$

2 Solución general.

$$x = x_0 + k\frac{b}{d} \Longrightarrow x = -5 + k\frac{-13}{1} \Longrightarrow x = -5 - 13k$$

3 Cálculo del inverso.

$$\begin{aligned} x = -5 - 13k &\iff x = 13(-k) - 5 \\ &\iff x - (-5) = 13(-k) \\ &\iff 13 \,|x - (-5) \\ &\iff x \equiv -5 \,(\text{mód } 13) \\ &\iff x = [-5] \\ &\iff x = [13 - 5] \\ &\iff x = [8] \end{aligned}$$

luego el inverso de [5] en $\mathbb{Z}_{13}$ es [8].

■

Ejemplo 6.16

Obtener los opuestos, los inversos y escribir las tablas de sumar y multiplicar en $\mathbb{Z}_5$ y $\mathbb{Z}_6$.

Solución

$\mathbb{Z}_5 = \{[0], [1], [2], [3], [4]\}$

- Opuestos.
  - El opuesto de [0] es, obviamente, [0].
  - El opuesto de [1] es, $[5 - 1] = [4]$.
  - El opuesto de [2] es, $[5 - 2] = [3]$.
  - El opuesto de [3] es, $[5 - 3] = [2]$.
  - El opuesto de [4] es, $[5 - 4] = [1]$.
- Inversos. Como el 5 es primo, todos los elementos de $\mathbb{Z}_5$, excepto el [0] poseen inverso.
  - El inverso de [1] es [1].
  - El inverso de [2] es [3].
  - El inverso de [3] es [2].
  - El inverso de [4] es [4].
- Tabla de sumar.

+	[0]	[1]	[2]	[3]	[4]
[0]	[0]	[1]	[2]	[3]	[4]
[1]	[1]	[2]	[3]	[4]	[0]
[2]	[2]	[3]	[4]	[0]	[1]
[3]	[3]	[4]	[0]	[1]	[2]
[4]	[4]	[0]	[1]	[2]	[3]

⁕ Tabla de multiplicar.

×	[0]	[1]	[2]	[3]	[4]
[0]	[0]	[0]	[0]	[0]	[0]
[1]	[0]	[1]	[2]	[3]	[4]
[2]	[0]	[2]	[4]	[1]	[3]
[3]	[0]	[3]	[1]	[4]	[2]
[4]	[0]	[4]	[3]	[2]	[1]

$\mathbb{Z}_6 = \{[0], [1], [2], [3], [4], [5]\}$

⁕ Opuestos.

- El opuesto de [0] es [0].
- El opuesto de [1] es [5].
- El opuesto de [2] es [4].
- El opuesto de [3] es [3].
- El opuesto de [4] es [2].
- El opuesto de [5] es [1].

⁕ Inversos. Como el [6] no es primo, no todos los elementos de $\mathbb{Z}_6$ tienen inverso.

- m.c.d.$(1, 6) = 1$, luego [1] tiene inverso, el [1].
- m.c.d.$(2, 6) = 2$, luego [2] no tiene inverso.
- m.c.d.$(3, 6) = 3$, luego [3] no tiene inverso.
- m.c.d.$(4, 6) = 2$, luego [4] no tiene inverso.
- m.c.d.$(5, 6) = 1$, luego [5] tiene inverso, el [5].

⁕ Tabla de sumar.

+	[0]	[1]	[2]	[3]	[4]	[5]
[0]	[0]	[1]	[2]	[3]	[4]	[5]
[1]	[1]	[2]	[3]	[4]	[5]	[0]
[2]	[2]	[3]	[4]	[5]	[0]	[1]
[3]	[3]	[4]	[5]	[0]	[1]	[2]
[4]	[4]	[5]	[0]	[1]	[2]	[3]
[5]	[5]	[0]	[1]	[2]	[3]	[4]

⁕ Tabla de multiplicar.

×	[0]	[1]	[2]	[3]	[4]	[5]
[0]	[0]	[0]	[0]	[0]	[0]	[0]
[1]	[0]	[1]	[2]	[3]	[4]	[5]
[2]	[0]	[2]	[4]	[0]	[2]	[4]
[3]	[0]	[3]	[0]	[3]	[0]	[3]
[4]	[0]	[4]	[2]	[0]	[1]	[2]
[5]	[0]	[5]	[4]	[3]	[2]	[1]

■

Nota 6.2 En $\mathbb{Z}$ se verifica la ley de cancelación, es decir, si a, b y c son tres números enteros con $a \neq 0$, se verifica que

$$ab = ac \Longrightarrow b = c$$

En $\mathbb{Z}_m$ esta ley, en general, no se verifica, es decir pueden encontrarse $[a] \neq [0]$, $[b]$ y $[c]$ tales que

$$[a] \cdot [b] = [a] \cdot [c] \text{ y, sin embargo, } [b] \neq [c]$$

Por ejemplo, en $\mathbb{Z}_4$

$$[2]\cdot[1]=[2]\cdot[3] \text{ y, sin embargo, } [1]\neq[3]$$

Obsérvese, también, que en $\mathbb{Z}$ no existen divisores de cero, es decir, para cualquier par de enteros a y b se verifica

$$ab=0\Longrightarrow a=0 \text{ ó } b=0$$

En $\mathbb{Z}_m$ si existen divisores de cero, es decir pueden encontrarse $[a]$ y $[b]$ tales que

$$[a]\cdot[b]=0 \text{ y, sin embargo, } [a]\neq[0] \text{ y } [b]\neq[0]$$

Por ejemplo en $\mathbb{Z}_6$ se tiene que

$$[3]\cdot[2]=[0] \text{ y, sin embargo, } [3]\neq[0] \text{ y } [2]\neq[0]$$

■

Ejemplo 6.17

Resolver el siguiente sistema de ecuaciones en $\mathbb{Z}_7$.

$$\left.\begin{array}{rcrcl} x & + & [2]\,y & = & [4] \\ [4]\,x & + & [3]\,y & = & [4] \end{array}\right\}$$

Solución

Lo resolvemos por los tres métodos tradicionales de la matemática elemental.

⊛ Sustitución.

Despejamos x en la primera ecuación y sustituimos en la segunda.

$$x+[2]\,y=[4]\Longrightarrow x=[4]-[2]\,y\Longrightarrow x=[4]+[-2]\,y\Longrightarrow x=[4]+[5]\,y$$

Entonces,

$$\left.\begin{array}{rcrcl} x & = & [4] & + & [5]\,y \\ [4]\,x & + & [3]\,y & = & [4] \end{array}\right\} \Longrightarrow [4]\,([4]+[5]\,y)+[3]\,y=[4]$$

$$\begin{aligned} &\Longrightarrow [4]\cdot[4]+[4]\cdot[5]\,y+[3]\,y=[4] \\ &\Longrightarrow [2]+[6]\,y+[3]\,y=[4] \\ &\Longrightarrow [2]\,y=[4]-[2] \\ &\Longrightarrow [2]\,y=[4]+[-2] \\ &\Longrightarrow [2]\,y=[4]+[5] \\ &\Longrightarrow [2]\,y=[2] \\ &\Longrightarrow y=[1] \end{aligned}$$

Entonces,,

$$\left.\begin{array}{rcrcl} x & = & [4] & + & [5]\,y \\ y & = & [1] & & \end{array}\right\} \Longrightarrow x=[4]+[5]\cdot[1]\Longrightarrow x=[9]\Longrightarrow x=[2]$$

⊛ Igualación.

Despejamos x en la primera ecuación,

$$x + [2]\,y = [4] \Longrightarrow x = [4] - [2]\,y \Longrightarrow x = [4] + [-2]\,y \Longrightarrow x = [4] + [5]\,y$$

y despejando, también x, en la segunda,

$$\begin{aligned}
[4]\,x + [3]\,y = [4] &\Longrightarrow [4]\,x = [4] - [3]\,y \\
&\Longrightarrow [4]\,x = [4] + [-3]\,y \\
&\Longrightarrow [4]\,x = [4] + [4]\,y \\
&\Longrightarrow x = [4]^{-1} \cdot [4] + [4]^{-1} \cdot [4]\,y \quad \left\{[4]^{-1} \text{ Inverso de } [4] \text{ en } \mathbb{Z}_7 \text{ es } [2]\right\} \\
&\Longrightarrow x = [2] \cdot [4] + [2] \cdot [4]\,y \\
&\Longrightarrow x = [1] + [1]\,y
\end{aligned}$$

Igualando ambos resultados,

$$\begin{aligned}
[4] + [5]\,y = [1] + [1]\,y &\Longrightarrow [5]\,y - [1]\,y = [1] - [4] \\
&\Longrightarrow [5]\,y + [-1]\,y = [1] + [-4] \\
&\Longrightarrow [5]\,y + [6]\,y = [1] + [3] \\
&\Longrightarrow [4]\,y = [4] \\
&\Longrightarrow y = [1]
\end{aligned}$$

Consecuentemente,

$$\left.\begin{array}{rcl} x &=& [4] + [5]\,y \\ y &=& [1] \end{array}\right\} \Longrightarrow x = [4] + [5] \cdot [1] \Longrightarrow x = [2]$$

⊛ Reducción.

Multiplicamos la primera ecuación por [3], la segunda por [1] y las sumamos.

$$\left.\begin{array}{rcl} x + [2]\,y &=& [4] \\ [4]\,x + [3]\,y &=& [4] \end{array}\right\} \Longrightarrow \left.\begin{array}{rcl} [3]\,x + [6]\,y &=& [5] \\ [4]\,x + [3]\,y &=& [4] \end{array}\right\} \Longrightarrow [2]\,y = [2] \Longrightarrow y = [1]$$

Análogamente, multiplicando la primera por [2], la segunda por [1] y sumándolas posteriormente,

$$\left.\begin{array}{rcl} x + [2]\,y &=& [4] \\ [4]\,x + [3]\,y &=& [4] \end{array}\right\} \Longrightarrow \left.\begin{array}{rcl} [2]\,x + [4]\,y &=& [1] \\ [4]\,x + [3]\,y &=& [4] \end{array}\right\}$$

$$\begin{aligned}
&\Longrightarrow [6]\,x = [5] \\
&\Longrightarrow x = [6]^{-1} \cdot [5] \\
&\Longrightarrow x = [6] \cdot [5] \\
&\Longrightarrow x = [2]
\end{aligned}$$

■

Ejemplo 6.18

Resolver la ecuación $[1]\,x^2 + [3]\,x + [4] = 0$ en $\mathbb{Z}_{11}$.

Solución

$$\begin{aligned}
x &= \frac{-[3] \pm \sqrt{([3])^2 - 4 \cdot [1] \cdot [4]}}{2 \cdot [1]} \\
&= \frac{[-3] \pm \sqrt{[3] \cdot [3] - [16]}}{[2]} \\
&= \frac{[8] \pm \sqrt{[9] + [-16]}}{[2]} \\
&= \frac{[8] \pm \sqrt{[9] + [6]}}{[2]} \\
&= \frac{[8] \pm \sqrt{[4]}}{[2]} \\
&= \frac{[8] \pm \sqrt{[2] \cdot [2]}}{[2]} \\
&= \frac{[8] \pm \sqrt{([2])^2}}{[2]} \\
&= ([8] \pm [2]) \cdot [2]^{-1} \\
&= ([8] \pm [2]) \cdot [6] && \{\text{El inverso de } [2] \text{ en } \mathbb{Z}_{11} \text{ es } [6]\} \\
&= [8] \cdot [6] \pm [2] \cdot [6] \\
&= [4] \pm [1] \\
&= \begin{cases} [5] \\ [3] \end{cases}
\end{aligned}$$

■

Ejemplo 6.19

Demostrar que en $\mathbb{Z}_p$, con p primo, se verifica la igualdad $(x+y)^p = x^p + y^p$.

Solución

Por el Teorema del Binomio, tendremos

$$(x+y)^p = x^p + \sum_{k=1}^{p-1} \binom{p}{k} x^{p-k} y^k + y^p \tag{6.2}$$

Pues bien,

$$\left(\begin{array}{c} p \\ k \end{array}\right) = \frac{p!}{k!(p-k)!} \implies k!\left(\begin{array}{c} p \\ k \end{array}\right) = \frac{p!}{(p-k)!}$$

$$\implies k!\left(\begin{array}{c} p \\ k \end{array}\right) = p(p-1)\cdots(p-k+1)$$

$$\implies p \left| k!\left(\begin{array}{c} p \\ k \end{array}\right)\right.$$

Por otra parte, como p es primo, p y k serán primos entre sí para $1 < k < p$, es decir,

$$\text{m.c.d.}(p,k) = 1,\ 1 < k < p$$

y aplicando reiteradamente el ejemplo 3.24 , tendremos que

$$\text{m.c.d.}\,(p,k!) = 1$$

Así pues,

$$p \left| k!\left(\begin{array}{c} p \\ k \end{array}\right)\right. \text{ y m.c.d.}\,(p,k!) = 1$$

luego por el Lema de Euclides,

$$p \left| \left(\begin{array}{c} p \\ k \end{array}\right)\right.$$

es decir,

$$\left(\begin{array}{c} p \\ k \end{array}\right) \equiv 0(\text{mód } p) \text{ para } 1 < k < p$$

o lo que es igual,

$$\left(\begin{array}{c} p \\ k \end{array}\right) = 0$$

para $1 < k < p$ en $\mathbb{Z}_p$. Por lo tanto,

$$\sum_{k=1}^{p-1}\left(\begin{array}{c} p \\ k \end{array}\right)x^{p-k}y^k = \sum_{k=1}^{p-1} 0x^{p-k}y^k = 0.$$

Sustituimos este resultado en (6.2) y

$$(x+y)^p = x^p + y^p$$

■

Ejemplo 6.20

Demostrar que para p, primo, $3^p + (-2)^p + (-1)^p$ es divisible por p.

Solución

Observemos lo siguiente: $3^p + (-2)^p + (-1)^p$ será divisible por p, si da resto cero al dividirlo por p, es decir, si

$$3^p + (-2)^p + (-1)^p \equiv 0(\text{mód } p) \text{ en } \mathbb{Z}$$

lo cual es lo mismo que decir que

$$3^p + (-2)^p + (-1)^p = 0 \text{ en } \mathbb{Z}_p.$$

Así pues, si probamos esto último, tendremos resuelta la demostración.

Pues bien,

$$\begin{aligned} 3^p + (-2)^p + (-1)^p &= (3 + (-2))^p + (-1)^p && \{\text{Ejemplo anterior}\} \\ &= 1^p + (-1)^p \\ &= (1 + (-1))^p && \{\text{Ejemplo anterior}\} \\ &= 0^p \\ &= 0 \end{aligned}$$

y, consecuentemente, el número propuesto es divisible por p.

■

Ejemplo 6.21

En el conjunto $\mathbb{Z}_5$ de las clases de restos módulo 5, se pide:

(a) Divisores de cero.

(b) Elementos invertibles.

(c) Resolver el siguiente sistema de ecuaciones.

$$\left.\begin{array}{rcrcl} [2]\,x & + & y & = & [2] \\ [3]\,x & + & [4]\,y & = & [3] \end{array}\right\}$$

Solución

(a) Veamos si $\mathbb{Z}_5$ tiene divisores de cero.

Recordemos que

$$\mathbb{Z}_5 \text{ no tiene divisores de cero } \iff \forall\, [a], [b] \in \mathbb{Z}_5 : [a] \cdot [b] = [0] \Longrightarrow [a] = [0] \text{ ó } [b] = [0]$$

por lo tanto,

$$\mathbb{Z}_5 \text{ tiene divisores de cero } \iff \exists\, [a], [b] \in \mathbb{Z}_5 : [a] \cdot [b] = 0 \text{ y } [a] \neq [0] \text{ y } [b] \neq [0]$$

Pues bien, sean $[a]$ y $[b]$ cualesquiera de $\mathbb{Z}_5$. Entonces,

$$\begin{aligned} [a] \cdot [b] = [0] \text{ en } \mathbb{Z}_5 &\iff ab \equiv 0(\text{mód } 5) \text{ en } \mathbb{Z} \\ &\iff 5|ab \text{ en } \mathbb{Z} \\ &\iff 5|a \text{ ó } 5|b \text{ en } \mathbb{Z} \ \{\text{Corolario 4.3.2}\} \\ &\iff a \equiv 0(\text{mód } 5) \text{ ó } b \equiv 0(\text{mód } 5) \text{ en } \mathbb{Z} \\ &\iff [a] = [0] \text{ ó } [b] = [0] \text{ en } \mathbb{Z}_5 \end{aligned}$$

Por lo tanto, $\mathbb{Z}_5$ no tiene divisores de cero.

(b) Elementos invertibles. Como 5 es primo todos los elementos de $\mathbb{Z}_5$, excepto el $[0]$, son invertibles.

(c) Resolvamos el sistema de ecuaciones propuesto.

$$\left.\begin{array}{rcrcl} [2]\,x & + & y & = & [2] \\ [3]\,x & + & [4]\,y & = & [3] \end{array}\right\}$$

Obsérvese que la segunda ecuación es igual a la primera multiplicada por $[4]$, luego ambas ecuaciones son equivalentes en $\mathbb{Z}_5$, entonces,

$$[2]\,x + y = [2] \Longleftrightarrow y = [2] - [2]\,x \Longleftrightarrow y = [2] + [-2]\,x \Longleftrightarrow y = [2] + [3]\,x : x \in \mathbb{Z}_5$$

y las soluciones serían:

Para $x = [0]\,,\ y = [2]$
Para $x = [1]\,,\ y = [0]$
Para $x = [2]\,,\ y = [3]$
Para $x = [3]\,,\ y = [1]$
Para $x = [4]\,,\ y = [4]$

■

6.5 Ecuaciones Lineales en $\mathbb{Z}_m$

Planteamos, a continuación, ecuaciones del tipo $ax = b$ donde a y b son de $\mathbb{Z}_m$ y x es la indeterminada. Resolver esta ecuación significa obtener todos los números en $\mathbb{Z}_m$ que al ser escritos en lugar de la indeterminada, verifiquen la ecuación.

Veremos que la resolución de una ecuación de este tipo equivale a la de una ecuación diofántica.

6.5.1 Teorema

La ecuación $[a]\,x = [b]$ tiene solución en $\mathbb{Z}_m$ si, y sólo si el máximo común divisor de a y m divide a b

Demostración

En efecto, sean $[a]$ y $[b]$ cualesquiera de $\mathbb{Z}_m$. Entonces,

$$\begin{array}{lll} \text{x es solución de la ecuación } [a]\,x = [b] \text{ en } \mathbb{Z}_m & \Longleftrightarrow & [ax] = [b] \\ & \Longleftrightarrow & ax \equiv b(\text{mód } m) \\ & \Longleftrightarrow & m|ax - b \\ & \Longleftrightarrow & \exists y \in \mathbb{Z} : ax - b = my \\ & \Longleftrightarrow & \exists y \in \mathbb{Z} : ax - my = b \\ & \Longleftrightarrow & \text{La ecuación diofántica } ax - my = b \text{ tiene solución en } \mathbb{Z} \\ & \Longleftrightarrow & \text{m.c.d.}(a, -m)|b \ \{5.2.1\} \\ & \Longleftrightarrow & \text{m.c.d.}(a, m)|b \end{array}$$

Ejemplo 6.22

Resolver las siguientes ecuaciones en los conjuntos de clases de restos que se indican.

(a) $[5]\,x = [8]$ en $\mathbb{Z}_6$.

(b) $[15]\,x = [6]$ en $\mathbb{Z}_{21}$

(c) $[3]\,x = [27]$ en $\mathbb{Z}_6$.

(d) $[3]\,x = [8]$ en $\mathbb{Z}_6$.

(e) $[12]\,x = [45]$ en $\mathbb{Z}_3$.

Solución

(a) $[5]\,x = [8]$ en $\mathbb{Z}_6$.

$$\begin{aligned} x \text{ es solución de } [5]\,x = [8] \text{ en } \mathbb{Z}_6 &\iff [5x] = [8] \\ &\iff 5x \equiv 8(\text{mód } 6) \\ &\iff 6 \,|5x - 8 \\ &\iff \exists y \in \mathbb{Z} : 5x - 8 = 6y \\ &\iff \exists y \in \mathbb{Z} : 5x - 6y = 8 \end{aligned}$$

La ecuación anterior será, por tanto, una ecuación diofántica del tipo $ax + by = c$ con $a = 5$, $b = -6$ y $c = 8$.

1 Veamos si la ecuación propuesta tiene solución.
Obtenemos el máximo común divisor de 5 y -6 mediante el algoritmo de Euclides y lo volvemos atrás para obtener los coeficientes p y q necesarios para el cálculo.

	1	5
6	5	1
1	0	

$$\Longrightarrow \quad d = \text{m.c.d.}(5, -6) = 1 \quad \Longrightarrow \quad 1 = 6 - 1 \cdot 5 \quad \Longrightarrow \quad 1 = -1 \cdot 5 + (-1)(-6)$$

Luego, $p = -1$ y $q = -1$.
Como 1, máximo común divisor de 5 y -6, divide a 8, según el teorema anterior, (6.5.1), la ecuación tiene solución.

2 Solución particular.

$$x_0 = \frac{cp}{d} \Longrightarrow x_0 = \frac{8(-1)}{1} \Longrightarrow x_0 = -8$$

3 Solución general.

$$x = x_0 + k\frac{b}{d}, k \in \mathbb{Z} \Longrightarrow x = -8 + k\frac{-6}{1}, k \in \mathbb{Z} \Longrightarrow x = -8 - 6k, k \in \mathbb{Z}$$

4 Solución de la ecuación propuesta.

$$\begin{aligned} x = -8 - 6k &\iff x = 6(-k) - 8 \\ &\iff x - (-8) = 6(-k) \\ &\iff 6 \,|x - (-8) \\ &\iff x \equiv -8 \,(\text{mód } 6) \\ &\iff x = [-8] \\ &\iff x = [6 - 2] \\ &\iff x = [4] \end{aligned}$$

(b) $[15]\,x = [6]$ en $\mathbb{Z}_{21}$.

$$\begin{aligned} x \text{ es solución de la ecuación } [15]\,x = 6 \text{ en } \mathbb{Z}_{21} &\iff [15x] = [6] \\ &\iff 15x \equiv 6(\text{mód } 21) \\ &\iff 21 \,|\, 15x - 6 \\ &\iff \exists y \in \mathbb{Z} : 15x - 6 = 21y \\ &\iff \exists y \in \mathbb{Z} : 15x - 21y = 6 \end{aligned}$$

Ecuación diofántica del tipo $ax + by = c$ con $a = 15$, $b = -21$ y $c = 6$.

1 Veamos, primero, si la ecuación propuesta tiene solución.
Obtenemos el máximo común divisor de 15 y -21 mediante el algoritmo de Euclides y lo volvemos atrás para obtener los coeficientes p y q necesarios para el cálculo.

		1	2	2
	21	15	6	3
	6	3	0	

$$\Longrightarrow \quad d = \text{m.c.d.}(15, -21) = 3 \quad \Longrightarrow \quad \begin{cases} 3 = 15 - 2 \cdot 6 \\ 6 = 21 - 1 \cdot 15 \end{cases}$$

$$\begin{aligned} &\Longrightarrow \quad 3 = 15 - 2(21 - 1 \cdot 15) \\ &\Longrightarrow \quad 3 = 3 \cdot 15 + 2(-21) \\ &\Longrightarrow \quad p = 3 \text{ y } q = 2 \end{aligned}$$

Como 3, máximo común divisor de 15 y -21, divide a 6, según el teorema anterior, (6.5.1), la ecuación tiene solución.

2 Solución particular.

$$x_0 = \frac{cp}{d} \Longrightarrow x_0 = \frac{6 \cdot 3}{3} \Longrightarrow x_0 = 6$$

3 Solución general.

$$x = x_0 + k_1 \frac{b}{d}, k \in \mathbb{Z} \Longrightarrow x = 6 + k\frac{-21}{3}, k \in \mathbb{Z} \Longrightarrow x = 6 - 7k, k \in \mathbb{Z}$$

4 Solución de la ecuación propuesta.
Tenemos que $x = -7k + 6$ y queremos que x sea igual a una potencia de 21 más un resto. Para conseguir esto dividimos k por 3, máximo común divisor obtenido anteriormente. Entonces, por el Teorema de existencia y unicidad de cociente y resto,

$$k = 3q + r, \ 0 \leqslant r < 3$$

Sustituyendo,

$$\left.\begin{aligned} x &= -7k + 6 \\ k &= 3q + r \end{aligned}\right\} \quad \Longrightarrow \quad x = -7(3q + r) + 6 \quad \Longrightarrow \quad x = 21(-q) + 6 - 7r, \ 0 \leqslant r < 3$$

luego,

- para $r = 0$,
$$x = 21(-q) + 6 \Longrightarrow x = [6]$$
- para $r = 1$,
$$x = 21(-q) - 1 \Longrightarrow x = [-1] \Longrightarrow x = [20]$$
- para $r = 2$,
$$x = 21(-q) - 8 \Longrightarrow x = [-8] \Longrightarrow x = [13]$$

(c) $[3]\,x = [27]$ en $\mathbb{Z}_6$.

$$\begin{aligned} x \text{ es solución de la ecuación } [3]\,x = [27] \text{ en } \mathbb{Z}_6 &\iff [3x] = [27] \\ &\iff 3x \equiv 27(\text{mód } 6) \\ &\iff 6|3x - 27 \text{ en } \mathbb{Z} \\ &\iff \exists y \in \mathbb{Z} : 3x - 6y = 27 \end{aligned}$$

Ecuación diofántica del tipo $ax + by = c$ con $a = 3$, $b = -6$ y $c = 27$.

1 Veamos, primero, si la ecuación propuesta tiene solución.
m.c.d.$(3, -6) = 3$ y como 3 divide a 27, según el teorema anterior, (6.5.1), la ecuación tiene solución. Por otra parte,

$$d = \text{m.c.d.}(3, -6) = 3 \Longrightarrow 3 = 1 \cdot 3 + 0(-6) \Longrightarrow p = 1 \text{ y } q = 0$$

2 Solución particular de la ecuación diofántica.

$$x_0 = \frac{cp}{d} \Longrightarrow x_0 = \frac{27 \cdot 1}{3} \Longrightarrow x_0 = 9$$

3 Solución general.

$$x = x_0 + k\frac{b}{d} \Longrightarrow x = 9 - 2k,\ k \in \mathbb{Z}$$

4 Solución de la ecuación propuesta.
Tenemos que $x = -2k + 9$ y queremos que x sea igual a una potencia de 6 más un resto. Para conseguir esto dividimos k por 3, máximo común divisor obtenido anteriormente. Entonces, por el Teorema de existencia y unicidad de cociente y resto,

$$k = 3q + r,\ 0 \leqslant r < 3$$

Sustituyendo,

$$\left.\begin{aligned} x &= -2k + 9 \\ k &= 3q + r \end{aligned}\right\} \Longrightarrow \quad x = -2(3q + r) + 9 \quad \Longrightarrow \quad x = 6(-q) + 9 - 2r,\ 0 \leqslant r < 3$$

luego,

- para $r = 0$,
$$x = 6(-q) + 9 \Longrightarrow x = [9] \Longrightarrow x = [3]$$
- para $r = 1$,
$$x = 6(-q) + 7 \Longrightarrow x = [7] \Longrightarrow x = [1]$$
- para $r = 2$,
$$x = 6(-q) + 5 \Longrightarrow x = [5]$$

(d) $[3]\,x = [8]$ en $\mathbb{Z}_6$.

$$\begin{aligned} \text{La ecuación } [3]\,x = [8] \text{ tiene solución en } \mathbb{Z}_6 &\iff [3x] = [8] \\ &\iff 3x \equiv 8(\text{mód } 6) \\ &\iff 6|3x - 8 \text{ en } \mathbb{Z} \\ &\iff \exists y \in \mathbb{Z} : 3x - 6y = 8 \\ &\iff \text{m.c.d.}(3, -6)\,|8 \\ &\iff 3\,|8 \end{aligned}$$

Como 3 no divide a 8, la ecuación propuesta no tiene solución.

(e) $[12]\,x = [45]$ en $\mathbb{Z}_3$.

Obsérvese que

$$[12] = [0] \text{ en } \mathbb{Z}_3 \text{ y } [45] = [0] \text{ en } \mathbb{Z}_3$$

luego,

$$\begin{aligned} [12]\,x = [45] \text{ en } \mathbb{Z}_3 &\iff [0]\,x = [0] \text{ en } \mathbb{Z}_3 \\ &\iff x \text{ es cualquiera de } \mathbb{Z}_3 \\ &\iff \begin{cases} x = [0] \text{ en } \mathbb{Z}_3 \\ \text{ó} \\ x = [1] \text{ en } \mathbb{Z}_3 \\ \text{ó} \\ x = [2] \text{ en } \mathbb{Z}_3 \end{cases} \end{aligned}$$

■