Elementos de Matemáticas I

Carlos Uzcátegui
Departamento de Matemáticas
Facultad de Ciencias
Universidad de Los Andes
uzca@ula.ve

Versión: Agosto 2006

Índice general

Prólogo **v**

1. Conjuntos **1**
1.1. Nociones básicas . . . 1
1.1.1. Definiciones por comprensión y por extensión . . . 1
1.1.2. Igualdad de conjuntos. . . . 6
1.1.3. El conjunto vacío . . . 7
1.1.4. Subconjuntos . . . 7
1.1.5. El conjunto potencia . . . 8
1.2. Las operaciones elementales . . . 11
1.2.1. Diagramas de Venn . . . 14
1.3. Ejercicios suplementarios del capítulo 1 . . . 18

2. Lógica Simbólica **21**
2.1. Proposiciones y fórmulas proposicionales . . . 21
2.1.1. Conectivos lógicos . . . 22
2.1.2. Tablas de verdad . . . 27
2.1.3. Otras expresiones formales . . . 31
2.2. Cálculo proposicional . . . 32
2.2.1. Equivalencia lógica . . . 33
2.2.2. Implicación lógica . . . 35
2.3. La lógica y las operaciones sobre conjuntos . . . 38
2.4. Cuantificadores . . . 38

3. Conjuntos (continuación) **47**
3.1. Propiedades de las operaciones entre conjuntos . . . 47
3.1.1. Algunas propiedades de la relación $\subseteq$ . . . 47
3.1.2. La igualdad de conjuntos . . . 49
3.1.3. Unión e intersección . . . 50
3.1.4. Complementación . . . 55
3.1.5. Diferencia simétrica . . . 57
3.2. Contraejemplos . . . 60
3.3. Lógica y álgebra Booleana (continuación) . . . 62
3.4. Demostraciones . . . 64
3.4.1. Afirmaciones condicionales . . . 64

3.4.2. Afirmaciones universales 64
3.4.3. Demostraciones por reducción al absurdo 64
3.4.4. Lógica de las igualdades 65
3.4.5. Resumen 66
3.5. Ejercicios suplementarios del capítulo 3 67

4. El Principio de Inducción Matemática 69
4.1. El Principio de buena ordenación 69
4.1.1. Máximo de un conjunto 72
4.2. Sucesiones 76
4.2.1. Sucesiones equivalentes 78
4.2.2. Sucesiones finitas 79
4.2.3. Sumatorias y productorias 80
4.3. El Principio de Inducción 83
4.3.1. Algunas aplicaciones del Principio de inducción 84
4.3.2. Variantes del principio de inducción 90
4.4. Definiciones por recursión 96

5. Los Números Enteros 101
5.1. El Teorema Fundamental de la Aritmética 101
5.2. El algoritmo de la división 106
5.3. El principio del mínimo entero 111
5.4. Demostración del algoritmo de la división 113
5.5. Divisibilidad 115
5.6. Ecuaciones diofánticas 117
5.7. El máximo común divisor 119
5.8. El algoritmo de Euclides 121
5.8.1. Demostración de la correctitud del algoritmo de Euclides 122
5.9. Propiedades del máximo común divisor 123
5.9.1. Demostración de las propiedades del mcd 128
5.10. La ecuación $ax + by = c$ 131
5.11. El mínimo común múltiplo 138
5.12. Algunas propiedades de los números primos 140
5.13. La relación de congruencia 144
5.13.1. ¿Cómo se usan las congruencias? 148
5.13.2. Ecuaciones de congruencia 150
5.14. Ejercicios suplementarios del capítulo 5 157

Prólogo

La naturaleza esencialmente abstracta de las matemáticas y el énfasis que hace en el rigor lógico de sus argumentos son sin duda dos de sus características mas importantes. Aquel que se inicie en el estudio de las matemáticas se enfrenta precisamente con esas dos dificultades: la abstracción y el rigor lógico. Estas dificultades están íntimamente ligadas entre sí a través del lenguaje especial que usamos para enunciar, transmitir y crear el conocimiento matemático. Por esta razón es fundamental que el estudiante conozca y domine ese lenguaje. En estas notas hemos tratado de presentar algunas de las ideas y herramientas básicas que necesitará un estudiante de matemáticas durante todos sus estudios de licenciatura. A pesar de la naturaleza abstracta de las matemáticas y de su parafernalia simbólica, creemos que sus ideas fundamentales se pueden motivar de tal manera que el estudiante no termine pensando que la matemática es sólo una inmensa cadena de teoremas entrelazados entre sí.

Estas notas están dirigidas a estudiantes que inician los estudios de licenciatura en Matemáticas. Los requisitos para su lectura se reducen a lo visto en el bachillerato. Fueron escritas entre los años 1997 y 1999 y desde entonces han sido objeto de varias revisiones. En varios momentos de su elaboración hemos consultado los libros [1, 5, 6, 9, 11, 12]. Deseo agradecer a los profesores Hernando Gaitán, Olga Porras, Oswaldo Araujo, Juan Rada, Ernesto Zamora, Giorgio Bianchi y María González y a sus estudiantes quienes han usado estas notas y me han hecho observaciones y sugerencias[1].

[1]Los comentarios, observaciones y sugerencias que el lector tenga sobre estas notas puede enviarlos al autor al correo electrónico uzca@ula.ve

Capítulo 1

Conjuntos

Se puede decir, sin exagerar, que todas las teorías matemáticas se pueden expresar en términos de la noción de conjunto. Sin embargo, es interesante también notar que fué sólo a comienzos del siglo XX cuando se inició el estudio sistemático de los conjuntos. Es decir, una parte importante de las matemáticas se desarrolló sin hacer uso de los conjuntos. Hoy en día son imprescindibles. En este capítulo introduciremos el lenguaje básico de los conjuntos. Más adelante (en el capítulo 3), después que tengamos a nuestra disposición las herramientas de la lógica, continuaremos con el estudio de sus propiedades.

1.1. Nociones básicas

Un conjunto es una colección de objetos. Usaremos letras mayúsculas como A, B, X para denotar conjuntos y letras minúsculas como a, b, c, x para denotar los objetos. Un objeto a que pertenece a un conjunto X se dice que es un **miembro** o **elemento** de X. Escribiremos $a \in X$ para indicar que a es un elemento del conjunto X. En caso que a no pertenezca a X escribiremos $a \notin X$. La expresión $a \in X$ puede leerse de varias maneras equivalentes: *a pertenece a X*, *a es un elemento de X*, *a está en X*.

1.1.1. Definiciones por comprensión y por extensión

Comenzaremos esta sección presentando algunos ejemplos de conjuntos.

Ejemplos 1.1. 1. Consideremos el conjunto formado por los números 1,2,3 y 4. Denotaremos este conjunto con el símbolo

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

Las llaves { } se usarán siempre en las definiciones de conjuntos. Es indiferente el orden en que se escriban los elementos de un conjunto. El conjunto anterior es igual a

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

Cuando un conjunto se define dando la lista completa de todos sus miembros decimos que el conjunto está definido por **extensión**.

2. En muchos casos no es posible o no es fácil dar la lista completa de todos los elementos de un conjunto, en su lugar se da una propiedad que satisfacen única y exclusivamente los elementos del conjunto. Por ejemplo, consideremos el conjunto formado por todos los números naturales que dividen a 2346. Denotemos con la letra A este conjunto. Si quisiéramos, podríamos dar la lista completa de todos los elementos de A, pero nos tomaría mucho tiempo hacerlo. Por ejemplo $2 \in A$, $6 \in A$, $7 \notin A$, $\frac{1}{4} \notin A$. Podemos expresar la definición de A de la manera siguiente

$$A = \{n : n \text{ es un número natural que divide a } 2346\}.$$

Este tipo de definiciones, muy frecuentes en matemáticas, se llaman definiciones por **comprensión**. Todas ellas tienen la siguiente forma

$$\{ : \quad \}.$$

Antes de los dos puntos : (que se leen *tal que*) se coloca una variable (por ejemplo n, x) que denota los objetos que forman al conjunto que estamos definiendo. Después de los dos puntos se escribe la propiedad que satisfacen única y exclusivamente los objetos que pertenecen al conjunto en cuestión.

3. Consideremos el conjunto de todos los números naturales que al dividirlos por 5 dan resto 2. Denotemos este conjunto con la letra A. Podemos verificar fácilmente que $7 \in A$ y $8 \notin A$. Si alguien nos dice un número podemos, después de algunos cálculos sencillos, determinar si el número en cuestión pertenece o no al conjunto A. Sin embargo, no podemos dar la lista completa de los elementos de A pues es infinita. Podemos expresar la definición de A de la manera siguiente

$$A = \{n : n \text{ es un número natural que al dividirlo por 5 da resto 2}\}.$$

Más adelante veremos otros ejemplos similares.

$\square$[1]

Algunos conjuntos en matemáticas aparecen con tanta frecuencia y son de tal importancia que han recibido una notación especial. Veamos algunos de ellos: El conjunto de los **números naturales** se denota con el símbolo $\mathbb{N}$.

$$\mathbb{N} = \{0, 1, 2, 3, 4 \cdots\}.$$

El conjunto de los **números enteros**

$$\cdots, -4, -3, -2, -1, 0, 1, 2, 3, 4, \cdots$$

que está formado por los números naturales junto con sus opuestos y lo denotamos con $\mathbb{Z}$. El conjunto de los **números racionales**, denotado con el símbolo $\mathbb{Q}$, consiste de los números

[1] El símbolo $\square$ lo usamos para indicar que hemos terminado una definición, una demostración o la presentación de un ejemplo.

fraccionarios, es decir, de las expresiones de la forma $\frac{n}{m}$ donde n y m son enteros y m es distinto de cero. Por ejemplo, los siguiente números son racionales

$$\frac{1}{2}, \frac{35}{6}, -\frac{3}{5}, \frac{12}{55}, \frac{3}{7}.$$

Los números racionales contienen a todos los enteros, pues la fracción de la forma $\frac{n}{1}$ representa al entero n. Por ejemplo, $\frac{2}{1}$ es el número 2 y $\frac{-5}{1}$ es el -5.

Los **números reales** se representa con expresiones decimales finitas e infinitas de la forma

$$3,141592653589\cdots \qquad 1,414213562373095\cdots$$

(por cierto, el primero es una aproximación del famoso número π que corresponde a la mitad de la longitud de una circunferencia de radio 1 y el segundo es una aproximación de $\sqrt{2}$). El conjunto de los números reales se denota por $\mathbb{R}$.

Teniendo estos conjuntos a nuestra disposición, ahora es más fácil definir otros conjuntos por comprensión.

Ejemplos 1.2. 1. El orden de los números enteros lo denotamos con el símbolo $<$. La expresión $n < m$ se lee *"n es menor que m"*. También escribiremos $n > m$ para indicar lo mismo que $n < m$. En general, también usará el símbolo $<$ para el orden entre los números reales. El símbolo $\leq$ se lee *"menor o igual que"*. Por ejemplo $n \leq m$ indica que n es menor que m o que n es igual a m. Esto también se escribe $n \geq m$.

Podemos usar $<$ para definir conjuntos. Por ejemplo:

$$\{m : m \in \mathbb{Z} \text{ y } -4 < m\}$$

que consiste de todos los enteros mayores que -4. Observe que después de los dos puntos se escribe la condición que deben tener los elementos del conjunto que estamos definiendo. En este caso, pedimos dos condiciones: que sean enteros y que sean mayores que -4.

2. Consideremos el siguiente conjunto

$$\{m : m \in \mathbb{Q} \text{ y } -4 < m\}.$$

Notemos la similitud de esta definición con la que aparece en el ejemplo anterior. Sin embargo, estos dos conjuntos no son iguales, pues $\frac{-7}{2}$ pertenece al que acabamos de definir pero no pertenece al que definimos en el ejemplo anterior (¿por qué?).

3. También es común usar la siguiente notación

$$\{m \in \mathbb{Z} : -4 < m\}$$

que de inmediato le indica al lector el tipo de objetos que forman el conjunto que se define, en este caso, el conjunto contiene sólo números enteros. Es importante que el

lector comprenda que estas dos formas de describir los conjuntos son equivalentes. Es decir,

$$\{m : m \in \mathbb{Z} \text{ y } -4 < m\} = \{m \in \mathbb{Z} : -4 < m\}.$$

La descripción de la derecha es de uso más frecuente que la de la izquierda.

4. En general la forma de definir conjuntos por comprensión es la siguiente: Tenemos un conjunto X y una propiedad P. Definimos otro conjunto como sigue

$$\{x \in X : x \text{ tiene la propiedad } P\}.$$

En resumen tenemos que

$$\{x \in X : x \text{ tiene la propiedad } P\} = \{x : x \in X \text{ y } x \text{ tiene la propiedad } P\}.$$

5. El siguiente es otro ejemplo de un conjunto definido por compresión

$$\{x \in \mathbb{N} : 3 \leq x < 8\}.$$

En este caso es fácil dar una lista completa de sus elementos

$$\{3, 4, 5, 6, 7\}.$$

6. Recuerde que es irrelevante la letra usada para la variable en las definiciones por compresión. Por ejemplo

$$\{x \in \mathbb{N} : 3 \leq x < 8\} = \{n \in \mathbb{N} : 3 \leq n < 8\}.$$

□

Ejemplo 1.3. Considere el siguiente conjunto

$$A = \{x \in \mathbb{Z} : x = n^2 - n \text{ para algún } n \in \{1, 2, 3, 4\}\}.$$

El conjunto A está definido por comprensión. Sin embargo, en este caso podemos también dar una descripción de A por extensión, es decir, podemos dar una lista completa de todos sus elementos:

n	$n^2 - n$
1	0
2	2
3	6
4	12

En resumen, tenemos que

$$A = \{0, 2, 6, 12\}.$$

Note que la frase *"para algún $n \in \{1, 2, 3, 4\}$"* indica que la variable n puede tomar cualquiera de los valores 1,2,3 o 4 y además, para hacer la lista completa de los elementos de A, debemos considerar todas esas alternativas.

□

El primer conjunto definido en los ejemplos 1.2 también suele representarse de la siguiente manera

$$\{-3, -2, -1, 0, 1, 2, 3, 4, \cdots\}.$$

Los 3 puntos $\cdots$ es la manera de decir *etcétera* en matemáticas. El contexto debe aclarar el significado de $\cdots$. Es importante tener presente que este tipo de notación para conjuntos es algo ambigua, pues presupone que el lector es capaz de inferir los otros elementos del conjunto. La práctica enseñará al lector la manera correcta de usar $\cdots$.

Ilustraremos ahora otra manera de presentar los conjuntos definidos por comprensión. Considere el conjunto X de todos los números naturales que son el cuadrado de algún natural. Podemos expresar la definición de X de la siguiente forma:

$$X = \{n \in \mathbb{N} : \ n = m^2 \text{ para algún número natural } m\}.$$

Por ejemplo tenemos que $4 \in X$, $6 \notin X$, $9 \in X$, $7 \notin X$. Sin embargo, es más frecuente usar la siguiente notación para describir al conjunto X

$$X = \{m^2 : \ m \in \mathbb{N}\}.$$

Queremos resaltar que estas dos maneras de describir la colección de todos los cuadrados de números naturales son equivalentes, es decir,

$$\{n \in \mathbb{N} : \ n = m^2 \text{ para algún número natural } m\} = \{m^2 : \ m \in \mathbb{N}\}.$$

La ventaja que tiene la segunda descripción, aparte de ser más corta, es que ella señala explícitamente el procedimiento que debemos seguir para obtener todos los elementos del conjunto. En nuestro ejemplo, el procedimiento consiste en tomar el cuadrado de los números naturales. Podemos también describir al conjunto X usando la notación ambigua que mencionamos anteriormente

$$\{0, 1, 4, 9, 16, 25, 36, 49, 64, \cdots\}.$$

Con esta notación ambigua uno espera que el lector adivine cuál es el procedimiento que debe seguirse para obtener todos los elementos del conjunto.

Veamos otros ejemplos que usaremos con frecuencia.

$$\{0, 2, 4, 6, 8, 10, 12, 14, 16, \cdots\} \qquad \{1, 3, 5, 7, 9, 11, 13, 15, \cdots\}.$$

El lector seguramente reconoció que el primero es el conjunto de los números naturales **pares** y el segundo es el de los números **impares**. Si quisiéramos evitar la ambigüedad de los $\cdots$ podemos describirlos de la manera siguiente

$$\{2n : \ n \in \mathbb{N}\} \qquad \{2n + 1 : \ n \in \mathbb{N}\}.$$

A veces se usa o mas bién se abusa del símbolo de igualdad y se describen conjuntos de la siguiente manera

$$\{2n : \ n = 0, 1, 2, 3, 4\}.$$

Esta notación quiere indicar que la variable n puede tomar los valores 0,1,2,3 ó 4. Tenemos entonces que

$$\{2n : \ n = 0, 1, 2, 3, 4\} = \{0, 2, 4, 6, 8\}.$$

Ejemplo 1.4. Considere el siguiente conjunto

$$A = \{6, 10, 14, 18, 22, 26, 30, \cdots\}$$

Lo que observamos de los elementos que nos dan de A es que la diferencia entre dos consecutivos es 4. Por lo tanto entre el primero 6 y el tercero 14 la diferencia es de $2 \cdot 4$. Esto sugiere lo siguiente:

$$A = \{4n + 2 : \ n \in \mathbb{N} \text{ y } n \geq 1\}$$

Insistimos que la última descripción del conjunto A es mejor que la primera.

1.1.2. Igualdad de conjuntos.

Hemos usado el símbolo de igualdad entre conjuntos de manera intuitiva: dos conjuntos son iguales cuando tienen los mismos elementos. El concepto de igualdad de conjuntos es muy simple pero sumamente importante en matemáticas y por esta razón lo resaltamos a continuación.

Definición 1.5. *Dos conjuntos A y B son iguales si tienen los mismos elementos. Es decir $A = B$ si se cumplen las siguientes dos condiciones:*

(i) Todo elemento de A también pertenece a B.

(ii) Todo elemento de B también pertenece a A.

Dos conjuntos A y B no son iguales si existe un elemento de A que no pertenece a B ó si existe algún elemento de B que no pertenece a A. Por ejemplo, si A es el conjunto $\{1, 4, 5\}$ y B es el conjunto $\{4, 5\}$ entonces $A \neq B$, pues $1 \in A$ pero $1 \notin B$. Cuando dos conjuntos no son iguales escribimos $A \neq B$.

Ejemplos 1.6. 1. Considere los conjuntos A y B definidos a continuación

$$\begin{aligned} A &= \{2n^3 : \ n \in \mathbb{N} \text{ y } 0 \leq n \leq 3\} \\ B &= \{2, 0, 16, 54\}\} \end{aligned}$$

Queremos saber si A es igual a B. Por la forma en que A está definido, podemos dar una lista completa de sus elementos como lo hicimos en el ejemplo 1.3. Tenemos que

$$A = \{0, 2, 16, 54\}$$

Como A y B contienen los mismos elementos, entonces son iguales.

2. Considere ahora los siguientes conjuntos

$$\begin{aligned} A &= \{1, 2\} \\ B &= \{1, 2, 3\} \end{aligned}$$

Por inspección se obtiene que $3 \in B$, pero $3 \notin A$. En consecuencia, $A \neq B$.

Observe que para mostrar que dos conjuntos no son iguales basta conseguir un elemento de uno de ellos que no pertenece al otro conjunto.

1.1.3. El conjunto vacío

Ahora introduciremos un conjunto muy especial. Consideremos los siguientes conjuntos:

$$\{n \in \mathbb{N} : \ 1 < n < 2\} \qquad \{r \in \mathbb{R} : \ r^2 < 0\}$$
$$\{q \in \mathbb{Q} : \ q < 0 \text{ y } q > 7\} \qquad \{x \in \mathbb{R} : x^2 + 1 = 0\}$$

Estos cuatro conjuntos tienen una propiedad en común: no contienen elementos. Así que todos ellos son iguales (nótese que cada par de ellos satisfacen la definición de igualdad de conjuntos dada en la definición 1.5). Al conjunto que no tiene elementos se le llama **conjunto vacío** y se denota por $\emptyset$.

El conjunto vacío pudiera parecer inútil, pero no lo es. El juega un papel tan importante en la teoría de conjuntos como lo hace el número cero en la aritmética.

Teniendo a nuestra disposición la noción de conjunto vacío, podemos introducir otra noción que se usa con frecuencia. Diremos que dos conjuntos son **disjuntos** si no tienen elementos en común. En símbolos, los conjuntos A y B son disjuntos, si $A \cap B = \emptyset$. Un ejemplo de dos conjuntos disjuntos son el conjunto de los números pares y el de números impares.

1.1.4. Subconjuntos

Otro concepto que está muy relacionado con la igualdad de conjuntos es el de subconjunto.

Definición 1.7. *Sean A y B dos conjuntos, diremos que A es un **subconjunto** de B y escribiremos $A \subseteq B$ si todo elemento de A también pertenece a B.*

Simbólicamente, $A \subseteq B$ si para todo $x \in A$, se cumple que $x \in B$.

Ejemplos 1.8. 1. Por inspección se verifica que $\{1, 3, 4\} \subseteq \{1, 2, 3, 4, 5\}$.

2. Ya sabemos que $\mathbb{N} \subseteq \mathbb{Z}$, $\mathbb{Z} \subseteq \mathbb{Q}$ y $\mathbb{Q} \subseteq \mathbb{R}$.

3. Considere los conjuntos

$$A = \{n \in \mathbb{N} : \ n(n-1)(n-2) = 0\}$$

$$B = \{0, 1, 2, 3, 4\}.$$

Para determinar si $A \subseteq B$ ó $B \subseteq A$ debemos primero conocer los elementos de A. Por simple inspección vemos que $0 \in A$, $1 \in A$ y $2 \in A$ ¿habrán otros? Para que un número natural n pertenezca a A debe satisfacer la ecuación

$$n(n-1)(n-2) = 0.$$

Recordemos que el producto de varios enteros es igual a cero sólo cuando alguno de ellos es igual a cero. De esto obtenemos que $n(n-1)(n-2) = 0$, sólo si $n = 0$, $n-1 = 0$ ó $n-2 = 0$. Por lo tanto los únicos elementos de A son $0, 1$ y 2, es decir $A = \{0, 1, 2\}$. Ahora es fácil verificar que $A \subseteq B$.

Por otra parte, como $4 \in B$ y $4 \notin A$, entonces B no es un subconjunto de A. Esto usualmente se escribe

$$B \not\subseteq A.$$

□

La relación de subconjunto satisface lo siguiente:

Para cualquier par de conjuntos A y B:

$$\begin{array}{lll} \emptyset & \subseteq & A \\ A & \subseteq & A \end{array}$$

¿Puede el lector justificar estas afirmaciones?

Observemos que dos conjuntos A y B son iguales si se cumple que $A \subseteq B$ y $B \subseteq A$. Este hecho simple lo usaremos repetidamente y por esta razón lo resaltamos a continuación

Para mostrar que dos conjuntos A y B son iguales, es suficiente mostrar que

$$A \subseteq B \text{ y } B \subseteq A$$

1.1.5. El conjunto potencia

Podemos formar conjuntos cuyos elementos sean a su vez conjuntos. Por ejemplo,

$$\{\{1\}, \{2,3\}, \{1,3,6\}\}$$

es un conjunto con tres elementos: $\{1\}$, $\{2,3\}$ y $\{1,3,6\}$. Otro ejemplo es $\{\emptyset\}$ cuyo único elemento es $\emptyset$. Observemos que $\emptyset \in \{\emptyset\}$ y como $\emptyset$ no contiene elementos, entonces tenemos que $\emptyset \neq \{\emptyset\}$.

El conjunto formado por todos los subconjuntos de un conjunto dado A se llama el **conjunto potencia** o **conjunto de partes** de A y lo denotamos por $\mathcal{P}(A)$.

$$\mathcal{P}(A) = \{B : \ B \subseteq A\}$$

Notemos que $\emptyset \in \mathcal{P}(A)$ y también que $A \in \mathcal{P}(A)$ para cualquier conjunto A.

Ejemplos 1.9. 1. $\mathcal{P}(\emptyset) = \{\emptyset\}$

2. Consideremos el conjunto $\{1\}$. Los subconjuntos de $\{1\}$ son $\emptyset$ y $\{1\}$. Por esto

$$\mathcal{P}(\{1\}) = \{\emptyset, \{1\}\}.$$

En general, si un conjunto A tiene un sólo elemento, digamos por ejemplo $A = \{a\}$, entonces los subconjuntos de A son $\emptyset$ y $\{a\}$. Es decir,

$$\mathcal{P}(\{a\}) = \{\emptyset, \{a\}\}.$$

3. Si $A = \{1, 2\}$, entonces $\mathcal{P}(A) = \{\{1, 2\}, \{1\}, \{2\}, \emptyset\}$.

4. Considere ahora los siguientes conjuntos

$$\begin{array}{rcl} X & = & \mathcal{P}(\{1, 2\}) \\ Y & = & \mathcal{P}(\{1, 2, 3\}) \end{array}$$

Por inspección se obtiene que $\{3\} \in Y$, pero $\{3\} \notin X$, pues $\{3\} \not\subseteq \{1, 2\}$. En consecuencia, $X \neq Y$.

5. Si A tiene 3 elementos, digamos que $A = \{a, b, c\}$, entonces

$$\mathcal{P}(\{a, b, c\}) = \{\{a, b, c\}, \{a, b\}, \{a, c\}, \{b, c\}, \{a\}, \{b\}, \{c\}, \emptyset\}.$$

6. Notemos que $\mathcal{P}(\{a, b, c\})$ tiene 2^3 elementos. Un resultado general, que se verá más adelante, dice que si A tiene n elementos, entonces $\mathcal{P}(A)$ tiene 2^n elementos. Por ejemplo, $\mathcal{P}(\{1, 2, 3, 4, 5\})$ tiene 2^5 elementos.

7. Podemos repetir la operación de tomar el conjunto potencia. Por ejemplo, $\mathcal{P}(\mathcal{P}(\{1\}))$. Para calcular todos sus elementos recordemos que $\mathcal{P}(\{1\}) = \{\emptyset, \{1\}\}$. Por esto

$$\mathcal{P}(\mathcal{P}(\{1\})) = \{\{\emptyset, \{1\}\},\ \{\emptyset\},\ \{\{1\}\},\ \emptyset\}$$

Observe que este conjunto tiene 2^{2^1} elementos.

8. El tamaño de los conjuntos obtenidos al tomar repetidamente el conjunto potencia crece con mucha rapidez. Por ejemplo,

$$\mathcal{P}(\mathcal{P}(\mathcal{P}(\{1, 2\})))$$

tiene $2^{2^{2^2}} = 2^{16} = 65.536$ elementos. Si aplicamos una vez más la operación de tomar el conjunto potencia, tenemos

$$\mathcal{P}(\mathcal{P}(\mathcal{P}(\mathcal{P}(\{1, 2\}))))$$

Este conjunto tiene $2^{2^{2^{2^2}}} = 2^{2^{16}} = 2^{65536}$. Intente el lector calcular este número (necesitará varias páginas para escribirlo).

□

Ejemplo 1.10. Le recomendamos al lector que preste especial atención al uso de los símbolos de pertenencia, $\in$, y de inclusión, $\subseteq$. Con cierta frecuencia lo estudiantes al comienzo no los usan correctamente. Por ejemplo, suponga que $A \subseteq \mathbb{N}$, las siguiente expresiones son equivalentes:

$$3 \in A \text{ y } \{3\} \subseteq A.$$

Pero no tiene sentido decir que $3 \subseteq A$.

En general, observe que decir que $x \in A$ es equivalente a decir que $\{x\} \subseteq A$. Pero puede ocurrir que no tenga ningún sentido escribir $x \subseteq A$.

Ejercicios 1.1

1. De una lista completa de los elementos de cada uno de los siguientes conjuntos:

   a) $\{x \in \mathbb{N} : \ 3 \leq x < 9\}$

   b) $\{1/n^2 : \ n \in \mathbb{N}, \ n \text{ es par y } 0 < n < 11\}$

   c) $\{z \in \mathbb{Q} : \ 0 \leq z^2 \leq 10 \text{ y } z^3 \in \mathbb{N}\}$

   d) $\{x \in \mathbb{Z} : \ x = n^2 - n^3 \text{ para algún } n \in \{1, 2, 3, 4\}\}$

   e) $\mathcal{P}(\mathcal{P}(\{1, 2\}))$

2. Lea cuidadosamente lo dicho en los ejemplos 1.2 y determine si las siguientes definiciones son correctas. En caso que lo sea, halle dos elementos del conjunto y en caso que no sea correcta justifique porqué no lo es.

   a) $A = \{n \in \mathbb{N} : \ 3n + 2\}$

   b) $A = \{3n + 2 : \ n \in \mathbb{N}\}$

   c) $A = \{x \in \mathbb{Q} : \ y + 1 \geq 6\}$

   d) $A = \{z \in \mathbb{Q} : \ z = y + 1 \text{ para algún } y \in \mathbb{Q} \text{ con } y \geq 6\}$

   e) $A = \{2x + 1 \in \mathbb{Q} : \ x \leq 6\}$.

   f) $A = \{y : \ y \in \mathbb{R}\}$.

3. Halle 6 elementos de cada uno de los siguientes conjuntos.

   (i) $\{2n + 1 : n \in \mathbb{N}\}$ (ii) $\{2n : n \in \mathbb{N}\}$

   (iii) $\{n^2 : n \in \mathbb{N}\}$ (iv) $\{n^3 - 4 : n \in \mathbb{Z}\}$

   (v) $\{1 - n^2 : n \in \mathbb{Z}\}$ (vi) $\{2^n : \ n \in \mathbb{N}\}$

   (vii) $\{r \in \mathbb{Q} : \ 0 < r < 1\}$ (viii) $\mathcal{P}(\{1, 2, 3, 4, 5\})$

4. Determine si los conjuntos A y B son iguales (revise lo hecho en los ejemplos 1.6):

   a) $A = \{2n^2 : \ n \in \mathbb{N} \text{ y } 0 \leq n \leq 3\}$
   $B = \{2, 0, 8, 18\}$

b) $A = \{n^2 + 1 : \ n \in \mathbb{N} \text{ y } 0 \leq n \leq 3\}$
$B = \{x \in \mathbb{Q} : \ x = n^2 + 1 \text{ para algún } n \in \mathbb{Q} \text{ con } 0 \leq n \leq 3\}$

c) $A = \{n \in \mathbb{N} : \ n + 1 \geq 2\}$
$B = \{n \in \mathbb{Z} : \ n + 1 \geq 2\}$

d) $A = \{n \in \mathbb{N} : 3 \leq n \leq 6\}$
$B = \{x : \ x \in \mathbb{N} \text{ y } 3 \leq x \leq 6\}$

e) $A = \{n \in \mathbb{Q} : n \in \mathbb{N}\}$
$B = \{n \in \mathbb{N} : n \in \mathbb{Q}\}$

f) $A = \mathcal{P}(\{1, 2\})$
$B = \{X \in \mathcal{P}(\{1, 2, 3\}) : \ 3 \notin X\}$

g) $A = \{\emptyset\}$ y $B = \emptyset$

h) $A = \{\emptyset\}$ y $B = \{\emptyset, \{\emptyset\}\}$

i) $A = \{\{\emptyset\}\}$ y $B = \{\emptyset\}$.

5. Considere los conjuntos

$A = \{n : \ n = 0, 1, 2, 3, 4\}$ $\quad$ $B = \{4n + 1 : \ n = 0, 1, 2, 3\}$
$C = \{n^2 : \ n = 1, 2, 3\}$ $\quad$ $D = \{0, 2, 4\}$

¿Cuál es subconjunto de cuál? Considere las diesiséis posibilidades.

6. Considere los conjuntos

$A = \{2n + 1 : n \in \mathbb{N}\}$ $\quad$ $B = \{4n + 1 : n \in \mathbb{N}\}$
$C = \{n^2 + 1 : n \in \mathbb{N}\}$ $\quad$ $D = \{2n : n \in \mathbb{N}\}$

¿Cuál es subconjunto de cuál? Considere las diesiséis posibilidades.

7. Para cada uno de los siguientes conjuntos halle una propiedad que sirva para definirlos por comprensión:

(i) $\{0, 3, 6, 9, 12, 15, 18, 21, \cdots\}$ $\quad$ (ii) $\{1, 4, 7, 10, 13, 16, 19, 22, \cdots\}$
(iii) $\{0, 5, 10, 15, 20, 25, 30, 35, \cdots\}$ $\quad$ (iv) $\{0, 1, 8, 27, 64, 125, 216, \cdots\}$
(v) $\{2, 4, 8, 16, 32, 64, \cdots\}$ $\quad$ (vi) $\{7, 11, 15, 19, 23, 27, 31, \cdots\}$
(vii) $\{1, 8, 15, 22, 29, 36, 43, 50, \cdots\}$ $\quad$ (viii) $\{0, -1, 2, -3, 4, -5, 6, -7, \cdots\}$

1.2. Las operaciones elementales

Comenzaremos definiendo la unión y la intersección.

$$A \cup B = \{x : \ x \in A \text{ ó } x \in B\}$$
$$A \cap B = \{x : \ x \in A \text{ y } x \in B\}$$

Observemos que para cualquier par de conjuntos A y B se cumple lo siguiente

$$\begin{aligned} A \cap B &\subseteq A \\ A &\subseteq A \cup B. \end{aligned}$$

Dados dos conjuntos A, B la **diferencia** de A menos B, denotada por $A \setminus B$, se define de la siguiente manera

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

Observe que A y $B \setminus A$ son disjuntos, es decir, $A \cap (B \setminus A) = \emptyset$.
La **diferencia simétrica**, denotada por $A \triangle B$, se define de la siguiente manera

$$\boxed{A \triangle B = (A \setminus B) \cup (B \setminus A)}$$

Observe que x pertenece a $A \triangle B$ cuando ocurre que $x \in A$ ó $x \in B$ pero no ocurre que x pertenezca a ambos conjuntos A y B. En algunos textos se usa el símbolo $\oplus$ para denotar la diferencia simétrica.
Veamos ejemplos de todas las operaciones que hemos definido.

Ejemplo 1.11. Sea $A = \{n \in \mathbb{N} : \ n \leq 7\}$, $B = \{2n : \ n \in \mathbb{N} \text{ y } n \leq 8\}$ y $C = \{n : \ n \in \mathbb{N} \text{ y } n \text{ es par}\}$. Entonces tenemos que

$$\begin{aligned} A \cup B &= \{0, 1, 2, 3, 4, 5, 6, 7, 8, 10, 12, 14, 16\} \\ A \cap B &= \{0, 2, 4, 6\} \\ A \setminus B &= \{1, 3, 5, 7\} \\ B \setminus A &= \{8, 10, 12, 14, 16\} \\ A \triangle B &= \{1, 3, 5, 7, 8, 10, 12, 14, 16\} \\ B \setminus C &= \emptyset \\ C \setminus B &= \{2n : \ n > 8 \text{ y } n \in \mathbb{N}\} \\ B \triangle C &= \{2n : \ n > 8 \text{ y } n \in \mathbb{N}\} \\ A \cap C &= \{0, 2, 4, 6\} \\ A \triangle C &= \{1, 3, 5, 7\} \cup \{2n : \ n \geq 4 \text{ y } n \in \mathbb{N}\} \end{aligned}$$

□

Ejemplo 1.12. Imagínese la siguiente situación. Sobre una mesa hay 6 objetos dorados marcados con las letras a, b, c, d, e y f. Hay cuatro personas A, B, C y D que deben determinar cuales de esos objetos son realmente de oro y cuales son imitaciones. La elección de cada persona la expresaremos por un conjunto que contiene las letras correspondientes a los objetos que la persona considera son de oro.

$$\begin{aligned} A &= \{a, b, c, e, f\} & B &= \{a, b, c, d, e\} \\ C &= \{d\} & D &= \{e, f\} \end{aligned}$$

Ahora bien, los objetos realmente de oro son a y f. ¿Quién de las cuatro personas se acercó más a la respuesta correcta? Si sólo nos interesara saber quienes eligieron los objetos correctos tenemos que A sería el que se acercó más a la respuesta. Sin embargo, si también queremos incluir la información adicional sobre los objetos incorrectos que cada persona eligió, entonces debemos escoger a D. Pues D mostró tener mejor criterio que A, ya que eligió uno sólo de los objetos de oro y además eligió sólo uno incorrecto. Por otro lado, A eligió 3 objetos incorrectos, C eligió solamente un objeto incorrecto, pero no eligió ninguno correcto.

Veamos la diferencia simétrica de los conjuntos A, B, C y D con la respuesta correcta $\{a, f\}$

$$\begin{array}{ll} A\triangle\{a,f\} = \{b,c,e\} & B\triangle\{a,f\} = \{b,c,d,e,f\} \\ C\triangle\{a,f\} = \{a,d,f\} & D\triangle\{a,f\} = \{a,e\} \end{array}$$

Con este ejemplo vemos que la operación de diferencia simétrica nos permite estimar qué tan parecidos son dos conjuntos. El número de elementos que tiene la diferencia simétrica entre la respuesta de cada persona y la respuesta correcta provee de un criterio para decidir cuál (o cuáles) de las personas es la ganadora. En nuestro caso vemos que $D\triangle\{a, f\}$ tiene el menor número de elementos, por esta razón podemos decir que D es quien mostró poseer el mejor criterio. □

Nuestro próximo ejemplo ilustra como se puede mostrar una propiedad general sobre las operaciones sobre conjuntos. El lector debería prestarle bastante atención a este ejemplo, pues el método usado en él se repetirá con frecuencia en todo el curso.

Ejemplo 1.13. Sean A y B conjuntos cualesquiera. Mostraremos que

$$A \setminus B = A \setminus (A \cap B). \tag{1.1}$$

Por dicho en la sección 1.1.4 basta mostrar las siguientes afirmaciones:

$$A \setminus B \;\subseteq\; A \setminus (A \cap B) \tag{1.2}$$

y

$$A \setminus (A \cap B) \;\subseteq\; A \setminus B. \tag{1.3}$$

Veamos la primera afirmación. Lo que deseamos hacer es mostrar que cualquier elemento de $A \setminus B$ también pertenece a $A \setminus (A \cap B)$. Para hacerlo, denotemos con x un elemento cualquiera de $A \setminus B$. Entonces, por definición de la diferencia, se tiene que $x \in A$ y $x \notin B$. Por lo tanto, también se tiene que $x \notin A \cap B$. Como x se tomó en A, hemos mostrado que $x \in A \setminus (A \cap B)$. Ya que x representa un elemento *cualquiera* de $A \setminus B$, podemos concluir que $A \setminus B \subseteq A \setminus (A \cap B)$.

La segunda afirmación se trata de manera análoga. Tomemos un elemento cualquiera x en $A \setminus (A \cap B)$. Entonces, por definición de la diferencia, se tiene que $x \in A$ y $x \notin A \cap B$. Por lo tanto, se tiene que $x \notin B$ (pues, si no fuera así, entonces $x \in A \cap B$ lo que no puede ser).

Como x se tomó en A, hemos mostrado que $x \in A \setminus B$. Ya que x representa un elemento *cualquiera* de $A \setminus (A \cap B)$, podemos concluir que $A \setminus (A \cap B) \subseteq A \setminus B$.

Lo dicho hasta ahora es una justificación precisa de que las afirmaciones (1.2) y (1.3) son válidad. Esto precisamente dice que los conjuntos $A \setminus B$ y $A \setminus (A \cap B)$ tienen los mismos elementos. Es decir, la afirmación (1.1) es válida.

Este tipo de justificaciones *precisas y apropiadas* es lo que llamamos **rigor matemático** y esto es la característica principal de las demostraciones en matemáticas.

□

Los problemas en matemáticas generalmente tratan sobre las propiedades de algún conjunto particular, por ejemplo $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ o $\mathcal{P}(\mathbb{N})$. El conjunto en cuestión usualmente se denomina **universo** o **conjunto universal**. En relación a un conjunto universal U prefijado se define el **complemento** de un subconjunto $A \subseteq U$, denotado por A^c, de la siguiente manera

$$A^c = U \setminus A.$$

Esta notación es un poco ambigua pues A^c depende obviamente del conjunto U que se use. Tendremos el cuidado de que cada vez que usemos la operación de complementación el conjunto universal U esté claramente especificado.

Ejemplo 1.14. Supongamos que nuestro universo son los números naturales y sea A el conjunto de números pares, es decir, $A = \{2n : \ n \in \mathbb{N}\}$ y $U = \mathbb{N}$. Entonces tenemos que A^c es el conjunto de números impares, pues

$$\mathbb{N} \setminus A = \{2n + 1 : \ n \in \mathbb{N}\}.$$

Ahora bien, si nuestro universo hubiese sido el de todos los números enteros, es decir $U = \mathbb{Z}$, entonces tendríamos que

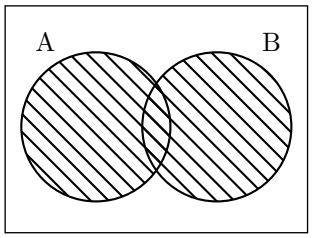
$$A^c = \{n \in \mathbb{Z} : \ n \leq -1\} \cup \{2n + 1 : \ n \in \mathbb{N}\}.$$

□

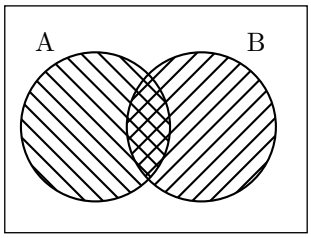
Ejemplo 1.15. Sea $A = \{n \in \mathbb{N} : n \text{ es divisible por } 3 \}$. Y sea $B = \{n \in \mathbb{N} : n \text{ no es divisible por } 3 \}$. Si nuestro universo es $\mathbb{N}$, entonces $A = B^c$ y $B = A^c$. □

1.2.1. Diagramas de Venn

Una manera de representar las operaciones entre conjuntos es a travéz de los **diagramas de Venn**. A continuación presentaremos los diagramas correspondientes a las operaciones de unión e intersección:

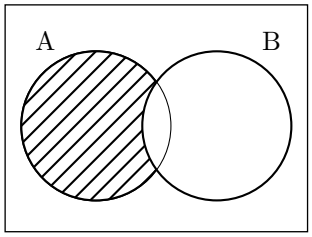


$A \cup B$

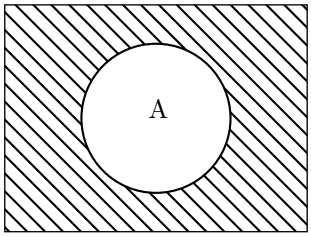


$A \cap B$

Los diagramas correspondientes a las operaciones de diferencia y complementación son los siguientes:



$A \backslash B$

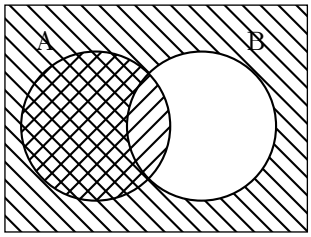


A^c

Observemos que usando la operación de complementación podemos describir la diferencia de dos conjuntos de la manera siguiente: Suponga que A y B son subconjuntos de un conjunto universal U, entonces

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

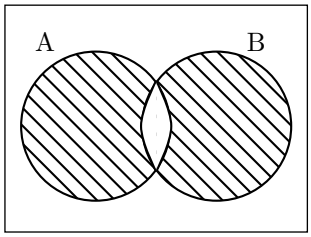
Esto lo podemos verificar fácilmente usando diagramas de Venn. Haremos un diagrama de Venn que represente $A \cap B^c$ y lo compararemos con el que hicimos arriba para $A \setminus B$.



$A \cap B^c$

Vemos que ambos diagramas determinan el mismo conjunto. De lo anterior obtenemos otra forma de expresar la diferencia simétrica

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



$A\triangle B$

Ejercicios 1.2

1. Sean $A = \{1, 3, 5, 7, 9, 11\}$, $B = \{2, 3, 5, 7, 11\}$, $C = \{2, 3, 6, 12\}$, $D = \{2, 4, 8\}$. Determine por extensión los siguientes conjuntos. En las partes (iii) y (ix) considere primero que el conjunto universal U es

   $$\{1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12\}$$

   y después resuelva las preguntas (iii) y (ix) usando como conjunto universal a $\mathbb{N}$.

(i) $A \cup B$	(ii) $A \cap C$	(iii) $(A \cup B) \cap (C^c \cup D)$
(iv) $A \setminus B$	(v) $C \setminus D$	(vi) $B\triangle D$
(vii) $(A \cap C) \cup B$	(viii) $(A \cup C) \cap B$	(ix) $(B^c\triangle D^c)\triangle A^c$

2. *a*) Muestre que $\{1, 3\}\triangle\{2\} \neq \{3, 4\}$.

   b) Halle un subconjunto C de $\{1, 2, 3, 4\}$ tal que $\{1, 3\}\triangle C = \{3, 4\}$.

3. Sea A un conjunto. Muestre que $A\triangle A = \emptyset$ y $A\triangle\emptyset = A$.

4. Exprese los siguientes enunciados usando las operaciones elementales entre conjuntos.

   a) Todos los elementos de A están en B o están en C.

   b) Si un elemento de A está en C, entonces también está en B.

   c) Los elementos de A y los de B están en C.

   d) Todo elemento de A o de B pertenece a C o a D.

5. *a*) Haga el diagrama de Venn de los siguientes conjuntos: $(A \cup B) \cap C$, $A \cup (B \cap C)$.

b) Halle tres conjuntos A, B y C no vacíos tales que

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

y halle también tres conjuntos D, E y F tales que

$$(D \cup E) \cap F = D \cup (E \cap F).$$

(*Sugerencia:* No busque ejemplos complicados, todos los conjuntos pueden ser subconjuntos de $\mathbb{N}$).

6. *a*) Haga el diagrama de Venn de los siguientes conjuntos: $A \cap (B \cup C)$, $(A \cap B) \cup (A \cap C)$.

   b) Use los diagramas anteriores para convencerse que

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

7. De manera similar a como se hizo en el ejemplo 1.13 justifique las siguientes afirmaciones:

   a) $A \subseteq A \cup B$

   b) $A \cap B \subseteq A \cup B$

   para cualquier par de conjuntos A y B.

8. De manera similar a como se hizo en el ejemplo 1.13, justifique las siguientes afirmaciones:

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

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

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

   d) $(A \setminus B) \setminus C = A \setminus (B \cup C)$.

9. Las siguientes afirmaciones son falsas. Proporcione conjuntos A, B y C que no cumplan con lo expresado.

   a) $A \cup B = A \cap B$.

   b) $A \cap B = A \triangle B$.

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

   d) $(A \setminus B) \setminus C = A \setminus (B \setminus C)$.

   e) $A \triangle (B \cup C) = (A \triangle B) \cup (A \triangle C)$.

   f) $A \triangle (B \cap C) = (A \triangle B) \cap (A \triangle C)$.

1.3. Ejercicios suplementarios del capítulo 1

1. De una lista completa de los elementos de cada uno de los siguientes conjuntos:

   $\{2+(-1)^n : \ n \in \mathbb{N}\}$ $\quad$ $\{1/n : \ n = 1,2,3,4\}$

   $\mathcal{P}(\{1,2,3\}) \cap \mathcal{P}(\{2,3,4\})$ $\quad$ $\mathcal{P}(\mathbb{N}) \cap \mathbb{N}$

2. Determine si las siguientes definiciones son correctas. En caso que lo sea, encuentre dos elementos del conjunto y en caso que no, justifique porqué no lo es.

   a) $A = \{x + y : \ x \in \mathbb{Z}\}$.

   b) $A = \{m : \ m \in A\}$.

   c) $A = \{x \in \mathbb{R} : \ (x+2)^2\}$.

   d) $A = \{(x+2)^2 : \ x \in \mathbb{R}\}$.

   e) $A = \{x \in \mathbb{R} : \ (x+2)^2 = 1\}$.

   f) $A = \{x : \ x \in B\}$ y $B = \{x : \ x \in A\}$.

   g) $A = \{x : \ x \in x\}$.

   h) $A = \{x : \ x \notin x\}$.

3. Encuentre una propiedad que sirva para definir por comprensión el siguiente conjunto:

   $$\{3, 7, 11, 15, 19, 23, \cdots\}.$$

4. Sean $A = \{1,3,5,7,9,11\}$, $B = \{2,3,5,7,11\}$, $C = \{2,3,6,12\}$ y $U = \{n \in \mathbb{N} : 0 < n \leq 12\}$ el conjunto universal. Determine los conjuntos siguientes:

   (a) $A \triangle B$

   (b) $(A \cup C) \cap (C^c \cup B)$

5. Determine si los conjuntos A y B son iguales.

   a) $A = \{n \in \mathbb{N} : \ n+1 \geq 2\}$ y $B = \{n \in \mathbb{Q} : \ n+1 \geq 2\}$.

   b) $A = \{n \in \mathbb{Z} : \ 2 \leq n\}$ y $B = \{n \in \mathbb{N} : \ \ 2 \leq n\}$.

   c) $A = \{y \in \mathbb{Q} : \ y+3 \geq 7\}$ y $B = \{x : x \in \mathbb{Q} \text{ y } x \geq 4\}$

   d) $A = \{3n-4 : \ n \in \mathbb{N}\}$ y $B = \{x \in \mathbb{Q} : \ x = 3n-4 \text{ para algún } n \in \mathbb{N}\}$

   e) $A = \{3n-4 : \ n \in \mathbb{N}\}$ y $B = \{x \in \mathbb{Q} : \ \frac{x+4}{3} \in \mathbb{N}\}$.

   f) $A = \mathcal{P}(\{5,7\})$ y $B = \{X \in \mathcal{P}(\{5,6,7\}) : \ 6 \notin X\}$.

6. Halle conjuntos A y B tales que

   a) $A \triangle \{1,2,3\} = \{3,4,5\} \triangle B$,

   b) $A \triangle \{3,4\} = B \cap \{2,3,7\}$.

7. Halle dos conjuntos A y B tales que $A \triangle B = A \cup B$.

8. Halle dos conjuntos A y B tales que $A \triangle B \neq A \cup B$.

9. Sean A, B y X conjuntos con $A, B \subseteq X$. Muestre que existe un conjunto C tal que $A \triangle C = B$.

Capítulo 2

Lógica Simbólica

En matemáticas es fundamental poder reconocer cuándo un argumento es correcto y también saber cómo construirlo. Por esta razón en este capítulo trataremos con los rudimentos de la lógica, pues es esta disciplina la que se ocupa del estudio de los razonamientos correctos. Nos ocuparemos primero de las propiedades formales de las proposiciones, esta es una parte de la lógica llamada **lógica proposicional**. Uno de los objetivos de este capítulo es introducir algunas nociones de la lógica (por ejemplo: la implicación y la equivalencia lógica) que son imprescindibles para el estudio de las matemáticas. Todo esto con el fin de facilitar el aprendizaje de los métodos para hacer demostraciones.

2.1. Proposiciones y fórmulas proposicionales

Una **proposición** es una afirmación de la que podemos decir, sin ambigüedad, si es verdadera o falsa. Las proposiciones corresponden a las oraciones declarativas del lenguaje español.

Ejemplos 2.1. Las siguientes afirmaciones son proposiciones:

1. Mérida es el nombre de una ciudad andina.
2. $1 + 1 = 2$.
3. $1 + 1 = 3$.
4. El cuadrado de todo número par también es par.
5. Todo entero par mayor que 4 es la suma de dos números primos.

□

Ejemplos 2.2. Las siguientes oraciones no son proposiciones:

1. Espérame!
2. ¿Por qué estudias matemáticas?

3. $x + y = x$

4. ¡A estudiar!

La oración 3) no es una proposición, pues no hemos especificado el significado de los símbolos x e y y por esto no podemos decir si es verdadera o falsa. Si dijéramos que

$$x + y = x \text{ para algún } x, y \in \mathbb{Z},$$

entonces esa afirmaición es una proposición verdadera. Pues tenemos, por ejemplo, que cuando $x = 1$ y $y = 0$ se cumple que $x + y = x$. □

Ejercicios 2.1

1. ¿Cuáles de las siguientes son proposiciones? En caso que sea un proposición diga si es verdadera o falsa.

   a) $5 + 2 = 7$.

   b) $2^4 < 3^2$.

   c) El Presidente actuó en contra de la Ley.

   d) Tu voto es tu opinión.

   e) ¿Te duele?

   f) Me duele.

   g) El polo norte es frío y el polo sur es caliente.

   h) Perro que ladra no muerde.

2.1.1. Conectivos lógicos

Las proposiciones se pueden combinar para obtener otras proposiciones utilizando los *conectivos lógicos* (también llamados *enlaces*). Los conectivos son los siguientes:

Negación: *" **No** tengo frío "*.
Disyunción: *" El carro es de color rojo **o** blanco "*.
Conjunción: *" $5 < 8$ **y** $13 < 27$"*.
Condicional: *" **Si** llueve, **entonces** no voy al cine "*.
Bicondicional: *" Voy al cine **si, y sólo si**, no llueve"*.

Una proposición que no contenga ningún conectivo se dice que es una **proposición simple**, también se les llama **proposiciones atómicas**. Por ejemplo, la afirmación *" 3^4 es menor que 100"* es una proposición simple. Las proposiciones que contengan algún conectivo se llaman **proposiciones compuestas**. Un ejemplo de proposición compuesta es *" 3 es un número impar y 28 es par"*.

En general, la oración declarativa con que se expresa una proposición puede ser larga y compleja y por esto es conveniente, para simplificar su presentación y manipulación, sustituirla por un letra. Usaremos las letras P, Q, $R \cdots$ para simbolizar proposiciones. De igual manera, los conectivos serán representados en forma simbólica de la siguiente manera:

$\neg$	para la negación
$\vee$	para la disyunción
$\wedge$	para la conjunción
$\rightarrow$	para el condicional
$\leftrightarrow$	para el bicondicional

$\neg P$	se lee	"no P"
$P \vee Q$	se lee	P ó Q
$P \wedge Q$	se lee	P y Q
$P \rightarrow Q$	se lee	Si P, entonces Q
$P \leftrightarrow Q$	se lee	P si, y sólo si Q

Ejemplo 2.3. Considere las siguiente propocisiones:

P	=	"está lloviendo"
Q	=	"el Sol está brillando"
R	=	"hay nubes en el cielo"

Con estas tres proposiciones simples podemos construir varias proposiciones compuestas como se ilustra a continuación.

Está lloviendo y el Sol está brillando	$P \wedge Q$
Si está lloviendo, entonces hay nubes en el cielo	$P \rightarrow R$
Si no está lloviendo, entonces el Sol no está brillando y hay nubes en el cielo	$\neg P \rightarrow (\neg Q \wedge R)$
El Sol está brillando si, y sólo si, no está lloviendo	$Q \leftrightarrow \neg P$
Si no hay nubes en el cielo, entonces el Sol está brillando	$\neg R \rightarrow Q$

□

Ejemplo 2.4. Sean P, Q y R como en el ejemplo 2.3. Considere las siguientes proposiciones compuestas.

1. $(P \wedge Q) \rightarrow R$
2. $\neg P \leftrightarrow (Q \vee R)$
3. $\neg(P \vee Q) \wedge R$
4. $(P \rightarrow R) \rightarrow Q$
5. $\neg(P \leftrightarrow (Q \vee R))$

La primera de ellas dice "Si está lloviendo y el sol está brillando, entonces hay nubes en el cielo". La tercera podría traducirse como: "no es el caso que esté lloviendo o el sol esté brillando, pero hay nubes en el cielo". Se recurrió a la frase "pero..." en lugar de "y..." para indicar que la frase que seguía no estaba afectada por la expresión "no es el caso". Dejamos a cargo del lector traducir las otras proposiciones a oraciones en español. Tenga presente que al hacerlo puede obtener oraciones, como antes, que no son de uso frecuente en español.

□

Existen dos tipos de disyunción: La inclusiva y la exclusiva. Un ejemplo de disyunción exclusiva se encuentra en la frase *"O corre o se encarama"*. En cambio la "o" en su sentido inclusivo la encontramos en la frase *"Los que estén hablando o estén de pie"*. La disyunción inclusiva se usa cuando ambas alternativas son posibles (o permitidas). En cambio, se usa la disyunción exclusiva cuando sólo una de las alternativas es posible. Otros ejemplos de estos dos tipos de disyunción son las operaciones de unión y diferencia simétrica. [1]

Las proposiciones que tienen la forma

$$\text{"}\textit{Si } P\textit{, entonces } Q\text{"}$$

se llaman **proposiciones condicionales**. P se llama *hipótesis* y Q *conclusión o tesis*. Usando la notación simbólica, las proposiciones condicionales se denotan por $P \to Q$.

La **recíproca** de una proposición condicional $P \to Q$ es la proposición

$$Q \to P.$$

La **contrarrecíproca** (también llamada **contrapositiva**) de una proposición condicional $P \to Q$ es la proposición

$$\neg Q \to \neg P.$$

Ejemplo 2.5. Considere la proposición

Si está lloviendo, entonces hay nubes en el cielo.

Usando la notación del ejemplo 2.3 podemos expresar simbólicamente esta proposición por $P \to R$. La recíproca expresada simbólicamente es $R \to P$ y dice

Si hay nubes en el cielo, entonces está lloviendo

En cambio la contrapositiva, que simbólicamente se escribe $\neg R \to \neg P$, dice

Si no hay nubes en el cielo, entonces no está lloviendo.

□

Ejemplo 2.6. En este ejemplo calcularemos la negación de algunas proposiciones. Usaremos las proposiciones presentadas en el ejemplo 2.3.

1. La negación de

   Está lloviendo y el Sol está brillando

   es

   No está lloviendo o el Sol no está brillando.

   Es decir, la negación de una proposición de la forma $P \wedge Q$ dice lo mismo que la siguiente proposición

   $$\neg P \vee \neg Q.$$

[1] El símbolo $\vee$ para la disyunción viene de la palabra latina *vel* que significa "o" [2].

2. La negación de

Está lloviendo o el Sol está brillando

es

No está lloviendo y el Sol no está brillando.

Pero usualmente decimos: *Ni está lloviendo ni el sol está brillando.*

Es decir, la negación de una proposición de la forma $P \vee Q$ dice lo mismo que la proposición siguiente

$$\neg P \wedge \neg Q.$$

3. La negación de

Si está lloviendo, entonces hay nubes en el cielo

es

Está lloviendo y no hay nubes en el cielo.

La negación de un proposición condicional $P \rightarrow Q$ dice lo mismo que la proposición

$$P \wedge \neg Q.$$

□

Ejercicios 2.1.1

1. Sean P, Q y R las proposiciones siguientes:

$$\begin{array}{rcl} P & = & \text{“Juan llega demasiado pronto”} \\ Q & = & \text{“María llega demasiado tarde”} \\ R & = & \text{“El jefe se molesta”} \end{array}$$

Traduzca las siguientes oraciones a notación lógica utilizando las letras P, Q, R y los conectivos lógicos.

a) Si Juan llega demasiado pronto ó María demasiado tarde, entonces el jefe se molesta.

b) Si María llega demasiado tarde, entonces Juan no llega demasiado pronto.

c) O el jefe se molesta ó María no llega demasiado tarde.

d) María llega demasiado tarde, Juan llega demasiado pronto y el jefe se molesta.

e) Si el jefe no se molesta, entonces Juan no llega demasiado pronto y María no llega demasiado tarde.

f) O María no llega demasiado tarde o Juan llega demasiado pronto.

g) Si María no llega demasiado tarde y Juan no llega demasiado pronto, entonces el jefe no se molesta.

2. Traduzca cada una de las siguientes oraciones a notación lógica de manera análoga a lo hecho en el ejercicio 1 (introduzca las letras que le haga falta).

a) El número de cédula de Genaro es menor que 5 millones o es mayor que seis millones.

b) Alejandra está comiendo, bebiendo y divirtiéndose.

c) El gordo Alberto vive para comer y come para vivir.

d) O yo estoy equivocado, o la pregunta número uno es cierta y la pregunta número dos es falsa.

e) Si el libro cuesta más de Bs. 20.000, entonces Ramón no podrá comprarlo.

f) Si el número en la pantalla es menor que cuatro o mayor que diez, entonces no es igual a seis.

3. Niegue las siguientes proposiciones:

a) Ganaremos el primer partido o el segundo.

b) $5 \geq 3$.

c) Las rosas son rojas y las margaritas amarillas.

d) Alejandra quiere comer fruta pero no helado.

e) Si $2^{10} < 3^5$, entonces $10^{10} < 15^5$.

4. Proporcione la recíproca y la contrapositiva de cada una de las siguientes proposiciones.

a) Si soy listo, entonces soy rico.

b) Si $2 + 2 = 4$, entonces $2 + 4 = 8$.

c) Si Juan llega demasiado pronto ó María demasiado tarde, entonces el jefe se molesta.

5. Considere la proposición "si a es un número real y $a > 0$, entonces $a^2 > 0$ ".

a) Proporcione la recíproca y la contrapositiva de la proposición.

b) ¿Cuál (o cuáles) de las siguientes proposiciones es verdadera: la proposición original, la recíproca o la contrapositiva?

2.1.2. Tablas de verdad

Dijimos que una proposición es una afirmación que es verdadera o falsa, no puede ser ambigüa. Ahora bien, las proposiciones compuestas pueden ser complejas. Por ejemplo, considere una proposición que tenga la siguiente forma

$$((P \to Q) \ \wedge \ (Q \to R)) \to (P \to R).$$

Aun sabiendo cuales de las proposiciones P, Q y R son verdaderas, no es del todo claro como decidir si la proposición de arriba es verdadera o no. Este es el problema que analizaremos en esta sección.

Comenzaremos con un ejemplo relativamente sencillo. Considere las siguientes proposiciones:

$$\begin{array}{lcl} P & = & \text{“ } 2^5 < 3^3 \text{ ”} \\ Q & = & \text{“ } 3 < 16 \text{ ”} \\ R & = & \text{“ } 2^{2999} < 12^{1000} \text{ ”}. \end{array}$$

¿Cuáles de las siguientes proposiciones son verdaderas (y en consecuencia, cuáles son falsas)?: $P \vee Q$, $P \wedge Q$, $P \to Q$, $\neg P$, $R \to Q$, $R \wedge P$. Antes de dar respuesta a estas preguntas, debemos saber cuales de las proposiciones P, Q y R son verdaderas. Un cálculo sencillo nos muestra que P es falsa pues $2^5 = 32$ y $3^3 = 27$. Q es verdadera. Es claro que R es una proposición pues necesariamente alguna de las siguientes dos alternativas se cumple: (i) $2^{2999} < 12^{1000}$ o (ii) $2^{2999} \not< 12^{1000}$. Dejaremos al lector averiguar cual de las dos alternativas se cumple.

(i) Podemos concluir que $P \vee Q$ es verdadera, pues al menos Q lo es. Note que también podemos afirmar que $P \vee R$ es verdadera, aún cuando no sabemos si R es verdadera o no.

(ii) La proposición $P \wedge Q$ es falsa, pues P es falsa. Lo mismo ocurre con $P \wedge R$. ¿Qué podemos decir acerca de $Q \wedge R$? Hasta tanto no resolvamos si R es verdadera o no, no podemos decir nada.

(iii) La proposición $\neg P$ es verdadera, pues P es falsa.

(iv) Un momento de reflexión debería convencer al lector que una proposición condicional *“ Si S, entonces T ”* solamente puede ser falsa, cuando S es verdadera y T no lo es. En todos los otros casos necesariamente es verdadera (pues no hay otra alternativa). Por esto $Q \to P$ es falsa, pues Q es verdadera y P no lo es. Por otra parte, $R \to Q$ es verdadera, independientemente de si R es o no verdadera.

Los **valores de verdad** son las dos alternativas que tenemos para una proposición: ser verdadera o ser falsa. Serán denotados, respectivamente, con las letras V y F. Si una proposición es verdadera diremos que su valor de verdad es V y si es falsa, diremos que es F. El valor de verdad de una proposición compuesta depende exclusivamente del los valores de verdad de las proposiciones simples que aparecen en ella. Por esto el comportamiento de

los conectivos lógicos en relación con el valor de verdad es muy sencillo de establecer y se hace a través de las *tablas de verdad* [2].

Comenzaremos con la tabla de verdad para $\neg$. Es claro que $\neg P$ debe ser verdadera exactamente cuando P no lo es.

P	$\neg P$
V	F
F	V

Una disjunción es verdadera cuando al menos una de las proposiciones es verdadera. La tabla de la disyunción es:

P	Q	$P \vee Q$
V	V	V
V	F	V
F	V	V
F	F	F

Estas tablas se leen horizontalmente. Por ejemplo, la primera línea dice que si P es verdadera y Q es verdadera, entonces $P \vee Q$ también es verdadera. La tercera línea dice que si P es falsa y Q es verdadera, entonces $P \vee Q$ es verdadera etc.

Las tablas de verdad para los otros conectivos son:

P	Q	$P \wedge Q$
V	V	V
V	F	F
F	V	F
F	F	F

P	Q	$P \rightarrow Q$
V	V	V
V	F	F
F	V	V
F	F	V

Ahora veremos algo fundamental para todo lo que sigue en este capítulo. Volvamos al ejemplo al comienzo de esta sección. Si en lugar de las proposiciones P y Q usamos las siguientes (P' se lee P *prima*).

$$\begin{aligned} P' &= \text{“ } 2^4 < 3^2 \text{ ”} \\ Q' &= \text{“ } 5 < 10 \text{ ”} \end{aligned}$$

Entonces P y P' son ambas falsas y Q y Q' son ambas verdaderas. Como el valor de verdad de una proposición compuesta depende *exclusivamente* de los valores de verdad de las proposiciones simples que aparecen en ella, podemos concluir que $P' \vee Q'$ es verdadera; $P' \wedge Q'$ es falsa; $\neg P'$ es verdadera y $Q' \rightarrow P'$. Lo mismo es válido si en lugar de P colocamos cualquier otra proposición que sea falsa y en lugar de Q usamos cualquier otra proposición que sea verdadera.

[2] Las tablas de verdad en forma tabular aparecen en 1918 con los trabajos de Lukasiewicz, Post, Wittgenstein (ver [3, pag. 87]).

Por lo dicho arriba, en el estudio de la lógica proposicional no trabajaremos con proposiciones concretas, en su lugar usaremos simplemente letras que llamaremos **variables proposicionales**. Con estas variables y los conectivos lógicos se construyen las **fórmulas proposicionales** de la misma manera que se construyeron las proposiciones compuestas. Usaremos las letras p, q, r, etc. para denotar las variables proposicionales.

Ejemplo 2.7. A continuación presentamos algunos ejemplos de fórmulas proposicionales.

$(p \wedge q) \rightarrow r$

$\neg p \leftrightarrow (q \vee r)$

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

$(p \rightarrow r) \rightarrow q$

$\neg(p \leftrightarrow (q \vee r))$

$(p \wedge q) \vee \neg(p \rightarrow q).$

$((p \rightarrow q) \ \wedge \ (q \rightarrow r)) \rightarrow (p \rightarrow r)$

Observación: Si cada una de las variables que aparecen en una fórmula proposicional se sustituye por una proposición, lo que se obtiene es un proposición (compuesta). Por ejemplo, considere la fórmula $(p \wedge q) \rightarrow r$. Sustituiremos p por la proposición " $3^7 < 4^8$ ", q por la proposición " $4^8 < 3^{15}$ y r por la proposición " $3^7 < 3^{15}$. Obtenemos la proposición que dice:

"*Si* $3^7 < 4^8$ *y* $4^8 < 3^{15}$, *entonces* $3^7 < 3^{15}$".

De ahora en adelante simplemente diremos fórmula en lugar de fórmula proposicional. Usualmente denotaremos las fórmulas con letras del alfabeto griego, ϕ, ψ, ρ que se leen, respectivamente, " *fi* ", " *si*" (como en la palabra psicología) y " *ro* ". Usaremos la misma terminología que usamos para las proposiciones. Por ejemplo, si ϕ y ψ son fórmulas, entonces la negación de ϕ es $\neg\phi$, la recíproca de $\phi \rightarrow \psi$ es $\psi \rightarrow \phi$ y la contrarecíproca es $\neg\psi \rightarrow \neg\phi$.

A cada fórmula le asociamos una *tabla de verdad*. Construiremos la tabla de verdad para la fórmula

$$(p \wedge q) \vee \neg(p \rightarrow q).$$

Las primeras columnas de la tabla serán ocupadas por las variables involucradas, en este caso p y q. Observe que tendremos 4 filas que corresponden al número de posibles combinaciones distintas de los valores de verdad de p y q.

p	q	$p \wedge q$	$p \rightarrow q$	$\neg(p \rightarrow q)$	$(p \wedge q) \vee \neg(p \rightarrow q)$
F	F	F	V	F	F
F	V	F	V	F	F
V	F	F	F	V	V
V	V	V	V	F	V

Un hecho importante que se deduce de la tabla de verdad de una fórmula es el siguiente. La tabla nos indica el valor de verdad que tiene la proposición obtenida cuando cada variable de la fórmula se sustituye por una proposición. Por ejemplo, si en la fórmula $(p \wedge q) \vee \neg(p \to q)$ sustituimos p por una proposición verdadera y q por una falsa, entonces la proposición obtenida es verdadera (pues su valor viene dado por la tercera fila de la tabla de $(p \wedge q) \vee \neg(p \to q)$).

Ejemplo 2.8. Hay una manera más simple de presentar las tablas de verdad. En la última fila indicaremos a que paso del procedimiento corresponde esa columna.

	p	q	$p \wedge q$	$\vee$	$\neg\ (p \to q)$	
	F	F	F	F	F	V
	F	V	F	F	F	V
	V	F	F	V	V	F
	V	V	V	V	F	V
paso	1	1	2	4	3	2

Los valores en la columna 4 nos dan la tabla de verdad de la fórmula original.

□

Algunas fórmula tienen la propiedad de recibir sólo el valor **V**. Es decir, en su tabla de verdad la última columna sólo contiene **V**. Un ejemplo es la fórmula $p \vee \neg p$. Este tipo de fórmulas reciben el nombre de **tautologías**. Las tautologías forman una clase muy importante de fórmulas.

Ejemplos 2.9. 1. $p \to p$ es una tautología.

p	$p \to p$
V	V
F	V

2. $[p\ \wedge\ (p \to q)] \to q$ es una tautología.

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

□

Un fórmula que reciba **F** en cada una de las filas de su tabla de verdad se dice que es una **contradicción**. Note que una fórmula es una contradicción si, y sólo si, su negación es una tautología. La contradicción más simple es $p \wedge \neg p$.

Ejercicios 2.1.2

1. Considere las siguientes fórmulas:

$$p \to q, \qquad \neg p \to \neg q, \qquad q \to p, \qquad \neg q \to \neg p,$$

$$p \to (q \wedge r), \quad \neg p \to (q \vee r), \quad (p \vee q) \to \neg r, \quad (p \wedge \neg q) \to r$$

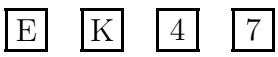
Para cada una de ellas responda las siguientes preguntas:

a) ¿Cuál es la recíproca?

b) ¿Cuál es la contrapositiva?

2. Construya la tabla de verdad de cada una de la fórmulas dadas en el ejemplo 2.7.

3. Cada una de las tarjetas indicadas tiene en un lado un número y en el otro una letra.



Alguien afirmó: todas las tarjetas que tienen una vocal en una cara tienen un número par en la otra. ¿Cuál es la menor cantidad de tarjetas que hay que voltear para verificar si tal afirmación es verdadera? ¿Cuáles hay que voltear?

4. José está mirando una fotografía de un hombre. Alguien llega y le pregunta: ¿quién es la persona que aparece en la foto?. José responde diciendo: No tengo hermanos ni hermanas. Pero el padre del hombre de la foto es el hijo de mi padre. ¿Quién es la persona que aparece en la foto? (a) El abuelo de José. (b) El padre de José. (c) José. (d) El hijo de José. (e) Ninguna de las anteriores.

5. En un pueblo sus habitantes siempre dicen la verdad o siempre dicen mentiras. El grupo $\mathbb{V}$ está formado por aquellos que dicen siempre la verdad y el grupo $\mathbb{M}$ por aquellos que siempre dicen mentiras. Tres habitantes P, Q y R del pueblo estaban conversando en la plaza. Una persona que caminaba por la plaza le preguntó a P: ¿Eres del grupo $\mathbb{V}$ o del grupo $\mathbb{M}$? Como no pudo escuchar la respuesta de P, entonces le preguntó a Q: ¿Qué fué lo que dijo P? Y Q respondió: "P dijo que él era del grupo $\mathbb{M}$". En este momento R habló y dijo: "No le creas a Q, él está mintiendo" ¿A qué grupo pertenecen Q y R?

2.1.3. Otras expresiones formales

En Matemáticas con frecuencia trabajamos con expresiones que no son necesariamente proposiciones pues contienen variables no especificadas (llamadas *variables libres*). Esto ocurre con expresiones algebraicas como las siguientes

$$x^2 + y^2 = z^2, \quad x^3 + z^4 \geq y^3 - x.$$

Observe que una vez que las variables se sustituyen por números obtenemos una proposición. Por ejemplo, colocando $x = 3$, $y = 4$ y $z = 5$ obtenemos

$$3^2 + 4^2 = 5^2, \quad 3^3 + 5^4 \geq 4^3 - 3.$$

Ambas, en este caso, son verdaderas. Pero si sustituimos $x = 0$, $y = 0$ y $z = 1$, entonces obtenemos en la primera $0 = 1$ y en la segunda $1 \geq 0$. Lo que queremos decir es que una expresión como $x^2 + y^2 = z^2$ no es ni verdadera ni falsa hasta tanto no se le den valores a las variables x, y y z. Esto es exactamente lo que ocurre con las fórmulas proposicionales. No son ni verdaderas ni falsas, hasta tanto cada variable proposicional se sustituya por una proposición (o lo que es lo mismo, hasta tanto se le asigne a cada variable alguno de los valores V o F).

Por otra parte, aún cuando las fórmulas algebraicas no son proposiciones, podemos manipularlas como si lo fueran. En el ejemplo de arriba, podemos negarla y obtener

$$x^2 + y^2 \neq z^2, \quad x^3 + z^4 \ngeq y^3 - x.$$

Podemos también formar expresiones más complejas. Por ejemplo

$$\text{Si } x \geq 5 \text{ y } y \leq 8, \text{ entonces } y^2 - x^2 \leq 39.$$

Y así podemos hablar de la recíproca o de la contrarecíproca de estas expresiones. En este ejemplo, tenemos que la recíproca es

$$\text{Si } y^2 - x^2 \leq 39, \text{ entonces } x \geq 5 \text{ y } y \leq 8$$

y la contrarecíproca es

$$\text{Si } y^2 - x^2 \nleq 39, \text{ entonces } x \ngeq 5 \text{ o } y \nleq 8.$$

Ejercicios 2.1.3

1. Proporcione la recíproca y la contrapositiva de cada una de las siguientes expresiones.

   a) Si $x + y = 1$, entonces $x^2 + y^2 \geq 1$,

   b) Si $x^2 = x$, entonces $x = 0$ ó $x = 1$.

2.2. Cálculo proposicional

Así como existe una teoría para realizar cálculos con números (la aritmética) ó con objetos más complejos como en el cálculo diferencial e integral, también existen reglas precisas para manejar proposiciones. En esta sección introduciremos los rudimentos del cálculo con proposiciones, o como usualmente se dice, cálculo proposicional. El cálculo proposicional provee los principios básicos que rigen la construcción de los razonamientos lógicamente correctos.

2.2.1. Equivalencia lógica

Algunas fórmulas aún siendo distintas tienen la misma tabla de verdad. Considere, por ejemplo, las fórmulas $\neg(p \vee q)$ y $\neg p \wedge \neg q$. A continuación calcularemos simultánemente las tablas de verdad de estas fórmulas.

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

Observemos que las columnas 4 y 7 son idénticas. Es decir, independientemente de los valores de verdad que se le asigne a las variables p y q las proposiciones $\neg(p \vee q)$ y $\neg p \wedge \neg q$ reciben el mismo valor.

Para entender lo que esto significa notemos que $\neg(p \vee q)$ es verdadera exactamente cuando $p \vee q$ no lo es. Lo cual ocurre exactamente cuando ni p ni q es verdadera. Es decir, cuando p y q son falsas. Esto es, cuando $\neg p \wedge \neg q$ es verdadera. En otras palabras, desde el punto de vista de su veracidad, las fórmulas $\neg(p \vee q)$ y $\neg p \wedge \neg q$ dicen lo mismo (pero de manera diferente).

Veamos otro ejemplo. Considere ahora las fórmulas $p \to q$ y $\neg q \to \neg p$. La tabla de verdad de ellas (calculadas simultáneamente) es la siguiente:

p	q	$p \to q$	$\neg p$	$\neg q$	$\neg q \to \neg p$
V	V	V	F	F	V
V	F	F	F	V	F
F	V	V	V	F	V
F	F	V	V	V	V

De nuevo obtenemos que $p \to q$ y $\neg q \to \neg p$ tienen tablas de verdad idénticas. Esto muestra que una fórmula condicional y su contrarecíproca son equivalentes en el sentido de que afirman los mismo.

Dos fórmulas ϕ y ψ se dicen que son **lógicamente equivalentes** si sus tablas de verdad son idénticas. Usaremos la siguiente notación para expresar que ϕ y ψ son lógicamente equivalentes

$$\phi \Leftrightarrow \psi$$

La noción de equivalencia lógica también está presente en el lenguaje natural cotidiano. Esto se observa cuando en el transcurso de una converzación o discusión se usan expresiones como: "Bueno, en realidad estamos diciendo la misma cosa, pero cada uno lo dice a su manera". La equivalencia lógica es entonces una forma de hacer precisa y rigurosa la noción común de "estar hablando de la misma cosa".

La siguiente tabla muestra algunas equivalencias lógicas importantes. Dejamos a cargo del lector comprobar estas equivalencias haciendo las correspondientes tablas de verdad.

Equivalencias Lógicas

1	$\neg(\neg p) \Leftrightarrow p$	Doble negación
2a	$p \vee q \Leftrightarrow q \vee p$	Leyes conmutativas
2b	$p \wedge q \Leftrightarrow q \wedge p$	
3a	$p \vee (q \vee r) \Leftrightarrow (p \vee q) \vee r$	Leyes asociativas
3b	$p \wedge (q \wedge r) \Leftrightarrow (p \wedge q) \wedge r$	
4a	$p \ \wedge \ (q \vee r) \Leftrightarrow (p \wedge q) \ \vee \ (p \wedge r)$	Leyes distributivas
4b	$p \ \vee \ (q \wedge r) \Leftrightarrow (p \vee q) \ \wedge \ (p \vee r)$	
5a	$\neg(p \vee q) \Leftrightarrow (\neg p \wedge \neg q)$	Leyes de De Morgan
5b	$\neg(p \wedge q) \Leftrightarrow (\neg p \vee \neg q)$	
6	$p \rightarrow q \Leftrightarrow \neg q \rightarrow \neg p$	contrapositiva
7	$p \rightarrow q \Leftrightarrow \neg p \vee q$	implicación
8	$(p \rightarrow r) \ \wedge (q \rightarrow r) \ \Leftrightarrow (p \vee q) \rightarrow r$	prueba por casos

Otras propiedades importantes de la equivalencia lógica son las **reglas de sustitución**. Sean ϕ, ψ y ρ fórmulas. Supongamos que $\phi \Leftrightarrow \psi$. Entonces

Reglas de sustitución
Suponga $\phi \Leftrightarrow \psi$ y $\alpha \Leftrightarrow \beta$. Entonces

S1	$\neg\phi$	$\Leftrightarrow$	$\neg\psi$
S2	$\alpha \wedge \phi$	$\Leftrightarrow$	$\beta \wedge \psi$
S3	$\alpha \vee \phi$	$\Leftrightarrow$	$\beta \vee \psi$

La primera afirmación es válida, pues la ultima columna de tabla de verdad $\neg\phi$ se obtienen de la de ϕ sustituyendo V por F y viceversa. Y lo mismo ocurre con ψ y $\neg\psi$. Dejamos al lector la tarea de convencerse de las otras afirmaciones.

A travéz de equivalencias lógicas es posible transformar las fórmulas y en algunos casos obtener expresiones mas simples. Ilustraremos con un ejemplo como simplificar un formula del tipo $\neg\phi$. Pero para hacerlo necesitaremos otra regla de sustitución:

Transitividad Si $\phi \Leftrightarrow \psi$ y $\psi \Leftrightarrow \rho$, entonces $\phi \Leftrightarrow \rho$.

Ejemplo 2.10. Considere la siguiente fórmula:

$$\neg(p \to (q \vee r)) \tag{2.1}$$

Usaremos las equivalencias presentadas en la tabla de arriba junto con la propiedad que enunciamos justo después de la tabla. En cada paso indicamos las reglas usadas.

(1)	$(p \to (q \vee r))$	$\Leftrightarrow$	$\neg p \vee (q \vee r)$	implicación
(2)	$\neg(p \to (q \vee r))$	$\Leftrightarrow$	$\neg((\neg p) \vee (q \vee r))$	sustitución S1, linea (1)
(3)	$\neg((\neg p) \vee (q \vee r))$	$\Leftrightarrow$	$\neg(\neg p) \wedge \neg(q \vee r)$	De Morgan
(4)	$\neg(\neg p)$	$\Leftrightarrow$	p	doble negación
(5)	$\neg(q \vee r)$	$\Leftrightarrow$	$\neg q \wedge \neg r$	De Morgan
(6)	$\neg(\neg p) \wedge \neg(q \vee r)$	$\Leftrightarrow$	$p \wedge (\neg q \wedge \neg r)$	sustitución S2, lineas (4) y (5)
(7)	$\neg(p \to (q \vee r))$	$\Leftrightarrow$	$\neg(\neg p) \wedge \neg(q \vee r)$	Transitividad, (2) y (3)
(8)	$\neg(p \to (q \vee r))$	$\Leftrightarrow$	$p \wedge (\neg q \wedge \neg r)$	Transitividad, (7) y (6)

La linea (8) nos dice que la fórmula $\neg(p \to (q \vee r))$ es lógicamente equivalente a $p \wedge \neg q \wedge \neg r$, que es claramente mas simple que la primera.

□

2.2.2. Implicación lógica

Diremos que una fórmula ϕ **implica lógicamente** a otra fórmula ψ, si " ψ es verdadera cada vez que ϕ lo sea". Mas precisamente, en las tablas de verdad de ϕ y de ψ, las filas donde ϕ tiene una V, también ψ tiene una V. Note que, a diferencia de lo que ocurre con la equivalencia lógica, sólo nos interesa las filas donde ϕ tiene valor V.

Usaremos la siguiente notación para la implicación lógica

$$\phi \Rightarrow \psi.$$

Hay otras maneras equivalentes de leer $\phi \Rightarrow \psi$:

(1) ψ es una **consecuencia lógica** de ϕ.
(2) ϕ es una **condición suficiente** para ψ.
(3) ψ es una **condición necesaria** para ϕ.

Ejemplo 2.11. Considere las fórmulas $[p \ \wedge \ (p \to q)]$ y q.

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

Vemos entonces que $[p \wedge (p \to q)] \Rightarrow q$. Observe también que ellas no son lógicamente equivalentes. □

Ejemplo 2.12. El ejemplo anterior se puede ilustrar con situaciones de la vida diaria. Por ejemplo, considere las proposiciones: "Juan compró la entrada para el cine", denotémosla con la letra P y "Juan tiene derecho a entrar al cine", que denotaremos con la letra Q. La regla $P \to Q$ dice que "si Juan tiene un ticket, entonces tiene derecho a entrar al cine". El ejemplo anterior nos dice que de $P \wedge (P \to Q)$ se concluye lógicamente Q. Es decir, podemos concluir que Juan tiene derecho a entrar al cine. □

La siguiente tabla contiene algunas implicaciones lógicas importantes. Dejamos a cargo del lector hacer las correspondientes tablas de verdad.

Implicaciones Lógicas

1	$p \Rightarrow (p \vee q)$	adición
2	$(p \wedge q) \Rightarrow p$	simplificación
3	$[p \wedge (p \to q)] \Rightarrow q$	*Modus Ponens*
4	$[\neg q \wedge (p \to q)] \Rightarrow \neg p$	*Modus Tollens*
5	$\neg q \wedge (p \vee q) \Rightarrow p$	silogismo disyuntivo
6	$((p \to q) \wedge (q \to r)) \Rightarrow (p \to r)$	silogismo hipotético

Finalmente, observemos que $\phi \Leftrightarrow \psi$ es equivalente a que se cumplan simultáneamente que $\phi \Rightarrow \psi$ y también que $\psi \Rightarrow \phi$. Por esta razón cuando se quiere establecer la equivalencia lógica entre dos proposiciones, uno puede hacerlo mostrando dos implicaciones lógicas.

Ejercicios 2.2

1. Demuestre las equivalencias lógicas y las implicaciones lógicas de las tablas dadas en la secciones 2.2.1 y 2.2.2. Es decir, compare las correspondientes tablas de verdad.
2. Simplifique las siguientes fórmulas siguiendo un procedimiento similar al usado en el ejemplo 2.10.

a) $\neg(\neg p \to q)$

b) $\neg((p \wedge q) \to r)$

c) $\neg(p \to (q \vee r))$.

d) $\neg(p \to \neg(q \wedge r))$.

e) $\neg((p \wedge q) \to (r \vee s))$

f) $\neg(\neg(\neg p \vee \neg q) \to (\neg r \vee \neg p))$

g) $\neg(\ p \to (\neg(q \to \neg r) \to (r \to \neg s)))$.

3. Use lo hecho en el ejercicio 2 para mostrar las siguientes equivalencias

a) $\neg(\neg(\neg p \vee \neg q) \to (\neg r \vee \neg p)) \Leftrightarrow r \wedge p \wedge q$.

b) $\neg(\ p \to (\neg(q \to \neg r) \to (r \to \neg s))) \Leftrightarrow p \wedge q \wedge r \wedge s$.

4. Determine si las siguientes afirmaciones son válidas:

a) $\neg(p \leftrightarrow (q \vee r)) \Leftrightarrow (\neg p \leftrightarrow (\neg q \wedge \neg r))$

b) $((\neg p \wedge \neg r) \to \neg q) \Leftrightarrow \neg((p \vee r) \to q)$

5. Muestre que $\phi \Leftrightarrow \psi$ si, y sólo si, $\phi \Rightarrow \psi$ y $\psi \Rightarrow \phi$.

6. Muestre que $\phi \Leftrightarrow \psi$ si, y sólo si, $\phi \leftrightarrow \psi$ es una tautología.

7. Muestre que $\phi \Rightarrow \psi$ si, y sólo si $\phi \to \psi$ es una tautología.

8. Yoana, una niña de 7 años, acaba de conocer a Elena, la hija de Carmen. Carmen dice que Yoana se parece bastante a su mamá y le pregunta a Yoana: *¿a quien se parece Elena?* Yoana nunca a visto al padre de Elena pero dice que Elena se parece a su papá. ¿Cuál pudo ser el razonamiento usado por Yoana para concluir esto?

9. (Este problema es tomado de [7]) Un prisionero debe hacer una elección entre dos puertas: detrás de una de ellas está una hermosa dama y detrás de la otra se halla un tigre hambriento. Suponga que cada una de las puertas tuviera un letrero y el prisionero sabe que solamente un letrero es verdadero. El letrero de la primera puerta dice:

En este cuarto hay un dama y en el otro cuarto hay un tigre.

El letrero de la segunda puerta dice:

En uno de estos cuartos hay uno dama y en uno de estos cuartos hay un tigre.

Con esta información, el prisionero es capaz de elegir la puerta correcta (¿la del tigre?).

2.3. La lógica y las operaciones sobre conjuntos

Las operaciones sobre conjuntos y los conectivos de la lógica proposicional son similares. En la tabla que sigue señalamos la analogía existente entre ambas

$A \cap B$	$p \wedge q$
$A \cup B$	$p \vee q$
A^c	$\neg p$

Todas las expresiones que involucran la relación de pertenencia $\in$ y las operaciones elementales entre conjuntos se traducen en proposiciones lógicas:

$x \in A \cap B$	$x \in A$ y $x \in B$
$x \notin A \cap B$	$x \notin A$ ó $x \notin B$
$x \in A \cup B$	$x \in A$ ó $x \in B$
$x \notin A \cup B$	$x \notin A$ y $x \notin B$
$x \in A^c$	$x \notin A$
$x \notin A^c$	$x \in A$
$x \in A \setminus B$	$x \in A$ y $x \notin B$
$x \notin A \setminus B$	$x \notin A$ ó $x \in B$

Es importante que el lector comprenda y recuerde esta tabla pues es fundamental para trabajar con los conjuntos. En particular, observe el significado de $x \notin A \cap B$ y $x \notin A \cup B$. Como es costumbre en matemáticas, no hemos mencionado el conjunto universal, pues el contexto debe indicarlo.

2.4. Cuantificadores

El lenguaje de la lógica proposicional es insuficiente para expresar la mayoría de los resultados de la matemática. Hace falta introducir otros símbolos. Por ejemplo, la noción de subconjunto $A \subseteq B$ se define diciendo que todo elemento de A debe pertenecer a B. La expresión *"todo elemento de"* ocurre con mucha frecuencia en matemáticas y refleja una de sus características más importantes: la posibilidad de mostrar hechos generales sobre los elementos del universo que se esté analizando. El símbolo que se usa para abreviar esa expresión es $\forall$, que se lee "para todo", y se llama **cuantificador universal**.

Ahora podemos enunciar la definición de la relación de subconjunto usando el cuantificador universal:

$A \subseteq B$	$\forall x(x \in A \rightarrow x \in B)$

Otro cuantificador que se usa en lógica es el **cuantificador existencial** que se denota con el símbolo $\exists$ y se lee "existe". Este cuantificador ocurre, por ejemplo, al expresar que un subconjunto no está contenido en otro. En efecto, si $A \not\subseteq B$, entonces debe existir un elemento que pertenece a A y que no pertenece a B. En símbolos:

$A \not\subseteq B$	$\exists x(x \in A \ \wedge \ x \notin B)$

En la siguiente tabla veremos algunas relaciones entre conjuntos que se expresan usando cuantificadores.

$A \subseteq B$	$\forall x \ (x \in A \rightarrow x \in B)$
$A \not\subseteq B$	$\exists x \ (x \in A \wedge x \notin B)$
$A = B$	$\forall x \ (x \in A \leftrightarrow x \in B)$
$A \neq B$	$\exists x \ [(x \in A \wedge x \notin B) \vee (x \notin A \wedge x \in B)]$
$A \cap B \neq \emptyset$	$\exists x \ (x \in A \wedge x \in B)$
$A \cap B = \emptyset$	$\forall x \ (x \notin A \vee x \notin B)$

La tabla anterior también sirve para ilustrar cómo se comportan los cuantificadores cuando se niega una expresión que los contiene. *Al negar un cuantificador universal se obtiene uno existencial y, viceversa, al negar un cuantificador existencial se obtiene uno universal.*

$\neg\forall x\psi$	$\exists x\neg\psi$
$\neg\exists x\psi$	$\forall x\neg\psi$

También escribiremos $\nexists$ en lugar de $\neg\exists$.

Ejemplo 2.13. (i) Considere la siguiente fórmula:

$$\neg(\forall x \ (x \in A \rightarrow x \in B))$$

Ella es equivalente a

$$\exists x \ \neg(x \in A \rightarrow x \in B)$$

La cual, a su vez, es equivalente a

$$\exists x \ (x \in A \ \wedge \ x \notin B)$$

(ii) Veamos otro ejemplo

$$\begin{aligned} \neg(\exists x\ (x \notin A\ \vee\ x \in B)) &\Leftrightarrow \forall x\ \neg(x \notin A\ \vee\ x \in B) \\ &\Leftrightarrow \forall x\ (x \in A\ \wedge\ x \notin B) \end{aligned}$$

□

Ejemplo 2.14. Las desigualdades con frecuencia se expresan usando ∀. Por ejemplo: Todo número real elevado al cuadrado no es negativo. En símbolos:

$$\forall x \in \mathbb{R}\ (x^2 \geq 0).$$

Todo número natural x cumple que $x < x + 1$. En símbolos:

$$\forall x \in \mathbb{N}\ (x < x + 1).$$

□

Ejemplos 2.15. También es importante saber cuando una afirmación cuantificada es verdadera o no.

1. Considere la afirmación

$$\forall n \in \mathbb{N}\ (n^3 < 9) \tag{2.2}$$

Para mostrar que ella no es válida, basta observar que si sustituimos n por 3, obtenemos una proposición falsa. En efecto, $3^3 = 27$ y $27 \not< 9$. El 3 se dice que es un **contraejemplo** de la afirmación (volveremos mas adelante sobre este tema de los contraejemplos). ¿Puede conseguir otro contraejemplo?

2. Ahora considere la afirmación

$$\forall x \in \mathbb{R}\ ((x + 1)^2 \geq x^2).$$

Vemos entonces que $x = -1$ es un contraejemplo (verificarlo) y por lo tanto esa afirmación es falsa.

Dejamos a cargo del lector encontrar otros contraejemplos. ¿Puede servir de contraejemplo cualquier número negativo?

3. Considere la afirmación

$$\exists n \in \mathbb{N}\ (18 < n^2 + 3 < 20). \tag{2.3}$$

Para ver si ella es verdadera, debemos hallar un natural que satisfaga la condición especificada. Si sustituimos en la expresión n^2+3 la variable n por los valores $0, 1, 2, 3, 4$ obtenemos, respectivamente, 3, 4, 7, 12 y 19. Vemos entonces que al sustituir n por 4, obtenemos la siguiente proposición verdadera "$18 < 4^2 + 3 < 20$". Por lo tanto, la afirmación (2.3) es verdadera.

4. Observemos que la negación de la afirmación (2.2) es

$$\exists n \in \mathbb{N}\,(n^3 \geq 9).$$

Como (2.2) es falsa, entonces su negación es verdadera. En efecto, vimos que $3^3 \geq 9$.

□

Ejemplos 2.16. En cada uno de los siguientes casos queremos hallar conjuntos A y B de números naturales que satisfagan la propiedad indicada.

1. $\exists x \in \mathbb{N}\,(x \in A \wedge x \in B)$.

Considere los conjuntos $A = \{1, 2, 3\}$ y $B = \{2, 3, 4\}$. Este par de conjuntos satisfacen la propiedad indicada, pues por ejemplo cuando x es igual a 2 se cumple que $x \in A$ y $x \in B$. ¿Qué podemos decir en general?, en otras palabras, ¿Cuáles pares de conjuntos A y B satisfacen esta propiedad? Veamos:

$$\begin{aligned} \exists x \in \mathbb{N}\,(x \in A \wedge x \in B) &\Leftrightarrow \exists x \in \mathbb{N}\,(x \in A \cap B) \\ &\Leftrightarrow A \cap B \neq \emptyset \end{aligned}$$

Esto nos dice que cualquier par de conjuntos A y B tales que $A \cap B \neq \emptyset$ satisfacen la propiedad indicada.

2. $\nexists x \in \mathbb{N}\,(x \in A \wedge x \in B)$.

En este caso basta tomar dos conjuntos disjuntos, por ejemplo, $A = \{1, 2, 3\}$ y $B = \{4, 5\}$. Tenemos que no existe x tal que $x \in A$ y $x \in B$.

De lo visto en el ejemplo anterior, tenemos que

$$\nexists x \in \mathbb{N}\,(x \in A \wedge x \in B) \Leftrightarrow A \cap B = \emptyset$$

3. $\exists x \in \mathbb{N}\,(x \in A \vee x \in B)$.

Por ejemplo, $A = \{1, 2, 3\}$ y $B = \{4\}$ satisface la propiedad indicada. Pues haciendo x igual a 1 se cumple que $x \in A \vee x \in B$. En otras palabras, 1 es un ejemplo de que existe un x con la propiedad indicada. También 4 sirve como ejemplo. En general tenemos lo siguiente

$$\begin{aligned} \exists x \in \mathbb{N}\,(x \in A \vee x \in B) &\Leftrightarrow \exists x \in \mathbb{N}\,(x \in A \cup B) \\ &\Leftrightarrow A \cup B \neq \emptyset \end{aligned}$$

Esto nos dice que cualquier par de conjuntos A y B tal que $A \cup B$ no sea vacío es un ejemplo donde la propiedad indicada es verdadera.

4. $\exists x \in \mathbb{N}\,(x \notin A \wedge x \notin B)$.

   Considere $A = \{1, 2\}$ y $B = \{4, 5\}$. Entonces haciendo x igual a 6 se tiene que $x \notin A$ y $x \notin B$. En general tenemos que

$$\begin{array}{rcl} \exists x \in \mathbb{N}\,(x \notin A \wedge x \notin B) & \Leftrightarrow & \exists x \in \mathbb{N}\,(x \in A^c \wedge x \in B^c) \\ & \Leftrightarrow & \exists x \in \mathbb{N}\,(x \in A^c \cap B^c) \\ & \Leftrightarrow & A^c \cap B^c \neq \emptyset \end{array}$$

   Por lo tanto, un par de conjuntos A y B satisface la propiedad indicada si y sólo si $A^c \cap B^c$ no es vacío. Observe que esto ocurrió con el ejemplo que dimos antes: Si $A = \{1, 2\}$ y $B = \{4, 5\}$, entonces $A^c \cap B^c = \mathbb{N} \setminus \{1, 2, 4, 5\}$.

5. $\exists x \in \mathbb{N}\,(x \notin A \vee x \notin B)$.

   Los mismos conjuntos A y B que en el ejemplo anterior satisfacen esta propiedad. En general, tenemos que

$$\begin{array}{rcl} \exists x \in \mathbb{N}\,(x \notin A \vee x \notin B) & \Leftrightarrow & \exists x \in \mathbb{N}\,(x \in A^c \vee x \in B^c) \\ & \Leftrightarrow & \exists x \in \mathbb{N}\,(x \in A^c \cup B^c) \\ & \Leftrightarrow & A^c \cup B^c \neq \emptyset \end{array}$$

6. $\nexists x \in \mathbb{N}\,(x \in A \vee x \in B)$.

   En este caso, el único ejemplo es $A = B = \emptyset$. En efecto,

$$\begin{array}{rcl} \nexists x \in \mathbb{N}\,(x \in A \vee x \in B) & \Leftrightarrow & \forall x \in \mathbb{N}\,\neg(x \in A \vee x \in B) \\ & \Leftrightarrow & \forall x \in \mathbb{N}\,(x \notin A \wedge x \notin B) \\ & \Leftrightarrow & \forall x \in \mathbb{N}\,(x \in A^c \wedge x \in B^c) \\ & \Leftrightarrow & \forall x \in \mathbb{N}\,(x \in A^c \cap B^c) \\ & \Leftrightarrow & A^c \cap B^c = \mathbb{N} \end{array}$$

□

Ejemplo 2.17. Considere el siguiente conjunto

$$A = \{x \in \mathbb{N} :\ \forall y \in \mathbb{N}\,(x \leq 10 + y)\}$$

Para que un número natural x pertenezca al conjunto A debe cumplir cada una de las siguientes condiciones

$$\begin{array}{rcl} x & \leq & 10 + 0 \\ x & \leq & 10 + 1 \\ x & \leq & 10 + 2 \\ x & \leq & 10 + 3 \\ x & \leq & 10 + 4 \\ x & \leq & 10 + 5 \\ x & \leq & 10 + 6 \\ & \vdots & \end{array}$$

Hemos colocado $\vdots$ pues el cuantificador $\forall y \in \mathbb{N}$ impone, para cada $y \in \mathbb{N}$, una condición. Vemos entonces que $A = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$.

□

Ejemplo 2.18. También es frecuente usar expresiones donde aparecen ambos cuantificadores. Por ejemplo, para expresar que todo número real positivo tiene una raíz cuadrada lo hacemos de la siguiente manera:

$$\forall x \in \mathbb{R}\, [x > 0 \to \exists y \in \mathbb{R}\, (y^2 = x)]$$

Se puede simplificar esta expresión introduciendo un símbolo para denotar los números reales positivos, normalmente se usa $\mathbb{R}^+$. Podemos entonces escribir la afirmación anterior de la siguiente manera:

$$\forall x \in \mathbb{R}^+\, \exists y \in \mathbb{R}\, (y^2 = x).$$

Esta expresión usualmente se lee así: Para todo x en $\mathbb{R}^+$, existe un y en $\mathbb{R}$ tal que y^2 es igual a x. Observe que la expresión "tal que" no aparece sino que fue sustituida por los parétesis ( ).

□

Ejercicios 2.4

1. Vea el ejemplo 2.15 para responder este ejercicio.

   a) Muestre que $n = 2$ es un contraejemplo de que la afirmación

   $$\forall n \in \mathbb{N}\, (n^4 < 15)$$

   no es válida. ¿Puede conseguir otro?

   b) Considere la proposición

   $$\forall x \in \mathbb{R}\, ((x-1)^3 \geq x^3).$$

   Muestre que $x = 0$ es un contraejemplo. Encuentre otro contraejemplo.

   c) Determine si la siguiente afirmación es verdadera

   $$\forall n \in \mathbb{N}\, (33 < n^3 + 2n + 1 < 35).$$

   d) Determine si la siguiente afirmación es verdadera

   $$\exists n \in \mathbb{N}\, (33 < n^3 + 2n + 1 < 35).$$

2. Muestre que las siguientes afirmaciones son lógicamente equivalentes. En otras palabras, muestre que $(a) \Leftrightarrow (b)$, $(b) \Leftrightarrow (c)$, $(c) \Leftrightarrow (d)$ y $(d) \Leftrightarrow (a)$.

a) $A \subseteq B$.

b) $\forall x(x \notin A \vee x \in B)$.

c) $\forall x(x \notin B \to x \notin A)$.

d) $B^c \subseteq A^c$.

3. Muestre que las siguientes afirmaciones son lógicamente equivalentes:

a) $A \cap B = \emptyset$.

b) $\forall x(x \in A \to x \notin B)$.

c) $\forall x(x \in B \to x \notin A)$.

d) $\forall x(x \notin B \vee x \notin A)$.

4. Determine si la siguiente afirmación es válida.

$$A \cap B = \emptyset \;\Leftrightarrow\; \forall x\,[\,(x \in A \wedge x \notin B) \vee (x \notin A \wedge x \in B)]$$

5. En cada uno de los ejercicios que siguen, halle conjuntos A, B, C todos ellos subconjuntos de $\mathbb{N}$ tales que

a) $\forall x \in \mathbb{N}\,(x \in A \wedge x \in B \wedge x \notin C)$.

b) $\forall x \in \mathbb{N}\,(x \notin A \to (x \in B \vee x \notin C))$.

c) $\exists x \in \mathbb{N}\,((x \in A \vee x \in B) \wedge (x \notin A \vee x \in C))$.

d) $\forall x \in \mathbb{N}\,\exists y \in \mathbb{N}\,(x \in A \to y \in B)$.

e) $\forall x \in \mathbb{N}\,\exists y \in \mathbb{N}\,(x \in A \to (y \in B \cap A) \wedge (y \neq x))$.

f) $\forall x \in \mathbb{N}\,\exists y \in \mathbb{N}\,(x \in A \to ((y \in B \wedge x \notin C))$.

6. Determine cuales de las siguientes proposiciones son verdaderas y en caso que sean falsas de un contraejemplo.

a) $\forall x \in \mathbb{R}\,\exists y \in \mathbb{R}\,(x + y \geq 0)$.

b) $\exists y \in \mathbb{R}\,\forall x \in \mathbb{R}\,(x + y \geq 0)$.

c) $\forall x \in \mathbb{R}\,\forall y \in \mathbb{R}\,(x^2 + y^2 \geq 0)$.

d) $\forall y \in \mathbb{R}\,\forall x \in \mathbb{R}\,(x^2 + y^2 > 0)$.

e) $\exists y \in \mathbb{R}\,\exists x \in \mathbb{R}\,(x^2 + y^2 > 0)$.

7. Simplifique las siguientes fórmulas siguiendo el procedimiento que se ilustra en el ejemplo 2.13.

a) $\neg\,(\exists y \in \mathbb{R}\,\exists x \in \mathbb{R}\,(x^2 + y^2 > 0))$.

b) $\neg\,(\forall x \in \mathbb{R}\,\forall y \in \mathbb{R}\,(x^2 + y^2 \geq 0))$.

c) $\neg\,(\forall y \in \mathbb{R}\ \exists z \in \mathbb{R}\ [y > 0 \to (x < z < x + y)])$.

d) $\neg\,(\forall x\ \exists y\ [\,(x \in A \wedge y \in B)\ \to\ x \in C]\,)$.

e) $\neg\,(\exists x[\,x \in C\ \to\ (\exists y(x \in A \wedge y \in B))\,]\,)$.

f) $\neg\,(\exists x\ [\,(\exists y(x \in A \wedge y \in B))\ \to\ x \in C\,]\,)$.

8. Determine al menos un elemento de cada uno de los siguientes conjuntos

a) $\{x \in \mathbb{N} :\ \exists z \in \mathbb{N}\ (z \geq 2\,,\ z < x$ y z divide a $x)\}$.

b) $\{x \in \mathbb{N} :\ \exists z \in \mathbb{N}\ (2z$ divide a $x)\}$.

c) $\{x \in \mathbb{R} :\ \forall y \in \mathbb{R}\ (y > 0 \to xy > 0)\}$.

d) $\{x \in \mathbb{R} :\ \exists y \in \mathbb{R}\ (y > 0\ \wedge\ xy > 0)\}$.

e) $\{x \in \mathbb{R} :\ \forall y \in \mathbb{R}\ \exists z \in \mathbb{R}\ [y > 0 \to (x < z < x + y)]\}$.

9. Considere los siguientes conjuntos

$$\begin{array}{rcl} A & = & \{x \in \mathbb{N} :\ \text{Si } x \geq 9, \text{ entonces } x \text{ es impar}\} \\ B & = & \{x \in \mathbb{N} :\ \text{Si } x + 5 \geq 10, \text{ entonces } x \leq 20\} \\ C & = & \{x \in \mathbb{R} :\ x \leq 10 \text{ y } x \geq -8\} \\ D & = & \{x \in \mathbb{R} :\ x \leq -7 \text{ o } x \geq 22\} \end{array}$$

Determine cuáles de las siguientes proposiciones son verdaderas y cuáles son falsas.

(i)	$5 \in A$	(v)	$9 \in C$
(ii)	$10 \in A$	(vi)	$-15/2 \in C \cap D$
(iii)	$6 \in B$	(vii)	$35 \in D$
(iv)	$16 \in B$	(viii)	$7 \in B \cap C$

10. Sea A un subconjunto de $\mathbb{N}$. Considere los siguientes conjuntos

$$\begin{array}{rcl} B & = & \{x \in \mathbb{N} :\ \text{Si } x \in A, \text{ entonces } x \text{ es par}\} \\ C & = & \{x \in \mathbb{N} :\ x \in A \text{ y } x \text{ es impar}\} \\ D & = & \{x \in \mathbb{N} :\ \text{Si } x \notin A, \text{ entonces } x \text{ es par}\} \end{array}$$

Muestre que (independientemente de quien sea el conjunto A) se cumple lo siguiente:

a) $\mathbb{N} = B \cup C$.

b) $B \cup D = \{x \in \mathbb{N} :\ x$ es par$\}$.

Capítulo 3

Conjuntos (continuación)

En este capítulo continuaremos estudiando las propiedades de los conjuntos pero ahora haciendo uso de las herramientas de la lógica que vimos en el capítulo 2. En particular, introduciremos por primera vez las *demostraciones*. Demostrar una afirmación en matemáticas es una forma muy especial de justificar dicha afirmación. En una demostración debe darse un razonamiento lógicamente correcto que tenga como conclusión la afirmación en cuestión. En matemáticas las afirmaciones, para ser consideradas válidas, deben ser demostradas. Lo dicho arriba no es una definición de la noción de demostración. En realidad está fuera de los objetivos de este texto el dar una definición precisa de esta noción, sin embargo al final de este capítulo haremos una aproximación a una definición de demostración. Esperamos que los numerosos ejemplos de demostraciones que veremos le den una idea al lector de como hacerlas.

3.1. Propiedades de las operaciones entre conjuntos

En esta sección estudiaremos algunas propiedades básicas de las operaciones entre conjuntos.

3.1.1. Algunas propiedades de la relación $\subseteq$

Comenzaremos con una propiedad que se conoce por el nombre de **propiedad transitiva**.

$$\text{Si } A \subseteq B \text{ y } B \subseteq C, \text{ entonces } A \subseteq C.$$

La propiedad transitiva de $\subseteq$ nos permite usar expresiones como la que sigue sin que haya ninguna ambigüedad

$$A \subseteq B \subseteq C$$

Esta expresión abrevia la conjunción de tres afirmaciones: $A \subseteq B$, $B \subseteq C$ y $A \subseteq C$. Por ejemplo, $\mathbb{N} \subseteq \mathbb{Z} \subseteq \mathbb{Q}$. Algo similar estamos acostumbrados a hacer con números, pues escribimos $x \leq y \leq z$ en lugar de escribir la expresión más larga: $x \leq y$, $y \leq z$ y $x \leq z$.

La forma como se enuncia la propiedad transitiva es un ejemplo de una afirmación *condicional*. Pues ella afirma que $A \subseteq C$ bajo la condición de que $A \subseteq B$ y $B \subseteq C$. En el enunciado de la propiedad transitiva, la hipótesis consiste de dos afirmaciones: $A \subseteq B$ y $B \subseteq C$. Y la conclusión es $A \subseteq C$.

Para mostrar la validez de la propiedad transitiva supongamos que tenemos tres conjuntos A, B y C tales que $A \subseteq B$ y $B \subseteq C$. Mostraremos que entonces se cumple que $A \subseteq C$. En símbolos, lo que debemos mostrar es que:

$$\forall x\ (x \in A \to x \in C).$$

Para ver esto, sea x un elemento de A arbitrario (pero fijo). Queremos mostrar que $x \in C$. En efecto, una de nuestras suposiciones es que $A \subseteq B$ y como x lo tomamos en A, podemos concluir que $x \in B$. La segunda suposición es que $B \subseteq C$, pero como ya mostramos que $x \in B$, podemos finalmente concluir que $x \in C$.

Observación 3.1. La justificación de la propiedad transitiva que acabamos de ver es un ejemplo de lo que en Matemáticas se llama una **demostración**. Este es además un ejemplo de una demostración de una afirmación condicional. El lector debe tomar nota de lo que hicimos, pues lo encontraremos con bastante frecuencia. A continuación lo resaltamos.

Para demostrar una afirmación condicional suponga que la hipótesis se cumple y muestre que la conclusión también se cumple.

□

Observación 3.2. Usualmente la demostración de una afirmación como $A \subseteq C$ comienza con frases como: *"Fijemos un elemento arbitrario x de A...."* o también *"Sea x un elemento arbitrario, pero fijo, de A.."*. Recomendamos al lector que use estas expresiones o alguna otra equivalente cuando esté demostrando afirmaciones como la anterior. □

Otra propiedad de la relación de subconjunto $\subseteq$ es la siguiente:

Ejemplo 3.3. Sean A y B conjuntos cualesquiera. Mostraremos que:

$$\textit{Si } A \subseteq B, \textit{ entonces } B^c \subseteq A^c. \tag{3.1}$$

Para mostrar (3.1) haremos uso de una de las equivalencias lógicas vistas en el capítulo 2. Recordemos que una proposición condicional es lógicamente equivalente a su contrarecíproca. En símbolos:

$$\phi \to \psi \Leftrightarrow \neg\psi \to \neg\phi$$

Por esto, la afirmación (3.1) es equivalente a la siguiente afirmación:

$$\textit{Si } B^c \not\subseteq A^c, \textit{ entonces } A \not\subseteq B. \tag{3.2}$$

Por lo tanto para demostrar que (3.1) es válida, basta que mostremos que (3.2) lo es. Supongamos que A y B son conjuntos tales que $B^c \not\subseteq A^c$ y mostremos que $A \not\subseteq B$. Como por hipótesis $B^c \not\subseteq A^c$, entonces existe un elemento x que pertenece a B^c pero no a A^c. Es decir, existe x tal que $x \in B^c$ y $x \notin A^c$. En otras palabras, existe x tal que $x \notin B$ y $x \in A$. Esto precisamente dice que $A \not\subseteq B$ y así hemos mostrado (3.2).

□

3.1.2. La igualdad de conjuntos

Otra manera de enunciar la equivalencia lógica de dos proposiciones es a travéz de la expresión *si, y sólo si*. Es decir, $\phi \Leftrightarrow \psi$ dice lo mismo que ϕ si, y sólo si ψ. Recordemos, además, que esto último también es equivalente a decir que se cumple simultáneamente que $\phi \Rightarrow \psi$ y que $\psi \Rightarrow \phi$. El siguiente ejemplo ilustra el uso del *si, y sólo si*.

Ejemplo 3.4.

$$A \cap B = A \text{ si, y sólo si, } A \subseteq B. \tag{3.3}$$

En este ejemplo tenemos las proposiciones

$$\textit{Si } A \cap B = A, \textit{ entonces } A \subseteq B \tag{3.4}$$

y

$$\textit{Si } A \subseteq B, \textit{ entonces } A \cap B = A. \tag{3.5}$$

Recordemos que cuando decimos que *"Q si, y sólo si P"* estamos afirmando que las proposiciones Q y P son *equivalentes*. Esto significa que Q se cumple, si P se cumple y viceversa, P se cumple, si Q se cumple.

Ahora demostraremos (3.3). Primero veremos la afirmación (3.4). Nuestra hipótesis es que $A \cap B = A$. Sabemos que $A \cap B \subseteq B$. Luego sustituyendo iguales por iguales (es decir, sustituyendo $A \cap B$ por A) obtenemos que $A \subseteq B$.

La afirmación (3.5) se demuestra de manera similar. Nuestra hipótesis ahora es que $A \subseteq B$ y queremos mostrar que $A \cap B = A$. Ya sabemos que $A \cap B \subseteq A$ (¿por qué?), así que resta mostrar que $A \subseteq A \cap B$. Tomemos $x \in A$, por hipótesis $A \subseteq B$, luego $x \in B$ y en consecuencia $x \in A \cap B$. □

El ejemplo anterior nos dice que, desde el punto de vista de la lógica, afirmar que un conjunto A es subconjunto de otro conjunto B es equivalente a afirmar que $A \cap B = A$.

El esquema que hemos usado en la demostración anterior se repetirá con mucha frecuencia y es importante que el lector le preste atención:

Para demostrar una afirmación del tipo

Q si, y sólo si, P

se deben mostrar las siguientes afirmaciones condicionales:

(1) *Si P, entonces Q.*
(2) *Si Q, entonces P.*

Las equivalencias (lógicas) con frecuencia facilitan la búsqueda de la respuesta a una pregunta. Considere el siguiente ejemplo.

Ejemplo 3.5. Queremos determinar todos los conjuntos A que cumplan con la siguiente ecuación

$$A \cap \{1, 3, 5\} = A.$$

Por lo visto anteriormente, sabemos que un conjunto A cumple con esta ecuación si, y sólo si, satisface la siguiente condición

$$A \subseteq \{1, 3, 5\}.$$

Por lo tanto, los únicos conjuntos que cumplen con la ecuación indicada son

$$\emptyset, \{1\}, \{3\}, \{5\}, \{1, 3\}, \{1, 5\}, \{3, 5\}, \{1, 3, 5\}.$$

□

Por último es bueno que el lector tome nota que la expresión P si, y sólo si Q abrevia una mas larga: Si Q, entonces P y P, sólo si Q.

3.1.3. Unión e intersección

Comenzaremos con algunas de las propiedades de la unión y de la intersección. En lo que sigue A, B y C denotan conjuntos.

1a	$A \cup B = B \cup A$	**Leyes conmutativas**
1b	$A \cap B = B \cap A$	
2a	$A \cup (B \cup C) = (A \cup B) \cup C$	**Leyes asociativas**
2b	$A \cap (B \cap C) = (A \cap B) \cap C$	
3a	$A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$	**Leyes distributivas**
3b	$A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$	
4a	$A \cup A = A$	**Leyes de idempotencia**
4b	$A \cap A = A$	
4c	$A \cup \emptyset = A$	**Leyes de la Identidad**
4d	$A \cap \emptyset = \emptyset$	

Estas leyes (junto con otras que veremos más adelante) se conocen como las **Leyes del álgebra de conjuntos** ó también como las leyes del **álgebra Boolena** en honor al matemático inglés George Boole (1815-1864).

Las *leyes conmutativas* dicen que el orden en que se unan o intersecten dos conjuntos es irrelevante. Si vemos con detenimiento la definición de $A \cap B$ notamos que en efecto el orden en que se coloquen los conjuntos A y B no es relevante. Algo similar ocurre con la definición $A \cup B$.

Las *leyes asociativas* son importantes, pues garantizan que el uso de los paréntesis no es necesario en las expresiones que usan sólo uniones o sólo intersecciones. Es decir, ya que $A \cup (B \cup C) = (A \cup B) \cup C$, entonces podemos definir un conjunto a través de la expresión $A \cup B \cup C$ sin que haya ninguna ambigüedad acerca de cuál conjunto estamos definiendo. De manera similar podemos escribir $A \cap B \cap C$ sin problemas de ambigüedad. Esto no sucede, por ejemplo, si tenemos una expresión como la siguiente

$$A \cup B \cap C.$$

En este caso no queda claro qué conjunto estamos definiendo, pues tenemos dos alternativas

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

y

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

Estas dos expresiones no denotan en general el mismo conjunto (vea el ejercicio 5 de la sección 1.2). Por esto el uso de los paréntesis es necesario.

Todavía nos queda por justificar la validez de las *leyes distributivas*. La demostración de esta ley no es tan directa y recurriremos a un argumento un poco más elaborado.

Ejemplo 3.6. Veamos la primera ley distributiva:

$$A \cup (B \cap C) = (A \cup B) \cap (A \cup C). \tag{3.6}$$

Antes de dar una demostración le sugerimos al lector que haga los diagramas de Venn correspondientes a $A \cup (B \cap C)$ y $(A \cup B) \cap (A \cup C)$. Y observe que en ambos diagramas obtenemos la misma región sombreada. Los diagramas de Venn como herramientas para guiarnos en nuestros razonamientos son útiles pero tienen limitaciones. Por ejemplo, cuando se está trabajando con más de tres conjuntos los diagramas se vuelven muy engorrosos[1].

Demostración de (3.6): Mostraremos que el conjunto $A \cup (B \cap C)$ tiene los mismos elementos que el conjunto $(A \cup B) \cap (A \cup C)$, y por lo tanto, por la definición de igualdad de conjuntos, concluiremos que $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$. Comencemos mostrando que

$$A \cup (B \cap C) \subseteq (A \cup B) \cap (A \cup C).$$

En símbolos, queremos mostrar

$$\forall x \, [x \in A \cup (B \cap C) \, \rightarrow \, x \in (A \cup B) \cap (A \cup C)].$$

Para verlo, tomemos un elemento x, arbitrario pero fijo, perteneciente a $A \cup (B \cap C)$ y mostremos que x también pertenece a $(A \cup B) \cap (A \cup C)$. Por definición de unión de conjuntos tenemos que hay sólo dos casos posibles: $x \in A$ o $x \in B \cap C$. Mostraremos que $x \in (A \cup B) \cap (A \cup C)$ en ambos casos.

Caso a: Supongamos que $x \in A$. Entonces $x \in A \cup B$ y también $x \in A \cup C$. Luego $x \in (A \cup B) \cap (A \cup C)$.

Caso b: Supongamos que $x \in B \cap C$. Entonces $x \in B$ y por lo tanto $x \in A \cup B$. Pero también tenemos que $x \in C$, luego $x \in A \cup C$. En consecuencia $x \in (A \cup B) \cap (A \cup C)$.

Hemos mostrado de que dado cualquier $x \in A \cup (B \cap C)$, independientemente de si $x \in A$ o si $x \in B \cap C$, se tiene que $x \in (A \cup B) \cap (A \cup C)$. Esto demuestra que $A \cup (B \cap C) \subseteq (A \cup B) \cap (A \cup C)$.

Ya hemos probado la mitad de lo que queríamos. Nos falta mostrar que

$$(A \cup B) \cap (A \cup C) \subseteq A \cup (B \cap C).$$

En símbolos, queremos mostrar

$$\forall x \, [x \in (A \cup B) \cap (A \cup C) \, \rightarrow \, x \in A \cup (B \cap C)].$$

Es decir queremos mostrar que si $x \in (A \cup B) \cap (A \cup C)$, entonces $x \in A \cup (B \cap C)$. Para esto, sea $x \in (A \cup B) \cap (A \cup C)$ un elemento arbitrario. Por definición de intersección de conjuntos tenemos que $x \in A \cup B$ y también que $x \in A \cup C$. Consideraremos dos casos: $x \in A$ o $x \notin A$. Mostraremos que $x \in A \cup (B \cap C)$ en ambos casos. En efecto:

[1] En el libro *Máquinas lógicas y Diagramas* de Martin Gardner [4] se estudian otros tipos de diagramas. Por ejemplo, cuando se trabaja con cuatro conjuntos, Venn propuso usar elipses en lugar de círculos.

Caso a: Supongamos que $x \in A$. Entonces $x \in A \cup (B \cap C)$.

Caso b: Supongamos que $x \notin A$. Entonces como $x \in A \cup B$, necesariamente se tiene que $x \in B$. De igual manera, ya que $x \in A \cup C$, entonces $x \in C$. Con esto hemos mostrado que $x \in B \cap C$ y por lo tanto $x \in A \cup (B \cap C)$.

Hemos mostrado de que dado cualquier $x \in (A \cup B) \cap (A \cup C)$, independientemente de si $x \in A$ o si $x \notin A$, se tiene que $x \in A \cup (B \cap C)$. Esto demuestra que $(A \cup B) \cap (A \cup C) \subseteq A \cup (B \cap C)$.

□

Observación 3.7. Notemos que la demostración tiene dos partes. La primera consistió en mostrar que

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

y en la segunda parte mostramos que

$$(A \cup B) \cap (A \cup C) \subseteq A \cup (B \cap C).$$

El lector debe prestar mucha atención al esquema de esta demostración, pues lo repetiremos cada vez que queramos demostrar la igualdad de dos conjuntos: Para demostrar que dos conjuntos H y F son iguales se demuestran dos cosas: (i) $H \subseteq F$ y (ii) $F \subseteq H$.

Observación 3.8. ***(Prueba por casos)*** La demostración anterior tiene otra peculiaridad que deseamos resaltar. El argumento usado se separó en casos. Lo que ocurrió fué lo siguiente. En la primera parte de la demostración, una vez fijado un elemento arbitrario x, se separó el argumento en dos casos: $x \in A$ o $x \in B \cap C$. Considere entonces las siguientes proposiciones:

P	$x \in A \cup (B \cap C)$
Q	$x \in A$
R	$x \in B \cap C$
S	$x \in (A \cup B) \cap (A \cup C)$

Lo que queremos demostrar es la siguiente proposición:

$$P \to S$$

El caso a) consistió en demostrar que $Q \to S$ y el caso b) mostró que $R \to S$. Por otra parte, por definición de unión se tiene que $P \to Q \vee R$. Ahora bien, ¿Cuáles reglas de la lógica permiten concluir que S es válida?. Veamos, la regla *"prueba por casos"* (ver la sección 2.2.1) precisamente dice que

$$(q \to s) \wedge (r \to s) \Leftrightarrow (q \vee r) \to s.$$

Por consiguiente, concluimos que $Q \vee R \to S$. Ahora, la *ley del silogismo hipotético* nos dice que

$$((p \to q) \ \wedge \ (q \to r)) \Rightarrow (p \to r).$$

En consecuencia, concluimos que $P \to S$. Y esto es lo que queríamos demostrar.

La introducción de los casos es un recurso que con frecuencia facilita las demostraciones. En situaciones como esta, se dice que se ha hecho una *prueba por casos*. Este tipo de demostraciones son bastante comunes en matemáticas, más adelante tendremos muchas oportunidades de ver otros ejemplos donde ocurren. □

Ejemplo 3.9. Sean A y B conjuntos. Afirmamos que:

$$\text{Si } \mathcal{P}(A) = \mathcal{P}(B), \text{ entonces } A = B. \tag{3.7}$$

En efecto, mostraremos la contrapositiva. Es decir:

$$\text{Si } A \neq B, \text{ entonces } \mathcal{P}(A) \neq \mathcal{P}(B). \tag{3.8}$$

Supongamos que $A \neq B$. Entonces $A \not\subseteq B$ ó $B \not\subseteq A$. Consideraremos estos dos alternativas por separado.

Caso 1: Supongamos que $A \not\subseteq B$. Entonces por definición del conjunto potencia, tenemos que $A \notin \mathcal{P}(B)$. Pero claramente $A \in \mathcal{P}(A)$. Por lo tanto $\mathcal{P}(A) \neq \mathcal{P}(B)$.

Caso 2: Supongamos que $B \not\subseteq A$. Entonces, al igual que en el caso 1, se concluye que $B \notin \mathcal{P}(A)$. Pero $B \in \mathcal{P}(B)$. Por lo tanto $\mathcal{P}(A) \neq \mathcal{P}(B)$.

Como en ambos casos se mostró que $\mathcal{P}(A) \neq \mathcal{P}(B)$, entonces podemos concluir que la afirmación (3.8) es verdadera y por lo tanto la afirmación original (3.7) también lo es.

Es importante verificar que los casos considerados cubran todas las posibilidades. Por ejemplo, dados dos conjuntos A y B hay tres alternativas posibles: (i) $A \not\subseteq B$ (ii) $B \not\subseteq A$ y (iii) $A = B$. En el ejemplo de arriba, la tercera alternativa no se considera pues la hipótesis precisamente dice que $A \neq B$. Por esto sólo quedan las alternativas (i) y (ii), las cuales son los casos que hay que analizar. □

El próximo ejemplo ilustramos otra manera de escribir las demostraciones en la que queda mas claro cual es la justificación de cada paso de la demostración.

Ejemplo 3.10. Ahora veremos una generalización de las leyes distributivas. Mostraremos que para cada tres conjuntos A, B y C cualesquiera se cumple que

$$(A \cup B) \cap (C \cup D) = (A \cap C) \cup (A \cap D) \cup (B \cap C) \cup (B \cap D). \tag{3.9}$$

La manera de demostrar esta afirmación es diferente a las anteriores. Ahora haremos usos de las leyes del álgebra de conjuntos que hemos visto anteriormente.

$$\begin{array}{lcll}(A\cup B)\cap(C\cup D) & = & [(A\cup B)\cap C]\cup[(A\cup B)\cap D] & \text{Distributiva 3b}\\ & = & [(A\cap C)\cup(B\cap C)]\cup[(A\cap D)\cup(B\cap D)] & \text{Distributiva 3b}\\ & = & (A\cap C)\cup(B\cap C)\cup(A\cap D)\cup(B\cap D) & \text{Asociativa}\end{array}$$

□

El lector puede preguntarse porqué la demostración hecha en el ejemplo anterior es distinta a la hecha en el ejemplo 3.6. En realidad se puedo hacer de otra manera. Le sugerimos que de otra demostración de (3.9) mostrando las siguientes dos afirmaciones

$$(A\cup B)\cap(C\cup D)\ \subseteq\ (A\cap C)\cup(A\cap D)\cup(B\cap C)\cup(B\cap D)$$

y

$$(A\cap C)\cup(A\cap D)\cup(B\cap C)\cup(B\cap D)\ \subseteq\ (A\cup B)\cap(C\cup D).$$

3.1.4. Complementación

Ahora enunciaremos las propiedades básicas de la complementación. Las letras A y B denotarán subconjuntos de un conjunto universal U.

5a	$(A\cup B)^c = A^c\cap B^c$	**Leyes de De Morgan**
5b	$(A\cap B)^c = A^c\cup B^c$	
6a	$A\cup U = U$	**Leyes de la Identidad**
6b	$A\cap U = A$	
7a	$(A^c)^c = A$	
7b	$A\cap A^c = \emptyset$	
7c	$A\cup A^c = U$	
7d	$U^c = \emptyset$	
7e	$\emptyset^c = U$	

Observemos que decir que

$$x\in A^c$$

es equivalente a decir que

$$x\in U \text{ y } x\notin A.$$

Sin embargo el conjunto universal U estará usualmente implícito y por consiguiente escribiremos simplemente

$$x\notin A.$$

Demostraremos algunas de estas leyes y las otras las dejaremos a cargo del lector.

5a Fijemos un elemento $x \in U$ arbitrario. Tenemos entonces

$$\begin{array}{rcll} x \in (A \cup B)^c & \Leftrightarrow & x \notin A \cup B & \text{Definición de complemento} \\ & \Leftrightarrow & \neg(x \in A \cup B) & \\ & \Leftrightarrow & \neg(x \in A \vee x \in B) & \text{Definición de unión} \\ & \Leftrightarrow & x \notin A \wedge x \notin B & \text{Ley de De Morgan para la lógica} \\ & \Leftrightarrow & x \in A^c \wedge x \in B^c & \text{Definición de complemento} \\ & \Leftrightarrow & x \in A^c \cap B^c & \text{Definición de intersección} \end{array}$$

Esto demuestra que

$$\forall x\,[x \in (A \cup B)^c \Leftrightarrow x \in A^c \cap B^c\,]$$

En consecuencia, por la definición de la igualdad de conjuntos, $(A \cup B)^c = A^c \cap B^c$.

7a Mostremos que $A \subseteq (A^c)^c$ y que $(A^c)^c \subseteq A$. En efecto, sea $x \in A$, entonces $x \notin A^c$, es decir $x \in (A^c)^c$. Ahora veamos que $(A^c)^c \subseteq A$. Tomemos $x \in (A^c)^c$, es decir $x \notin A^c$ y por lo tanto $x \in A$.

7b Veamos que $A \cap A^c = \emptyset$. Por definición de A^c vemos que ningún elemento de A puede pertenecer a A^c, así que $A \cap A^c$ no tiene elementos, y por lo tanto $A \cap A^c$ es el conjunto vacío. □

Ejemplo 3.11. Mostraremos que

$$A^c \cap (A \cup B) \subseteq B.$$

En efecto,

$$\begin{array}{rcll} A^c \cap (A \cup B) & = & (A^c \cap A) \cup (A^c \cap B) & \text{Distributiva 3b} \\ & = & \emptyset \cup (B \cap A^c) & \text{ley conmutativa 1b y 7b} \\ & = & B \cap A^c & \text{ley de identidad 4c} \end{array}$$

Por último, de la definición de $\cap$ es inmediato que $B \cap A^c \subseteq B$. □

Ejemplo 3.12. Sean A, B y C conjuntos. Queremos determinar si la siguiente afirmación es válida

$$A \subseteq [\,(B \setminus C)^c \setminus A\,]^c \tag{3.10}$$

Para responder esta pregunta, primero simplificaremos la expresión de la derecha y para ello usaremos las reglas del álgebra Booleana.

$$\begin{array}{rcll} [\,(B \setminus C)^c \setminus A\,]^c & = & [\,(B \cap C^c)^c \cap A^c\,]^c & \text{Definición de diferencia} \\ & = & (B \cap C^c) \cup A & \text{Ley de De Morgan 5b y regla 7a} \end{array}$$

De la última igualdad se deduce inmediatamente que la afirmación (3.10) es verdadera. □

3.1.5. Diferencia simétrica

La primera propiedad de $\triangle$ es que para dos conjuntos cualesquiera A y B se cumple que

$$A \triangle B = B \triangle A.$$

Esto se deduce inmediatamente de la definición de $\triangle$. En efecto,

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

La segunda igualdad está justificada por la ley conmutativa 1a para la unión. Esta propiedad de $\triangle$ usualmente se expresa diciendo que $\triangle$ es *conmutativa*.

Veremos ahora que $\triangle$ es una operación asociativa. Es decir, mostraremos que dados tres conjuntos A, B y C cualesquiera se cumple que

$$(A \triangle B) \triangle C = A \triangle (B \triangle C).$$

Como la demostración es un poco larga, la dividiremos en partes. Primero observemos que de la definición de $\triangle$ tenemos que:

$$(A \triangle B) \triangle C = ((A \triangle B) \cap C^c) \ \cup \ (C \cap (A \triangle B)^c) \tag{3.11}$$

Esto sugiere que antes de continuar es conveniente conocer una expresión sencilla para $(A \triangle B)^c$. Afirmamos que

$$(A \triangle B)^c = (A^c \cap B^c) \ \cup \ (B \cap A) \tag{3.12}$$

En efecto,

$$\begin{aligned} (A \triangle B)^c &= [(A \cap B^c) \ \cup \ (B \cap A^c)]^c && \text{Definición de } \triangle \\ &= (A \cap B^c)^c \ \cap \ (B \cap A^c)^c && \text{5a} \\ &= (A^c \cup B) \ \cap \ (B^c \cup A) && \text{5b} \\ &= (A^c \cap B^c) \ \cup \ (A^c \cap A) \cup \\ &\quad (B \cap B^c) \ \cup \ (B \cap A) && \text{Ejemplo 3.10} \\ &= (A^c \cap B^c) \ \cup \ \emptyset \ \cup \ \emptyset \ \cup \ (B \cap A) && \text{7b} \\ &= (A^c \cap B^c) \ \cup \ (B \cap A) && \text{6a} \end{aligned}$$

Ahora afirmamos que

$$(A \triangle B) \triangle C = (A \cap B^c \cap C^c) \ \cup \ (B \cap A^c \cap C^c) \ \cup \ (C \cap A^c \cap B^c) \ \cup \ (C \cap B \cap A) \tag{3.13}$$

En efecto, sustituyendo en (3.11) lo que vimos en (3.12) obtenemos

$$(A\triangle B)\triangle C \;=\; (\,[(A\cap B^c)\cup(B\cap A^c)]\cap C^c\,)\;\cup\;(\,C\cap[(A^c\cap B^c)\;\cup\;(B\cap A)]\,)$$

y usando la ley distributiva 3b obtenemos lo buscado:

$$(A\triangle B)\triangle C \;=\; (A\cap B^c\cap C^c)\;\cup\;(B\cap A^c\cap C^c)\;\cup\;(C\cap A^c\cap B^c)\;\cup\;(C\cap B\cap A).$$

Ya casi llegamos al final. Veamos ahora como calculamos $A\triangle(B\triangle C)$. Para esto observemos que $\triangle$ es una operación conmutativa, por esto

$$A\triangle(B\triangle C) = (B\triangle C)\triangle A$$

Pero (3.13) nos permite también calcular $(B\triangle C)\triangle A$. En efecto, sustituyendo A por B, B por C y C por A en (3.13) obtenemos

$$(B\triangle C)\triangle A = (B\cap C^c\cap A^c)\;\cup\;(C\cap B^c\cap A^c)\;\cup\;(A\cap B^c\cap C^c)\;\cup\;(A\cap C\cap B) \quad (3.14)$$

Comparando (3.13) y (3.14) podemos concluir (por fin!) que $(A\triangle B)\triangle C = A\triangle(B\triangle C)$.

Ejercicios 3.1

1. Escriba las demostraciones de la propiedades 7a y 7b como se hizo en la demostración de la parte (ii) de 5a (hechas en la sección 3.1.4).

2. Muestre la ley distributiva:

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

   Sugerencia: Demuestre las siguientes dos afirmaciones: $A\cap(B\cup C)\subseteq(A\cap B)\cup(A\cap C)$ y $(A\cap B)\cup(A\cap C)\subseteq A\cap(B\cup C)$.

3. Muestre la ley de De Morgan 5b: $(A\cap B)^c = A^c\cup B^c$.

4. Muestre las siguientes afirmaciones donde U es el conjunto universal y $A, B\subseteq U$

   a) $A\cup A^c = U$

   b) $U^c = \emptyset$ y $\emptyset^c = U$

5. Muestre que $A\subseteq A\cup B$ y $A\cap B\subseteq A\cup B$ para cualquier par de conjuntos A y B.

6. Muestre la siguiente generalización de la ley de De Morgan

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

   (*Sugerencia:* Use las leyes de De Morgan 5a con los conjuntos A y $B\cup C$).

7. Demuestre lo siguiente

a) $A \cup B = B$ si, y sólo si, $A \subseteq B$.

b) $A \subseteq C$ y $B \subseteq C$ si, y sólo si, $A \cup B \subseteq C$.

c) Si $A \subseteq B$, $B \subseteq C$ y $C \subseteq A$, entonces $A = B$ y $B = C$.

8. Demuestre la siguiente generalización de la ley distributiva 3a

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

9. Revise el ejemplo 3.9 y de una demostración directa de la siguiente afirmación:

$$\text{Si } \mathcal{P}(A) = \mathcal{P}(B), \text{ entonces } A = B.$$

10. Sean A y B subconjuntos de un conjunto universal U.

a) Considere la siguiente afirmación:

$$\text{Si } A \subseteq B^c, \text{ entonces } A \cap B = \emptyset.$$

Demuéstrela directamente, es decir, suponga que $A \subseteq B^c$ y demuestre que se cumple lo siguiente

$$\forall x \in U\, [x \notin A \cap B].$$

b) Demuestre directamente la contrarecíproca de la afirmación anterior, es decir,

$$\text{Si } A \cap B \neq \emptyset, \text{ entonces } A \not\subseteq B^c.$$

11. Sean A y B dos conjuntos. Muestre que

a) $A \triangle B = (A \cup B) \setminus A \cap B$.

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

12. Demuestre lo siguiente

a) $A \triangle (A \triangle B) = B$ (*Sugerencia:* Use la ley asociativa para $\triangle$).

b) Si $A \triangle B = A \triangle C$, entonces $B = C$ (*Sugerencia:* Use la parte (a)).

13. *a*) Halle un conjunto C tal que $\{1, 2, 3, 6, 8\} \triangle C = \{2, 3, 8, 9, 10\}$. (*Sugerencia:* Si no consigue la respuesta, siga a la parte (b)).

b) En este problema resolveremos de manera general una pregunta similar a la hecha en (a). Sean $A, B \subseteq \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$ dos subconjuntos cualesquiera. Muestre que existe un subconjunto C de $\{1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$ tal que $A \triangle C = B$. (*Sugerencia:* Use el ejercicio 12 y razone como si estuviera despejando una ecuación, es decir, piense que C es la incógnita).

14. En este ejercicio no olvide que los elementos de $\mathcal{P}(A)$ también son conjuntos. Demuestre lo siguiente

a) $A \subseteq B$ si, y sólo si $\mathcal{P}(A) \subseteq \mathcal{P}(B)$.

b) $\mathcal{P}(A \cap B) = \mathcal{P}(A) \cap \mathcal{P}(B)$.

c) $\mathcal{P}(A) \cup \mathcal{P}(B) \subseteq \mathcal{P}(A \cup B)$.

3.2. Contraejemplos

Hasta ahora nos hemos concentrado en ilustrar algunos de los métodos usados para demostrar la validez de una afirmación. Ahora veremos cómo podemos mostrar que una afirmación general **no** es válida. Es importante saber mostrar que algo no es válido, pues esto nos puede llevar a intuir o sospechar que es lo que sí es válido.

Ejemplo 3.13. Supongamos que alguien afirma que $A \subseteq A \cap B$ para cualquier par de conjuntos A y B. ¿Es esta afirmación correcta? Veamos dos ejemplos concretos:

(1) $A = \{1, 2\}$ y $B = \{1, 2, 3\}$. En este caso tenemos que $\{1, 2\} \subseteq \{1, 2\} \cap \{1, 2, 3\}$.

(2) $A = \{1, 2\}$ y $B = \{2, 3\}$. Entonces $\{1, 2\} \cap \{2, 3\} = \{2\}$ pero $\{1, 2\} \not\subseteq \{2\}$.

Vemos entonces que la afirmación no es válida en general, pues se cumple para algunos conjuntos pero para otros no. □

Los ejemplos donde falla una proposición (como la anterior) son llamados **contraejemplos**. En el caso que analizamos los conjuntos $\{1, 2\}$ y $\{2, 3\}$ (para A y B respectivamente) son un contraejemplo a la afirmación inicial.

Ejemplo 3.14. También podemos conseguir *contraejemplos* para afirmaciones condicionales. ¿Será cierto que para cualquier par de conjuntos A y B se cumple que

$$\text{Si } A \neq \emptyset \text{ y } B \neq \emptyset, \text{ entonces } A \cap B \neq \emptyset \text{ ?} \tag{3.15}$$

Veamos algunos ejemplos que aclaren la pregunta.

(a) Si $A = \{1, 2, 3\}$ y $B = \mathbb{N}$ tenemos que A y B no son vacíos y además que $A \cap B = \{1, 2, 3\}$ no es vacío. Pero esto no es suficiente para garantizar que la afirmación se cumple en general, pues sólo la verificamos en un caso particular.

(b) Veamos otro caso, dejemos A igual, es decir $A = \{1, 2, 3\}$ pero hagamos B más pequeño, digamos $\{n \in \mathbb{N} : n \geq 4\}$. En este caso tenemos que $\{1, 2, 3\} \cap \{n \in \mathbb{N} : n \geq 4\} = \emptyset$ y además ninguno de ellos es vacío. Así, $A = \{1, 2, 3\}$ y $B = \{n \in \mathbb{N} : n \geq 4\}$ son un contraejemplo a la afirmación.

Por lo tanto la afirmación (3.15) es falsa. □

Ejemplo 3.15. Dados tres conjuntos cualesquiera A, B y C, ¿Será cierto que

$$\text{Si } A \subseteq B \cup C, \text{ entonces } A \subseteq B \text{ ó } A \subseteq C \text{ ?.} \tag{3.16}$$

Pongamos $A = \{1, 3, 5\}$, $B = \{0, 1, 2, 3\}$ y $C = \{4, 5, 6\}$. Vemos entonces que

$$\{1, 3, 5\} \subseteq \{0, 1, 2, 3\} \cup \{4, 5, 6\}.$$

Pero $\{1, 3, 5\} \not\subseteq \{0, 1, 2, 3\}$ y $\{1, 3, 5\} \not\subseteq \{4, 5, 6\}$. Por lo tanto la afirmación (3.16) es falsa. □

En general podemos decir lo siguiente sobre cómo refutar una afirmación:

1. Para refutar la fórmula

$$p \wedge q$$

debemos hallar un ejemplo donde valga $\neg(p \wedge q)$. Como $\neg(p \wedge q) \Leftrightarrow \neg p \vee \neg q$, entonces debemos conseguir un ejemplo donde valga $\neg p \vee \neg q$. Es decir, un ejemplo donde valga $\neg p$ o $\neg q$.

2. Para refutar una proposición de la forma

$$p \vee q$$

debemos hallar un ejemplo donde valga $\neg(p \vee q)$. Como $\neg(p \vee q) \Leftrightarrow \neg p \wedge \neg q$, entonces debemos conseguir un ejemplo donde valga $\neg p \wedge \neg q$. Es decir, un ejemplo donde valga $\neg p$ y también $\neg q$.

3. En general, para refutar una fórmula condicional

$$p \rightarrow q$$

debemos hallar un ejemplo donde valga $\neg(p \rightarrow q)$. Como $\neg(p \rightarrow q) \Leftrightarrow p \wedge \neg q$, entonces debemos conseguir un ejemplo donde valga $p \wedge \neg q$.

Ejercicios 3.2

1. Diga cuáles de las siguientes afirmaciones son verdaderas y cuáles son falsas. Para las verdaderas dé una demostración y para las falsas proporcione un ejemplo en el que la afirmación no se cumpla.

   a) Si $A \neq \emptyset$ o $B \neq \emptyset$, entonces $A \cup B \neq \emptyset$.

   b) Si $A \neq \emptyset$ o $B \neq \emptyset$, entonces $A \cap B \neq \emptyset$.

   c) Si $A \cap B \subseteq C$, entonces $A \subseteq C$ o $B \subseteq C$.

   d) Si $A \cup B = A \cap B$, entonces $A = B$.

   e) Si $A \subseteq B$ o $A \subseteq C$, entonces $A \subseteq B \cup C$.

   f) $\mathcal{P}(A) \cup \mathcal{P}(B) = \mathcal{P}(A \cup B)$.

2. En los siguientes ejercicios haremos una afirmación y propondremos un "demostración". Diga si la demostración es correcta. En caso que no lo sea, si es posible de una demostración correcta o sino de un contraejemplo que muestre que la afirmación es falsa.

a) **Afirmación:** Si A y B son conjuntos tales que $\mathcal{P}(A) \subseteq \mathcal{P}(B)$, entonces $A \subseteq B$.
"Demostración":

$$\begin{aligned} x \in A &\Rightarrow \{x\} \subseteq A \\ &\Rightarrow \{x\} \in \mathcal{P}(A) \\ &\Rightarrow \{x\} \in \mathcal{P}(B) \\ &\Rightarrow \{x\} \subseteq B \\ &\Rightarrow x \in B \end{aligned}$$

Esto muestra que si $x \in A$, entonces $x \in B$. Por lo tanto $A \subseteq B$.

b) **Afirmación:** Sean A, B y C conjuntos. Si $A \subseteq B$, $B \subseteq C$, entonces $A \subseteq C$.
"Demostración": Si $x \in C$, entonces como $B \subseteq C$, tenemos que $x \in B$. Ya que $A \subseteq B$ y $x \in B$, entonces $x \in A$. Esto muestra que si $x \in C$, entonces $x \in A$. Por lo tanto $A \subseteq C$.

c) **Afirmación:** Si A, B y C conjuntos tales que $A \subseteq B$, $B \subseteq C$, entonces $A \subseteq C$.
"Demostración": Considere los siguientes conjuntos: $A = \{1, 5, 8\}$, $B = \{1, 4, 5, 8, 10\}$ y $C = \{1, 2, 4, 5, 6, 8, 10\}$. Entonces $A \subseteq B$, $B \subseteq C$ y $A \subseteq C$.

d) **Afirmación:** Si $X = \{x \in \mathbb{N} : x^2 < 14\}$ y $Y = \{0, 1, 2, 3\}$, entonces $X = Y$.
"Demostración": Como $0^2 = 0$ y $0 < 14$, $1^2 = 1$ y $1 < 14$; $2^2 = 4$ y $4 < 14$; y $3^2 = 9$ y $9 < 14$. Entonces $X = Y$.

e) **Afirmación:** $A \cap \emptyset = A$.
"Demostración": Sabemos que $x \in A \cap \emptyset$ si, y sólo si, $x \in A$ y $x \in \emptyset$. Como $x \in \emptyset$ es falso, entonces $x \in A$ y $x \in \emptyset$ si, y sólo si, $x \in A \cap \emptyset$. Esto muestra que $A \cap \emptyset = A$.

f) **Afirmación:** $\mathcal{P}(A \setminus B) \setminus \{\emptyset\} \subseteq \mathcal{P}(A) \setminus \mathcal{P}(B)$.
"Demostración": Sea $x \in \mathcal{P}(A \setminus B) \setminus \{\emptyset\}$. Entonces $x \in \mathcal{P}(A) \setminus \mathcal{P}(B)$. Por lo tanto $\mathcal{P}(A \setminus B) \subseteq \mathcal{P}(A) \setminus \mathcal{P}(B)$. □

g) **Afirmación:** Si $A \cap B = A \cap C$, entonces $B \subseteq C$.
"Demostración": Sea $x \in B$. Consideraremos dos casos: $x \in A$ o $x \in C$.
Caso 1: Supongamos que $x \in A$. Entonces $x \in A \cap B$. Como por hipótesis $A \cap B = A \cap C$, concluimos que $x \in A \cap C$. Por lo tanto $x \in C$.
Caso 2: Supongamos que $x \in C$. En este caso no hay nada que probar. □

3.3. Lógica y álgebra Booleana (continuación)

Ya dijimos que las operaciones del álgebra de conjuntos y de la lógica proposicional son similares. Y que las leyes del álgebra Booleana se pueden traducir a leyes de la lógica proposicional sustituyendo $\cap$ por $\wedge$, $\cup$ por $\vee$ y ^{c} por $\neg$. Y viceversa, cada una de las leyes del cálculo proposicional se puede traducir al álgebra Booleana (el condicional $p \rightarrow q$ se traduce usando uno de sus equivalentes lógicos: $\neg p \ \vee \ q$). Veamos un ejemplo, una de las leyes de De Morgan dice

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

La correspondiente ley del cálculo proposicional también se llama ley de De Morgan y dice

$$\neg(p \wedge q) \Leftrightarrow \neg p \ \vee \ \neg q.$$

Es decir, la igualdad entre conjuntos $=$ se traduce en equivalencia lógica $\Leftrightarrow$ y viceversa.

Ejemplo 3.16. Por ejemplo, considere la siguiente equivalencia lógica

$$[p \vee (q \wedge r)] \Leftrightarrow [(p \vee q) \wedge (p \vee r)].$$

Al traducirla al lenguaje del álgebra de Boole, obtenemos lo siguiente

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

Es decir, una ley distributiva de la lógica se traduce en una ley distributiva del álgebra de Boole. □

La implicación lógica $\Rightarrow$ se puede interpretar como la relación de subconjunto. Por ejemplo, la regla *modus ponens* dice

$$[p \wedge (p \to q)] \Rightarrow q.$$

Veamos que dice esta regla al traducirla al álgebra de conjuntos. Recordemos que para traducir $p \to q$ usamos su equivalente $\neg p \vee q$. La traducción del *modus ponens* es:

$$[A \cap (A^c \cup B)] \subseteq B.$$

Veamos que esta última afirmación es válida. En efecto,

$$\begin{array}{rcl} A \cap (A^c \cup B) & = & (A \cap A^c) \cup (A \cap B) \\ & = & \emptyset \cup (A \cap B) \\ & = & A \cap B \\ & \subseteq & B. \end{array}$$

En la primera igualdad hemos usado una de las leyes distributivas, en la segunda el hecho que $A \cap A^c = \emptyset$ y la última afirmación se deduce de la definición de $\subseteq$.

Ejercicios 3.3

1. Traduzca las siguientes leyes sobre la implicación lógica en leyes del álgebra Booleana:

   a) $p \Rightarrow (p \vee q)$.
   b) $(p \wedge q) \Rightarrow p$.
   c) $(p \to q) \wedge \neg q \Rightarrow \neg p$.
   d) $[(p \to q) \wedge (q \to r) \Rightarrow (p \to r)$.

2. Traduzca las siguientes leyes sobre la equivalencia lógica en leyes del álgebra Booleana.

   a) $[p \wedge (q \vee r)] \Leftrightarrow [(p \wedge q) \vee (p \wedge r)]$.
   b) $[(p \vee q) \to r] \Leftrightarrow [(p \to r) \wedge (q \to r)]$.
   c) $[(p \wedge q) \to r] \Leftrightarrow [(p \to r) \vee (q \to r)]$.

3.4. Demostraciones

Como dijéramos al comienzo de este capítulo, no pretendemos dar una definición rigurosa de lo que se entiende por una demostración en matemáticas. Pero con la experiencia acumulada hasta ahora podemos intentar aproximarnos a una definición. Primero recordaremos brevemente algunos de los tipos de demostración vistos hasta ahora.

3.4.1. Afirmaciones condicionales

Para demostrar una afirmación condicional $R \to Q$ ya hemos dicho que lo usual es *suponer* que R se cumple y mostrar que Q también se cumple. El método descrito se llama una **demostración directa** de $P \to Q$. Un ejemplo típico de este tipo de demostración ocurre cuando queremos mostrar que un conjunto está contenido en otro. En lo visto hasta ahora tenemos varios ejemplos de este tipo de demostraciones, es un buen ejercicio para el lector revisar de nuevo los resultados vistos y determinar cuáles demostraciones son de este tipo.

Ahora bien, también se puede demostrar una proposición condicional $R \to Q$ demostrando su contrarecíproca $\neg Q \to \neg R$. Pues como vimos ellas son lógicamente equivalentes. Por supuesto para demostrar $\neg Q \to \neg R$ uno hace como con cualquier proposición condicional: supone que $\neg Q$ se cumple y muestra que $\neg R$ también se cumple.

¿Cómo podemos saber cuando es más fácil mostrar la contrarrecíproca de una afirmación condicional que la afirmación misma? Esta pregunta podríamos incluirla en la lista de *las preguntas de las sesenta y cuatro mil lochas*[2]. No podemos ofrecerle al lector una receta que le permita decidir cuando es conveniente demostrar la contrarrecíproca de una proposición condicional. Sin embargo, sí podemos aconsejarle que cada vez que quiera demostrar una proposición condicional y no vea cómo hacerlo, entonces enuncie la contrarrecíproca de la proposición que quiere demostrar e intente probarla. En muchos casos la prueba de la contrarrecíproca es clara y transparente.

3.4.2. Afirmaciones universales

Las afirmaciones universales son las que tienen la forma siguiente

$$\forall x \; P(x)$$

donde $P(x)$ significa que el elemento x tiene la propiedad P. Esto ya lo hemos visto al demostrar algunas de las propiedades de los conjuntos. Recordemos que normalmente la demostración de una afirmación universal comienza con frase *"Sea x un elemento arbitrario. Mostraremos que x tiene la propiedad P..."*

3.4.3. Demostraciones por reducción al absurdo

Otro tipo de demostraciones, que hasta ahora no hemos usado, es el llamado método de **reducción al absurdo**. Lo ilustraremos con un ejemplo.

[2]Una locha es una moneda fuera de circulación que valía $\frac{1}{8}$ de un Bolívar.

Es fácil conseguir tres enteros consecutivos a, b, c que cumplan con la ecuación $a^2+b^2 = c^2$. Por ejemplo, $3^2+4^2 = 5^2$. Sin embargo, mostraremos que NO existen tres enteros consecutivos a, b, c que satisfagan la ecuación $a^3 + b^3 = c^3$.

Razonaremos indirectamente. Supondremos que existen enteros consecutivos a, b, c tales que $a^3 + b^3 = c^3$ y mostraremos que esto conduce a una contradicción.

Como los enteros a, b y c son consecutivos, entonces son de la forma $x - 1$, x y $x + 1$. Es decir, $a = x - 1$, $b = x$ y $c = x + 1$ para algún entero x. Nuestra suposición es que

$$(x - 1)^3 + x^3 = (x + 1)^3.$$

Efectuando las operaciones obtenemos

$$x^3 - 3x^2 + 3x - 1 + x^3 = x^3 + 3x^2 + 3x + 1.$$

Agrupando tenemos

$$2x^3 - 3x^2 + 3x - 1 = x^3 + 3x^2 + 3x + 1.$$

Agrupando las potencias de x de un lado de la igualdad, obtenemos

$$x^3 - 6x^2 = 2.$$

Factorizando obtenemos

$$x^2(x - 6) = 2. \tag{3.17}$$

Como x^2 es positivo, entonces $x - 6$ también lo es y por lo tanto $x - 6$ es mayor o igual que 1. Luego x es mayor o igual que 7 y así x^2 es mayor o igual que 49. Luego $x^2(x-6)$ es mayor o igual que 49, lo cual contradice la igualdad (3.17).

El haber deducido una contradicción (a partir de la suposición de que si existían tres enteros a, b y c consecutivos tales que $a^3 + b^3 = c^3$) nos garantiza que la suposición inicial no puede ser verdadera. En consecuencia tales enteros no existen y con esto hemos demostrado la afirmación[3].

Más adelante tendremos oportunidad de ver otros ejemplos donde se usa el método de reducción al absurdo.

3.4.4. Lógica de las igualdades

Ahora bien, no todas las demostraciones que hemos hecho han sido exactamente de alguno de los tipos descritos anteriormente. Le pedimos al lector que vea de nuevo la demostración de la asociatividad de $\triangle$ dada en la sección 3.1.5. Nos referimos a la demostración de lo siguiente:

$$(A \triangle B) \triangle C = A \triangle (B \triangle C).$$

[3]Es natural preguntarse si es imprescindible razonar indirectamente. El lector interesado puede tratar de hacerlo directamente. Muestre que si $x^3 + (x + 1)^3 = (x + 2)^3$, entonces lo mismo ocurre si en lugar de x colocamos $x - 1$. Ahora, reflexione si este hecho es suficiente para justificar la afirmación.

El lector observará que la demostración consistió en ir transformando la expresión $(A \triangle B) \triangle C$ (el lado izquierdo de la igualdad) hasta que se "convirtió" en $A \triangle (B \triangle C)$ (el lado derecho de la igualdad). En en el transcurso de esa demostración se usaron algunas de las leyes del álgebra de conjuntos (5a, 5b, 7b y 6a) y también un resultado que se había demostrado previamente (ejemplo 3.10). Las leyes del álgebra de conjuntos estipulan la igualdad de algunos conjuntos. Algunas demostraciones, como la mencionada arriba, consisten en usar esas igualdades para ir paso a paso transformando una expresión en otra. En cada paso la regla básica es que uno puede sustituir una expresión por cualquier otra que sea igual a ella (*"'sustituir iguales por iguales"*). Este tipo de argumentos es muy frecuente en el contexto del álgebra.

3.4.5. Resumen

Podemos decir que una demostración de una afirmación P consiste de una sucesión de afirmaciones P_1, P_2, $\cdots$, P_n tales que cada afirmación P_i se deduce de las anteriores usando algún razonamiento lógico y además la última de ellas, P_n, debe ser la afirmación P que se quería demostrar. Las proposiciones P_i pueden ser resultados ya demostrados anteriormente o proposiciones que se deducen de las definiciones básicas de la teoría de conjuntos (es decir, de la relación $\in$, conjunto potencia, $\subseteq$, etc.). Ahora bien, cuando decimos que se "deducen" de las anteriores queremos decir que

$$P_1 \wedge\ P_2\ \wedge \cdots \wedge P_i\ \Rightarrow\ P_{i+1}$$

Es decir, la proposición P_{i+1} es una consecuencia lógica de las proposiciones ya demostradas.

Insistimos en que esto no es una definición precisa de la noción de demostración. En el curso de la lectura de estas notas el lector estudiará muchas demostraciones de resultados muy variados las cuales le ayudarán a formarse una idea más precisa de lo que se entiende por demostración, y algo aún más importante, irá aprendiendo a cómo hacerlas y cómo escribirlas para que otros las entiendan.

Es común en los textos de Matemáticas indicar el comienzo y el final de las demostraciones de la siguiente manera: *Demostración....*$\square$. De ahora en adelante lo haremos así. Otra costumbre es llamar **Teorema** a las proposiciones que se demuestran.

3.5. Ejercicios suplementarios del capítulo 3

1. Use las leyes del algebra Booleana para simplificar las siguientes expresiones

   a) $[A^c \setminus (B^c \cup C^c)]^c$

   b) $[(B \cup C)^c \setminus A]^c$

   c) $[\,[A \cup (B \cup C)^c]^c \cap [A \cap (B \cap C)^c]^c\,]^c$

2. Muestre la siguiente generalizaciones de la ley de De Morgan: sean A, B, C y D conjuntos arbitrarios, entonces

   a) $(A \cap B \cap C)^c = A^c \cup B^c \cup C^c$.

   b) $(A \cup B \cup C \cup D)^c = A^c \cap B^c \cap C^c \cap D^c$.

3. Sean A, B y C tres conjuntos arbitrarios. Muestre lo siguiente

   a) $(A \setminus B) \setminus C \subseteq A \setminus (B \setminus C)$

   b) $A \setminus (A \setminus B) \subseteq B$

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

   d) $A \setminus (B \cup C) = (A \setminus B) \cap (A \setminus C)$.

4. Demuestre la siguiente generalización de la ley distributiva 3a: Sean A, B, C y D cuatro conjuntos arbitrarios.

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

5. En los ejercicios que siguen U denotará el conjunto universal, A, B, C y D denotarán subconjuntos de U. Demuestre las afirmaciones que se indican. En las partes donde se hace una pregunta dé una demostración en caso que sea verdadera y en el caso que sea falsa dé un contraejemplo.

   a) $A \cap B = \emptyset$ si, y sólo si, $A \subseteq B^c$

   b) $A \cup B = U$ si, y sólo si, $B^c \subseteq A$

   c) Si $A \cup B \neq \emptyset$, entonces $A \neq \emptyset$ o $B \neq \emptyset$

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

   e) $(A \cup B) \setminus C = (A \setminus C) \cup (B \setminus C)$

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

   g) Si $A \subseteq C$ o $B \subseteq C$, entonces $A \cap B \subseteq C$

   h) $A \subseteq B$ y $A \subseteq C$ si, y sólo si, $A \subseteq B \cap C$

   i) $A \cap (B \triangle C) = (A \cap B) \triangle (A \cap C)$

   j) ¿Es cierto que $A \cap B = A^c \cup B^c$?

k) ¿Es cierto que $(A \cap \emptyset) \cup B = B$ para todo A, B?

l) ¿Es cierto que $A \setminus B = B \setminus A$?

m) ¿Será cierto que si $A \cap B = A \cap C$, entonces $B = C$?

n) ¿Si $A \cup B = A \cup C$, entonces $B = C$?

$\tilde{n}$) ¿Será cierto que si $A \cap B = A \cap C$ y $A \cup B = A \cup C$, entonces $B = C$?

o) ¿Será cierto que $A^c \triangle B^c = A \triangle B$?.

Capítulo 4

El Principio de Inducción Matemática

En este capítulo estudiaremos el **Principio de Inducción Matemática**. En él se basa una herramienta fundamental en matemáticas: las demostraciones por indución. El principio de inducción permite establecer leyes universales acerca de los números naturales. Por ejemplo, considere la siguiente afirmación:

$$n < 2^n \text{ para todo número natural } n. \tag{4.1}$$

Sin mucho esfuerzo se verifica que esta afirmación es válida para $n = 0, 1, 2, 3$ y el lector podría, con un poco de paciencia, verificarla para muchos otros valores de n. Sin embargo, esto no justifica que esa afirmación sea verdadera. La herramienta usada para demostrar afirmaciones como la enunciada en (4.1) y otras similares será estudiada en este capítulo.

4.1. El Principio de buena ordenación

El principio de inducción está estrechamente relacionado con las propiedades del orden de los números naturales. Consideremos los siguientes conjuntos de números naturales:

1. $C_1 = \{1, 2, 3\}$.
2. $C_2 = \{11, 12, 13, 14\}$.
3. $C_3 = \{0, 2, 4, 6, 8, \cdots\}$, es decir, C_3 es el conjunto de todos los números pares.
4. $C_4 = \{21, 22, 23, 24, 25, \cdots\}$, es decir, C_4 es el conjunto de todos los números naturales mayores que 20.

Estos cuatro conjuntos tienen en común que todos ellos tiene un primer elemento. Por ejemplo: 21 es el primer elemento de C_4, 11 es primero de C_3.

Sea C un conjunto de números naturales, diremos que m es el **mínimo** de C, si se verifican las dos condiciones siguientes:

(i) $m \in C$.
(ii) Si $n \in C$, entonces $m \leq n$.

Notemos que todo conjunto tiene a lo sumo un elemento mínimo. Pues si m y m' son dos elementos que verifican las condiciones (i) y (ii), se tendría que $m, m' \in C$ y además, por la condición (ii), se tendría que $m' \leq m$ y $m \leq m'$. Por lo tanto $m = m'$.

La propiedad que observamos en los conjuntos C_1, C_2, C_3 y C_4 es válida para todos los subconjuntos (no vacíos) de $\mathbb{N}$. Esta propiedad es de tanta importancia que se establece como un Principio.

Principio de buena ordenación: *Todo conjunto no vacío de números naturales tiene un elemento mínimo.*

Este principio no se puede deducir de las propiedades algebraicas de los números naturales (aquellas que se refieren a las operaciones de suma y multiplicación) o de las propiedades elementales de los conjuntos (álgebra Booleana).

El concepto de elemento mínimo de un conjunto también está definido para subconjuntos arbitrarios de números, no necesariamente números naturales. Sin embargo, es muy importante observar que si el conjunto en cuestión no es un subconjunto de $\mathbb{N}$, no es cierto en general que el conjunto tenga un elemento mínimo. Esto lo ilustramos en los ejemplos que presentamos a continuación.

Ejemplos 4.1. 1. Considere el conjunto $\mathbb{Z}$ de todos los números enteros. Es fácil convencerse que $\mathbb{Z}$ no tiene un elemento mínimo, pues dado cualquier entero m tenemos que $m - 1 < m$ y $m - 1$ también es un entero.

2. Considere el siguiente conjunto de números racionales

$$C = \left\{1, \frac{1}{2}, \frac{1}{3}, \frac{1}{4}, \cdots, \frac{1}{n}, \cdots\right\}.$$

C no tiene mínimo. ¿Como podríamos verificar esta afirmación? Basta mostrar que para cualquier elemento de C existe otro elemento de C menor que él. Sea $x \in C$ cualquiera, entonces x debe ser igual a $\frac{1}{n}$ para algún número natural $n > 0$. Como $\frac{1}{n+1} < \frac{1}{n}$ y $\frac{1}{n+1}$ también pertenece a C, entonces $\frac{1}{n}$ no es el mínimo de C.

3. Por supuesto que algunos subconjuntos de $\mathbb{Q}$ (o de $\mathbb{Z}$) sí tienen primer elemento. Por ejemplo, $\{\frac{2}{3}, \frac{4}{15}, \frac{5}{7}\}$ tiene primer elemento ¿Cuál es?. Lo importante acerca del Principio de buena ordenación es que asegura que **cualquier** subconjunto de $\mathbb{N}$ (no vacío) tiene primer elemento.

4. Considere el conjunto

$$C = \{x \in \mathbb{Q} : \ 3 < x\}.$$

Este conjunto no tiene un elemento mínimo. Pues dado cualquier número $x \in C$, veremos que existe otro $y \in C$ con $y < x$. En efecto, considere $y = \frac{x+3}{2}$. Es claro que y es un racional (¿porqué?). Mostraremos que $y \in C$ y además que $y < x$. En efecto, notemos que

$$y - 3 = \frac{x+3}{2} - 3 = \frac{x-3}{2}.$$

Como $x > 3$, entonces $x - 3 > 0$. De esto se concluye que $y - 3 > 0$, es decir $y > 3$ y por lo tanto $y \in C$. De igual forma tenemos que $y < x$: Pues $x - y = x - \frac{x+3}{2} = \frac{x-3}{2}$ y de aquí , al igual que antes, concluimos que $x - y > 0$ y por lo tanto $x > y$.

□

Lo que hace tan importante al Principio de buena ordenación es que se refiere a **cualquier** subconjunto no vacío de $\mathbb{N}$, sin importar la manera usada para definir el conjunto. Los siguientes dos ejemplos ilustran lo que acabamos de decir.

Ejemplo 4.2. Considere la siguiente situación. Supongamos que realizamos un experimento donde participan los estudiantes de la Facultad de Ciencias. Cada estudiante lanza una moneda 100 veces y anota el número de veces que salió "cara". Definimos el siguiente conjunto

$$C = \{n \in \mathbb{N} : \ n \text{ es el número de veces que obtuvo "cara" alguno de los estudiantes}\}$$

Es claro que $C \subseteq \{0, 1, 2, \cdots, 100\}$ y además que C no es vacío. El principio de buena ordenación nos dice que C debe tener un primer elemento, es decir, que alguno (o algunos) de los estudiantes fué el que obtuvo el menor número de "caras". Si en lugar de lanzar la moneda 100 veces lo hicieran 1000 veces el conjunto correspondiente tendrá un mínimo. El Principio del mínimo entero puede parecer bastante obvio en este ejemplo particular, sin embargo, es precisamente la generalidad con que se enuncia lo que hace de él un principio fundamental en Matemáticas. □

Ejemplo 4.3. Usaremos el Principio de buena ordenación para mostrar que existe un primer número natural n que cumple con la siguiente condición

$$1^n + 2^n + \cdots + 99^n < (100)^n. \tag{4.2}$$

Considere el conjunto

$$C = \{n \in \mathbb{N} : \ 1^n + 2^n + \cdots + 99^n < (100)^n\}.$$

Es fácil ver que $1 \notin C$, pues $1 + 2 + \cdots + 99 > 100$. También tenemos que $2 \notin C$, pues $99^2 = 9801$, $98^2 = 9604$ y $9801 + 9604 = 19405$; y por otra parte $100^2 = 10.000$. El Principio de buena ordenación nos dice que, en caso que C no sea vacío, entonces debe tener un elemento mínimo. Observemos que el mínimo de C es precisamente el menor número natural que satisface la desigualdad (4.2).

Bastaría entonces que mostráramos que $C \neq \emptyset$. Notemos que los números que estamos sumando en el lado izquierdo de (4.2) son todos menores o iguales que 99^n. Por esto tenemos que

$$1^n + 2^n + \cdots + 99^n \leq 99(99)^n.$$

Es suficiente entonces conseguir un natural n tal que

$$99(99)^n < (100)^n.$$

Pues en este caso, n también cumpliría (4.2). El problema ahora consiste en conseguir n tal que $99 < (\frac{100}{99})^n$. Usando una calculadora de mano se puede verificar que

$$99^{458} < \left(\frac{100}{99}\right)^{458}$$

Por lo tanto, $458 \in C$. Observe que no estamos afirmando que 458 sea el mínimo de C, sólo podemos asegurar que el mínimo de C es menor o igual a 458. ¿Cuál es el menor elemento de C? El principio de buena ordenación no nos ayuda a conseguir el número buscado, sólo nos asegura que existe. □

4.1.1. Máximo de un conjunto

El Principio de buena ordenación se refiere al primer elemento de un conjunto de números naturales. Ahora veremos qué podemos decir acerca del último elemento de un conjunto. Se dice que m es el **máximo** (o último elemento) de un conjunto $C \subseteq \mathbb{N}$ si se cumplen las dos condiciones siguientes:

(i) $m \in C$.
(ii) Todo elemento de C es menor o igual que m.

Observe la analogía entre estas dos condiciones y las que definen el mínimo de un conjunto. Como ya hemos visto un conjunto de números naturales puede no tener un máximo (por ejemplo $\mathbb{N}$ no tiene máximo ¿que otro ejemplo conoce el lector?).

Hay dos conceptos relacionados con los conceptos de máximo y mínimo que introducimos a continuación.

Diremos que un conjunto C de números naturales es **acotado superiormente** si existe un número natural p tal que todo elemento de C es menor o igual que p; en este caso decimos que p es una **cota superior** de C. Notemos que decir que p es una cota superior de C es equivalente a decir que se cumple lo siguiente

$$C \subseteq \{0, 1, 2, \cdots, p\}.$$

Haremos dos observaciones útiles sobre las cotas y los conjuntos acotados superiormente.

(i) Si m es el máximo de un conjunto C, entonces m es una cota superior de C.

(ii) Si un conjunto tiene una cota superior, entonces tiene muchas cotas superiores. Pues si p es una cota superior de C, es fácil verificar que $p + 1$, $p + 2$, etc., también son cotas superiores de C.

Los siguiente ejemplos ilustrarán mejor el concepto de cota superior.

Ejemplos 4.4. 1. Consideremos el conjunto $\{11, 12, 13, 14\}$. Es claro que 14,15, 16, etc., son cotas superiores de este conjunto. Además 14 es el máximo de este conjunto. Es importante no confundir el concepto de cota superior con el de máximo. Observe que existen muchas cotas superiores pero sólo una de ellas puede ser el máximo.

2. Sea C el conjunto $\{n \in \mathbb{N} : n < 24\}$. De la definición de C se ve que 24 es una cota superior de C. Pero también 23,25, 26, etc. son cotas superiores. Pero 22 no es cota superior, pues existe un elemento de C que es mayor que 22 (¿cuál?). Es claro que 23 es el máximo de C.

3. El conjunto $\{n \in \mathbb{N} : n$ es múltiplo de $15\}$ no es acotado superiormente. Para mostrarlo basta ver que cualquier natural que tomemos es menor que algún elemento de este conjunto. En efecto, sea m un natural mayor que 0. Entonces $m < 15m$, y $15m$ pertenece al conjunto. Por lo tanto m no es una cota superior de ese conjunto. (¿qué pasa con $m = 0$?) □

4. El concepto de conjunto acotado superiormente también tiene sentido para conjuntos de números no necesariamente naturales. Por ejemplo, considere el conjunto $C = \{x \in \mathbb{Q} : x < 4\}$. De la propia definición de C vemos que 4 es una cota superior. De hecho cualquier número racional mayor que 4 también es una cota superior de C. Sin embargo, C no tiene máximo (le dejamos al lector la tarea de mostrarlo siguiendo un razonamiento similar al usado en el ejemplo 4.1).

Ejemplo 4.5. Considere el conjunto

$$C = \{n \in \mathbb{N} : \ n^2 \text{ divide a } 397.902.050\}.$$

Dar una lista de todos los elementos de C no es del todo fácil. Por ejemplo, $1 \in C$, $2 \notin C$ (aunque 2 divide a 397.902.050), $3 \notin C$, $4 \notin C$, $5 \in C$ (verifíquelo!). Así que no podemos determinar por inspección si C tiene o no un elemento máximo. Sin embargo, si podemos mostrar que todos los elementos de C son menores que 397.902.050. En efecto, de la definición del conjunto C tenemos que para cada $n \in C$, se cumple que $n^2 \leq 397.902.050$. Como $n \geq 1$, entonces $n \leq n^2$. Luego necesariamente $n \leq 397.902.050$. En otras palabras, 397.902.050 es una cota superior de C. Ya observamos anteriormente que esto significa que

$$C \subseteq \{1, 2, 3, \cdots, 397.902.050\}.$$

Por esto es bastante natural sospechar que C sí debe tener un elemento máximo. Es claro que 397.902.050 no es el máximo, pues no pertenece a C. Si 397.902.049 estuviera en C, él sería el máximo de C. Si 397.902.049 no está en C, entonces 397.902.048 podría ser el máximo,...etc. De esta manera continuamos descendiendo (con mucha paciencia) hasta que nos topemos por primera vez con un elemento de C, ese número es el máximo de C (!). □

Los ejemplos anteriores sugieren que $\mathbb{N}$ tiene la siguiente propiedad: todo conjunto (no vacío) de números naturales que admita una cota superior necesariamente tiene un elemento máximo. Uno estaría tentado a tomar esta propiedad como un nuevo principio acerca de $\mathbb{N}$, al igual que se hizo con el Principio de buena ordenación. Sin embargo, no hace falta hacerlo, pues como veremos a continuación se puede deducir lógicamente del Principio de buena ordenación.

Teorema 4.6. *Todo conjunto no vacío de números naturales que sea acotado superiormente tiene un máximo.*

Demostración: Sea C un subconjunto de números naturales no vacío y acotado superiormente. Considere el siguiente conjunto

$$A = \{n : \ n \text{ es una cota superior para } C\}.$$

Nuestra hipótesis simplemente dice que A no es vacío. Luego por el Principio de buena ordenación A tiene un elemento mínimo. Sea m el mínimo de A. Mostraremos que m es el máximo de C. Como m pertenece a A, entonces m es una cota superior para C, es decir, todo elemento de C es menor o igual que m. Así que nos queda sólo por mostrar que m pertenece a C. Haremos la prueba por reducción al absurdo. Supondremos que $m \notin C$ y veremos que esto conduce a una contradicción. Ya que suponemos que $m \notin C$ y a la vez sabemos que m es una cota superior de C, entonces podemos concluir que $n < m$ para todo $n \in C$. Por lo tanto, para todo $n \in C$ se tiene que $n \leq m - 1$. Esto dice que $m - 1$ es una cota para C, es decir, que $m - 1 \in A$, pero esto contradice que m es el mínimo de A. Esta contradicción vino de suponer que m no pertenecía a C. Por lo tanto $m \in C$ y con esto termina la demostración. □

Veamos con ejemplos lo que se hizo en la demostración del teorema anterior:

1. Sea $C = \{1, 5, 9, 24\}$. C es acotado y es obvio que 24 es el máximo de C. El conjunto A de todas las cotas de C (que usamos en la demostración anterior) consiste, en este caso, de todos los números naturales mayores o iguales a 24, es decir, $A = \{24, 25, 26, 27, 28, \cdots, \}$. El mínimo de A es 24 y es precisamente el máximo de C.

2. Supongamos que nuestro conjunto C es ahora aquel que encontramos en 4.4

   $$C = \{n \in \mathbb{N} : \ n^2 \text{ divide a } 397.902.050\}.$$

   Ya dimos un argumento que muestra que 397.902.050 es una cota superior de C. El conjunto A, usado en la demostración anterior, es en este caso el conjunto $\{n : n \text{ es una cota superior de } C\}$. Por ejemplo, $397.902.049 \in A$. La demostración del teorema 4.6 garantiza que el mínimo de A es precisamente el máximo de C. Esto no nos dice gran cosa! ¿Cuál será el máximo de C?

A continuación daremos una definición que será necesaria para responder algunos de los ejercicios de esta sección.

Definición 4.7. *Sea C es un conjunto de números (pueden ser naturales, enteros, racionales o reales) diremos que*

1. *p es una **cota superior** para C, si todo elemento de C es menor o igual a p.*
2. *p es el **máximo** de C, si $p \in C$ y todo elemento de C es mayor o igual a p*
3. *q es una **cota inferior** para C, si todo elemento de C es mayor o igual a q.*
4. *q es el **mínimo** de C, si $q \in C$ y todo elemento de C es mayor o igual a q.*

Ejercicios 4.1

1. Considere los siguientes conjuntos de números. Lea las definiciones dadas en 4.7. En cada caso determine si el conjunto es acotado superior o inferiormente y si tiene máximo o mínimo. En el caso que el conjunto tenga máximo y/o mínimo determínelos. Justifique su respuesta.

   (a) $\{3, 2, 26, 5, 1, 0\}$

   (b) $\{n^2 : \ n \in \mathbb{N}\}$

   (c) $\{x \in \mathbb{N} : 4 < x \leq 6\}$

   (d) $\{x \in \mathbb{Q} : 4 < x \leq 6\}$

   (e) $\{5n - 1 : n \in \mathbb{N}\}$

   (f) $\{3n + 2 : n \in \mathbb{Z}\}$

   (g) $\{n \in \mathbb{Z} : n < 0\}$

   (h) $\{\frac{n}{2n+1} : n = 0, 1, 2, 3\}$

   (i) $\{2 + (-1)^n : n \in \mathbb{N}\}$

   (j) $\{\frac{1}{n+1} : \ n \in \mathbb{N}\}$

   (k) $\{7 - \frac{1}{2n} : \ n \in \mathbb{N} \text{ y } n \geq 1\}$

2. Determine si el siguiente conjunto tiene mínimo y/o máximo

   $$\{n \in \mathbb{N} : 13 \leq n \text{ y } n \text{ divide a } 82.861\}.$$

   Justifique su respuesta. No necesita hallar el mínimo ni el máximo (en caso que existieran).

3. Determine si el siguiente conjunto tiene mínimo y/o máximo

   $$\{n : \ n \text{ es el número de cédula de algún estudiante de la ULA}\}$$

   Justifique su respuesta.

4. Determine si el siguiente conjunto tiene mínimo.

   $$C = \{n \in \mathbb{N} : \ 1^n + 2^n + 3^n + 4^n < 5^n\}.$$

   ¿Puede decir cuál es el mínimo? (*Sugerencia:* Vea lo hecho en el ejemplo 4.3).

5. Determine si los siguientes conjuntos tienen máximo, en caso afirmativo halle el máximo y compruebe que en realidad lo es.

   a) $\{n \in \mathbb{N} : \ n^2 \text{ divide a } 240\}$

   b) $\{n \in \mathbb{N} : \ n^2 \text{ divide a } 44.100\}$

   (*Sugerencia:* Halle la descomposición en factores primos de 240 y de 44.100).

6. ¿Cuál es el máximo de $\{n \in \mathbb{N} : \ n^2 \text{ divide a } 397.902.050\}$?

7. En cada uno de los ejercicios que siguen determine si el rango de la función dada tiene mínimo y/o máximo.

   a) $f : \mathbb{N} \to \mathbb{N}$ dada por $f(n) = n + 3$.

   b) $f : \mathbb{N} \to \mathbb{N}$ dada por $f(n) = 2n + 1$.

   c) $f : \mathbb{N} \to \mathbb{N}$ dada por $f(n) = 4$.

   d) $f : \mathbb{N} \to \mathbb{N}$ dada por $f(n) = 6 + (-1)^n$.

   e) $f : \mathbb{N} \to \mathbb{N}$ definida por partes de la manera siguiente

$$f(x) = \begin{cases} x + 30 & \text{, si } 0 \leq x \leq 20 \\ 40 & \text{, si } 21 \leq x. \end{cases}$$

8. Sea $f : \mathbb{N} \to \mathbb{N}$ dada por $f(n) = n + 3$. Definimos el siguiente conjunto

$$C = \{n \in \mathbb{N} : \ f(n) \leq 10\}.$$

   Es decir, en C están aquellos elementos cuya imagen bajo f es menor o igual a 10. En otras palabras, $C = \{n \in \mathbb{N} : \ n + 3 \leq 10\}$. Halle (si es posible) 3 elementos del conjunto C y determine si C tiene mínimo y/o máximo.

9. Responda las mismas preguntas que en el ejercicio anterior para cada una de las funciones siguientes (observe que en cada caso, el conjunto C es diferente)

   a) $f : \mathbb{N} \to \mathbb{N}$ dada por $f(n) = 2n + 1$.

   b) $f : \mathbb{N} \to \mathbb{N}$ dada por $f(n) = 4$.

   c) $f : \mathbb{N} \to \mathbb{Z}$ dada por $f(n) = 6 + (-1)^n$.

   d) $f : \mathbb{N} \to \mathbb{Q}$ dada por $f(n) = 5 + \frac{1}{n+1}$.

   e) $f : \mathbb{N} \to \mathbb{Q}$ dada por $f(n) = 7 - \frac{1}{n}$.

4.2. Sucesiones

Las funciones que tienen dominio $\mathbb{N}$ se usan con mucha frecuencia en Matemáticas y reciben un nombre especial: **sucesiones**. Una sucesión sobre un conjunto A es una función que asigna a cada número natural un elemento de A.

Ejemplos 4.8. 1. Consideremos la sucesión de todos los números pares.

$$0, 2, 4, 6, 8, \cdots,$$

   Podemos ver esta colección de números de la manera siguiente. Consideremos la función $f : \mathbb{N} \to \mathbb{N}$ definida por $f(n) = 2n$. Es claro que el rango de f es precisamente la colección de todos los números pares.

2. Consideremos la colección de números racionales de la forma $\frac{1}{2^n}$:

$$1, \frac{1}{2}, \frac{1}{4}, \frac{1}{8}, \frac{1}{16}, \cdots,$$

Podemos entonces definir esta colección por compresión de la manera siguiente

$$\{\tfrac{1}{2^n} : n \in \mathbb{N}\}.$$

Podemos ver este conjunto como el rango de la función $f : \mathbb{N} \to \mathbb{Q}$ definida por $f(n) = \frac{1}{2^n}$.

□

Las sucesiones se pueden ver también como una lista etiquetada de objetos donde las etiquetas son los números naturales. Es usual denotar las etiquetas con **subíndices**. Vistas de este modo, las sucesiones se escriben de la siguiente forma

$$a_0, a_1, a_2, a_3, a_4, \cdots \tag{4.3}$$

donde a_0 indica el primer elemento de la sucesión, es decir, el elemento que se asigna al cero, a_1 es el segundo elemento de la sucesión, etc. En general, a_n es el elemento asignado a n. La sucesión completa la representamos con $(a_n)_n$. Es usual llamar a_n el **término general** de la sucesión $(a_n)_n$.

Ejemplos 4.9. 1. Asignando al número 0 el 3, al 1 el 4, al 2 el 5, y en general al n el $n + 3$, obtenemos

$$3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, \cdots$$

Con frecuencia el término general de una sucesión viene dado por una regla. Por ejemplo, la sucesión descrita arriba viene dada por la regla $a_n = n + 3$ para $n \geq 0$.

2. Asignando a todo número natural un mismo número, por ejemplo el número 3, obtenemos la sucesión

$$3, 3, 3, 3, 3, \cdots$$

donde $a_0 = 3$, $a_1 = 3$, $a_2 = 3$, y en general $a_n = 3$. Se dice en este caso que la *sucesión es constante*. Este tipo de sucesiones corresponde a las funciones constantes. En nuestro ejemplo, tenemos la función $f : \mathbb{N} \to \mathbb{N}$ dada por $f(n) = 3$ para todo $n \in \mathbb{N}$.

□

Para definir una sucesión es necesario indicar la manera en que se asigna a cada número natural el correspondiente elemento de la sucesión. Por ejemplo, si decimos que $a_n = n^2$ queda completamente determinada la sucesión: $0, 1, 4, 9, 16, 25, \cdots$.

La notación para sucesiones varía de acuerdo al contexto. De hecho es muy frecuente que las sucesiones se presenten como listas indizadas donde los subíndices comienzan en el 1 en lugar del 0. Es decir,

$$a_1, a_2, a_3, a_4, \cdots$$

Cada vez que usemos sucesiones dejaremos bien claro cual es el conjunto de índices que estamos usando. En la sección que sigue veremos que la elección del conjunto de índices no es en realidad importante. La letra usada para los subíndices no tiene que ser necesariamente la letra n, también escribiremos $(a_i)_i$, $(a_k)_k$ o $(a_m)_m$.

4.2.1. Sucesiones equivalentes

Consideremos la sucesión cuyo término general a_n viene dado por

$$a_n = 2n + 1$$

para $n \geq 0$. Es decir, la sucesión a_n es

$$1, 3, 5, 7, 9, 11, \cdots$$

la cual corresponde a la sucesión de todos los números impares. También podemos representar esta sucesión usando índices en los naturales positivos. Pongamos

$$b_n = 2n - 1$$

para $n \geq 1$. El lector puede verificar que $b_1 = 1$, $b_2 = 3$, $b_3 = 5$, etc. Es decir, las sucesiones $(a_n)_{n\geq 0}$ y $(b_n)_{n\geq 1}$ en "realidad son la misma" (aunque formalmente son diferentes, pues no usan el mismo conjunto de índices). En este caso diremos que estas dos sucesiones son **equivalentes**. En otras palabras, dos sucesiones son equivalentes si sus primeros elementos son iguales, sus segundos elementos son iguales, ... etc. Podemos dar una regla que "traduce" los índices de una sucesión en los correspondientes índices de la otra sucesión. En efecto, observemos que

$$b_1 = a_0, b_2 = a_1, b_3 = a_2, b_4 = a_3.$$

Vemos entonces que

$$b_{n+1} = a_n \text{ para todo } n \geq 0.$$

pues $b_{n+1} = 2(n + 1) - 1 = 2n + 1 = a_n$.

Ejemplos 4.10. 1. Considere la sucesión a_n dada por $a_n = 3n + 1$ para $n \geq 1$. Los primeros términos de esta sucesión son

$$a_1 = 4, a_2 = 7, a_3 = 10, a_4 = 13.$$

Queremos representar esta sucesión usando como índices todos los naturales. Es decir, queremos una sucesión $(b_n)_{n\geq 0}$ tal que $b_0 = 4$, $b_1 = 7$, $b_2 = 10$, etc. Tomemos $b_n = 3(n + 1) + 1 = 3n + 4$ para $n \geq 0$. La sucesión b_n satisface lo deseado, pues se cumple que $b_n = a_{n+1}$ para $n \geq 0$ y esto dice que $b_0 = a_1$, $b_1 = a_2$, etc. Por lo tanto $(b_n)_{n\geq 0}$ y $(a_n)_{n\geq 1}$ son sucesiones equivalentes.

2. El conjunto de índices puede ser cualquier subconjunto de $\mathbb{N}$. Por ejemplo, la sucesión del ejemplo anterior también podemos darla con la siguiente regla

$$c_n = 3n - 11 \text{ para } n \geq 5.$$

En efecto, observemos que $c_n = 3(n-4)+1 = a_{n-4}$ para cada $n \geq 5$. Así que $c_5 = 4 = a_1$, $c_6 = 7 = a_2$, $c_7 = 10 = a_3$, etc. Por lo tanto $(c_n)_{n\geq 5}$, $(b_n)_{n\geq 0}$ y $(a_n)_{n\geq 1}$ son sucesiones equivalentes.

3. Considere las sucesiones $(a_n)_n$ dada por $a_n = 5n - 2$ para $n \geq 1$ y $(b_n)_n$ dada por $b_n = 5n - 17$ para $n \geq 4$ ¿Serán equivalentes? Calculemos los primeros términos de estas sucesiones

$$a_1 = 3, a_2 = 8, a_3 = 13, a_4 = 18$$

$$b_4 = 3, b_5 = 8, b_6 = 13, b_7 = 18.$$

Verifiquemos que estas dos sucesiones son equivalentes. En efecto, se tiene que $b_n = a_{n-3}$ para $n \geq 4$.

4. Sean $(a_n)_n$ dada por $a_n = 5n + 2$ para $n \geq 0$ y $(b_n)_n$ dada por $b_n = 5n - 8$ para $n \geq 3$ ¿Serán equivalentes? Notemos que el primer elemento de a_n es $a_0 = 5 \cdot 0 + 2 = 2$, en cambio el primer elemento de b_n es $b_3 = 5 \cdot 3 - 8 = 7$. Por lo tanto no son equivalentes. □

4.2.2. Sucesiones finitas

En lugar de asignar un número a todo natural n, como en (4.3), podemos asignarle elementos sólo a un número finito de ellos, por ejemplo al 0, 1 y al 2 y de esta forma tendríamos una sucesión de tres elementos

$$a_0, a_1, a_2.$$

En general, indicaremos con

$$a_0, a_1, a_2, a_3, \cdots, a_n$$

una **sucesión finita** de $n+1$ elementos. Las sucesiones finitas también las podemos ver como funciones. Por ejemplo la sucesión

$$8, 3, 67, 56.$$

La podemos representar con la función $f : \{0,1,2,3\} \to \{3,8,56,67\}$ definida por $f(0) = 8$, $f(1) = 3$, $f(2) = 67$ y $f(3) = 56$.

Observe que en un conjunto el orden en que se escriban los elementos no es importante. Pero en una sucesión es crucial el orden. El contradominio de f es el conjunto $\{3,8,56,67\}$. Lo importante es que la regla de correspondencia asigne las imágenes en el orden deseado.

4.2.3. Sumatorias y productorias

Introduciremos una notación muy útil para representar las sumas de los elementos de una sucesión $(a_i)_i$. Usaremos la letra griega Σ (que se lee "sigma") para denotar una suma. Sea $(a_i)_{i\geq 1}$ una sucesión de números. Definimos

$$\sum_{i=1}^{n} a_i = a_1 + a_2 + \cdots + a_n. \tag{4.4}$$

Este símbolo se lee "la sumatoria de a_i desde i igual a 1 hasta n". Por ejemplo,

$$\sum_{i=1}^{3} a_i = a_1 + a_2 + a_3.$$

Aunque parezca quizá inútil, el caso n igual a 1 también está permitido, y se tendría que

$$\sum_{i=1}^{1} a_i = a_1.$$

Ejemplo 4.11. Considere la sucesión a_i dada para $a_i = i + 1$ para $i \geq 1$. Entonces

$$\sum_{i=1}^{4} (i+1) = (1+1) + (2+1) + (3+1) + (4+1) = 14.$$

□

Ejemplo 4.12. Considere la sucesión constante $a_i = 1$ para $i \geq 0$. Tenemos que

$$\sum_{i=1}^{3} a_i = a_1 + a_2 + a_3 = 1 + 1 + 1 = 3.$$

En general tenemos lo siguiente

$$\sum_{i=1}^{n} a_i = n.$$

Notemos que si empezamos en $i = 0$ tenemos un sumando más y por lo tanto el resultado es

$$\sum_{i=0}^{n} a_i = n + 1.$$

□

También tenemos una notación similar para los productos. Usaremos la letra griega Π (se lee "pi").

$$\prod_{i=1}^{n} a_i = a_1 \cdot a_2 \cdots a_n. \tag{4.5}$$

Este símbolo se lee "el producto de a_i desde i igual a 1 hasta n" (también se dice "la productoria" en analogía con el símbolo de suma). Por ejemplo,

$$\prod_{i=1}^{4} a_i = a_1 \cdot a_2 \cdot a_3 \cdot a_4.$$

Ejemplo 4.13. Considere la sucesión a_i dada para $a_i = i + 1$ para $i \geq 1$. Entonces

$$\prod_{i=1}^{3} (i+1) = (1+1) \cdot (2+1) \cdot (3+1) = 24.$$

□

El caso particular cuando a_i es igual a i nos da la definición del **factorial** de un número natural $n \geq 1$. Más precisamente, el factorial de n, denotado por $n!$, se define de la siguiente manera:

$$n! = \prod_{i=1}^{n} i = 1 \cdot 2 \cdot 3 \cdot 4 \cdots (n-1) \cdot n.$$

Por convención $0! = 1$. Por ejemplo,

$$6! = 1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 \cdot 6 = 720.$$

La sucesión de factoriales $a_n = n!$ crece muy rápidamente como veremos más adelante. El símbolo fué introducido por el matemático Alemán Christian Kramp en 1808 y muestra el asombro que le causó observar los números tan grandes que se obtienen. Por ejemplo,

$$20! = 2.432.902.008.176.640.000.$$

El número 1.000.000! tiene 5.565.709 cifras. En la tabla que sigue mostraremos los primeros términos de las sucesiones 2^n y $n!$. Mostraremos más adelante que $2^n < n!$ para $n \geq 4$.

n	2^n	$n!$
0	1	1
1	2	1
2	4	2
3	8	6
4	16	24
5	32	120
6	64	720
7	128	5.040
8	256	40.320
9	512	362.880
10	1.024	3.628.800

Ejercicios 4.2

1. En cada uno de los siguientes ejercicios determine una sucesión $(b_n)_n$ que sea equivalente a $(a_n)_n$.

   a) $(a_n)_n$ dada por $a_n = 4n$ para $n \geq 0$. Hallar $(b_n)_{n\geq 1}$.

   b) $(a_n)_n$ dada por $a_n = 4n$ para $n \geq 0$. Hallar $(b_n)_{n\geq 6}$.

   c) $(a_n)_n$ dada por $a_n = 7n + 3$ para $n \geq 1$. Hallar $(b_n)_{n\geq 3}$.

   d) $(a_n)_n$ dada por $a_n = n^2$ para $n \geq 1$. Hallar $(b_n)_{n\geq 0}$.

2. Determinar si las siguientes sucesiones son equivalentes.

   a) $(a_n)_n$ dada por $a_n = 6n+3$ para $n \geq 0$ y $(b_n)_n$ dada por $b_n = 6n-15$ para $n \geq 3$.

   b) $(a_n)_n$ dada por $a_n = 2n^2$ para $n \geq 1$ y (b_n) dada por $b_n = 2n^2 - 16n + 32$ para $n \geq 5$.

   c) $(\{a_n)_n$ dada por $a_n = 3n + 2$ para $n \geq 0$ y (b_n) dada por $b_n = 3n - 8$ para $n \geq 3$.

3. Para cada una de las sucesiones que se indican determinar el valor de $\sum_{i=1}^{n} a_i$ y $\prod_{i=1}^{n} a_i$.

   a) $a_i = i$ y $n = 4$.

   b) $a_i = i^2$ y $n = 3$.

   c) $a_i = 3i + 2$ y $n = 4$.

   d) $a_i = i^3$ y $n = 4$.

   e) $a_i = i^5$ y $n = 1$.

   f) $a_i = 3$ y $n = 1$.

4. Efectúe las siguientes operaciones:

   (*a*) $\displaystyle\sum_{i=4}^{7}(i+3)$ (*b*) $\displaystyle\sum_{i=2}^{6}(3i-1)$ (*c*) $\displaystyle\sum_{i=2}^{6} i^2$

   (*d*) $\displaystyle\sum_{i=2}^{6}\frac{1}{i}$ (*e*) $\displaystyle\prod_{i=2}^{5}(2i+1)$ (*f*) $\displaystyle\prod_{i=3}^{5} i^2$

   (*g*) $\displaystyle\prod_{i=2}^{6}\frac{1}{i}$ (*h*) $\displaystyle\prod_{i=2}^{7}(-1)^i$ (*i*) $\displaystyle\prod_{i=2}^{8}(-1)^i$

   (*j*) $\displaystyle\sum_{i=2}^{8} 5$ (*k*) $\displaystyle\sum_{i=3}^{8} 2$ (*l*) $\displaystyle\sum_{i=6}^{10} 2$

4.3. El Principio de Inducción

Supongamos que varias personas, paradas en una fila, están enumerada como se indica a continuación

$$P_0, P_1, P_2, P_3, \cdots$$

Supongamos además que cada una de ellas al recibir un mensaje lo trasmite a la persona que está en la fila inmediatamente después de ella. Es decir, si la persona que ocupa el primer lugar de la fila (la persona denotada con P_0) recibiera el mensaje lo trasmitiría a la persona en el segundo lugar (es decir, a P_1); la que está en el segundo lugar (es decir P_1) lo trasmitiría a la que está en el tercer lugar (es decir a P_2); y así sucesivamente, la que está en el lugar n-ésimo (es decir P_{n-1}) lo trasmitiría a la que está en el lugar $n+1$-ésimo (es decir a P_n). Vemos entonces que si la persona en el primer lugar de la fila (es decir P_0) recibe el mensaje, necesariamente todas las personas en la fila lo recibirán (imagine lo que pasaría en la fila del comedor cuando la primera persona en la fila se entera que se acabó la comida!).

Denotaremos por A al conjunto de todos los naturales n tales que la persona P_n recibió el mensaje. En símbolos,

$$A = \{n \in \mathbb{N} : \ P_n \text{ recibió el mensaje}\}.$$

Estamos suponiendo dos cosas. Primero que P_0 recibió el mensaje, es decir que $0 \in A$. Y además que si P_n recibe el mensaje, entonces lo trasmite a P_{n+1}. En otras palabras, el conjunto A satisface las siguientes dos condiciones

(i) $0 \in A$.

(ii) Si $k \in A$, entonces $k+1 \in A$.

El principio de inducción nos asegura que A tiene que ser igual a $\mathbb{N}$. Es decir, todas las personas en la fila reciben el mensaje.

Lo que sucede en esta situación hipotética es análogo a lo que se conoce como el *efecto dominó*. Probablemente el lector ha visto esos arreglos de las piezas del dominó donde las piezas están dispuestas de tal manera que al inclinarse la primera de ellas, las otras van sucesivamente cayendo como en una reacción en cadena.

Ahora enunciaremos el principio de inducción de manera precisa.

Teorema 4.14. *(**Principio de Inducción**) Sea A un subconjunto de números naturales que satisface las siguientes dos condiciones:*
(i) $0 \in A$.
(ii) Para todo $k \in \mathbb{N}$, si $k \in A$, entonces $k+1 \in A$.
Entonces se tiene que $A = \mathbb{N}$.

¿Cómo podemos demostrar la validéz del Principio de inducción? Supongamos que $A \subseteq \mathbb{N}$ satisface las dos condiciones (i) y (ii) en la hipótesis de 4.14. Queremos mostrar que A contiene a todos los números naturales. La condición (i) nos dice que 0 está en A, y por la condición (ii) sabemos que entonces 1 también está en A. Pero entonces 2 también debe estar, y así sucesivamente. Este argumento intuitivo podríamos considerarlo suficiente para convencernos que A debe ser $\mathbb{N}$. Sin embargo, queremos dar un argumento aún más convincente, pues es un poco vago decir "y así sucesivamente". Veamos pues una demostración matemática del Principio de inducción basada en el Principio de buena ordenación.

Demostración de 4.14: Supongamos que $A \subseteq \mathbb{N}$ satisface las dos condiciones (i) y (ii). Queremos mostrar que A contiene a todos los números naturales. La demostración la haremos por reducción al absurdo. Supondremos que A no es igual a $\mathbb{N}$ y veremos que ésto conduce a una contradicción.

Como $A \neq \mathbb{N}$, entonces el conjunto $B = \mathbb{N} \setminus A$ no es vacío. Por el Principio de buena ordenación sabemos que B tiene un primer elemento que denotaremos con la letra m. Como $0 \in A$, entonces $m > 0$ y por lo tanto $m - 1 \geq 0$. Por ser m el mínimo de B, se tiene que $m - 1 \notin B$. Por lo tanto $m - 1 \in A$ y por la condición (ii) concluimos que $m \in A$. Pero esto contradice que m es el mínimo de B, pues en particular $m \in B$, es decir, $m \notin A$. La contradicción provino de suponer que $B \neq \emptyset$, es decir, de suponer que $A \neq \mathbb{N}$. Por consiguiente podemos concluir que $A = \mathbb{N}$. □

El Principio de inducción se usa con mucha frecuencia y tendremos oportunidad de "verlo en acción" en numerosas ocasiones durante este curso.

4.3.1. Algunas aplicaciones del Principio de inducción

El Principio de inducción se usa, entre otras cosas, para establecer la validez de fórmulas generales. Veamos algunos ejemplos.

Ejemplo 4.15. Mostraremos que para cada $n \geq 0$, se cumple que

$$\sum_{i=0}^{n} i = \frac{n(n+1)}{2}. \tag{4.6}$$

En otras palabras, mostraremos que

$$0 + 1 + 2 + \cdots + n = \frac{n(n+1)}{2}.$$

Sea A el siguiente conjunto

$$A = \{n \in \mathbb{N} : \text{la igualdad 4.6 es válida para } n\}.$$

Si sustituimos n por 0 en la ecuación (4.6) vemos que ambos miembros son iguales a cero, esto muestra que la ecuación (4.6) se cumple cuando n es igual a cero y por lo tanto $0 \in A$. Ahora veremos que A satisface la segunda condición del Principio de inducción, es decir que si $k \in A$, entonces $k + 1 \in A$. En otras palabras, supondremos que la igualdad (4.6) se

cumple cuando n es igual a k y mostraremos que también se cumple cuando n es igual a $k+1$. Denotaremos por s_k la suma de los números naturales del 0 hasta k, es decir,

$$s_k = 0 + 1 + 2 + 3 + \cdots + k.$$

Observemos que $s_{k+1} = s_k + (k+1)$. Nuestra suposición de que $k \in A$ nos indica que

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

por lo tanto

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

De aquí obtenemos

$$s_{k+1} = (k+1)\left(\frac{k}{2} + 1\right) = \frac{(k+1)(k+2)}{2}.$$

Y esto muestra que (4.6) se cumple cuando n es igual a $k+1$. En otras palabras, $k+1 \in A$. Por el Principio de inducción concluimos que A es igual a $\mathbb{N}$ y por lo tanto concluimos también que (4.6) se cumple para todo natural n. □

Ejemplo 4.16. Consideremos la sucesión de los números impares

$$1, 3, 5, 7, 9, 11, \cdots$$

El término general de esta sucesión viene dado por $2n+1$ para $n \geq 0$. Ahora calcularemos la suma de los primeros números impares. Probaremos que para todo natural n se cumple que

$$1 + 3 + 5 + \cdots + (2n+1) = (n+1)^2. \tag{4.7}$$

Podemos expresar la fórmula anterior con el símbolo de sumatoria

$$\sum_{i=0}^{n} 2i + 1 = (n+1)^2. \tag{4.8}$$

Denotemos esta suma por s_n, es decir

$$s_n = 1 + 3 + 5 + \cdots + (2n+1).$$

Definimos un conjunto A de la manera siguiente

$$A = \{n \in \mathbb{N} : \text{la igualdad 4.7 es válida para } n\}.$$

Sustituyendo n por cero en (4.7) vemos que ambos miembros son iguales a cero, y por lo tanto (4.7) se cumple cuando n es igual a 0, en otras palabras, $0 \in A$. Supongamos que (4.7)

es válida cuando n es igual a k, es decir, supongamos que $k \in A$ y mostremos que $k+1 \in A$. Observemos que

$$s_{k+1} = s_k + (2(k+1)+1) = s_k + 2k + 3.$$

Nuestra hipótesis inductiva es que $k \in A$, es decir que $s_k = (k+1)^2$. Sustituyendo s_k por $(k+1)^2$ en la igualdad anterior y efectuando las operaciones indicadas obtenemos

$$s_{k+1} = (k+1)^2 + (2k+3) = k^2 + 2k + 1 + (2k+3) = k^2 + 4k + 4 = (k+2)^2.$$

Esto muestra que (4.7) se cumple cuando n es igual a $k+1$. Por el Principio de inducción concluimos que A es igual a $\mathbb{N}$, en otras palabras, hemos mostrado que (4.7) se cumple para todo n. □

El Principio de inducción también se enuncia de la siguiente forma:

Sean $P_0, P_1, P_2, P_3, \cdots, P_n, \cdots$, proposiciones matemáticas. Supongamos que

(i) P_0 es válida.

(ii) Para todo $k \in \mathbb{N}$, si P_k es válida, entonces P_{k+1} también es válida.

Entonces P_n es válida para todo natural n.

Por "proposición matemática" se entiende afirmaciones del tipo que hemos estudiado en el capítulo dedicado a la lógica. La afirmación que para todo natural n se cumple la ecuación (4.6) es un ejemplo de una proposición matemática. Los ejemplos que presentaremos en todo este capítulo aclararán mejor el significado de esta expresión.

Es importante enfatizar que en el segundo paso de una demostración por inducción, uno **no** muestra que P_{k+1} es verdadera. Lo que se demuestra es la proposición condicional:

Si P_k es verdadera, entonces P_{k+1} es verdadera.

Así que en realidad uno demuestra una colección infinita de proposiciones condicionales: si P_0 es verdadera, entonces P_1 es verdadera; si P_1 es verdadera, entonces P_2 es verdadera; si P_2 es verdadera, entonces P_3 es verdadera... etc.

Como se ve en los dos ejemplos que hemos presentado, el uso del conjunto A no es esencial, pues juega un papel auxiliar. De ahora en adelante presentaremos las demostraciones que usen el principio de inducción siguiendo el esquema siguiente:

1. Se verifica que la ecuación (o la propiedad) que queremos mostrar es válida para el primer caso. Esto se llama frecuentemente **base de la inducción**.

2. Se demuestra que si la ecuación (o la propiedad) es válida para k entonces también es válida para $k+1$. Esto se llama frecuentemente **paso inductivo**. La suposición que la ecuación (o propiedad) es válidad para k se llama **hipótesis inductiva**.

Las demostraciones que sigan este esquema se llamarán **demostraciones por inducción**.

Ejemplo 4.17. Mostraremos que para todo número natural n se cumple que

$$n < 2^n. \tag{4.9}$$

(i) *Base de la inducción:* Como $0 < 1$, es claro que (4.9) es válido cuando n es igual a 0.

(ii) *Paso inductivo:* Para todo $k \in \mathbb{N}$, si $k < 2^k$, entonces $k + 1 < 2^{k+1}$.

Hipótesis inductiva: Sea $k \in \mathbb{N}$ tal que $k < 2^k$.

Debemos mostrar: $k + 1 < 2^{k+1}$.

Notemos primero que si k fuera igual a cero entonces lo que deseamos mostrar se cumple obviamente, pues $0 + 1 < 2^{0+1}$. Por esto supondremos que $k \geq 1$. Multiplicando por 2 ambos miembros de la desigualdad dada en la hipótesis inductiva obtenemos que

$$2k < 2^{k+1}. \tag{4.10}$$

Ahora bien, ya vimos que podemos suponer que $1 \leq k$. Luego sumando k a ambos miembros de esta desigualdad obtenemos que $k + 1 \leq 2k$. Y usando la desigualdad (4.10) y la transitividad de la relación de orden obtenemos que $k + 1 < 2^{k+1}$.

Por el Principio de inducción concluimos que (4.9) es válido para todo número natural n.

□

Continuaremos presentando ejemplos de demostraciones por inducción.

Ejemplo 4.18. Mostraremos que si un conjunto A tiene n elementos entonces $\mathcal{P}(A)$ tiene 2^n elementos.

(i) *Base de la inducción:* El caso $n = 0$ corresponde a $A = \emptyset$. En este caso tenemos que

$$\mathcal{P}(\emptyset) = \{\emptyset\}.$$

Luego $\mathcal{P}(\emptyset)$ tiene 1 elemento y por lo tanto se satisface que $\mathcal{P}(\emptyset)$ tiene 2^0 elementos.

(ii) *Paso inductivo:* Para todo $k \in \mathbb{N}$, si para todo conjunto A con k elementos se cumple que $\mathcal{P}(A)$ tiene 2^k elementos, entonces para todo conjunto B con $k + 1$ elementos se cumple que $\mathcal{P}(B)$ tiene 2^{k+1} elementos.

Hipótesis inductiva: Sea $k \in \mathbb{N}$ tal que para todo conjunto A con k elementos se cumple que $\mathcal{P}(A)$ tiene 2^k elementos.

Debemos mostrar: Dado un conjunto B con $k+1$ elemento, entonces se cumple que $\mathcal{P}(B)$ tiene 2^{k+1} elementos.

Sea B un conjunto con $k+1$ elementos y tomemos un elemento cualquiera $x \in B$. Considere el conjunto $A = B \setminus \{x\}$. Entonces A tiene k elementos. Por otra parte tenemos que

$$\mathcal{P}(B) = \{C \subseteq B : \ x \notin C\} \cup \{C \subseteq B : \ x \in C\}.$$

Observemos que

$$\mathcal{P}(A) = \{C \subseteq B : \ x \notin C\}.$$

Luego tenemos que

$$\mathcal{P}(B) = \mathcal{P}(A) \cup \{C \subseteq B : \ x \in B\}. \tag{4.11}$$

Notemos que el conjunto $\{C \subseteq B : \ x \in C\}$ tiene exactamente el mismo número de elementos que $\mathcal{P}(A)$. En efecto, observe que a cada conjunto $D \in \mathcal{P}(A)$, le asociamos el conjunto $D \cup \{x\}$. Y viceversa, si $C \subseteq B$ y $x \in C$, entonces el conjunto $C \setminus \{x\} \in \mathcal{P}(A)$. [1]

Para finalizar la demostración observemos que

$$\mathcal{P}(A) \cap \{C \subseteq B : \ x \in B\} = \emptyset.$$

Ahora usamos (4.11) y a la hipótesis inductiva para concluir que

$$\mathcal{P}(B) = 2 \cdot 2^k = 2^{k+1}.$$

□

Ejemplo 4.19. Queremos calcular el valor de

$$1 + 2 + 2^2 + 2^3 + \cdots + 2^n.$$

Llamemos s_n esta suma, es decir,

$$s_n = 1 + 2 + 2^2 + 2^3 + \cdots + 2^n.$$

Multiplicando por 2 ambos lados de la igualdad anterior, obtenemos

$$2s_n = 2 + 2^2 + 2^3 + 2^4 + \cdots + 2^{n+1}.$$

Ahora bien, como $s_{n+1} = 1 + 2^2 + 2^3 + \cdots + 2^{n+1}$, entonces $2s_n = s_{n+1} - 1$. Por otra parte tenemos que

$$s_{n+1} = s_n + 2^{n+1}.$$

[1] Para el lector versado en funciones biyectivas, note que $f : \mathcal{P}(A) \to \{C \subseteq B : \ x \in B\}$ dada por $f(C) = C \cup \{x\}$, es una biyección.

Por lo tanto, $s_n + 2^{n+1} = 2s_n + 1$. Despejando s_n obtenemos que $s_n = 2^{n+1} - 1$. La fórmula buscada es entonces

$$1 + 2 + 2^2 + 2^3 + \cdots + 2^n = 2^{n+1} - 1. \tag{4.12}$$

El argumento anterior debería ser suficientemente convincente, sin embargo, podemos también dar una prueba basada en el principio de inducción. La fórmula que queremos demostrar podemos escribirla con la notación de sumatoria de la siguiente manera:

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

(i) *Base de la inducción:* Para $n = 0$ tenemos que

$$\sum_{i=0}^{0} 2^i = 2^0 = 1 = 2^{0+1} - 1.$$

(ii) *Paso inductivo:* Para todo $k \in \mathbb{N}$, si $\sum_{i=0}^{k} 2^i = 2^{k+1} - 1$, entonces $\sum_{i=0}^{k+1} 2^i = 2^{k+2} - 1$.

Hipótesis inductiva: Sea $k \in \mathbb{N}$ tal que $\sum_{i=0}^{k} 2^i = 2^{k+1} - 1$.

Queremos mostrar: $\sum_{i=0}^{k+1} 2^i = 2^{k+2} - 1$.

Notemos primero que

$$\sum_{i=0}^{k+1} 2^i = \sum_{i=0}^{k} 2^i + 2^{k+1}. \tag{4.13}$$

Usando la ecuación dada en la hipótesis inductiva, obtenemos que

$$\sum_{i=0}^{k} 2^i + 2^{k+1} = 2^{k+1} - 1 + 2^{k+1}. \tag{4.14}$$

Juntando esta dos últimas igualdades obtenemos que

$$\sum_{i=0}^{k+1} 2^i = 2 \cdot 2^{k+1} - 1 = 2^{k+2} - 1.$$

que es precisamente lo que queríamos demostrar.

□

Ejemplo 4.20. (**La Leyenda del ajedrez**) [2] Dice una leyenda que el ajedrez fué inventado por un joven Indú llamado Lahur Sessa para darle un poco de distracción a un príncipe aburrido y deprimido por las calamidades producidas por guerras interminables. El príncipe, en agradecimiento por tan maravilloso invento, ofreció darle a Lahur Sessa lo que él pidiera. El joven no deseaba nada a cambio de su invento. El príncipe, molesto por tanta modestia, insistió. Lahur Sessa expresó que no quería ni joyas, ni tierras, ni palacios. Deseaba su recompensa en granos de trigo. Dijo:

[2] Tomado del libro de Malba Tahan "El Hombre que Calculaba" [10]

" dadme un grano por la primera casilla, dos por la segunda, cuatro por la tercera, ocho por la cuarta, y así duplicando sucesivamente hasta llegar a la sexagésima cuarta y última casilla del tablero".

Los algebristas del palacio del príncipe calcularon el número exacto de granos de trigos que debía recibir el joven indú y constataron que ni sembrando toda las tierras de la India podrían reunir tal cantidad de granos. El príncipe tuvo que reconocer su falta de moderación al ofrecer una recompensa cuyo tamaño no sabía estimar ¿Cuántos eran los granos de trigo? Los números que representan los granos pedidos forman la siguiente sucesión

$$1, 2, 4, 8, 16, 32, \cdots, 2^{63}.$$

Así que el número total es

$$\sum_{i=0}^{63} 2^i = 2^{64} - 1 = 18.446.744.073.709.551.615.$$

□

Las dos condiciones (i) y (ii) en el enunciado del Principio de inducción son necesarias como lo muestran los siguientes ejemplos.

Ejemplo 4.21. Para cada n considere la proposición "$(n+1)^2+n+1$ es impar", denotémosla por P_n. Es claro que P_0 es falsa (¿por qué?). Sin embargo, mostraremos que si P_k es verdadera, entonces P_{k+1} también es verdadera. En efecto, tenemos lo siguiente

$$\begin{aligned}(k+2)^2 + k + 2 &= k^2 + 4k + 4 + k + 2 \\ &= k^2 + 2k + 1 + k + 1 + 2k + 4 \\ &= (k+1)^2 + (k+1) + 2(k+2).\end{aligned}$$

Como hemos supuesto que P_k es verdadera, entonces $(k+1)^2 + k + 1$ es impar. El lado derecho de la última igualdad es entonces la suma de un número impar más otro par, por lo tanto el resultado es impar (¿porqué?). Esto muestra que $(k+2)^2 + k + 2$ es impar. □

Ejemplo 4.22. Recordemos que un natural $n > 1$ se dice que es primo si sus únicos divisores son 1 y n. Considere la proposición P_n: "$n^2 - n + 41$ es un número primo". Podemos verificar que P_1 es cierta, sin embargo ésto no indica que P_n sea válida para todo n. Tenemos que P_1, $P_2, \cdots, P_{40}$ son verdaderas. Sin embargo P_{41} es falsa, pues $(41)^2 - 41 + 41$ claramente no es primo.

□

4.3.2. Variantes del principio de inducción

En algunos casos la ecuación o propiedad que estamos estudiando es válida a partir de cierto valor. Un ejemplo de esto, que veremos dentro de poco, es la desigualdad $2^n < n!$ que vale si $n \geq 4$. Para verificar esta desigualdad por inducción necesitaremos otra versión del principio de inducción, la cual presentamos a continuación.

Teorema 4.23. *Sea m un número natural y A un subconjunto de números naturales tal que:*

(i) $m \in A$.

(ii) Para todo $k \in \mathbb{N}$, *si* $k \in A$, *entonces* $k+1 \in A$.

Entonces $\{n \in \mathbb{N} : m \leq n\} \subseteq A$. □

La demostración de este resultado la dejamos como ejercicio (ver ejercicio 10). Podemos enunciar el teorema anterior en términos de "proposiciones matemáticas".

Teorema 4.24. *Sea m un número natural y $P_m, P_{m+1}, P_{m+2}, \cdots, P_n, \cdots$, proposiciones matemáticas para cada $n \geq m$. Supongamos que*

(i) P_m *es válida.*

(ii) Para todo $k \in \mathbb{N}$, *si* P_k *es válida, entonces* P_{k+1} *también es válida.*

Entonces P_n *es válida para todo* $n \geq m$. □

Ejemplo 4.25. Mostraremos que $2^n < n!$ si $n \geq 4$.

(i) *Base de la inducción:* Cuando n es igual a 4, tenemos que $2^4 = 16$ y $4! = 24$. Luego $2^4 < 4!$.

(ii) *Paso inductivo:* Si $k \geq 4$ y $2^k < k!$, entonces $2^{k+1} < (k+1)!$.

Hipótesis inductiva: Sea $k \in \mathbb{N}$ tal que $k \geq 4$ y $2^k < k!$.

Queremos demostrar: $2^{k+1} < (k+1)!$. Como estamos suponiendo que $k \geq 4$, entonces es claro que $2 < k+1$. Por hipótesis inductiva tenemos que $2^k < k!$. Multiplicando por 2 ambos miembros de esta desigualdad obtenemos que

$$2 \cdot 2^k < 2k!.$$

Como $2 \cdot 2^k = 2^{k+1}$, entonces

$$2^{k+1} < 2k!.$$

Ahora bien, como $2 < k+1$, entonces

$$2k! < (k+1)k!.$$

Observemos que $(k+1)! = (k+1)k!$. Por lo tanto, tenemos que

$$2k! < (k+1)!.$$

Tenemos entonces que $2^{k+1} < 2k!$ y $2k! < (k+1)!$. Por la transitividad de $<$ concluimos que

$$2^{k+1} < (k+1)!.$$

Por el teorema 4.24 concluimos que $2^n < n!$ para todo $n \geq 4$. Observe el lector que esta desigualdad no es válida cuando $n \leq 3$. □

Ejemplo 4.26. Probaremos que para todo $n \geq 1$ se cumple

$$1^3 + 2^3 + 3^3 + 4^3 + \cdots + n^3 = \frac{n^2(n+1)^2}{4}. \tag{4.15}$$

(i) *Base de la inducción:* Sustituyendo n por 1 en (4.15) vemos que ambos miembros son iguales a 1, esto muestra que (4.15) es válida para n igual a 1.

(ii) *Paso inductivo:* Si (4.15) es válida cuando n es igual a k, entonces (4.15) es válida cuando n es igual a $k+1$.

Hipótesis inductiva: Sea $k \in \mathbb{N}$ tal que s

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

Sumando $(k+1)^3$ a ambos miembros de la igualdad dada en la hipótesis inductiva obtenemos

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

Con esto hemos verificado que (4.15) es válida cuando n es igual a $k+1$.

Por el Principio de inducción concluimos que (4.15) es válida para todo n. □

Vimos en (4.6) que

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

De esto se deduce inmediatamente que

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

Por consiguiente podemos expresar de manera elegante la suma de los primeros cubos como sigue

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

□

Para finalizar enunciaremos el llamado **Principio de Inducción Fuerte** o **Principio de inducción completa**.

Teorema 4.27. *(**Principio de Inducción Fuerte**) Sea A un subconjunto de números naturales tal que:*

(i) $0 \in A$.

(ii) Para todo $k \in \mathbb{N}$, *si* $\{0, 1, 2, 3, \cdots k\} \subseteq A$, *entonces* $k+1 \in A$.

Entonces $A = \mathbb{N}$.

Note que la condición (ii) es más fuerte que la correspondiente condición en 4.14. La demostración de este resultado la dejamos como ejercicio (ver el ejercicio 11)

Ejercicios 4.3.1

1. Determine para que valores de n se cumple la desigualdad indicada

   a) $2^n + 8 \leq 2^{n+1}$.

   b) $32(n+1)! \leq (n+2)!$.

2. En los siguientes ejercicios muestre por inducción la fórmula que se indica.

   (a) $\displaystyle\sum_{i=0}^{n} 3i = \frac{(3n)(n+1)}{2}$ (b) $\displaystyle\sum_{i=1}^{n} i^2 = \frac{n(n+1)(2n+1)}{6}$

   (c) $\displaystyle\sum_{i=1}^{n} (2i)^2 = \frac{2n(n+1)(2n+1)}{3}$ (d) $\displaystyle\sum_{i=1}^{n} (2i)^3 = 2[n(n+1)]^2$

   (e) $\displaystyle\sum_{i=0}^{n} 2^i = 2^{n+1} - 1$ (f) $\displaystyle\sum_{i=0}^{n} i(i+1) = \frac{1}{3}n(n+1)(n+2)$

   (g) $\displaystyle\sum_{i=1}^{n} (3i-2) = \frac{n(3n-1)}{2}$ (h) $\displaystyle\sum_{i=1}^{n} 3^i = \frac{3(3^n-1)}{2}$

   (i) $1 + \displaystyle\sum_{i=1}^{n} i(i!) = (n+1)!$ (j) $\displaystyle\sum_{i=1}^{n} 4^i = \frac{4(4^n-1)}{3}$.

3. Halle el valor de las siguientes sumatorias

   (a) $\sum_{i=1}^{100} i$ (b) $\sum_{i=1}^{100} i^2$ (c) $\sum_{i=1}^{100} i^3$ (d) $\sum_{i=0}^{5} 3^i$.

4. Muestre por inducción las siguientes afirmaciones

   a) $2n^2 > (n+1)^2$ para todo número natural $n \geq 3$.

   b) $2^n > n^2$ para todo número natural $n > 4$.

   c) $2^{2n} > 4n^2$ para todo número natural $n > 4$.

   d) $3^n > n^2$ para todo número natural n.

   e) $3^n > n^3$ para todo número natural $n \geq 4$.

   f) $4^n < (2n)!$ para todo número natural $n \geq 2$.

   g) $n^2 + n$ es divisible por 2 para todo número natural n.

   h) $3^{4n} + 9$ es divisible por 10 para todo número natural n.

   i) $3 \cdot 5^{2n+1} + 2^{3n+1}$ es divisible por 17 para todo número natural n.

   j) Muestre por inducción que para todo número natural $n \geq 1$ se cumple que $1+9n \leq 10^n$.

   k) Sea a un entero con $a \geq 2$. Muestre por inducción que para todo $n \geq 1$ se cumple que $1 + (a-1)n \leq a^n$. Observe que cuando $a = 10$ obtenemos el resultado del ejercicio $(4j)$.

5. Encuentre una fórmula para cada una de las siguientes expresiones. Observe que los valores de i van hasta $n+2$. (*Sugerencia:* Es más fácil de lo que parece.)

   (a) $\sum_{i=1}^{n+2} i$ (b) $\sum_{i=1}^{n+2} i^3$ (c) $\sum_{i=0}^{n+2} (2i+1)$ (d) $\sum_{i=0}^{n+2} 2i + 1$.

6. Encuentre una fórmula para $\sum_{i=1}^{n} (2i-1)^2$. ¿Qué relación guarda esta expresión con $1^2 + 2^2 + 3^2 + 4^2 + 5^2 + \cdots + n^2$?.

7. Encuentre una fórmula para cada una de las siguientes sumatorias.

   (a) $\sum_{i=1}^{n} (1+i)$ (b) $\sum_{i=1}^{n} (3+i^2)$

   (c) $\sum_{i=1}^{n} (i^2 - i)$ (d) $\sum_{i=1}^{n} (2+i^3)$

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

8. Halle el error en la siguiente prueba.

Todo natural n es igual a 0.

Prueba: La demostración es por inducción. Es claro que para $n = 0$ se cumple que $0 = 0$. Supongamos que se cumple para k y mostrémoslo para $k+1$. Por hipótesis inductiva tenemos que $k = k - 1 = 0$. Luego $k + 1 = k$. Y por lo tanto $k + 1 = 0$.

9. Halle el error en la siguiente prueba.

   Para todo $n \in \mathbb{N}$ con $n \geq 1$ se cumple que en todo conjunto de n caballos todos los caballos son del mismo color.

   Prueba: La demostración se hará por inducción. Es claro que en un conjunto con un sólo caballo todos los caballos de ese conjunto son del mismo color. Supongamos que la afirmación se cumple para k y lo mostraremos para $k+1$. Sea A un conjunto de $k+1$ caballos. Elija uno de ellos cualquiera y considere el conjunto B de k caballos que se obtiene sacando el caballo escogido. Por hipótesis inductiva todos los caballos de B tienen el mismo color. Como esto es válido para cualquier caballo que escojamos es claro que todos los caballos de A tienen el mismo color.

10. Demostrar el teorema 4.23. *Sugerencia:* Sean m y A como en el enunciado del teorema 4.23. Defina

$$B = \{0, 1, 2, 3, ..., m - 1\} \cup A.$$

    Muestre que B satisface las condiciones del principio de inducción y concluya que $B = \mathbb{N}$. De esto deduzca que $\{n \in \mathbb{N} : m \leq n\} \subseteq A$.

11. Demuestre el Teorema 4.27. Es decir, si A es un subconjunto de números naturales tal que:

    (i) $0 \in A$.

    (ii) Para todo $k \in \mathbb{N}$, si $\{0, 1, 2, 3, \cdots k\} \subseteq A$, entonces $k + 1 \in A$.

    Entonces $A = \mathbb{N}$.

    (*Sugerencia:* Siga un razonamiento análogo al usado en la demostración del teorema 4.14. Es decir, suponga que A es como en la hipótesis. Razone por reducción al absurdo. Suponga que $A \neq \mathbb{N}$ y use el principio de buena ordenación en el conjunto $\mathbb{N} \setminus A$.)

12. Determine si el siguiente principio es válido. Sea A un subconjunto de números naturales tal que:

    (i) $0 \in A$.

    (ii) Para todo $k \in \mathbb{N}$, si existe m tal que $0 \leq m < k$ y $m \in A$, entonces $k \in A$.

    Entonces $A = \mathbb{N}$.

4.4. Definiciones por recursión

Un sucesión bastante famosa por lo frecuente que aparece en problemas de índole muy variada es la **sucesión de Fibonacci**. Esta sucesión, que denotaremos con $(r_n)_n$, cumple con las siguientes condiciones

(i) $r_0 = r_1 = 1$

(ii) $r_n = r_{n-1} + r_{n-2}$ para todo $n \geq 2$

Analizando estas condiciones podemos ver que $r_2 = r_1 + r_0$ y por lo tanto $r_2 = 2$. De igual manera obtenemos que $r_3 = 2 + 1 = 3$, $r_4 = 3 + 2 = 5$, $r_5 = 5 + 3 = 8$, etc. Vemos entonces que si conocemos los primeros n elementos de la sucesión podemos, usando la condición (ii), calcular el elemento $n + 1$ de la sucesión.

Los primeros términos de la sucesión de Fibonacci son los siguientes:

n	r_n
0	1
1	1
2	2
3	3
4	5
5	8
6	13
7	21
8	34

Las sucesiones definidas de esta manera se conocen como **sucesiones recursivas** o definidas por **recursión**. La ecuación usada para definir la sucesión (como (ii) arriba) se conoce como **ecuación de recurrencia**.

Fibonacci (1180-1250) (cuyo verdadero nombre fue Leonardo de Pisa) fué un matemático italiano que en su libro *Liber Abaci* presentó un problema que dió origen a la sucesión que lleva su nombre. El problemas fué el siguiente:

> *¿Cuántas parejas de conejos tendremos mensualmente a partir de una pareja de conejos jóvenes si se cumplen las siguientes dos condiciones: (1) Cada conejo es fértil a partir del segundo mes de vida y cada pareja cuando es fértil produce dos conejillos y (2) supondremos que ningún conejo muere.*

La suseción de Fibonacci también aparece relacionada con la distribución de las ramas de algunas plantas, el número de pétalos de algunas flores y en muchas otras situaciones.

Veamos otro ejemplo.

Ejemplo 4.28. Considere la siguiente situación. El crecimiento anual de las ramas de un árbol es dos veces el del año anterior. Si denotamos por t_n la longitud de las ramas al finalizar el año n, tenemos que el crecimiento de las ramas del árbol en el año $n-1$ es

$$t_{n-1} - t_{n-2}.$$

Luego la condición descrita la podemos expresar de la manera siguiente

$$t_n = t_{n-1} + 2(t_{n-1} - t_{n-2}).$$

Es decir

$$t_n = 3t_{n-1} - 2t_{n-2}.$$

Por ejemplo, si durante el primer año el crecimiento fué igual a 1 tendríamos que $t_0 = 0$ y $t_1 = 1$. Con estos datos y la ecuación de recurrencia podemos conseguir cualquier término que queramos. Por ejemplo, para hallar t_3 debemos calcular primero t_2 y luego obtenemos que $t_3 = 2t_2 - t_1$. Los primeros cinco términos de esta sucesión son los siguientes:

n	t_n
0	0
1	1
2	3
3	7
4	15
5	31
6	63
7	127
8	255

□

Algunas sucesiones definidas por recursión también pueden expresarse con una regla. Por ejemplo, la sucesión de Fibonacci también se puede expresar de la siguiente manera:

$$r_n = \frac{1}{\sqrt{5}}\left(\frac{1+\sqrt{5}}{2}\right)^{n+1} - \frac{1}{\sqrt{5}}\left(\frac{1-\sqrt{5}}{2}\right)^{n+1}.$$

¿Cómo se llegó a este resultado? La respuesta a esta pregunta no la incluiremos en este libro. En el ejercicio 3 le pedimos al lector que verifique que en efecto la sucesión anterior satisface la recurrencia

$$r_n = r_{n-1} + r_{n-2}$$

y las condiciones iniciales $r_0 = r_1 = 1$.

La sucesión del ejemplo 4.28 también la podemos expresar de la siguiente forma

$$t_n = 2^n - 1.$$

Dejamos al lector verificar que en efecto esta sucesión satisface la ecuación de recurrencia

$$t_n = 3t_{n-1} - 2t_{n-2}$$

y las condiciones iniciales $t_0 = 0$ y $t_1 = 1$.

Ejercicios 4.4

1. Halle el término indicado de cada una de las siguientes sucesiones definidas por recurción.

   a) $t_n = t_{n-1} - 4t_{n-2}$ con $t_0 = -1$ y $t_1 = 4$. Halle t_5.

   b) $s_{n+2} + 3s_{n+1} + 2s_n = 0$ con $s_0 = \frac{1}{2}$ y $s_1 = \frac{1}{4}$. Halle s_5.

   c) $t_n = \frac{t_{n-1}}{t_{n-2}}$ con $t_0 = 2$ y $t_1 = 3$. Halle t_6.

   d) $a_n = a_{n-1} - a_{n-2} - n^2$ con $a_0 = \sqrt{2}$ y $a_1 = 0$. Halle a_4.

2. Las siguientes dos sucesiones definidas por recursión son conocidas. Puede el lector determinar cuál es en cada caso.

   a) $r_0 = 1$ y $r_n = n \cdot r_{n-1}$.

   b) $r_0 = 1$ y $r_n = 2 \cdot r_{n-1}$.

3. Verifique que la sucesión

$$r_n = \frac{1}{\sqrt{5}}\left(\frac{1+\sqrt{5}}{2}\right)^{n+1} - \frac{1}{\sqrt{5}}\left(\frac{1-\sqrt{5}}{2}\right)^{n+1}$$

   satisface la ecuación de recurrencia $r_n = r_{n-1} + r_{n-2}$ y las condiciones iniciales $r_0 = r_1 = 1$.

4. Verifique que la sucesión

$$t_n = 2^n - 1$$

   satisface la ecuación de recurrencia $t_n = 3t_{n-1} - 2t_{n-2}$ y las condiciones iniciales $t_0 = 0$ y $t_1 = 1$.

5. Verifique que la sucesión

$$a_n = 3^n + 2^n$$

   satisface la ecuación de recurrencia $a_n = a_{n-1} + 6a_{n-2} - 2^n$ y las condiciones iniciales $a_0 = 2$ y $a_1 = 5$.

6. Muestre que la sucesión $\{s_n\}$ de Fibonacci satisface

$$\sum_{i=0}^{n-2} s_i = s_n - 1.$$

(*Sugerencia:* Pruébelo por inducción en n y use la ecuación de recurrencia que define la sucesión de Fibonacci.)

Capítulo 5

Los Números Enteros

En este capítulo estudiaremos las propiedades básicas de los números enteros. Usaremos el símbolo $\mathbb{Z}$ para denotar al conjunto de los enteros. Como es conocido por el lector, los enteros constan de los números naturales junto con los enteros negativos:

$$\cdots -5, -4, -3, -2, -1, 0, 1, 2, 3, 4, 5, \cdots$$

Entre los objetivos de este capítulo está el demostrar el *teorema fundamental de la Aritmética*, el algoritmo de la división, el algoritmo de Euclides y algunas propiedades de la relación de congruencia.

5.1. El Teorema Fundamental de la Aritmética

Definición 5.1. *Dados dos enteros n y m con $n \neq 0$, diremos que m es **divisible por** n, si existe otro entero q tal que $m = q \cdot n$.*

Notación: Si m es divisible por n escribiremos $n|m$. Otras maneras equivalentes de expresar que m es divisible por n son: "n **divide** a m", "n es un **divisor** de m" o "m es un **múltiplo** de n". Cuando n no divida m escribiremos $n \not| m$.

Ejemplo 5.2. (i) $4|20$, $7|98$. Observe que $12 = (12/5) \cdot 5$, pero esto no quiere decir que 5 divida a 12. De hecho 5 no divide a 12.

(ii) Los divisores de 14 son -14, -7, -2, -1, 1, 2, 7, 14.

(iii) Cero es divisible por todo entero no nulo.

(iv) Todo entero n mayor que 1 tiene por lo menos dos divisores positivos: 1 y n.

□

Definición 5.3. *Sea $p > 1$ un entero. Si los únicos divisores positivos de p son 1 y p se dice que p es **primo**. Si un entero tiene más de dos divisores mayores que 1 se dice que es **compuesto**.*

Por la defínción anterior se tiene que, dado un entero positivo n, existen 3 alternativas: $n = 1$, n es primo o n es compuesto. Los números primos menores que 1000 son:

2 3 5 7 11 13 17 19 23 29 31 37 41 43 47 53 59 61 67 71 73 79 83 89 97 101 103 107 109 113 127 131 137 139 149 151 157 163 167 173 179 181 191 193 197 199 211 223 227 229 233 239 241 251 257 263 269 271 277 281 283 293 307 311 313 317 331 337 347 349 353 359 367 373 379 383 389 397 401 409 419 421 431 433 439 443 449 457 461 463 467 479 487 491 499 503 509 521 523 541 547 557 563 569 571 577 587 593 599 601 607 613 617 619 631 641 643 647 653 659 661 673 677 683 691 701 709 719 727 733 739 743 751 757 761 769 773 787 797 809 811 821 823 827 829 839 853 857 859 863 877 881 883 887 907 911 919 929 937 941 947 953 967 971 977 983 991 997

Veremos más adelante que existe una cantidad infinita de números primos. El número primo más grande que se conocía hasta marzo del 2006 era

$$2^{30402457} - 1.$$

Este número tiene 9.152.052 cifras. Sus primeras y últimas cifras se pueden ver en la tabla 5.1[1].

Una de las propiedades mas importantes de los enteros es que cada uno de ellos es igual al producto de números primos.

Teorema 5.4. *(*Fundamental de la Aritmética*) Todo natural mayor que 1 se escribe como el producto de potencias de números primos.*

Antes de dar la demostración de este resultado veremos algunos ejemplos de descomposición en producto de potencias de primos.

El número 1820 es compuesto, pues $1829 = 4 \cdot 455$. Continuando la factorización obtenemos que $4 = 2 \cdot 2$ y $455 = 5 \cdot 91$. El número 2 es primo y por lo tanto no puede ser factorizado. En cambio, $91 = 7 \cdot 13$. En definitiva tenemos que

$$1820 = 2 \cdot 2 \cdot 5 \cdot 7 \cdot 13 = 2^2 \cdot 5 \cdot 7 \cdot 13.$$

Los números 2, 5, 7 y 13 se llaman los factores primos de 1820. Otros ejemplos de factorización:

$$45 = 3^2 \cdot 5 \qquad 112 = 2^4 \cdot 7.$$

Observaciones 5.5. Las siguientes indicaciones servirán para hallar todos los divisores de un entero dado. Quizá no es claro en este momento porqué siguiendo este procedimiento obtendremos todos los divisores de un entero, pero el lector puede usarlo cuando lo necesite.

[1]La historia completa de este descubrimiento y mucha más información sobre los números primos se puede obtener por internet visitando las siguientes páginas web: http://www.mersenne.org, http://primes.utm.edu.

315.416.475.618.846.080.
936.303.028.664.545.170.126.519.656.262.323.870.316.323.710.795.135.387.449.
006.934.620.943.862.947.517.029.663.623.614.229.944.506.869.166.986.866.002.
790.395.934.468.934.329.365.512.042.063.478.236.587.664.406.687.540.253.076.
642.098.774.020.969.609.945.983.292.505.783.928.283.570.842.567.724.222.472.
424.177.384.530.775.747.071.585.395.344.060.062.523.282.594.879.423.792.439.
476.204.892.243.486.584.703.502.878.859.359.504.778.085.017.945.823.039.155.
923.890.235.713.341.998.460.191.949.344.821.892.482.974.239.714.173.671.467.
853.449.201.071.870.288.546.168.896.136.805.550.813.765.522.736.431.390.661.
998.086.660.013.200.159.184.799.586.344.310.640.160.882.662.896.619.835.513.
624.965.683.427.527.228.832.614.627.235.339.926.202.140.626.135.740.059.405.
043.680.416.024.569.579.111.847.687.787.990.404.031.488.827.076.477.863.844.
056.446.059.444.671.549.364.021.284.052.464.026.385.325.864.856.787.588.052.
074.866.037.795.846.568.024.415.615.128.074.480.530.889.245.304.132.769.857.
903.104.792.753.927.594.096.429.588.870.747.694.476.778.455.686.462.581.130.
357.179.495.540.007.112.806.849.012.797.583.398.279.772.692.025.012.125.112.
023.957.367.805.032.874.051.785.391.678.878.370.592.978.874.601.926.917.387.
349.902.038.487.496.399.522.256.226.198.420.249.841.538.863.603.112.340.978.
224.699.085.370.428.583.974.221.121.204.957.131.101.735.878.906.042.417.046.
357.865.399.959.344.256.412.869.274.835.252.666.969.750.614.040.193.704.172.

⋮

se omitieron 9.149.915 cifras....

⋮

861.983.331.229.581.628.207.456.688.985.381.475.299.696.888.669.508.558.504.
278.748.073.197.358.728.645.195.413.205.077.188.414.558.626.363.748.071.809.
343.742.824.231.207.947.364.055.564.889.786.735.473.630.583.611.687.800.813.
481.838.607.806.644.426.776.936.989.853.027.146.133.071.440.348.824.506.688.
021.313.705.278.144.989.975.582.967.825.054.191.304.730.044.534.830.053.397.
364.407.890.458.476.033.029.500.124.128.466.260.212.152.881.163.713.339.474.
804.241.604.224.301.155.306.880.130.370.430.126.791.618.460.303.273.056.109.
833.913.616.048.174.397.153.970.015.426.138.934.501.849.880.828.016.521.917.
314.085.583.880.907.581.595.027.922.635.669.209.358.268.396.989.078.969.371.
512.732.556.316.616.650.377.629.399.758.833.050.561.337.572.640.865.692.485.
634.850.804.929.425.117.658.541.656.367.807.541.210.697.699.674.377.703.424.
089.741.881.912.147.693.576.259.349.898.745.419.485.840.888.781.837.881.135.
768.597.159.036.449.464.805.655.834.112.235.437.194.842.063.983.380.878.668.
807.573.495.396.673.051.572.043.177.306.280.808.594.114.546.780.708.413.436.
546.553.615.651.742.720.117.385.307.720.895.536.323.410.591.196.239.399.206.
498.094.640.477.861.486.238.804.050.892.515.010.126.326.135.955.683.299.045.
184.502.541.709.583.894.239.304.960.675.189.653.422.547.853.529.862.010.437.
135.830.915.777.499.500.274.882.218.550.846.708.611.134.297.411.652.943.871

Cuadro 5.1: El número primo más grande conocido hasta marzo de 2006

1. Si conocemos la factorización de un número n en potencias de primos, entonces es fácil determinar todos los divisores de n. Por ejemplo

$$882 = 2 \cdot 3^2 \cdot 7^2.$$

Por lo tanto, los divisores positivos de 882 son los siguientes:

1	2	3	7	
3^2	7^2	$2 \cdot 3$	$2 \cdot 7$	$3 \cdot 7$
$2 \cdot 3^2$	$2 \cdot 7^2$	$3 \cdot 7^2$	$3^2 \cdot 7$	$2 \cdot 3 \cdot 7$
$3^2 \cdot 7^2$	$2 \cdot 3 \cdot 7^2$	$2 \cdot 3^2 \cdot 7$		
$2 \cdot 3^2 \cdot 7^2$.				

Así que 882 tiene 18 divisores positivos. Cambiándoles el signo a todos los anteriores obtenemos los divisores negativos de 882. Observe que hemos incluido en la lista anterior todos los números de la forma

$$2^a \cdot 3^b \cdot 7^c$$

donde a, b y c cumplen que $0 \leq a \leq 1$, $0 \leq b \leq 2$ y $0 \leq c \leq 2$. En efecto, todo número que tenga esta forma es un divisor de $2 \cdot 3^2 \cdot 7^2$. Y viceversa, todo divisor positivo de $2 \cdot 3^2 \cdot 7^2$ necesariamente es un número que, al descomponerlo en un producto de potencias de primos, debe tener la forma $2^a \cdot 3^b \cdot 7^c$ donde a, b y c cumplen que $0 \leq a \leq 1$, $0 \leq b \leq 2$ y $0 \leq c \leq 2$.

2. ¿Cuántos divisores tiene un número? Podemos responder fácilmente esta pregunta si sabemos la descomposición en factores primos del número en cuestión. Por ejemplo, si un número x está factorizado de la siguiente manera

$$p^a \cdot q^b \cdot r^c \cdot t^d$$

donde p, q, r, t son números primos y a, b, c, d son positivos, entonces el número de divisores positivos de x es

$$(a+1) \cdot (b+1) \cdot (c+1) \cdot (d+1)$$

3. Notemos que

$$1620 = 2^2 \cdot 3^4 \cdot 5.$$

Por lo tanto 1620 tiene $(2+1) \cdot (4+1) \cdot (1+1) = 30$ divisores positivos. Los divisores positivos de 1620 son todos los números que tienen la forma siguiente

$$2^a \cdot 3^b \cdot 5^c$$

donde $0 \leq a \leq 2$, $0 \leq b \leq 4$ y $0 \leq c \leq 1$. Le dejamos al lector la tarea de hacer la lista completa de los divisores de 1620.

□

Demostración del Teorema Fundamental de la Aritmética: Considere el siguiente subconjunto de $\mathbb{N}$:

$$A = \{0, 1\} \cup \{n \in \mathbb{N} : \ n \geq 2 \text{ y } n \text{ es igual a un producto de números primos}\}$$

Lo que debemos mostrar es que $A = \mathbb{N}$. Para hacerlo, usaremos el principio de inducción fuerte (Teorema 4.27). Debemos entonces verificar que A satisface las siguientes condiciones:

(i) $0 \in A$.

(ii) Para todo $k \in \mathbb{N}$, si $\{0, 1, 2, 3, \cdots k\} \subseteq A$, entonces $k + 1 \in A$.

En efecto, es obvio que por la misma definición del conjunto A tenemos que $0 \in A$.

Para ver que (ii), supongamos que $k \in \mathbb{N}$ es tal que $\{0, 1, 2, 3, \cdots k\} \subseteq A$. Queremos demostrar que $k + 1 \in A$. Para hacerlo consideraremos dos casos:

Caso 1: $k = 0$. En este caso no hay nada que demostrar pues $1 \in A$.

Caso 2: $k \geq 1$. Consideraremos dos subcasos.

Caso 2a: $k + 1$ es primo. Note que todos los números primos pertenecen a A, en particular $k + 1 \in A$.

Caso 2b: $k+1$ no es primo. Como $k+1 \geq 2$, entonces existen naturales n, m diferentes de 1 y $k + 1$ tales que $k + 1 = m \cdot n$. En particular n, m son menores que $k + 1$ y en consecuencia, por la hipótesis (ii), tenemos que $m, n \in A$. Por lo tanto, n y m son, cada uno respectivamente, igual a un producto de números primos. Digamos

$$n = p_1 \cdot p_2 \cdots p_r \qquad \text{y} \qquad m = q_1 \cdot q_2 \cdots q_s$$

donde los números $p_1, \ldots, p_r$ y $q_1, \ldots, q_s$ son primos. En consecuencia

$$n \cdot m = p_1 \cdot p_2 \cdots p_r \cdot q_1 \cdot q_2 \cdots q_s$$

y esto muestra que $n \cdot m \in A$. Es decir, $k + 1 \in A$.

□

Para terminar, queremos señalar que cada natural admite una sola fatorización en producto de números primos. Este resultado lo demostraremos mas adelante.

Ejercicios 5.4

1. Hallar todos los divisores de 144, 1540, 4235 (*Sugerencia:* Halle la descomposición en factores primos de cada uno de los números dados y siga las indicaciones dadas en 5.5).

2. Hallar todos lo valores de n para los cuales 3^n divide a 972. Hallar todos los valores de m tales que $2^m \cdot 3^m$ divide a 972.

3. Sea $a > 1$ un entero. Use el Principio de buena ordenación para mostrar que existe el menor entero p mayor que 1 tal que $p|a$. Muestre que p es primo. Concluya que todo entero tiene un divisor primo. (*Sugerencia:* Defina $A = \{q \in \mathbb{N} : \ q > 1 \text{ y } q|a\}$ Muestre que A no es vacío. Sea p el mínimo de A, verifique que p es un número primo).

5.2. El algoritmo de la división

En esta sección veremos uno de los resultados más útiles para el estudio de los números enteros.

Teorema 5.6. *(**Algoritmo de la división**) Sean a y b números enteros con $a > 0$. Entonces existen enteros q y r tales que*

$$b = qa + r \quad y \quad 0 \leq r < a. \tag{5.1}$$

Además, tanto q como r están unívocamente determinados por a y b.

La demostración la dejaremos para mas adelante. Por ahora nos concentraremos en entender el significado del algoritmo de la división y dar algunos ejemplos que ilustren como se usa.

Ejemplo 5.7. Para $a = 4$ y $b = -45$ tenemos que $-45 = -12 \cdot 4 + 3 = -48 + 3$. Luego *el resto de dividir* -45 entre 4 es 3 y el cociente es -12. □

Haremos algunas observaciones sobre el significado del Algoritmo de la división.

Observaciones 5.8. 1. Los números q y r dados por el algoritmo de la división se llaman respectivamente **cociente** y **resto** de la división de b entre a. Por ejemplo, si $a = 3$ y $b = 13$, entonces $13 = 4 \cdot 3 + 1$, luego $q = 4$ y $r = 1$. Observe que al dividir 13 entre 3 obtenemos como resto 1 y cociente 4.

2. Observe que el resto r es igual a cero precisamente cuando b es divisible entre a. Por ejemplo, con $b = 14$ y $a = 7$ se tiene que $14 = 2 \cdot 7 + 0$.

3. El algoritmo de la división nos permite clasificar los números enteros de acuerdo al resto que se obtiene al dividirlos por otro número. Por ejemplo, para $a = 2$ obtenemos que todo entero b se puede escribir como $2q$ o como $2q + 1$. Como ya sabemos, los primeros se llaman **enteros pares** y los otros **enteros impares**. Para el caso $a = 3$ obtenemos que todo entero está en una de las siguientes listas

$$\cdots, -15, -12, -9, -6, -3, 0, 3, 6, 9, 12, 15, \cdots \quad \text{números de la forma } 3q$$

$$\cdots, -14, -11, -8, -5, -2, 1, 4, 7, 10, 13, 16, \cdots \quad \text{números de la forma } 3q + 1$$

$$\cdots, -13, -10, -7, -4, -1, 2, 5, 8, 11, 14, 17, \cdots \quad \text{números de la forma } 3q + 2$$

Notemos que los enteros de la forma $3k+2$ son precisamente aquellos que al dividirlos por 3 dejan resto 2. De igual manera, los enteros de la forma $3k + 1$ son aquellos que al dividirlos por 3 dejan resto 1. Y por último, los enteros de la forma $3k$ son aquellos que dejan resto cero al dividirlos por 3.

En general, dados dos enteros a y r con $a > 0$, diremos que un entero b es de la forma $ak + r$ si existe un entero k tal que $b = ak + r$.
Por ejemplo, los enteros de la forma $7k + 5$ son

$$\cdots, -16, -9, -2, 5, 12, 19, 26, 33, \cdots$$

que corresponden a los números que se obtiene dándole a k los valores -3,-2,-1,0,1,2,3 y 4 respectivamente. Veamos otro ejemplo: los enteros de la forma $5k - 1$ son

$$\cdots, -16, -11, -6, -1, 4, 9, 14, \cdots$$

Observación: El algoritmo de la división nos dice que dado un entero $a > 0$, se cumple que todo entero b es de la forma $ak + r$ para un único r con $0 \leq r < a$, donde r es precisamente el resto que deja b al dividirlo por a.

Como veremos a continuación, el algoritmo de la división es el ingrediente fundamental para demostrar muchas de las propiedades fundamentales de los enteros.

Proposición 5.9. *Para todo entero n, n es par si y sólo si n^2 es par.*

Demostración: Debemos mostrar dos implicaciones:

1. *Si n es par, entonces n^2 es también par.* Sea n un entero par, entonces existe otro entero k tal que $n = 2k$. Luego tenemos que $n^2 = 4k^2$ y así $n^2 = 2(2k^2)$. Esto muestra que n^2 es par.

2. *Si n^2 es par, entonces n es par.* Sabemos que esto es equivalente a mostrar la contrarecíproca. Es decir, si n no es par, entonces n^2 tampoco es par.

   Sea n un entero que no es par, luego por el algoritmo de la división, sabemos que n es impar. Por lo tanto existe otro entero k tal que $n = 2k + 1$. Luego

   $$n^2 = (2k + 1)^2 = 4k^2 + 4k + 1 = 2(2k^2 + 2k) + 1.$$

   Por lo tanto n^2 es impar, es decir, no es par.

□

Observemos que dados dos enteros consecutivos n y $n+1$ necesariamente alguno de ellos es par. En efecto, sabemos por el algoritmo de la división que n es par ó impar. Luego n es par ó $n + 1$ es par. Este argumento lo haremos mas preciso durante la demostración de la siguiente proposición.

Proposición 5.10. *Para todo entero n se cumple que $n^2 - n$ es divisible por 2.*

Demostración: Sea n un entero cualquiera. Observemos que

$$n^2 - n = n(n - 1). \tag{5.2}$$

Esta factorización muestra que $n^2 - n$ es el producto de dos enteros consecutivos. Hay dos casos posibles.

(i) *n es par.* Entonces existe un entero k tal que $n = 2k$. Sustituyendo en (5.2) obtenemos que

$$n^2 - n = 2k(2k - 1).$$

Y de aquí se concluye que $n^2 - n$ es divisible por 2.

(ii) *n es impar.* Razonamos de manera análoga. Si n es impar existe otro entero k tal que $n = 2k + 1$. Sustituyendo en (5.2) obtenemos que $n^2 - n = (2k + 1)(2k) = 2(2k + 1)k$.

Como en los dos casos posibles se tiene que $n^2 - n$ es divisible por 2, entonces podemos concluir que $n^2 - n$ es divisible por 2. □

En el siguiente teorema mostraremos que dados tres enteros consecutivos n, $n+1$ y $n+2$ entonces alguno de ellos es divisible por 3.

Proposición 5.11. *Para todo entero n se cumple que $n^3 - n$ es divisible por 3.*

Demostración: Notemos que

$$n^3 - n = n(n^2 - 1) = n(n - 1)(n + 1). \tag{5.3}$$

Por el algoritmo de la división hay tres casos posibles. *(i):* n es de la forma $3k$. *(ii):* n es de la forma $3k+1$. *(iii):* n es de la forma $3k+2$. Mostraremos que en cada uno de los tres casos se cumple que $n^3 - n$ es divisible por 3.

(i) *Supongamos que n es de la forma $3k$.* Sustituyendo en (5.3) obtenemos que

$$n^3 - n = 3k(3k - 1)(3k + 1).$$

Por lo tanto $n = 3q$ donde $q = k(3k - 1)(3k + 1)$ y por lo tanto $n^3 - n$ es divisible por 3.

(ii) *Supongamos que n es de la forma $3k + 1$.* Sustituyendo en (5.3) obtenemos que

$$n^3 - n = (3k + 1)(3k)(3k + 2).$$

Por lo tanto $n = 3q$ donde $q = (3k + 1)(k)(3k + 2)$ y por lo tanto $n^3 - n$ es divisible por 3.

(iii) *Supongamos que n es de la forma $3k + 2$.* Sustituyendo en (5.3) obtenemos que

$$n^3 - n = (3k + 2)(3k + 1)(3k + 3).$$

Luego $n = 3q$ donde $q = (3k + 2)(3k + 1)(k + 1)$ y por lo tanto $n^3 - n$ es divisible por 3.

□

Las dos proposiciones anteriores nos dicen que el producto de dos enteros consecutivos es divisible por 2 y el producto de 3 enteros consecutivos es divisible por 3. ¿Será cierto que, en general, el producto de n enteros consecutivos es divisible por n? Dejaremos a cargo del lector el responder esta pregunta (ver el ejercicio 12).

Proposición 5.12. *Si n es un entero impar, entonces $n^2 - 1$ es divisible por 8.*

Demostración: Sea n un entero impar. Sea k un entero tal que $n = 2k + 1$. Notemos que $n^2 - 1 = (n - 1)(n + 1)$, luego sustituyendo en ésta ecuación n por $2k + 1$ obtenemos que

$$n^2 - 1 = (2k)(2k + 2) = 4k(k + 1). \tag{5.4}$$

Ahora bien, anteriormente vimos que el producto de dos enteros consecutivos es divisible por 2, luego $k(k + 1)$ es par. Esto es, existe un entero q tal que $k(k + 1) = 2q$. Sustituyendo $k(k + 1)$ por $2q$ en (5.4) obtenemos que

$$n^2 - 1 = 8q.$$

Y por lo tanto $n^2 - 1$ es divisible por 8. □

Ejercicios 5.2

1. Determine el cociente y el resto de las siguientes divisiones.

   a) 25 entre 3,

   b) 542 entre 8

   c) -15 entre 5

   d) 722 entre 6

   e) -887 entre 43.

2. Halle 5 enteros de la forma que se indica:

   a) $3k + 2$

   b) $7k - 4$

   c) $9k + 1$

   d) $5k - 3$.

3. Halle un entero que sea simultáneamente de la forma $3k - 17$ y de la forma $4m + 3$.

4. Sea k un entero. En cada caso determine el resto de la división indicada. Justifique su respuesta.

   a) $20k + 3$ dividido entre 4

   b) $20k + 3$ dividido entre 5

c) $20k + 4$ dividido entre 4

d) $20k + 4$ dividido entre 5

e) $49k + 5$ dividido entre 7

f) $49k + 5$ dividido entre 49

g) $49k + 27874$ dividido entre 7

h) $49k + 27874$ dividido entre 49.

5. *a*) Muestre que -3, -1, 1, 3 y 5 son de la forma $4k + 1$ o $4k + 3$.

   b) Muestre que todo entero impar es de la forma $4k + 1$ o $4k + 3$. Use esto para dar otra prueba de la proposición 5.12.

6. *a*) Muestre que 5, 7, 11, 13 y 17 son de la forma $6k + 1$ o $6k - 1$.

   b) Sea p un número primo mayor que 3. Muestre que p es de la forma $6k+1$ o $6k-1$.

7. Muestre:

   a) Todo entero de la forma $12k + 4$ también es de la forma $3m + 1$.

   b) Todo entero de la forma $15k + 7$ también es de la forma $5m + 2$.

8. Determine si las siguientes afirmaciones son verdaderas

   a) Si un entero es de la forma $9k + 5$, entonces también es de la forma $3m + 2$.

   b) Si un entero es de la forma $9k + 7$, entonces también es de la forma $3m + 2$.

   c) $n^4 - n$ es divisible por 4 para todo entero n.

   d) $n^4 - n^2$ es divisible por 4, para todo n.

   e) $3|(n^5 - n)$ para todo entero positivo n.

9. Muestre las siguientes afirmaciones

   a) $3|(n^3 + 5n)$ para todo entero positivo n.

   b) $4|(n^3 - n)$, si n es impar.

   c) $3|(n^3 - n)$, si n es impar.

   d) $8|(n^3 - n)$, si n es impar.

   e) $6|(n^3 + 5n)$ para todo entero positivo n.

10. Muestre por inducción que 4^n es de la forma $3k + 1$ para todo $n \in \mathbb{N}$.

11. Sea n un entero impar y $m = n + 2$. Muestre que $4|(n + m)$.

12. Muestre que el producto de n enteros consecutivos es divisible por n. (*Sugerencia:* Imite lo hecho en la prueba de 5.11).

5.3. El principio del mínimo entero

En esta sección estudiaremos una propiedad del orden de los enteros que será fundamental en la demostración del algoritmo de la división.

Como ya lo observáramos, el principio de buena ordenación no es válido en $\mathbb{Z}$. Sin embargo, algunos subconjuntos de números enteros si tienen elemento mínimo. Por ejemplo:

$$\{-2,-1,0,1,2,3,4,\cdots\} \qquad \{-8,-5,-2,3,7\} \qquad \{a\in\mathbb{Z} : a\geq 40\}$$

-2 es el mínimo del primer conjunto, -8 es el mínimo del segundo y 40 es el mínimo del tercero. Mostraremos que una versión del principio de buena ordenación se cumple en el conjunto de los números enteros. Primero necesitaremos recordar los conceptos de cota superior e inferior.

Definición 5.13. *Sea $C\subset\mathbb{Z}$ y $b\in\mathbb{Z}$.*

*(i) Diremos que b es una **cota inferior** de C si para todo $a\in C$ se cumple que $b\leq a$. En este caso diremos que C está **acotado inferiormente**.*

*(ii) Diremos que b es un **mínimo** de C si b es una cota inferior de C y además $b\in C$.*

La versión del principio de buena ordenación que es válida en $\mathbb{Z}$ es la siguiente.

Teorema 5.14. *(**Principio del mínimo entero**) Todo conjunto no vacío de números enteros que sea acotado inferiormente tiene un elemento mínimo.*

Demostración: Sea A un subconjunto no vacío de $\mathbb{Z}$ acotado inferiormente. Sea b una cota inferior para A. Consideremos el conjunto

$$B=\{a-b:\ a\in A\}.$$

Observe que $b\leq a$ para todo $a\in A$, por ser b una cota inferior de A. Por consiguiente tenemos que todos los elementos de B son mayores o iguales a cero, es decir,

$$B\subseteq\mathbb{N}.$$

Por el principio de buena ordenación para $\mathbb{N}$ sabemos que B tiene un primer elemento (observe que B no es vacío ¿por qué?). Sea m el primer elemento de B. Mostraremos que $m+b$ es el primer elemento de A. En efecto, como $m\in B$ entonces existe un elemento a de A tal que

$$m=a-b.$$

Por lo tanto, $m+b=a$ y en consecuencia $m+b\in A$.

Para concluir que $m+b$ es el mínimo de A faltaría verificar que $m+b$ es una cota inferior de A. Es decir, debemos mostrar lo siguiente:

$$\forall x\in A\ (m+b\leq x). \tag{5.5}$$

Fijemos $x \in A$. Entonces $x - b \in B$ y, como m es el primer elemento de B, se tiene que

$$m \leq x - b.$$

Por lo tanto $m + b \leq x$. Con esto hemos mostrado (5.5). □

Tenemos un resultado análogo en relación al máximo de un subconjunto de $\mathbb{Z}$.

Definición 5.15. *Sea $C \subset \mathbb{Z}$ y $b \in \mathbb{Z}$.*

*(i) Diremos que b es una **cota superior** de C si para todo $a \in C$ se cumple que $a \leq b$. En este caso diremos que C está **acotado superiormente**.*

*(ii) Diremos que b es un **máximo** de C si b es una cota superior de C y además $b \in C$.*

El siguiente resultado es la versión del teorema 4.6 en el contexto de los números enteros.

Teorema 5.16. *Todo conjunto no vacío de números enteros que sea acotado superiormente tiene un elemento máximo.* □

Ejercicios 5.3

1. Sea $A \subseteq \mathbb{Z}$ tal que -3 es una cota inferior de A. Considere el conjunto

$$B = \{a + 3 : \ a \in A\}$$

Muestre que todos los elementos de B son mayores o iguales a cero. Es decir, $B \subseteq \mathbb{N}$.

2. Sea $A \subseteq \mathbb{Z}$ tal que 7 es el máximo de A. Considere el conjunto

$$B = \{a - 8 : \ a \in A\}$$

Muestre que todos los elementos de B son negativos.

3. Sean $A \subset B \subset \mathbb{Z}$.

   a) Muestre que si B es acotado superiormente, entonces A también es acotado superiormente.

   b) Muestra también que si B es acotado inferiormente, A es acotado inferiormente.

4. Demuestre el teorema 5.16. (*Sugerencia:* Use el teorema 5.14 e imite los pasos de la demostración del teorema 4.6).

5.4. Demostración del algoritmo de la división

En esta sección daremos la demostración del algoritmo de la división. Recordemos este resultado

Teorema 5.17. *(**Algoritmo de la división**) Sean a y b números enteros con $a > 0$. Entonces existen enteros q y r tales que*

$$b = qa + r \ \ y \ \ 0 \leq r < a. \tag{5.6}$$

Además, tanto q como r están unívocamente determinados por a y b.

Veamos un ejemplo que ilustra la idea principal que usaremos en la demostración. Trataremos el caso particular $a = 3$ y $b = 25$. Considere el siguiente conjunto:

$$A = \{p \in \mathbb{Z} : \ 3p \leq 25\}.$$

Es fácil convencerse que

$$A = \{\cdots, -3, -2, -1, 0, 1, 2, 3, 4, 5, 6, 7, 8\}.$$

En particular, A es acotado superiormente y el máximo de A es 8. Notemos que

$$25 = 8 \cdot 3 + 1$$

Así que $q = 8$ y $r = 1$ son los números buscados. Como veremos a continuación, no es casualidad que el máximo de ese conjunto es precisamente el cociente de la división de 25 entre 3.

Fijemos dos enteros a, b con $a > 0$. Definimos un conjunto de la manera siguiente

$$A = \{p \in \mathbb{Z} : \ p \cdot a \leq b\}.$$

La idea de la demostración consiste en mostrar que el máximo de A es el entero q buscado y además que $0 \leq b - q \cdot a < a$. Pero primero que todo debemos asegurar que A tiene máximo. Para esto tenemos que ver que A no es vacío y es acotado superiormente.

1. *A no es vacío.* La demostración la dividimos en dos casos, mostrando en ambos un elemento de A.

   (a) Supongamos que $b \leq 0$. Mostraremos que $b \in A$. En efecto, para ver que $b \cdot a \leq b$, basta observar que $b - b \cdot a \geq 0$, pues $b - b \cdot a = b(1 - a)$, $a \geq 1$ y $b \leq 0$.

   (b) Supongamos que $b > 0$. En este caso se tiene que $-a \leq b$, pues $a > 0$. Esto muestra que $-1 \in A$.

2. *A es acotado superiormente.* De nuevo consideraremos los dos casos posibles. En ambos casos hallaremos una cota superior de A.

   (a) Supongamos que $b > 0$. Mostraremos que b es una cota superior de A. Sea $p \in A$. Si $p \geq 0$, entonces $p \leq p \cdot a$ pues $a > 0$. De esto se sigue que $p \leq b$, pues $p \cdot a \leq b$. Por otra parte, si $p \leq 0$, entonces como $b > 0$, obviamente se tiene que $p \leq b$.

(b) Supongamos que $b \leq 0$. En este caso mostraremos que 0 es una cota superior de A. Sea $p \in A$. Como $a > 0$, $b \leq 0$ y $p \cdot a \leq b$, entonces necesariamente $p \leq 0$.

Por el teorema 5.16 sabemos que A tiene máximo, el cual denotaremos por q. Sea $r = b - q \cdot a$. Mostraremos que q y r satisfacen (5.6). Es obvio que $b = qa + r$ y como $q \cdot a \leq b$, entonces $0 \leq r$. Nos falta mostrar que $r < a$. Esto lo haremos por reducción al absurdo. Supongamos que no fuera así, es decir, supongamos que $r \geq a$. Sea $s = r - a$. Entonces $0 \leq s$ y $r = a + s$. Por lo tanto se cumple que

$$\begin{aligned} b &= q \cdot a + r \\ &= q \cdot a + a + s \\ &= (q + 1) \cdot a + s. \end{aligned}$$

Como $s \geq 0$, entonces de la última ecuación se obtiene que $(q + 1) \cdot a \leq b$. Esto dice que $q+1 \in A$, lo cual contradice que q es el máximo de A. Esta contradicción provino de suponer que $r \geq a$. Por lo tanto $r < a$. Con esto hemos terminado la demostración de la existencia de los enteros q y r con las propiedades especificadas en el enunciado del teorema.

Para concluir la demostración, verificaremos que tanto q como r son únicos. Supongamos que existen otros dos enteros q', r' tales que $b = q' \cdot a + r'$ y $0 \leq r' < a$. Mostraremos que necesariamente $q' = q$ y $r' = r$.

Primero observemos que $q \cdot a + r = q' \cdot a + r'$. De esto se obtiene que

$$(q' - q) \cdot a = r - r'. \tag{5.7}$$

Tenemos dos casos posibles:

(a) Supongamos que $r' \leq r$. Como $0 \leq r$, $0 \leq r'$, $r < a$ y $r' < a$, entonces $0 \leq r - r' < a$. De esto y (5.7) se obtiene que

$$(q' - q) \cdot a < a$$

Por lo tanto

$$(q' - q - 1) \cdot a < 0$$

Como $a > 0$ y $q' - q \geq 0$ (por (5.7)), se concluye que

$$0 \leq q' - q < 1$$

Pero por ser $q' - q$ un entero, entonces necesariamente $q' - q = 0$ y también $r - r' = 0$. Por lo tanto, $q = q'$ y $r = r'$.

(b) Supongamos que $r < r'$. En este caso se razona de manera análoga a lo hecho en el caso anterior. Dejaremos a cargo del lector completar esta demostración.

5.5. Divisibilidad

Las propiedades básicas de la relación de divisibilidad son las siguientes:

Teorema 5.18. *Sean a, b y c números enteros.*

(i) Si $a|b$, entonces $a|(b \cdot d)$ para todo entero d.

(ii) Si $a|b$ y $b|c$, entonces $a|c$.

(iii) Si $a|b$ y $a|c$, entonces $a|(n \cdot b + m \cdot c)$ donde n y m son enteros cualesquiera.

(iv) Supongamos que $b > 0$. Si $a|b$, entonces $a \leq b$.

(v) Supongamos que $a > 0$, $b > 0$. Si $a|b$ y $b|a$, entonces $a = b$.

Demostración:

(i) Sea d un entero cualquiera y supongamos que $a|b$. Entonces existe un entero q tal que

$$b = q \cdot a.$$

Multiplicando por d ambos lados de la igualdad se concluye que

$$b \cdot d = q \cdot d \cdot a.$$

Esto muestra que $a|(b \cdot d)$.

(ii) Supongamos que $a|b$ y que $b|c$. Entonces existen enteros q y p tales que

$$b = q \cdot a \quad \text{y} \quad c = p \cdot b.$$

Sustituyendo b en la segunda igualdad obtenemos que

$$c = p \cdot (q \cdot a).$$

Luego $c = (p \cdot q) \cdot a$ y esto muestra que $a|c$.

(iii) Sean n y m dos enteros cualesquiera. Supongamos que $a|b$ y $a|c$. Entonces existen enteros p y q tales que

$$b = p \cdot a \quad \text{y} \quad c = q \cdot a.$$

Multiplicando por n la primera igualdad y por m la segunda tenemos

$$n \cdot b = n \cdot p \cdot a \quad \text{y} \quad m \cdot c = m \cdot q \cdot a.$$

Sumándolas miembro a miembro obtenemos

$$n \cdot b + m \cdot c = n \cdot p \cdot a + m \cdot q \cdot a.$$

Factorizando a obtenemos que

$$n \cdot b + m \cdot c = (n \cdot p + m \cdot q) \cdot a.$$

Y esto muestra que $a|(n \cdot b + m \cdot c)$.

(iv) Supongamos que $a|b$ y $b > 0$. Como $a|b$, entonces existe un entero q tal que $b = q \cdot a$. Luego $b - a = q \cdot a - a = (q - 1) \cdot a$. Consideremos los dos casos posibles:

(1) Supongamos que $a < 0$. Entonces es obvio que $a \leq b$, pues $b > 0$.

(2) Supongamos que $a > 0$. Como $b = q \cdot a$, $b > 0$ y $a > 0$, entonces $q > 0$. Luego $q \geq 1$ y por lo tanto $q-1 \geq 0$. De esto se sigue $(q-1)\cdot a \geq 0$. Es decir, $q\cdot a - a \geq 0$. Por lo tanto $b - a \geq 0$. Luego $b \geq a$.

(v) De la parte (iv) obtenemos que $a \leq b$ y $b \leq a$. Por lo tanto $a = b$.

□

Haremos a continuación algunas observaciones acerca del significado del teorema anterior.

1. Un hecho que se deduce de la parte (i) es que todo múltiplo de un número par es par. En efecto, sea a un número par, es decir, $2|a$; entonces $2|(ab)$ para todo b. Esto muestra que todo múltiplo de a también es par. De igual forma tenemos que, si $3|a$, entonces todo múltiplo de a es divisible por 3. ¿Será cierto que todo múltiplo de un número impar también es impar?

2. La parte (ii) dice que la relación de divisibilidad es una relación transitiva.

3. Cuando n y m son iguales a 1, obtenemos de (iii) que, si $a|b$ y $a|c$, entonces $a|(b + c)$. Análogamente, si m es igual a -1 obtenemos lo siguiente: si $a|b$ y $a|c$, entonces $a|(b-c)$. En palabras, si dos números b y c son ambos divisibles por un tercero a, entonces la suma y la diferencia entre b y c también es divisible por a. Por ejemplo, la suma de dos números divisibles por cinco también es divisible por cinco.

4. Es importante observar que el recíproco de lo dicho en (iii) no es válido. De hecho, existen números a, b y c tales que $a|(b + c)$, pero $a \nmid b$ y $a \nmid c$. Por ejemplo, $5 + 3$ es divisible por 2 pero ni 3 ni 5 lo son.

5. En la parte (iv) la suposición que $b > 0$ es crucial. Por ejemplo: $2| - 4$ pero $2 \not\leq -4$.

6. Es importante observar que la conclusión de la parte (v) no es válida sin la suposición que $a > 0$ y $b > 0$. Por ejemplo: $3| - 3$ y $-3|3$ pero $3 \neq -3$.

Ejercicios 5.5

1. Halle enteros a, b y c tales que

   a) $a|(b - c)$ pero $a \nmid b$ y $a \nmid c$.

   b) $a|(2b + 3c)$ pero $a \nmid b$ y $a \nmid c$.

2. Sean a, b enteros.

   a) Muestre que si $a + b$ y a son pares, entonces b también es par.

b) Si a, b son impares, entonces $a^2 - b^2$ es divisible por 4. (*Sugerencia:* Factorize $a^2 - b^2$.)

c) Muestre que si $a + b$ y a son divisibles por 3, entonces b también es divisible por 3.

d) Muestre que si $a - 2b$ y b son divisibles por 10, entonces a también es divisible por 10.

3. Sean a, b, c y d enteros con $a > 0$. Muestre que si $a|b$, $a|c$ y $a|d$, entonces $a|(b + c + d)$ y también $a|(a - b + c)$. ¿Será cierto que $a|(b - c - a)$ y que $a|(c - a + b)$?

4. Sean p, q, r, t números primos y a, b, c, d números naturales. De un argumento que muestre que $p^a \cdot q^b \cdot r^c \cdot t^d$ tiene $(a + 1) \cdot (b + 1) \cdot (c + 1) \cdot (d + 1)$ divisores positivos. (*Sugerencia:* Vea lo que se hizo en el ejemplo 5.5).

5.6. Ecuaciones diofánticas

Comenzaremos esta sección con un problema de la vida diaria.

Ejemplo 5.19. [2] Un apostador profesional tenía, entre sus tentadoras ofertas, la siguiente: Ofrecía 10 millones de bolívares a cambio de 500.000 bolívares. La única condición impuesta por el apostador era que se le debía entregar los 500.000 bolívares en 20 billetes y los billetes podían ser solamente de 5.000, 20.000 o 50.000 bolívares. ¿Aceptaría Ud. la apuesta?

Para ver resolver este acertijo, designaremos con las letras x, y y z el número de billetes, respectivamente, de 5.000, 20.000 y 50.000 bolívares que den una solución al reto planteado por el apostador. Las condiciones que él impuso son las siguientes:

$$\begin{aligned} 500.000 &= 5.000x + 20.000y + 50.000z \\ 20 &= x + y + z. \end{aligned}$$

La primera ecuación nos dice que x billetes de 5.000, y billetes de 20.000 y z billetes de 50.000 suman 500.000 bolívares. La segunda ecuación nos dice que en total tenemos 20 billetes. Estamos entonces buscando tres números naturales n, m y p tales que si sustituimos respectivamente x, y y z por n, m y p se cumplen las dos ecuaciones. Resolvamos este sistema de ecuaciones de la manera usual. Primero simplificaremos la primer ecuación dividiendo ambos lados por 5.000 y obtenemos.

$$100 = x + 4y + 10z. \tag{5.8}$$

Restando de esta última ecuación la segunda ecuación obtenemos

$$80 = 3y + 9z.$$

Factorizando apropiadamente obtenemos

$$80 = 3(y + 3z).$$

[2] Adaptado del libro *El divertido juego de las matemáticas* de Y. Perelman [8]

Observemos que si y y z son enteros, entonces el lado derecho de la última ecuación es un múltiplo de 3. Pero 80 no es múltiplo de 3. Esto muestra que el sistema de ecuaciones no tiene solución entera. Así que el apostador nunca perdería la apuesta.

Es importante que el lector comprenda claramente que el sistema de ecuaciones que estamos resolviendo sí tiene solución, pero no en los números enteros. Existen soluciones racionales de este sistema; una de ellas es $x = \frac{28}{3}$, $y = \frac{8}{3}$ y $z = 8$. Por supuesto que esta solución no dice nada acerca del problema del apostador, pues no tiene ningún sentido decir que usaremos $\frac{28}{3}$ billetes de 5.000, $\frac{8}{3}$ billetes de 20.000 y 8 billetes de 50.000. □

Este tipo de ecuaciones, donde los coeficientes son enteros y la solución deseada es también entera, reciben el nombre de **ecuaciones diofánticas**.

Ejemplo 5.20. Modificaremos ligeramente las condiciones del apostador requiriendo que los 500.000 Bolívares se entreguen en 25 billetes en lugar de 20. Las nuevas condiciones son las siguientes:

$$\begin{aligned} 500.000 &= 5.000x + 20.000y + 50.000z \\ 25 &= x + y + z. \end{aligned}$$

Siguiendo un razonamiento completamente análogo obtenemos la siguiente ecuación

$$75 = 3(y + 3z).$$

Dividiendo ambos lados por 3, obtenemos

$$25 = y + 3z.$$

Por inspección obtenemos que $y = 1$ y $z = 8$ es una solución de esta ecuación. Como $x = 25 - y - z$, entonces $x = 16$. En resumen, con 16 billetes de 5.000, uno de 20.000 y 8 de 50.000 se cumple lo requerido.

□

Ejemplo 5.21. Consideremos ahora la siguiente ecuación

$$4x + 6y = 2.$$

Mostraremos que esta ecuación tiene solución entera. Podemos simplificarla dividiendo por 2 y obtenemos

$$2x + 3y = 1.$$

Por inspección vemos que $x = -1$ e $y = 1$ forman una solución. Pues $2 \cdot (-1) + 3 \cdot 1 = 1$. ¿Cuál otra solución entera ve el lector? □

Ejemplo 5.22. Otra situación donde las ecuaciones diofánticas surgen naturalmente es la siguiente. Quisiéramos hallar los enteros que son de la forma $3k + 2$ y (simultáneamente) de la forma $7m + 6$. Es decir, queremos hallar los enteros x que cumplen con las siguientes dos condiciones:

$$\begin{aligned} x &= 3k + 2, \quad \text{para algún entero } k. \\ x &= 7m + 6, \quad \text{para algún entero } m. \end{aligned}$$

Esto es equivalente a conseguir enteros k y m tales que

$$3k + 2 = 7m + 6$$

Es decir, conseguir enteros k y m tales que

$$3k - 7m = 4$$

Es fácil verificar que esta ecuación se satisface si $k = -1$ y $m = -1$.

En las secciones que siguen estudiaremos una herramienta importante para resolver este tipo ecuaciones diofánticas de tal manera de poder describir todas las soluciones. □

5.7. El máximo común divisor

Sean a y b dos enteros no nulos. Diremos que un entero d es un **divisor común** de a y b si cumple que $d|a$ y $d|b$. Por ejemplo: los divisores de 25 son -25, -5, -1, 1, 5 y 25; y los divisores de 15 son -15, -5, -3, -1, 1, 3, 5 y 15. Así que los divisores comunes de 25 y 15 son -5, -1, 1, 5.

Un momento de reflexión hará evidente al lector que el conjunto formado por los divisores comunes de dos enteros (no nulos) tiene máximo y se llama el máximo común divisor. Este número juega un papel tan importante para lo que sigue que a continuación enfatizaremos su definición.

Definición 5.23. *Sean a y b dos enteros no nulos. El **máximo común divisor** de a y b se denota por $mcd(a, b)$. Es decir, $d = mcd(a, b)$ si*

(i) $d|a$ y $d|b$.

(ii) Si $c|a$ y $c|b$, entonces $c \leq d$.

□

Notemos que $mcd(a, b) > 0$. También es frecuente denotar el máximo común divisor de a y b simplemente por (a, b).

Ejemplos 5.24. (i) Los divisores de 25 son: -25, -5, -1, 1, 5, 25. Y los divisores de 15 son: -15, -5, -3, -1, 1, 3, 5, 15. Por lo tanto $mcd(25, 15) = 5$.

(ii) $mcd(30, -42) = 6$.

(iii) $mcd(13, 28) = 1$.

(iv) $mcd(-4, 8) = 4$.

□

Daremos algunas indicaciones sobre un método para hallar el máximo común divisor si conocemos la representación de los enteros a y b como producto de primos. Supongamos que

$$a = \quad p_1^{m_1} \cdot p_2^{m_2} \cdots p_k^{m_k}$$

$$b = \quad p_1^{n_1} \cdot p_2^{n_2} \cdots p_k^{n_k}.$$

Donde cada m_i y n_i es un entero no negativo (alguno de ellos puede ser igual a cero). Tenemos entonces que

$$mcd(a,b) = p_1^{\text{mín}\{m_1,n_1\}} \cdot p_2^{\text{mín}\{m_2,n_2\}} \cdots p_k^{\text{mín}\{m_k,n_k\}}.$$

Donde mín$\{m_i, n_i\}$ es el menor de los enteros m_i y n_i y máx$\{m_i, n_i\}$ es el mayor de los enteros m_i y n_i.

Veamos un ejemplo.

$$1998 = 2^1 \cdot 3^3 \cdot 7^0 \cdot 37^1 \cdot 73^0$$

y

$$9198 = 2^1 \cdot 3^2 \cdot 7^1 \cdot 37^0 \cdot 73^1$$

Por lo tanto,

$$mcd(1998, 9198) = 2^1 \cdot 3^2 \cdot 7^0 \cdot 37^0 \cdot 73^0 = 18.$$

El lector atento ya se habrá dado cuenta que lo anterior no es más que la "receta" aprendida en el bachillerato para calcular el máximo común divisor de dos o más números:

> *"$mcd(a,b)$ es el producto de los factores primos comunes con su menor exponente".*

Veamos otros ejemplos:

(i) Si $a = 450$ y $b = 140$, tenemos que $450 = 2 \cdot 3^2 \cdot 5^2$ y $140 = 2^2 \cdot 5 \cdot 7$. Los factores primos comunes de 450 y 140 son 2 y 5. Por lo tanto $mcd(450, 140) = 2 \cdot 5$.

(ii) Si $a = 2^2 \cdot 5^4 \cdot 7^3$ y $b = 2^4 \cdot 3^2 \cdot 7^2$, entonces $mcd(a,b) = 2^2 \cdot 7^2$.

Ejercicios 5.7

1. Calcular el máximo común divisor de los siguientes números:

   a) $328, 43$

   b) $324, 18$

   c) $3502, 1022$

   d) $3501, 1022$

   e) $2740, 8631$.

   (*Sugerencia:* Halle la factorización en potencias de primos).

5.8. El algoritmo de Euclides

Describiremos a continuación un procedimiento para calcular el máximo común divisor de dos enteros a y b. Primero haremos un ejemplo.

Ejemplo 5.25. Calcularemos $mcd(120, 35)$. Primero dividimos usamos el algoritmo de la división con 120 como dividendo y 35 como divisor y obtenemos

$$120 = 3 \cdot 35 + 15$$

Hacemos lo mismo con 35 como dividendo y 15 como divisor, y obtenemos

$$35 = 2 \cdot 15 + 5$$

De nuevo lo hacemos, pero ahora con 15 como dividendo y 5 como divisor:

$$15 = 3 \cdot 5 + 0$$

Como el resto que se obtuvo es cero, se tiene que $mcd(120, 35) = 5$.

Veamos otro ejemplo. Calculemos $mcd(340, 36)$

$$\begin{aligned} 340 &= 9 \cdot 36 + 16 \\ 36 &= 2 \cdot 16 + 4 \\ 16 &= 4 \cdot 4 + 0 \end{aligned}$$

Por lo tanto $mcd(340, 16) = 4$.

□

El patrón general detras de los cálculos hechos en el ejemplo anterior es el siguiente. Sean $a, b \in \mathbb{Z}$ enteros no nulos con $a > 0$. Aplicando repetidamente el algoritmo de la división (ver el teorema 5.6) obtenemos

$$\begin{aligned} b &= q_1 a + r_1 && \text{donde } 0 < r_1 < a \\ a &= q_2 r_1 + r_2 && \text{donde } 0 < r_2 < r_1 \\ r_1 &= q_3 r_2 + r_3 && \text{donde } 0 < r_3 < r_2 \\ r_2 &= q_4 r_3 + r_4 && \text{donde } 0 < r_4 < r_3 \\ &\vdots \end{aligned}$$

Como los restos r_i van decreciendo estrictamente, entonces existe un n tal que el resto de dividir r_n entre r_{n-1} es cero. En otras palabras, tenemos que para algún n

$$\begin{aligned} r_{n-2} &= q_n r_{n-1} + r_n \quad \text{donde } 0 < r_n < r_{n-1} \\ r_{n-1} &= q_{n+1} r_n. \end{aligned}$$

Como demostraremos mas adelante se cumple que

$$mcd(a, b) = r_n$$

El procedimiento descrito arriba se conoce como el **algoritmo de Euclides**.

Ejemplo 5.26. Usaremos el algoritmo de Euclides para calcular $mcd(440, 252)$. Usando el algoritmo de la división como indicáramos antes obtenemos lo siguiente:

$$\begin{array}{rcll} 440 &=& 1 \cdot 252 + 188 & q_1 = 1 \quad r_1 = 188 \\ 252 &=& 1 \cdot 188 + 64 & q_2 = 1 \quad r_2 = 64 \\ 188 &=& 2 \cdot 64 + 60 & q_3 = 2 \quad r_3 = 60 \\ 64 &=& 1 \cdot 60 + 4 & q_4 = 1 \quad r_4 = 4 \\ 60 &=& 15 \cdot 4 + 0 & q_5 = 15 \quad r_5 = 0. \end{array}$$

El último resto no nulo es 4, por lo tanto $mcd(440, 252) = 4$. □

5.8.1. Demostración de la correctitud del algoritmo de Euclides

Sean a, b enteros no nulos. El algortimo de Euclides produce las siguientes ecuaciones:

$$\begin{aligned} b &= q_1 a + r_1 \quad \text{donde } 0 < r_1 < a \\ a &= q_2 r_1 + r_2 \quad \text{donde } 0 < r_2 < r_1 \\ r_1 &= q_3 r_2 + r_3 \quad \text{donde } 0 < r_3 < r_2 \\ r_2 &= q_4 r_3 + r_4 \quad \text{donde } 0 < r_4 < r_3 \\ &\vdots \\ r_{n-2} &= q_n r_{n-1} + r_n \quad \text{donde } 0 < r_n < r_{n-1} \\ r_{n-1} &= q_{n+1} r_n. \end{aligned}$$

Mostraremos que $mcd(a, b) = r_n$.

1. Primero veremos que r_n es un divisor común de a y b. De la última ecuación se tiene que r_n divide a r_{n-1} y por lo tanto r_n divide a $q_n r_{n-1} + r_n$. De la penúltima ecuación concluimos que r_n divide a r_{n-2}. Continuando de esta manera llegamos a que $r_n | r_2$ y $r_n | r_1$. Por lo tanto r_n divide a $q_2 r_1 + r_2$. De la segunda ecuación se obtiene que $r_n | a$. De esto se deduce que r_n divide a $q_1 a + r_1$ y de la primera ecuación obtenemos que $r_n | b$.

2. Ahora mostraremos que r_n es mayor o igual que cualquier divisor de a y b. En efecto, sea c un divisor común de a y b. Luego $c|(b - q_1 a)$ y de la primera ecuación obtenemos que $c|r_1$. De manera similar obtenemos a partir de la segunda ecuación que $c|r_2$. Continuando este proceso finalmente tenemos que $c|r_n$. Como $r_n > 0$, entonces $c \leq r_n$.

Ejercicios 5.8

1. Use el algoritmo de Euclides para calcular el máximo común divisor de los siguientes números:

   a) $328, 43$

   b) $324, 18$

   c) $3502, 1022$

   d) $3501, 1022$

   e) $2740, 8631$.

5.9. Propiedades del máximo común divisor

El *m.c.d* juega un papel fundamental en el estudio de las propiedades de los enteros. El resultado que veremos a continuación es la clave de casi todas las demostraciones que haremos en esta sección. Su demostración la dejaremos para mas adelante.

Teorema 5.27. *Sean a y b dos enteros no nulos. Existen enteros m y n tales que*

$$mcd(a, b) = am + bn.$$

Observación 5.28. Si un entero d se puede escribir de la forma $aq + bq$ diremos que d es una **combinación lineal** de a y de b. El teorema anterior dice que el máximo común divisor de a y b es una combinación lineal de a y de b. Por ejemplo:

$$mcd(15, 25) = 5 = -3 \cdot 15 + 2 \cdot 25.$$

En este ejemplo, tenemos que $m = -3$ y $n = 2$. No es nada evidente cómo hallar esos valores m y n. En el próximo ejemplo veremos como el algoritmo de Euclides nos permite resolver este problema. □

Ejemplo 5.29. Queremos hallar x e y tales que

$$mcd(440, 252) = 440x + 252y \tag{5.9}$$

Lo primero que haremos es calcular $(440, 252)$ usando el algoritmo de Euclides.

$$\begin{array}{rcll} 440 &=& 1 \cdot 252 + 188 & q_1 = 1 \quad r_1 = 188 \\ 252 &=& 1 \cdot 188 + 64 & q_2 = 1 \quad r_2 = 64 \\ 188 &=& 2 \cdot 64 + 60 & q_3 = 2 \quad r_3 = 60 \\ 64 &=& 1 \cdot 60 + 4 & q_4 = 1 \quad r_4 = 4 \\ 60 &=& 15 \cdot 4 + 0 & q_5 = 15 \quad r_5 = 0. \end{array}$$

El último resto no nulo es 4, luego $mcd(440, 252) = 4$.

De las igualdades anteriores obtenemos que

$$\begin{aligned} 4 &= 64 - 60 \\ &= 64 - (188 - 2 \cdot 64) \\ &= -188 + 3 \cdot 64 \\ &= -188 + 3 \cdot (252 - 188) \\ &= 3 \cdot 252 - 4 \cdot 188 \\ &= 3 \cdot 252 - 4 \cdot (440 - 252) \\ &= -4 \cdot 440 + 7 \cdot 252. \end{aligned}$$

Tenemos entonces que $4 = -4 \cdot 440 + 7 \cdot 252$. Es decir, en este caso $x = -4$ y $y = 7$ son una solución de la ecuación (5.9).

Observe que para hallar x e y el procedimiento consiste en sustituir los restos en las igualdades que resultan de aplicar el algoritmo de Euclides comenzando por la última igualdad donde el resto no sea cero.

Existen otras soluciones para la ecuación (5.9). Por ejemplo

$$4 = 59 \cdot 440 + (-103) \cdot 252.$$

¿Puede el lector hallar otra solución?

□

El siguiente resultado da una caracterización muy útil del máximo común divisor.

Teorema 5.30. *Sean a y b dos enteros no nulos. Las siguientes proposiciones son equivalentes:*

(i) $d = mcd(a, b)$,

(ii) $d > 0$, $d|a$, $d|b$ y para todo entero c tal que $c|a$, $c|b$ se tiene que $c|d$.

Demostración: Debemos mostrar dos cosas:

$(i) \Rightarrow (ii)$ Supongamos que d es el máximo común divisor de a y b. Como todo entero siempre tiene un divisor positivo, se concluye que $d > 0$. Por definición del máximo común divisor, también tenemos que $d|a$ y $d|b$.

Veamos la última parte de la afirmación (ii). Sea c otro divisor común de a y b. Por el teorema 5.27 sabemos que existen enteros x y y tales que $d = ax + by$. Como c divide tanto a a como a b, entonces de la parte (iii) del teorema 5.18 concluimos que c divide a $ax + by$. De esto se concluye que $c|d$.

$(ii) \Rightarrow (i)$ Si $c|a$ y $c|b$, entonces por hipótesis, $c|d$. Al ser $d > 0$, por 5.18(iv), se sigue que $c \leq d$. Esto muestra que d es el máximo de los divisores comunes de a y b. Es decir, $d = mcd(a, b)$.

□

Las propiedades básicas del máximo común divisor son las siguientes.

Teorema 5.31. *Sean a y b enteros no nulos. Se cumple que*

(i) *Sea $d = mcd(a, b)$. Entonces $mcd(\frac{a}{d}, \frac{b}{d}) = 1$.*

(ii) *Si $a|bc$ y $mcd(a, b) = 1$, entonces $a|c$.*

(iii) *Sea $d = mcd(a, b)$. Si $a|bc$, entonces $\frac{a}{d}|c$.*

(iv) *Si $k > 0$, entonces $mcd(ka, kb) = k \cdot mcd(a, b)$.*

(v) *Si $mcd(a, b) = 1$, $a|c$ y $b|c$, entonces $ab|c$.*

La demostración de estas propiedades la veremos mas adelante.

Observaciones 5.32.

1. La parte (i) nos dice que después de dividir a a y a b entre $mcd(a, b)$ obtenemos dos números que no tienen ningún factor en común. Por ejemplo: si $a = 24$ y $b = 15$, entonces $mcd(24, 15) = 3$ y $mcd(8, 5) = 1$.

2. La conclusión de la parte (ii) no se cumple si $mcd(a, b) \neq 1$. Por ejemplo: si $a = 4$, $b = 2$ y $c = 6$. Entonces $a|bc$ pero $a \not| b$. Ahora bien, (iii) nos dice qué podemos concluir en este caso. En efecto, $mcd(a, b) = 2$, $\frac{a}{2} = 2$ y $2|c$.

3. La parte (iv) nos permite simplificar el cálculo de m.c.d. Por ejemplo: $mcd(16, 24) = 8mcd(2, 3) = 8$. Observe que si $k < 0$, entonces $mcd(ka, kb) = -k \cdot mcd(a, b)$ ¿por qué?. Por ejemplo: $mcd(-16, 24) = 8mcd(2, -3) = 8$.

4. La parte (v) no se cumple sin la hipótesis de que $mcd(a, b) = 1$. Por ejemplo, si $a = 4$, $b = 6$ y $c = 12$, se tiene que $4|12$ y $6|12$ pero 24 no divide a 12.

Ejemplo 5.33. Si un entero a es divisible por 2 y por 3, entonces es divisible por 6. En efecto, como $mcd(2, 3) = 1$ podemos usar la parte (v) del teorema 5.31 y concluir que $6|a$.
□

Ejemplo 5.34. Mostraremos que el producto de 3 enteros consecutivos es divisible por 6.

Sea a el producto de 3 enteros consecutivos. Por el ejemplo anterior, sabemos que es suficiente mostrar que a es divisible por 2 y por 3. En efecto, tenemos que $a = n(n+1)(n+2)$ donde n es algún entero. Ya hemos visto que el producto de 2 enteros consecutivos es par, por esto $n(n + 1)$ es par. De esto se concluye que a es par. Ahora mostraremos que a es divisible por 3. Por el algoritmo de la división, sabemos que $n = 3q + r$ donde $0 \leq r < 3$ y q es algún entero. Analizaremos por separado cada una de las tres alternativas. (i) Si $n = 3q$, entonces es claro que $a = 3q(3q + 1)(3q + 2)$ es divisible por 3. (ii) Si $n = 3q + 1$, entonces a es igual a $(3q + 1)(3q + 2)(3q + 3) = 3(3q + 1)(3q + 2)(q + 1)$ y es divisible por 3. (iii) Por último, si $n = 3q + 2$, entonces a es igual a $(3q + 2)(3q + 3)(3q + 4)$ y es divisible por 3.
□

Ejemplo 5.35. Sea a un entero tal que $mcd(a, 9) = 3$. Mostraremos que a es de la forma $9k+3$ ó $9k+6$. En efecto, por el algoritmo de la división sabemos que a es de la forma $9k+r$ donde $0 \leq r < 9$. Basta entonces mostrar que los únicos valores posibles para r son 3 o 6. Razonaremos indirectamente, mostrando que las otras 7 alternativas son imposibles.

1. Si $r = 0$, es decir, si $a = 9k$, entonces $mcd(a, 9) = 9$, lo cual es falso por hipótesis.

2. Supongamos ahora que $a = 9k + 1$. Como a y 9 son ambos divisibles por 3, entonces $a - 9k$ es divisible por 3. Pero esto contradice que $1 = a - 9k$.

3. De manera similar, el lector puede verificar que a no puede ser de la forma $9k + 2$, $9k + 4$, $9k + 5$, $9k + 7$ o $9k + 8$.

□

Ejercicios 5.9

1. En cada uno de los siguientes ejercicios, use el algoritmo de Euclides para calcular x e y tales que $ax + by = mcd(a, b)$

   a) $a = 328$, $b = 43$

   b) $a = 324$, $b = 18$

   c) $a = 3502$, $b = 1022$

   d) $a = 3501$, $b = 1022$

   e) $a = 2740$, $b = 8631$.

2. Muestre que:

   a) El producto de cuatro enteros consecutivos es divisible por 24.

   b) El producto de cinco enteros consecutivos es divisible por 120.

3. Sea a un entero. Muestre que:

   a) a es divisible por 12 si, y sólo si, a es divisible por 3 y por 4.

   b) a es divisible por 15 si, y sólo si, a es divisible por 3 y por 5.

   c) a es divisible por 21 si, y sólo si, a es divisible por 3 y por 7.

   d) a es divisible por 40 si, y sólo si, a es divisible por 8 y por 5.

4. Muestre que para todo entero n se cumple que $n^5 - n$ es divisible por 30.

5. Muestre que no existen enteros a y b tales que $a + b = 100$ y $mcd(a, b) = 3$.

6. Muestre que:

   a) Si $mcd(x, 4) = 2$, entonces x es de la forma $4k + 2$.

   b) Si $mcd(a, 4) = 2$ y $mcd(b, 4) = 2$, entonces $mcd(a + b, 4) = 4$.

7. Pruebe que si a es impar, entonces $mcd(a, 2^n) = 1$ para todo natural n.

8. Sean a y b enteros impares. Muestre que $a^3 - b^3$ es divisible por 2^n si, y sólo si, $a - b$ es divisible por 2^n.

9. Determine si las siguientes afirmaciones son verdaderas

   a) Un entero es divisible por 4 y por 6 si, y sólo si, es divisible por 24.

   b) Si un entero es divisible por 32, entonces es divisible por 16.

   c) Si un entero es divisible por 4 y por 10, entonces es divisible por 40.

   d) Si un entero es divisible por 4 y por 10, entonces es divisible por 20.

10. Sean a, b enteros tales que $mcd(a, b) = 1$. Muestre que $mcd(a^3, b^5) = 1$ (*Sugerencia:*. Halle los factores primos de a^3 en términos de los factores primos de a).

11. El máximo común divisor de tres números a, b, c se define como el mayor de los divisores comunes de ellos. Lo denotaremos por $mcd(a, b, c)$. Por ejemplo:

$$mcd(10, 15, 20) = 5 \qquad mcd(3, 5, 18) = 1.$$

   a) Halle $mcd(128, 420, 240)$, $mcd(32, 18, 46)$.

   b) Verifique que

$$mcd(128, 420, 240) = mcd(mcd(128, 420), 240) = mcd(128, mcd(420, 240)).$$

   En general, definimos el máximo común divisor de n enteros no nulos $a_1, a_2, \cdots, a_n$ como el mayor de todos sus divisores comunes y lo denotamos por $mcd(a_1, a_2, \cdots, a_n)$.

12. Si $mcd(a, b) = 1$ diremos que a y b son **coprimos** o **primos entre sí**. Por ejemplo 3 y 5 son coprimos. Recordemos que un natural p se dice que es primo si sus únicos divisores positivos son 1 y p. Por esto, si p y q son primos distintos, entonces p y q son coprimos.

   Sean a, b, c enteros, diremos que son **primos entre sí** cuando $mcd(a, b, c) = 1$ y diremos que son **coprimos dos a dos**, si $mcd(a, b) = mcd(a, c) = mcd(b, c) = 1$. En general, dada una colección cualquiera de enteros, diremos que son coprimos dos a dos, si cualesquiera dos de ellos son primos entre sí. Por ejemplo, 3, 5, 8, 77 son coprimos dos a dos. Por otra parte, 10, 15, 21 y 16 son primos entre sí pues $mcd(10, 15, 21, 16) = 1$. Sin embargo 10, 15, 21, 16 no son coprimos dos a dos, pues $mcd(10, 15) \neq 1$.

   Determine cuáles de las siguientes listas de números son primos entre sí y cuáles son coprimos dos a dos.

   a) 9, 14, 21

   b) 26, 39, 42, 65

   c) 9, 25, 14

   d) 13, 16, 17, 24.

5.9.1. Demostración de las propiedades del mcd

Ya dijimos que es intuitivamente claro que entre los divisores comunes de dos enteros existe uno que es máximo. Sin embargo, en matemáticas aún los resultados intuitivamente verdaderos deben poderse demostrar lógicamente. Por esto incluimos la siguiente proposición y su demostración.

Proposición 5.36. *Sean a y b dos enteros no nulos. Sea A el conjunto*

$$\{d \in \mathbb{Z} : d \text{ es un divisor común de } a \text{ y } b\}.$$

Entonces A tiene un máximo. Además, el máximo de A es un entero positivo d que es el máximo común divisor de a y b.

Demostración: Para mostrar que A tiene máximo es suficiente mostrar que A es no vacío y acotado superiormente.

(1) *A no es vacío:* Pues 1 pertenece a A.

(2) *A es acotado superiormente:* Consideraremos dos casos. (i) Supongamos primero que $b > 0$. Por el teorema 5.18 (iv) sabemos que todos los elementos de A son menores o iguales que b. Es decir que b es una cota superior de A. (ii) Si $b < 0$, entonces observemos que b y $-b$ tienen los mismos divisores (¿por qué?). Luego tenemos que A es igual a $\{d \in \mathbb{Z} : d$ es un divisor común de a y $-b\}$. Y por lo dicho en el caso anterior, tenemos que $-b$ es una cota superior de A.

Por el teorema 5.16 concluimos que A tiene un máximo. Como $1 \in A$, es claro que el máximo de A es mayor o igual a 1 y por lo tanto es un entero positivo. □

Ahora daremos la demostración del teorema 5.27. Primero recordaremos su enunciado.

Teorema. *Sean a y b dos enteros no nulos. Existen enteros m y n tales que*

$$mcd(a, b) = am + bn.$$

Demostración: Considere el siguiente conjunto:

$$C = \{x \in \mathbb{N} : x > 0 \text{ y } x = aq + bp \text{ para algunos } q, p \in \mathbb{Z}\}. \tag{5.10}$$

Notemos que

$$a = a(1) + b(0), \quad -a = a(-1) + b(0).$$

Por esto, dependiendo del signo de a, se tiene que $a \in C$ ó $-a \in C$. Por lo tanto, C no es vacío. Por el principio de buena ordenación C tiene un elemento mínimo. Sea e el menor entero en C. Por la definición del conjunto C sabemos que existen enteros t y s tales que $e = at + bs$. Para completar la prueba bastaría entonces mostrar que e es el máximo común divisor de a y b.

Debemos mostrar dos cosas. La primera que $e|a$ y $e|b$ y la segunda que e es el mayor de los divisores comunes de a y b. Veamos primero que $e|a$. De acuerdo con el algoritmo de la división existen enteros q y r tales que $a = qe + r$ y $0 \leq r < e$. Por lo tanto se tiene que

$$r = a - qe.$$

Como $e = at + bs$, sustituimos en la ecuación de arriba e por $at + bs$ y obtenemos, después de factorizar apropiadamente, que

$$r = a - q(at + bs) = a(1 - qt) + b(-sq).$$

Esto muestra que $r \in C$. Como e es el menor entero positivo de C y $0 \leq r < e$, entonces $r = 0$. Como r es el resto de dividir a entre e, entonces concluimos que $e|a$. La prueba de que $e|b$ es análoga y la dejamos como ejercicio al lector.

Ahora mostraremos que e es el mayor de los divisores comunes de a y b. Sea c otro divisor común de a y b. Por 5.18(iii) sabemos que $c|(at+bs)$ y como $e = at+bs$, entonces concluimos que $c|e$. Finalmente, como $e > 0$ por 5.18 (iv) concluimos que $c \leq e$. □

Ahora demostraremos las propiedades básicas del máximo común divisor que enunciamos en el teorema 5.31. Recordemos el teorema.

Teorema. *Sean a y b enteros no nulos. Se cumple que*

(i) Sea $d = mcd(a, b)$. Entonces $mcd(\frac{a}{d}, \frac{b}{d}) = 1$.

(ii) Si $a|bc$ y $mcd(a, b) = 1$, entonces $a|c$.

(iii) Sea $d = mcd(a, b)$. Si $a|bc$, entonces $\frac{a}{d}|c$.

(iv) Si $k > 0$, entonces $mcd(ka, kb) = k \cdot mcd(a, b)$.

(v) Si $mcd(a, b) = 1$, $a|c$ y $b|c$, entonces $ab|c$.

Demostración:

(i) Como $mcd(a, b) = d$, por el teorema 5.27 existen dos enteros x e y tales que

$$d = ax + by.$$

Dividiendo entre d ambos lados de esta igualdad se obtiene que

$$1 = \frac{a}{d}x + \frac{b}{d}y.$$

Sea c un divisor común de $\frac{a}{d}$ y $\frac{b}{d}$ (observe que estos dos números son enteros ¿por qué?). De la última igualdad y de 5.18 (iii) obtenemos que $c|1$. Por lo tanto $c = 1$ o $c = -1$. De esto se deduce que $mcd(\frac{a}{d}, \frac{b}{d}) = 1$.

(ii) Como $mcd(a, b) = 1$, por el teorema 5.27 existen enteros x e y tales que

$$1 = ax + by.$$

Multiplicando por c ambos lados de esta igualdad obtenemos que

$$c = cax + cby.$$

Por hipótesis $a|bc$, por lo tanto existe un entero q tal que $bc = aq$. Sustituyendo bc en el lado derecho de la última ecuación y factorizando a obtenemos que

$$c = cax + aqy = a(cx + qy).$$

Esto muestra que $a|c$.

(iii) De nuevo, sean x e y enteros tales que

$$d = ax + by.$$

Multiplicando por c esta igualdad obtenemos que

$$cd = cax + cby.$$

Por hipótesis $a|(bc)$, por lo tanto existe un entero q tal que $bc = qa$. Sustituyendo bc por qa en la última ecuación y factorizando apropiadamente obtenemos que

$$cd = cax + qay = a(cx + qy).$$

Por lo tanto se tiene que

$$c = \frac{a}{d}(cx + qy).$$

Como $\frac{a}{d}$ es un entero, concluimos que $\frac{a}{d}$ divide a c.

(iv) Considere los siguientes conjuntos

$$\begin{aligned} C &= \{aq + bp : \ q, p \in \mathbb{Z}\} \\ D &= \{kaq + kbp : \ q, p \in \mathbb{Z}\}. \end{aligned}$$

Por el teorema 5.27 sabemos que $mcd(a, b)$ es el menor entero positivo en C y $mcd(ka, kb)$ es el menor entero positivo en D. Factorizando la expresión que define a D, tenemos que

$$D = \{k(aq + bp) : \ q, p \in \mathbb{Z}\}.$$

Y de esto se concluye inmediatamente que el menor entero positivo en D es igual al menor entero positivo en C multiplicado por k. Y esto es lo que se quería demostrar.

(v) Sean x e y enteros tales que

$$1 = ax + by.$$

Multiplicando por c ambos lados de esta igualdad obtenemos que

$$c = cax + cby.$$

Por hipótesis $a|c$ y $b|c$, por lo tanto existen enteros p y q tales que $c = ap$ y $c = bq$. Sustituyendo c apropiadamente en el lado derecho de la última ecuación y factorizando ab obtenemos que

$$c = bqax + apby = ab(qx + py).$$

Esto muestra que $ab|c$.

□

5.10. La ecuación $ax + by = c$

Sean a y b enteros y consideremos la ecuación lineal en dos variables x y y

$$ax + by = c. \tag{5.11}$$

Estamos interesados en determinar cuando (5.11) tiene soluciones enteras, es decir, queremos saber cuando existen enteros p y q tales que $ap+bq = c$. La ecuación (5.11) obviamente tiene solución racional. Veamos un ejemplo. Consideremos la ecuación

$$12x + 15y = 2.$$

Es claro que si x es igual a cero y y es igual a $\frac{2}{15}$ se cumple que $12x + 15y = 2$. Sin embargo, como lo veremos más adelante, no existen números *enteros* p y q tales que $12p + 15q = 2$.

Ahora estudiaremos un método general para determinar cuando la ecuación (5.11) tiene solución entera y además como hallar todas sus soluciones enteras. Observemos primero que si alguno de los coeficientes a o b es cero, entonces es fácil determinar cuándo (5.11) tiene solución en los enteros. En efecto, supongamos que $b = 0$, entonces (5.11) se convierte en $ax = c$. La cual tiene solución entera si y sólo si $a|c$. Análogamente, si $a = 0$ tenemos que (5.11) tiene solución entera si y sólo si $b|c$. Por esto el caso que más nos interesa es cuando tanto a como b son diferentes de cero.

El siguiente resultado resuelve completamente el problema.

Teorema 5.37. *Sean a y b enteros no nulos.*

1. *La ecuación*

$$ax + by = c$$

tiene solución entera si, y sólo si, $mcd(a, b)$ divide a c.

2. *Además, si x_0, y_0 es una solución de la ecuación $ax + by = c$, entonces cualquier otra solución entera satisface que*

$$x = x_0 + \frac{b}{mcd(a,b)}k, \quad y = y_0 - \frac{a}{mcd(a,b)}k \tag{5.12}$$

para algún entero k.

La demostración de este resultado la dejaremos para mas adelante. Por ahora nos concentraremos en ver algunos ejemplos donde se usa este teorema.

Ejemplo 5.38. Consideremos la ecuación

$$32x + 60y = 30.$$

Tenemos que $mcd(32, 60) = 4$ y $4 \not| 30$, se sigue del teorema 5.37 que esta ecuación no tiene solución entera. □

Ejemplo 5.39. Considere la siguiente ecuación

$$440x - 252y = 12.$$

Mostraremos que tiene solución entera. En efecto, tenemos que $mcd(440, 252) = 4$ y $4|12$, por el teorema 5.37 se tiene que la ecuación tiene soluciones enteras. Vimos en el ejemplo 5.26 que el algoritmo de Euclides nos permite conseguir enteros p y q tales que $440p + 252q = 4$. De hecho vimos que

$$(-4) \cdot 440 + 7 \cdot 252 = 4.$$

Multiplicando por 3 ambos lados de esta igualdad obtenemos que

$$(-12) \cdot 440 - (-21) \cdot 252 = 12.$$

Es decir que $x_0 = -12$ y $y_0 = -21$ es una solución particular de la ecuación $440x - 252y = 12$. Además por el teorema 5.37 sabemos que cualquier otra solución de esa ecuación tiene la forma

$$x = -12 + \frac{-252}{4}k\ , \quad y = -21 - \frac{440}{4}k\ , \quad \text{con } k \in \mathbb{Z}.$$

En otras palabras, las soluciones de la ecuación tienen la forma:

$$x = -12 - 63k\ , \quad y = -21 - 110k\ , \quad \text{con } k \in \mathbb{Z}.$$

Veamos algunos ejemplos de soluciones enteras de la ecuación que estamos estudiando. Para esto le daremos valores a k.

$$\begin{array}{lll} k = 0 & x = -12 & y = -21 \\ k = 1 & x = -75 & y = 131 \\ k = -1 & x = 51 & y = 89 \\ k = 2 & x = -138 & y = -241 \\ k = -2 & x = 114 & y = 199. \end{array}$$

□

Es importante observar que en el teorema 5.37 hace falta tener una solución x_0, y_0 de la ecuación (5.11) para conseguir las otras soluciones. Esta solución x_0, y_0 recibe el nombre de **solución particular**. La fórmula

$$x = x_0 + \frac{b}{(a,b)}k\ , \quad y = y_0 - \frac{a}{(a,b)}k\ , \quad \text{con } k \in \mathbb{Z}$$

provee un método para calcular cualquier otra solución, por esto recibe el nombre de **solución general**.

En el ejemplo 5.39 tenemos que $x_0 = -12$ y $y_0 = 21$ es una solución particular de la ecuación $440x - 252y = 12$ y la solución general viene dada por las fórmulas

$$x = -12 - 63k\ , \quad y = -21 - 110k$$

donde k es un entero cualquiera. En otras palabras, para cada entero k, las fórmulas anteriores nos dan una solución.

Queremos enfatizar que para hallar una solución particular de la ecuación $ax + by = c$ podemos usar el algoritmo de Euclides. El siguiente ejemplo lo ilustra.

Ejemplo 5.40. Considere la ecuación

$$15x + 39y = 9.$$

Como $mcd(15, 39) = 3$ y $3|9$, entonces sabemos que la ecuación tiene solución. Primero usaremos el algoritmo de Euclides para hallar x' y y' tales que $15x' + 39y' = 3$ y luego conseguiremos una solución de la ecuación inicial.

$$\begin{array}{rcl} 39 & = & 2 \cdot 15 + 9 \\ 15 & = & 1 \cdot 9 + 6 \\ 9 & = & 1 \cdot 6 + 3 \\ 6 & = & 2 \cdot 3 + 0. \end{array}$$

Ahora tenemos que

$$\begin{aligned} 3 &= 9-6 \\ &= 9-(15-9) \\ &= -15+2\cdot 9 \\ &= -15+2\cdot(39-2\cdot 15) \\ &= -5\cdot 15+2\cdot 39. \end{aligned}$$

Así que $x' = -5$ y $y' = 2$. Para hallar una solución de $15x+39y = 9$ multiplicamos la última ecuación por 3 y obtenemos

$$9 = -15\cdot 15+6\cdot 39$$

Por lo tanto $x_0 - 15$ y $y_0 = 6$ forman una solución de la ecuación original. □

Los pasos para resolver la ecuación $ax + by = c$ son los siguientes:

---

1. Verifique si $mcd(a, b)$ divide a c. Si no lo divide, entonces no hay solución entera. Si $mcd(a, b)$ divide a c continue.
2. Use el algoritmo de Euclides para hallar enteros m, n tales que
$$am + bn = mcd(a, b)$$
3. Una solución particular de la ecuación $ax + by = c$ viene dada por $x_0 = m \cdot mcd(a, b)$ y $y_0 = n \cdot mcd(a, b)$.
4. Use la fórmula (5.12) para hallar la solución general.

Ejemplo 5.41. Considere el siguiente sistema de ecuaciones

$$\begin{aligned} 6x+12y+2z &= 4 \\ -5x+2y-6z &= -5. \end{aligned}$$

Queremos determinar si tiene solución entera. Multiplicando la primera ecuación por 3 obtenemos $18x + 36y + 6z = 12$. Sumándola a la segunda obtenemos

$$13x + 38y = 7.$$

Como $mcd(13, 38) = 1$, entonces el teorema 5.37 nos asegura que $13x+38y = 7$ tiene solución entera. Ahora bien, con los valores de x e y podemos hallar z y obtener una solución del sistema.

Para hallar una solución particular de la ecuación $13x + 38y = 7$ observamos que

$$13 \cdot 3 + 38 \cdot (-1) = 1$$

(esto es lo que hubiéramos obtenido con el algoritmo de Euclides). Multiplicando por 7 obtenemos

$$13 \cdot (21) + 38 \cdot (-7) = 7.$$

Esto dice que $x_0 = 21$ y $y_0 = -7$ forman una solución de $13x + 38y = 7$. Ahora podemos hallar un solución del sistema. Sustituyendo en la primera ecuación del sistema obtenemos

$$126 - 84 + 2z = 4.$$

Despejando z obtenemos que $2z = -38$, por lo tanto $z = -19$. En definitiva, una solución particular del sistema es $x = 21$, $y = -7$ y $z = -19$.

□

Demostración de el teorema 5.37.

Veamos la primera la parte (1) del teorema 5.37. Para simplificar la escritura, pondremos

$$d = mcd(a, b)$$

Debemos mostrar dos cosas

1. Supondremos que la ecuación (5.11) tiene solución entera y mostraremos que d divide a c. Sea p y q enteros tales que $ap + bq = c$. Como d es un divisor común de a y b, entonces d divide a $ap + bq$, es decir d divide a c.

2. Supondremos que d divide a c y mostraremos que la ecuación (5.11) tiene solución entera. Por el teorema 5.27 existen enteros x' e y' tales que $ax' + by' = d$. Como d divide a c, entonces existe q tal que $c = q \cdot d$. Tenemos que $c = q \cdot (ax' + by') = aqx' + bqy'$. Por lo tanto los enteros aq y bq son una solución de la ecuación (5.11).

Ahora veremos la parte (2) del teorema 5.37. Supongamos que x_0 e y_0 son una solución entera de (5.11). Sean x e y otra solución entera de (5.11). Mostraremos que existe un entero k tal que

$$x = x_0 + \frac{b}{d}k \ , \quad y = y_0 - \frac{a}{d}k.$$

Usaremos repetidamente las propiedades del máximo común divisor que mostramos en 5.31. Tenemos que

$$\begin{aligned} ax_0 + by_0 &= c \\ ax + by &= c. \end{aligned}$$

Por lo tanto tenemos

$$ax_0 + by_0 = ax + by.$$

Y de esto se deduce que

$$a(x - x_0) = b(y_0 - y).$$

Por lo tanto b divide a $a(x-x_0)$ y, en consecuencia, $\frac{b}{d}|$ divide a $\frac{a}{d} \cdot (x - x_0)$. Pero por la parte (i) del teorema 5.31 sabemos que $\frac{a}{d}$ y $\frac{a}{d}$ son primos relativos. Por lo tanto, de la parte (ii) del teorema 5.31 concluimos que $\frac{b}{d}$ divide a $x - x_0$. Esto nos dice que existe un entero k tal que $x - x_0 = \frac{b}{d}k$. Por lo tanto

$$x = x_0 + \frac{b}{d}k.$$

Como x e y son una solución de (5.11) podemos sustituir en esa ecuación la expresión que obtuvimos para x y nos queda

$$a[x_0 + \frac{b}{d}\, k\,] + by = c.$$

Ahora despejaremos y. En uno de los pasos que siguen usaremos que x_0 y y_0 son una solución de (5.11) y por lo tanto cumplen que $by_0 = c - ax_0$.

$$\begin{aligned} c &= ax_0 + \frac{ab}{d}k + by \\ by &= c - ax_0 - \frac{ab}{d}k \\ by &= by_0 - \frac{ab}{d}k \\ y &= y_0 - \frac{a}{d}k. \end{aligned}$$

Con esto hemos mostrado lo que deseábamos.

Sólo nos queda verificar que cada par de enteros de la forma

$$x = x_0 + \frac{b}{d}k\ , \quad y = y_0 - \frac{a}{d}k$$

con $k \in \mathbb{Z}$, forman una solución de (5.11). En efecto, basta sustituirlos en (5.11) y verificar que se cumple la igualdad.

$$\begin{aligned} a[x_0 + \frac{b}{d}k] + b[y_0 - \frac{a}{d}k] &= ax_0 + \frac{ab}{d}k + by_0 - \frac{ba}{d}k \\ &= ax_0 + by_0 \\ &= c. \end{aligned}$$

La última igualdad se cumple pues, por hipótesis, x_0 y y_0 son una solución de la ecuación (5.11).

Ejercicios 5.10

1. Determine si las siguientes ecuaciones tienen soluciones enteras y en caso que tenga use el algoritmo de Euclides para hallar una solución particular y después usando el teorema 5.37 halle la solución general.

   a) $328x + 43y = 26$.

   b) $-324x - 126y = 36$.

   c) $3502x + 1022y = -3$.

   d) $2356x - 665y = -19$.

2. Considere el problema del apostador que vimos en el ejemplo 5.19. Si en lugar de 500.000 bolívares él pidiera 400.000 bolívares, ¿acepataría Ud la apuesta? ¿y si fueran 300.000 bolívares o 200.000 bolívares?

3. Resuelva el sistema de ecuaciones diofánticas

$$\begin{aligned} x + 2y + 3z &= 4 \\ 2x - z &= -1. \end{aligned}$$

4. Muestre que el sistema de ecuaciones diofánticas

$$\begin{aligned} 3x + 6y + z &= 2 \\ 4x + 10y + 2z &= 3. \end{aligned}$$

   no tiene soluciones enteras.

5. Halle todos los enteros de la forma $4n + 1$ que son divisibles por 7.

6. Halle todos los enteros de la forma $4n + 2$ que son divisibles por 8.

7. Muestre que todo múltiplo de 6 es de la forma $4k$ o $4k + 2$.

8. Para cada r en $\{0, 1, 2, 3, 6, 7\}$ sea A_r el siguiente conjunto

$$A_r = \{8k + r : \ 6|(8k + r) \text{ y } k \in \mathbb{Z}\}$$

   Es decir, A_r es la colección de enteros de la forma $8k + r$ que son divisibles por 6. Por ejemplo,

$$A_1 = \{8k + 1 : \ 6|(8k + 1) \text{ y } k \in \mathbb{Z}\}$$

   Determine para que valores de r el conjunto A_r es vacío y para cuales es infinito.

5.11. El mínimo común múltiplo

Sean a y b enteros no nulos, diremos que c es un **múltiplo común** de a y b si $a|c$ y $b|c$. Por ejemplo: (i) ab es un múltiplo común de a y b. (ii) 12 es un múltiplo común de 4 y 6.

Consideremos el siguiente conjunto

$$\{n \in \mathbb{N} : \ n \text{ es un múltiplo común de } a \text{ y } b\}.$$

Este conjunto no es vacío (¿por qué?) luego por el principio de buena ordenación existe un menor múltiplo común positivo de a y b, el cual se llama el **mínimo común múltiplo**. Denotaremos con $mcm[a, b]$ el mínimo común múltiplo de a y b. Por ejemplo: $mcm[3, 4] = 12$, $mcm[3, 6] = 6$, $mcm[4, 10] = 20$.

En general, si $a_1, a_2, \cdots, a_n$ son enteros no nulos, el menor múltiplo positivo de todos ellos se denota por $mcm[a_1, a_2, \cdots, a_n]$. Por ejemplo: $mcm[2, 6, 15] = 30$, $mcm[3, 4, 6] = 12$.

Teorema 5.42. *Sean a y b enteros no nulos.*

1. *Si c es un múltiplo de a y b, entonces $mcm[a, b]$ divide a c.*
2. *Si $a > 0$ y $b > 0$, entonces*

$$mcm[a, b] = \frac{ab}{mcd(a, b)}.$$

3. *Si $k > 0$, entonces $mcm[ka, kb] = k \cdot mcm[a, b]$.*

Demostración:

1. Sea c un múltiplo común de a y b. Mostraremos que $mcm[a, b]$ divide c. Por el algoritmo de la división sabemos que existen dos enteros q y r tales que

$$c = q \cdot mcm[a, b] + r$$

y $0 \leq r < mcm[a, b]$. Por lo tanto

$$r = c - q \cdot mcm[a, b].$$

Como c y $mcm[a, b]$ son múltiplos de a y b, entonces de la ecuación anterior se deduce que r es múltiplo de a y b (¿por qué?). Como $mcm[a, b]$ es el menor múltiplo común positivo de a y b y $0 \leq r < mcm[a, b]$, entonces concluimos que $r = 0$. Esto dice que $mcm[a, b]$ divide a c.

2. Como $mcd(a, b)$ es un divisor común de a y b, entonces $\frac{ab}{mcd(a,b)}$ es un múltiplo común de a y b. Usando la parte (i) tenemos que $mcm[a, b]$ divide a $\frac{ab}{mcd(a,b)}$. Como $mcm[a, b]$ es un múltiplo común de a y b, entonces existen enteros q y p tales que

$$mcm[a, b] = qa = pb.$$

Usando 5.27 sabemos que existen dos enteros x_0 y y_0 tales que

$$mcd(a,b) = ax_0 + by_0.$$

De esta última ecuación se deduce que

$$1 = \frac{a}{mcd(a,b)}x_0 + \frac{b}{mcd(a,b)}y_0.$$

Multiplicando por $mcm[a,b]$ y usando el hecho que $mcm[a,b] = qa = pb$ obtenemos que

$$\begin{aligned} mcm[a,b] &= mcm[a,b]\frac{a}{mcd(a,b)}x_0 + mcm[a,b]\frac{b}{mcd(a,b)}y_0 \\ &= pb\frac{a}{mcd(a,b)}x_0 + qa\frac{b}{mcd(a,b)}y_0 \\ &= (px_0 + qy_0)\frac{ab}{mcd(a,b)}. \end{aligned}$$

Esto muestra que $\frac{ab}{mcd(a,b)}$ divide a $mcm[a,b]$. Pero ya vimos que $mcm[a,b]$ divide a $\frac{ab}{mcd(a,b)}$ y ambos son enteros positivos, por lo tanto

$$mcm[a,b] = \frac{ab}{mcd(a,b)}.$$

3. De 5.31(v) sabemos que $(ka,kb) = k \cdot mcd(a,b)$ y usando lo probado en (ii) obtenemos que

$$\begin{aligned} [ka,kb] &= \frac{ka \cdot kb}{mcd(ka,kb)} \\ &= \frac{k^2ab}{k \cdot mcd(a,b)} \\ &= k\frac{ab}{mcd(a,b)} \\ &= k \cdot mcm[a,b]. \end{aligned}$$

□

Si conocemos la representación de los entero a y b como producto de primos, entonces es fácil conseguir $mcm[a,b]$. Supongamos que

$$\begin{aligned} a &= p_1^{m_1} \cdot p_2^{m_2} \cdots p_k^{m_k} \\ b &= p_1^{n_1} \cdot p_2^{n_2} \cdots p_k^{n_k}, \end{aligned}$$

donde cada m_i y n_i es un entero no negativo (alguno de ellos puede ser igual a cero). Nótese que ésta no es la forma canónica mencionada en el párrafo anterior. Tenemos entonces que

$$mcm[a,b] = p_1^{\text{máx}\{m_1,n_1\}} \cdot p_2^{\text{máx}\{m_2,n_2\}} \cdots p_k^{\text{máx}\{m_k,n_k\}},$$

donde mín$\{m_i, n_i\}$ es el menor de los enteros m_i y n_i y máx$\{m_i, n_i\}$ es el mayor de los enteros m_i y n_i. Por ejemplo: $1998 = 2^1 \cdot 3^3 \cdot \cdot 7^0 \cdot 37^1 \cdot 73^0$ y $9198 = 2^1 \cdot 3^2 \cdot 7^1 \cdot 37^0 \cdot 73^1$. Por lo tanto

$$mcm[1998, 9198] = 2^1 \cdot 3^3 \cdot 7^1 \cdot 37^1 \cdot 73^1 = 1020978.$$

Ejercicios 5.11

1. Determine el mínimo común múltiplo de los siguientes números:

   a) 24, 88

   b) 28974794, 2

   c) 34, 45

   d) 3, 5, 8

   e) 12, 6, 34, 14.

2. Suponga que el mínimo común múltiplo de los números 2^n, 3 y 5 es 240 . Halle n.

3. Sea n un entero positivo, determine $mcm[n, n+1]$.

4. Halle todos los enteros positivos a y b tales que $mcd(a,b) = 10$ y $mcm[a,b] = 100$.

5. Halle el menor número natural que es a la vez suma de 9 naturales consecutivos, suma de 10 naturales consecutivos y suma de 11 naturales consecutivos.

6. Sean a y b enteros positivos tales que $a|b$. Determine los valores de $mcd(a,b)$ y $mcm[a,b]$.

7. Dados dos enteros positivos d y l. Pruebe que existen enteros a y b tales que $mcd(a,b) = d$ y $mcm[a,b] = l$ si, y sólo si, $d|l$.

8. Daniel intercambió los dígitos de un número de 3 cifras diferentes, de modo que ninguno de ellos quedó en su posición original. Después buscó la diferencia entre esos dos números y ésta resultó ser un número de dos cifras que es cuadrado perfecto. Halle cuatro de los resultados que pudo obtener Daniel.

5.12. Algunas propiedades de los números primos

Comenzaremos mostrando que existe una única factorización de un número entero. Para hacerlo, necesitaremos la siguiente proposición.

Proposición 5.43. *Si p es primo y $p|ab$ entonces $p|a$ ó $p|b$. En general, si $a_1, a_2, \cdots, a_n$ son enteros, p es primo y $p|(a_1 \cdot a_2 \cdots a_n)$, entonces p divide a algún a_i.*

Demostración: Si $p|a$, no hay nada que mostrar. Supongamos que $p \not| a$, como p es primo, entonces $(a, p) = 1$. Como $p|ab$ y $(a, p) = 1$ podemos usar 5.31(iii) y concluir que $p|b$. La segunda afirmación se prueba de manera similar. □

Veamos, finalmente, que los primos que aparecen en la descomposición de un entero son únicos. Haremos la prueba por reducción al absurdo. Supongamos que existe un entero a con dos factorizaciones. Es decir, que existen dos colecciones de números primos $p_1, p_2, \cdots p_n$ y $q_1, q_2, \cdots q_m$ tales que

$$a = p_1 \cdot p_2 \cdots p_n = q_1 \cdot q_2 \cdots q_m.$$

Podemos suponer que $n \leq m$. Cancelando los p_i que aparecen en la lista $q_1, q_2, \cdots q_m$, podemos suponer que $p_i \neq q_j$ para todo $i \leq n$ y $j \leq m$. Por 5.43 sabemos que $p_1|q_j$ para algún j. Pero p_1 y q_j son primos, por lo tanto $p_1 = q_j$. Y esto es una contradicción. □

Ahora mostraremos un resultado antiquísimo pues ya Euclides lo conocía.

Teorema 5.44. *(Euclides) La colección de números primos es infinita.*

Demostración: La demostración la haremos por reducción al absurdo. Supongamos que $p_1, p_2, \cdots, p_n$ son todos los números primos. Sea

$$a = p_1 \cdot p_2 \cdots p_n + 1.$$

Mostraremos primero que $p_i \not| a$ para cada $i \leq n$. Pues si existiera un entero k tal que $a = kp_i$, entonces

$$kp_i - p_1 \cdot p_2 \cdots p_n = 1.$$

Por lo tanto

$$p_i \cdot (k - p_1 \cdot p_2 \cdots p_{i-1} \cdot p_{i+1}) = 1.$$

En consecuencia $p_i = 1$ y esto contradice que p_i es un número primo.

Por el teorema Fundamental de la Aritmética sabemos que a se escribe como un producto de números primos. Sea p un primo que divide a a, hemos mostrado antes que $p \neq p_i$ para cada $i \leq n$. Esto contradice nuestra suposición de que $p_1, p_2, \cdots, p_n$ era una lista completa de todos los números primos. □

El teorema anterior nos dice que existe una cantidad infinita de números primos. Ahora bién, aunque haya tal cantidad de primos, ellos tienden a estar separados por muchos números que no son primos. En efecto, sea n un natural cualquiera y considere la siguiente colección de n enteros consecutivos:

$$(n+1)! + 2, (n+1)! + 3, (n+1)! + 4, \cdots, (n+1)! + n, (n+1)! + (n+1).$$

Para cada k con $2 \leq k \leq n+1$, tenemos que $(n+1)! + k$ es divisible por k, y por consiguiente no es primo.

Por ejemplo, la siguiente lista de 10 números consecutivos son todos compuestos. Notemos que $11! = 39916800$

39916802 39916803 39916804 39916805 39916806

39916807 39916808 39916809 39916810 39916811

El problema de determinar si un número es primo o compuesto no es fácil y por consiguiente el problema de factorizar un número en sus factores primos es, en general, una tarea compleja. El siguiente resultado es útil para reducir el número de pasos en la verificación de si un número es o no primo.

Teorema 5.45. *Sea n un entero. Si n es compuesto, entonces existe un primo p tal que $p|n$ y $p \leq \sqrt{n}$.*

Demostración: La haremos por reducción al absurdo. Supongamos que n es un entero positivo compuesto tal que todos sus factores primos son mayores que $\sqrt{n}$. Sean p_1 y p_2 dos factores primos de n, es decir, que $n = p_1 \cdot p_2 \cdot b$ para algún entero $b \geq 1$. Por hipótesis, estamos suponiendo que $\sqrt{n} < p_1$ y $\sqrt{n} < p_2$. De esto se deduce que $n < p_1 \cdot p_2$. Lo cual es una contradicción, pues $p_1 \cdot p_2 \leq n$. □

Observemos que la contrarecíproca de la proposición anterior dice:

Si para todo primo $p \leq \sqrt{n}$ se cumple que p no divide a n, entonces n es un número primo.

Esto provee un método para determinar más rápidamente si un número es primo.

Ejemplo 5.46. Queremos determinar si 247 es primo. Primero estimamos el valor de $\sqrt{247}$. Tenemos que $15 < \sqrt{247} < 16$. Por consiguiente sólo debemos verificar si alguno de los primos menores que 15 es divisor de 247. Los primos menores que 15 son: 2, 3, 5, 7, 11 y 13. Como 13 divide a 247, entonces 247 es compuesto. Podemos ahora factorizar 247 y obtenemos que $247 = 13 \cdot 19$. Como 19 es primo, hemos conseguido todos los factores primos de 247. □

Ejemplo 5.47. ¿Será 983 un número primo? Tenemos que $\sqrt{983} < 32$ y los primos menores que 32 son

$$2,\ 3,\ 5,\ 7,\ 11,\ 13,\ 17,\ 19,\ 23,\ 29,\ 31.$$

Podemos verificar fácilmente que ninguno de estos primos divide a 983. Por lo tanto 983 es primo. □

Con este criterio a la mano se facilita hacer tablas de primos. Un método bien conocido es la *criba de Eratóstenes*. Este método permite determinar todos los números primos menores que un número prefijado n. El primer paso consiste en hacer una tabla con todos los números menores que n. El siguiente paso consiste en tachar todos los múltiplos de 2 excepto el 2. Después sistemáticamente se tachan todos los múltiplos del primer número no tachado (en el segundo paso sería el 3) excepto él mismo. Observe que el primer número no tachado después de cada paso es necesariamente un número primo (¿por qué?). Continuamos con este proceso hasta haber tachado todos los números que son múltiplo de algún primo menor o igual a $\sqrt{n}$. Al finalizar, los números no tachados son todos los primos menores o iguales a n.

Ejemplo 5.48. Del conjunto $\{1, 2, 3, 4, \cdots, 360\}$ escogemos 8 números compuestos. Veremos que por lo menos 2 de ellos son divisibles por un mismo primo. En efecto, notemos primero que $\sqrt{360} < 19$ y los primos menores que 19 son: 2,3,5,7,11,13 y 17. Por la proposición 5.45 sabemos que cada número compuesto menor o igual que 360 debe ser divisible por alguno de los 7 primos menores que 19. Por consiguiente de los 8 números compuestos escogidos al menos dos de ellos son ambos divisibles por uno de los 7 primos menores que 19. □

Ejercicios 5.12

1. Halle la descomposición en factores primos de los siguientes números: 156, 168, 249, 1.997, 2.764, 54.653, 202.020, 397.902.050 (*Sugerencia:* No trabaje más de la cuenta, use el criterio dado en la proposición 5.45).

2. Usando el procedimiento descrito como la Criba de Eratóstenes hacer una tabla de todos los primos menores que 200.

3. Diremos que dos números impares $a < b$ son consecutivos si $b - a = 2$. Por ejemplo: 5 y 7 son consecutivos. Para cada natural n muestre que existen n números impares consecutivos todos ellos compuestos. Halle 5 números compuestos que sean impares consecutivos.

4. Sea $\mathbb{N}^*$ el conjunto de números naturales mayores que 1. Definimos una función $f : \mathbb{N}^* \to \mathbb{N}$ dada por

   $$f(n) = \text{número de factores primos en la factorización de } n.$$

   Por ejemplo: $f(2) = 1$; $f(4) = 2$ (pues $4 = 2 \cdot 2$); $f(6) = 2$ (pues $6 = 2 \cdot 3$); $f(12) = 3$ (pues $12 = 2 \cdot 2 \cdot 3$). Muestre que

   $$2^{f(n)} \leq n$$

   para todo natural $n > 1$.

5. Sean p y q primos tales que $q > 3$ y $p = q + 2$. Muestre que $12|(p + q)$.

6. Sean $a \geq 2$, $n \geq 2$. Muestre que si $a^n - 1$ es primo, entonces $a = 2$. Halle los primeros 4 valores de n tales que $2^n - 1$ es primo. Por ejemplo, $2^2 - 1 = 3$ es primo. Los números de la forma $2^n - 1$ se llaman números de Mersenne, y los primos de la forma $2^n - 1$ se conocen como primos de Mersenne. (*Sugerencia:* Use la identidad $a^n - 1 = (a - 1)(a^{n-1} + a^{n-2} + \cdots + a + 1)$).

7. Si $2^n - 1$, con $n > 2$ es primo, entonces $2^n + 1$ es compuesto. (*Sugerencia:* Use el ejercicio 5).

5.13. La relación de congruencia

En esta sección estudiaremos una relación entre enteros que juega un papel muy importante en el estudio de los números. Nos referimos a la relación de congruencia. Esta relación fué introducida por Gauss.

Definición 5.49. *Sea $m > 1$ un entero. Diremos que dos enteros a y b son* ***congruentes módulo*** *m si $a - b$ es divisible por m. La relación de congruencia se denota por*

$$a \equiv b \,mód\, m.$$

Definición 5.50. *Sea m un entero positivo y b un entero cualquiera. El conjunto*

$$\{x : x \equiv b \,mód\, m\}$$

se llama la clase de congruencia de b módulo m.

Ejemplos 5.51. 1. $17 \equiv 5 \,\text{mód}\, 3$, $17 \equiv 2 \,\text{mód}\, 3$, $14 \equiv 4 \,\text{mód}\, 5$, $17 \equiv 5 \,\text{mód}\, 4$, $17 \equiv 1 \,\text{mód}\, 4$ y $16 \equiv 0 \,\text{mód}\, 4$.

2. En caso que a no sea congruente con b módulo m escribiremos $a \not\equiv b \,\text{mód}\, m$. Por ejemplo: $17 \not\equiv 1 \,\text{mód}\, 3$, $14 \not\equiv 3 \,\text{mód}\, 5$, $17 \not\equiv 2 \,\text{mód}\, 4$.

3. La clase de congruencia de 3 módulo 5 es

$$\{x : x \equiv 3 \,\text{mód}\, 5\} = \{\cdots, -12, -7 - 2, 3, 8, 13, 18, 23, \cdots\}.$$

4. La clase de congruencia de 3 módulo 6 es

$$\{x : x \equiv 3 \,\text{mód}\, 6\} = \{\cdots, -15, -9, -3, 3, 9, 15, 21, 27, \cdots\}.$$

□

El siguiente resultado nos dice que la relación de congruencia está estrechamente relacionada con el Algoritmo de la división.

Teorema 5.52. *Sean a, b, m enteros con $m > 0$. a y b son congruentes módulo m si, y solamente si, a y b dejan el mismo resto al dividirlos por m. Además, si r es el resto de dividir a por m entonces, $a \equiv r$ mód m. Por lo tanto, todo entero es congruente módulo m con uno y sólo uno de los siguientes enteros $0, 1, 2, \cdots, m - 1$.*

Demostración: Primero probaremos que si $a \equiv b \,\text{mód}\, m$, entonces a y b dejan el mismo resto al dividirlos por m. Supongamos entonces que $a \equiv b \,\text{mód}\, m$. Por el algoritmo de la división existen enteros q, q', r y r' tales que

$$a = qm + r$$
$$b = q'm + r'$$

y además $0 \leq r < m$ y $0 \leq r' < m$. Restando miembro a miembro estas dos ecuaciones obtenemos que

$$a - b = (q - q')m + (r - r').$$

Como $a \equiv b \,\text{mód}\, m$, entonces $a - b$ es divisible por m. En consecuencia tenemos que $r - r'$ también es divisible por m. Pero es claro que $-m < r - r' < m$. Por lo tanto $r - r' = 0$, es decir $r = r'$.

Ahora probaremos que si a y b dejan el mismo resto al dividirlos por m, entonces $a \equiv b \,\text{mód}\, m$. Sea r el resto que dejan a y b al dividirlos por m, y sean q y q' los respectivos cocientes, es decir tenemos que

$$\begin{aligned} a &= qm + r \\ b &= q'm + r \end{aligned}$$

y además sabemos que $0 \leq r < m$. Como antes, restando estas dos ecuaciones obtenemos que $a - b = (q - q')m$ y esto nos dice que $a \equiv b \,\text{mód}\, m$.

Para finalizar, observemos que si $a = qm + r$ con $0 \leq r < m$, es claro que $a - r$ es divisible por m y por lo tanto $a \equiv r \,\text{mód}\, m$. Por otra parte, si $0 \leq r, r' < m$ y $r \neq r'$, entonces por lo visto anteriormente $a \not\equiv r' \,\text{mód}\, m$. De esto se deduce que todo entero es congruente módulo m con uno, y sólo uno, de los siguientes enteros $0, 1, 2, \cdots, m - 1$. □

Veamos lo que dice el teorema anterior para algunos casos particulares.

Ejemplos 5.53. 1. Para $m = 2$ tenemos que todo entero es congruente módulo 2 con 0 o con 1. Así que los enteros quedan divididos en dos clases:

$$\cdots, -6, -4, -2, 0, 2, 4, 6, \cdots \quad n \text{ tales que } n \equiv 0 \,\text{mód}\, 2$$

$$\cdots, -5, -3, -1, 1, 3, 5, 7, \cdots \quad n \text{ tales que } n \equiv 1 \,\text{mód}\, 2.$$

Es decir, la relación de congruencia módulo 2 divide a los enteros en pares e impares. Los pares forman la clase de congruencia del 0 módulo 2 y los impares forman la clase de congruencia del 1 módulo 2.

2. Para $m = 3$ tenemos que todo entero es congruente módulo 3 con 0, con 1 o con 2. Los enteros quedan entonces divididos en tres clases:

$$\cdots, -9, -6, -3, 0, 3, 6, 9, \cdots \quad n \text{ tales que } n \equiv 0 \,\text{mód}\, 3$$

$$\cdots, -8, -5, -2, 1, 4, 7, 10, \cdots \quad n \text{ tales que } n \equiv 1 \,\text{mód}\, 3$$

$$\cdots, -7, -4, -1, 2, 5, 8, 11, \cdots \quad n \text{ tales que } n \equiv 2 \,\text{mód}\, 3.$$

La primera es la clase de congruencia del 0 módulo 3, la segunda es la clase de congruencia del 1 módulo 3 y la tercera es la clase de congruencia del 2 módulo 3.

3. En general hay m clases de congruencia módulo m.

□

Algunas de las propiedades más importantes de la relación de congruencias son las siguientes.

Teorema 5.54. *Sean a, b, c, d, m enteros con $m > 0$. Se tiene que*

1. $a \equiv a \pmod{m}$.
2. *Si* $a \equiv b \pmod{m}$, *entonces* $b \equiv a \pmod{m}$.
3. *Si* $a \equiv b \pmod{m}$ *y* $b \equiv c \pmod{m}$, *entonces* $a \equiv c \pmod{m}$.
4. *Si* $a \equiv b \pmod{m}$ *y* $c \equiv d \pmod{m}$, *entonces* $a + c \equiv b + d \pmod{m}$ *y* $a - c \equiv b - d \pmod{m}$.
5. *Si* $a \equiv b \pmod{m}$ *y* $c \equiv d \pmod{m}$, *entonces* $ac \equiv bd \pmod{m}$.
6. *Si* $a \equiv b \pmod{m}$, *entonces para todo natural* n *se cumple que* $a^n \equiv b^n \pmod{m}$.

Demostración: Demostraremos algunas de las afirmaciones y las otras las dejamos como ejercicio.

(3) Supongamos que $a \equiv b \pmod{m}$ y $b \equiv c \pmod{m}$, entonces existen enteros k y k' tales que $a - b = km$ y $b - c = k'm$. Sumando miembro a miembro estas dos igualdades obtenemos que $a - c = (k + k')m$. Por lo tanto $a \equiv c \pmod{m}$.

(4) Supongamos que $a \equiv b \pmod{m}$ y $c \equiv d \pmod{m}$, entonces existen enteros k y k' tales que $a - b = km$ y $c - d = k'm$. Sumando miembro a miembro estas dos igualdades obtenemos que $a + c - b - d = (k + k')m$. Por lo tanto $a + c - (b + d) = (k + k')m$ y de esto obtenemos que $a + c \equiv b + d \pmod{m}$. De manera similar restando ambas igualdades obtenemos $a - c \equiv b - d \pmod{m}$.

(5) Supongamos que $a \equiv b \pmod{m}$ y $c \equiv d \pmod{m}$, entonces existen enteros k y k' tales que $a - b = km$ y $c - d = k'm$. Por lo tanto $a = b + km$ y $c = d + k'm$. Multiplicando miembro a miembro esta dos igualdades obtenemos

$$ac = bd + bk'm + dkm + kk'm^2.$$

Por lo tanto $ac - bd = (bk' + dk + kk'm)m$ y esto nos dice que $ac \equiv bd \pmod{m}$.

□

La propiedades anteriores nos dicen que la relación de congruencia se comporta, en muchos casos, como la relación de igualdad. Podemos sumar, restar y multiplicar congruencias de la misma forma que lo hacemos con las ecuaciones. Por ejemplo, si tenemos que

$$\begin{aligned} a &\equiv b \pmod{m} \\ c &\equiv 3 \pmod{m} \\ 5 &\equiv d \pmod{m}. \end{aligned}$$

Entonces también tenemos que

$$\begin{gathered} a+c+5 \equiv b+3+d \,\text{mód}\, m \\ 5ac \equiv 3bd \,\text{mód}\, m \\ a-c+5 \equiv b-3+d \,\text{mód}\, m \\ ac+5 \equiv 3b+d \,\text{mód}\, m \\ a^2 \equiv b^2 \,\text{mód}\, m \\ a^n \equiv b^n \,\text{mód}\, m. \end{gathered}$$

Sin embargo, en general, al dividir ambos miembros de una congruencia no necesariamente obtenemos números que sean congruentes. Por ejemplo, $12 \equiv 6 \,\text{mód}\, 2$, pero al dividir por 2 a ambos miembros no obtenemos números congruentes módulo 2, pues $6 \not\equiv 3 \,\text{mód}\, 2$. El siguiente resultado nos dice cuándo podemos factorizar los miembros de una congruencia.

Proposición 5.55. *Sean a, b, c, m enteros con $m > 0$. Se tiene que*

1. *$ab \equiv ac$ mód m si, y sólo si, $b \equiv c$ mód $\frac{m}{(a,m)}$.*

2. *Si $(a, m) = 1$ y $ab \equiv ac$ mód m, entonces $b \equiv c$ mód m.*

Demostración:

1. Debemos mostrar dos cosas:

   a) Supongamos que $ab \equiv ac \,\text{mód}\, m$ y mostremos que $b \equiv c \,\text{mód}\, \frac{m}{(a,m)}$. Por hipótesis tenemos que $m|a(b-c)$. Luego $\frac{m}{(a,m)} \mid \frac{a}{(a,m)}(b-c)$. Como $\frac{m}{(a,m)}$ y $\frac{a}{(a,m)}$ son primos entre sí, se concluye de la proposición 5.31(v) que $\frac{m}{(a,m)}$ divide a $b-c$.

   b) Ahora supondremos que $b \equiv c \,\text{mód}\, \frac{m}{(a,m)}$ y mostraremos que $ab \equiv ac \,\text{mód}\, m$. Por hipótesis tenemos que $b-c$ es divisible por $\frac{m}{(a,m)}$. Luego m divide a $(a,m) \cdot (b-c)$ y como (a, m) divide a a, entonces se deduce que m divide a $a(b-c)$.

2. Supongamos que $(a, m) = 1$ y que $ab \equiv ac \,\text{mód}\, m$. Entonces m divide a $a(b-c)$. Por la parte (ii) del teorema 5.31 tenemos que m divide a $b-c$. En otras palabras, hemos mostrado que $b \equiv c \,\text{mód}\, m$.

□

Ejemplo 5.56. Por ejemplo, si $3b \equiv 6 \,\text{mód}\, 9$ para algún entero b, entonces podemos también afirmar que $b \equiv 2 \,\text{mód}\, 3$, pues $(3, 9) = 3$ y podemos hacer uso de la parte (i) del teorema anterior. Sin embargo, no es necesariamente cierto que $b \equiv 2 \,\text{mód}\, 9$; por ejemplo, sustituyendo b por 5 obtenemos que $15 \equiv 6 \,\text{mód}\, 9$ y obviamente $5 \equiv 2 \,\text{mód}\, 3$ y $5 \not\equiv 2 \,\text{mód}\, 9$. □

5.13.1. ¿Cómo se usan las congruencias?

La relación de congruencia es muy útil para estudiar las propiedades de los enteros. Veremos a continuación algunas de las aplicaciones de las congruencias.

Ejemplo 5.57. 1. Observemos que

$$10^n \equiv 0 \,\text{mód}\, 10$$

para todo $n \geq 1$. En consecuencia tenemos también que

$$a \cdot 10^n \equiv 0 \,\text{mód}\, 10$$

para todo natural a.

2. La notación normalmente usada para representar los números es la decimal. Por ejemplo, 1245 corresponde a

$$1 \cdot 10^3 + 2 \cdot 10^2 + 4 \cdot 10^1 + 5 \cdot 10^0.$$

Observemos que la cifra de las unidades corresponde al resto de dividir un número entre 10. Usando lo observado en la parte anterior y el hecho que podemos sumar congruencias obtenemos que

$$1 \cdot 10^3 + 2 \cdot 10^2 + 4 \cdot 10^1 + 5 \cdot 10^0 \equiv 5 \,\text{mód}\, 10.$$

3. ¿Cuál es la última cifra de 3^{400}? Ya vimos que la última cifra en la representación decimal de un número es precisamente el resto de dividir el número por 10. En otras palabras, si a es la última cifra en la representación decimal de n, entonces $n \equiv a \,\text{mód}\, 10$. Así que lo que queremos hallar es el único entero a entre 0 y 9 tal que $3^{400} \equiv a \,\text{mód}\, 10$. Calculemos entonces la clase de congruencia módulo 10 de las potencias de 3. Usaremos repetidamente la siguiente propiedad de las congruencias: si $a \equiv b \,\text{mód}\, m$, entonces $ca \equiv cb \,\text{mód}\, m$ para todo entero c.

$$\begin{aligned}
3 &\equiv 3 \,\text{mód}\, 10\\
3^2 &\equiv 9 \,\text{mód}\, 10\\
3^3 &\equiv 27 \,\text{mód}\, 10\\
27 &\equiv 7 \,\text{mód}\, 10\\
3^3 &\equiv 7 \,\text{mód}\, 10\\
3^4 &\equiv 21 \,\text{mód}\, 10\\
21 &\equiv 1 \,\text{mód}\, 10\\
3^4 &\equiv 1 \,\text{mód}\, 10.
\end{aligned}$$

De esta última ecuación se deduce que

$$\begin{aligned}
(3^4)^{100} &\equiv 1^{100} \,\text{mód}\, 10\\
3^{400} &\equiv 1 \,\text{mód}\, 10.
\end{aligned}$$

Por consiguiente, la última cifra de 3^{400} es 1.

□

Ejemplo 5.58. ¿Cuál es el resto de dividir 8^6 entre 5? Para responder esta pregunta basta conseguir el único entero r con $0 \leq r \leq 4$ tal que $8^6 \equiv r \,\text{mód}\, 5$. Calculemos la clase de congruencia módulo 5 de las potencias de 8.

$$
\begin{array}{rl}
8 \equiv 3 \,\text{mód}\, 5 & \\
8^2 \equiv 3^2 \,\text{mód}\, 5 & \\
8^2 \equiv 9 \,\text{mód}\, 5 & \\
9 \equiv 4 \,\text{mód}\, 5 & \\
8^2 \equiv 4 \,\text{mód}\, 5 & \text{Multiplicando por } 8 \equiv 3 \,\text{mód}\, 5 \text{ obtenemos} \\
8^3 \equiv 12 \,\text{mód}\, 5 & \\
12 \equiv 2 \,\text{mód}\, 5 & \\
8^3 \equiv 2 \,\text{mód}\, 5 & \text{Multiplicando por } 8 \equiv 3 \,\text{mód}\, 5 \text{ obtenemos} \\
8^4 \equiv 6 \,\text{mód}\, 5 & \\
6 \equiv 1 \,\text{mód}\, 5 & \\
8^4 \equiv 1 \,\text{mód}\, 5 & \text{Multiplicando por } 8 \equiv 3 \,\text{mód}\, 5 \text{ obtenemos} \\
8^5 \equiv 3 \,\text{mód}\, 5 & \\
9 \equiv 4 \,\text{mód}\, 5 & \\
8^6 \equiv 4 \,\text{mód}\, 5 &
\end{array}
$$

Hemos mostrado que el resto de dividir 8^6 entre 5 es 4.

□

Ejemplo 5.59. Haremos uso de las propiedades de las congruencias para probar algunos criterios de divisibilidad. Sea a un número natural y $c_n, c_{n-1}, \cdots, c_2, c_1, c_0$ los dígitos de su representación decimal, es decir,

$$a = c_0 + c_1 \cdot 10 + c_2 \cdot 10^2 + \cdots + c_{n-1} \cdot 10^{n-1} + c_n \cdot 10^n. \tag{5.13}$$

1. **Criterio de divisibilidad por 3**. Observemos que $10 \equiv 1 \,\text{mód}\, 3$ y por consiguiente para todo i se tiene que $10^i \equiv 1 \,\text{mód}\, 3$. Multiplicando ésta última congruencia por c_i con $0 \leq i \leq n$ obtenemos

   $$c_0 \equiv c_0 \,\text{mód}\, 3 \quad c_1 10 \equiv c_1 \,\text{mód}\, 3 \quad c_2 10^2 \equiv c_2 \,\text{mód}\, 3 \quad \cdots \quad c_n 10^n \equiv c_n \,\text{mód}\, 3.$$

   Sumando miembro a miembro todas estas congruencias obtenemos

   $$c_0 + c_1 10 + c_2 10^2 + \cdots + c_n 10^n \equiv c_0 + c_1 + \cdots + c_n \,\text{mód}\, 3. \tag{5.14}$$

   De (5.13) obtenemos entonces que

   $$a \equiv c_0 + c_1 + \cdots + c_n \,\text{mód}\, 3.$$

   Esta última congruencia nos dice que todo número es congruente módulo 3 con la suma de sus dígitos. Por consiguiente, a es divisible por 3 si y sólo si la suma de sus dígitos es divisible por 3.

   Veamos algunos ejemplos: (a) 1327 no es divisible por 3, pues $1 + 3 + 2 + 7 = 13$ y 13 no es divisible por 3. (b) 62130 es divisible por 3, pues $6 + 2 + 1 + 3 + 0 = 12$ y 12 es divisible por 3.

2. **Criterio de divisibilidad por 11**. Observemos que $10 \equiv -1 \,\text{mód}\, 11$ y que $10^2 \equiv 1 \,\text{mód}\, 11$. Se puede probar que en general $10^{2m+1} \equiv -1 \,\text{mód}\, 11$ y $10^{2m} \equiv 1 \,\text{mód}\, 11$, es decir las potencias impares de 10 son congruentes con 1 módulo 11 y las potencias pares lo son con 1 (ver ejercicio 5). Al igual que hicimos en la prueba del criterio de divisibilidad por 3 se tiene que

$$\begin{aligned} &c_0 \equiv c_0 \,\text{mód}\, 11 \\ &c_1 10 \equiv -c_1 \,\text{mód}\, 11 \\ &c_2 10^2 \equiv c_2 \,\text{mód}\, 11 \\ &\vdots \\ &c_n 10^n \equiv (-1)^n c_n \,\text{mód}\, 11. \end{aligned}$$

Hemos recurrido al siguiente "truco" para no tener que preocuparnos de la paridad de n: $(-1)^n$ es igual a 1 cuando n es par y es igual a -1 cuando n es impar.

Como antes, sumamos miembro a miembro todas estas desigualdades y obtenemos que

$$c_0 + c_1 10 + c_2 10^2 + \cdots + c_n 10^n \equiv c_0 - c_1 + c_2 \cdots + (-1)^n c_n \,\text{mód}\, 11$$

Y por (5.13) obtenemos entonces que

$$a \equiv c_0 - c_1 + c_2 - \cdots + (-1)^n c_n \,\text{mód}\, 11.$$

De ésta última congruencia se deduce que a es divisible por 11 si y sólo si $c_0 - c_1 + c_2 - \cdots + (-1)^n c_n$ es divisible por 11.

Veamos unos ejemplos:

(a) 987654321 no es divisible por 11, pues $1-2+3-4+5-6+7-8+9 = 5$. Sabemos además que $987654321 \equiv 5 \,\text{mód}\, 11$.

(b) 111111 es divisible por 11, pues 1-1+1-1+1-1=0. De la misma manera podemos ver que el número $11111\cdots1$ que consiste de n 1 seguidos será divisible por 11 si y sólo si n es par.

5.13.2. Ecuaciones de congruencia

Consideremos el problema de hallar los valores de x tales que

$$15x \equiv 6 \,\text{mód}\, 9.$$

Por simple inspección vemos que 1 es una solución, pues $15 \equiv 6 \,\text{mód}\, 9$, también 4, 7, -2 son soluciones (verifíquelo!). En esta sección estudiaremos cómo hallar todas las soluciones de ecuaciones de este tipo. En general, una **ecuación lineal de congruencia** es una expresión de la forma

$$ax \equiv b \,\text{mód}\, m. \tag{5.15}$$

Nos interesa hallar los valores de x que satisfacen (5.15). Primero veremos un criterio para determinar cuándo existe una solución y después nos preocuparemos de cómo hallar todas las soluciones.

Por definición de congruencia sabemos que (5.15) tiene una solución si y sólo si existen x y y tales que $ax - b = ym$. Es decir, si y sólo si la ecuación diofántica $ax - ym = b$ tiene solución. Sabemos por el teorema 5.37 que esto ocurre si y sólo si $(a, m)|b$. Esto provee un criterio para decidir cuándo una ecuación lineal de congruencia tiene solución. El siguiente teorema resuelve completamente el problema.

Teorema 5.60. *Sean a, b, m enteros con $m > 1$. La ecuación lineal de congruencia*

$$ax \equiv b \, mód \, m$$

tiene solución si, y sólo si, $mcd(a, m)|b$. Además, si x_0 es una solución de (5.15) (la cual llamaremos solución particular), entonces el conjunto solución de (5.15) es

$$\{x : x \equiv x_0 \, mód \, \tfrac{m}{mcd(a,m)}\}.$$

Demostración: Ya dijimos que la ecuación 5.15 tiene solución si, y sólo, si existen x e y tales que $ax - b = my$, o de forma equivalente, si, y sólo si, existen x e y que sean solución de la ecuación diofántica $ax - my = b$. Por el teorema 5.37 sabemos que ésta ecuación diofántica tiene solución si, y sólo si, $mcd(a, m)|b$. Esto muestra la primera parte del teorema.

Ahora supondremos que conocemos una solución particular x_0 de la ecuación de congruencia $ax \equiv b \,\text{mód}\, m$; en otras palabras, supondremos que tenemos un entero x_0 que satisface $ax_0 \equiv b \,\text{mód}\, m$. Por lo tanto existe un y_0 tal que $ax_0 - my_0 = b$. Por el teorema 5.37 sabemos que todas las soluciones de la ecuación $ax - my = b$ vienen dadas por las fórmulas

$$x = x_0 + \frac{m}{mcd(a, m)}k \ , \quad y = y_0 - \frac{a}{mcd(a, m)}k \ , \quad \text{con } k \in \mathbb{Z}$$

para algún entero k. Esto dice que las soluciones de la ecuación de congruencia $ax \equiv b \,\text{mód}\, m$ vienen dadas por

$$x = x_0 + \frac{m}{mcd(a, m)}k$$

para algún entero k. Lo cual es equivalente a decir que las soluciones de 5.15 son aquellos enteros que satisfacen que

$$x - x_0 = \frac{m}{mcd(a, m)}k$$

para algún entero k. Esto es equivalente a decir que

$$x \equiv x_0 \,\text{mód}\, \tfrac{m}{mcd(a,m)}.$$

□

Observación 5.61. Notemos que el teorema anterior además nos dice que en caso de existir una solución, entonces debe existir una solución entre 0 y $m-1$ (¿Por qué?). □

Ejemplos 5.62. Veamos algunos ejemplos:

1. Consideremos la ecuación

$$15x \equiv 6 \,\text{mód}\, 9.$$

Siguiendo la nomenclatura del teorema 5.60 tenemos $a = 15$, $b = 6$ y $m = 9$. Como $mcd(15, 9) = 3$ y 3 divide a 6, entonces por el teorema anterior sabemos que la ecuación tiene solución. Ya vimos por simple inspección que 1 es una solución particular, pues $15 \equiv 6 \,\text{mód}\, 9$. Por lo tanto el conjunto solución de la ecuación $15x \equiv 6 \,\text{mód}\, 9$ es

$$\{x : \ \ x \equiv 1 \,\text{mód}\, \tfrac{9}{mcd(15,9)}\} = \{x : \ \ x \equiv 1 \,\text{mód}\, 3\}.$$

En otras palabras, el conjunto solución es la clase de congruencia (módulo 3) del 1. Otras soluciones de la ecuación son: -8, -5, -2, 4, 7, 10, 13.

2. La ecuación $15x \equiv 7 \,\text{mód}\, 9$ no tiene solución pues $mcd(15, 9) \not| 7$.

3. Consideremos la ecuación $7x \equiv 6 \,\text{mód}\, 55$. Ya que $mcd(7, 55) = 1$ sabemos que la ecuación tiene solución. En este caso hallar una solución por inspección no es tan fácil como lo fué en el ejemplo (1). El siguiente teorema nos da un método para resolver este problema.

□

Teorema 5.63. *Sean a, b, m, n enteros con m y n mayores que 1. Se cumple que c es una solución de $ax \equiv b$ mód $[m, n]$ si, y sólo si, c es simultáneamente una solución de las ecuaciones $ax \equiv b$ mód m y $ax \equiv b$ mód n.*

Demostración: Debemos mostrar dos implicaciones:

1. Supongamos que c es una solución de la ecuación $ax \equiv b \,\text{mód}\, [m, n]$. Entonces existe un entero k tal que $ac - b = k[m, n]$. Por la parte 2 del teorema 5.42 sabemos que

$$[m, n] = \frac{mn}{mcd(m, n)}.$$

Por lo tanto tenemos que

$$ac - b = \frac{km}{mcd(m, n)}n$$

y también que

$$ac - b = \frac{kn}{mcd(m, n)}m.$$

Observe que $\frac{kn}{mcd(m,n)}$ y $\frac{km}{mcd(m,n)}$ son enteros (¿por qué ?). Por lo tanto $ac \equiv b \,\text{mód}\, m$ y $ac \equiv b \,\text{mód}\, n$. Esto dice que c es una solución de las dos ecuaciones $ax \equiv b \,\text{mód}\, m$ y $ax \equiv b \,\text{mód}\, n$.

2. Supongamos ahora que c es una solución de $ax \equiv b \,\text{mód}\, m$ y también de $ax \equiv b \,\text{mód}\, n$. Entonces existen enteros k y k' tales que $ac-b = kn$ y $ac-b = k'm$. Por lo tanto $ac-b$ es un múltiplo común de n y de m. Luego por la parte 1 del teorema 5.42 sabemos que $ac - b$ es un múltiplo de $[m, n]$, esto dice que $ac \equiv b \,\text{mód}\, [m, n]$. Por lo tanto c es una solución de $ax \equiv b \,\text{mód}\, [m, n]$.

□

Ejemplo 5.64. Usaremos el teorema 5.63 para resolver la ecuación $7x \equiv 6 \,\text{mód}\, 55$. Notemos que $55 = 5 \cdot 11$ y $[11, 5] = 55$ por lo tanto $7c \equiv 6 \,\text{mód}\, 55$ si y sólo si $7c \equiv 6 \,\text{mód}\, 5$ y $7c \equiv 6 \,\text{mód}\, 11$. En otras palabras, el teorema anterior nos dice que hallar una solución para la ecuación $7x \equiv 6 \,\text{mód}\, 55$ es equivalente a conseguir una solución *común* para las ecuaciones $7x \equiv 6 \,\text{mód}\, 11$ y $7x \equiv 6 \,\text{mód}\, 5$. Tenemos entonces dos ecuaciones que resolver.

(a) *Solución de* $7x \equiv 6 \,\text{mód}\, 5$. Como $6 \equiv 1 \,\text{mód}\, 5$ entonces la ecuación $7x \equiv 6 \,\text{mód}\, 5$ es equivalente a $7x \equiv 1 \,\text{mód}\, 5$ (¿por qué?). Por inspección vemos que 3 es una solución, pues $21 \equiv 1 \,\text{mód}\, 5$. Por lo tanto el conjunto solución es

$$S_a = \{x : x \equiv 3 \,\text{mód}\, 5\} = \{\cdots 3, 8, 13, 18, 23, 28, 33, 38, 43, 48, \cdots\}$$

(b) *Solución de* $7x \equiv 6 \,\text{mód}\, 11$: Vemos por inspección que 4 es una solución, pues $28 \equiv 6 \,\text{mód}\, 11$. Por lo tanto el conjunto solución es

$$S_b = \{x : x \equiv 4 \,\text{mód}\, 11\} = \{\cdots 4, 15, 26, 37, 48, 59, 70, \cdots\}$$

Ya que $48 \in S_a \cap S_b$, entonces 48 es una solución común de $7x \equiv 6 \,\text{mód}\, 11$ y $7x \equiv 6 \,\text{mód}\, 5$. Por el teorema 5.63 sabemos que 48 es una solución de $7x \equiv 6 \,\text{mód}\, 55$. Ahora por el teorema 5.60 el conjunto solución de ésta última ecuación es

$$\{x \in \mathbb{Z} : \ x \equiv 48 \,\text{mód}\, 55\}.$$

□

A continuación enunciamos un resultado importante sobre las congruencias.

Teorema 5.65. *(Fermat) Sea p un número primo y a un entero tal que $p \not| a$, entonces se cumple que*

$$a^{p-1} \equiv 1 \,\text{mód}\, p.$$

□

No presentaremos la demostración de este resultado. Usaremos el Teorema de Fermat para mostrar otros resultados interesantes. Observemos que la hipótesis que $p \not| a$ es necesaria, pues por ejemplo con $p = 3$ y $a = 9$, tenemos que 9^2 es divisible por 3 y por consiguiente $9^2 \equiv 0 \,\text{mód}\, 3$. Sin embargo, podemos enunciar un resultado que no requiere esa hipótesis.

Teorema 5.66. *Sea p un número primo y a un entero, entonces se cumple que*

$$a^p \equiv a \text{ mód } p.$$

Demostración: En efecto, hay dos casos posibles: $p \not| a$ o $p|a$. Mostraremos que en ambos casos se cumple que $a^p \equiv a \,\text{mód}\, p$.

1. Supongamos que $p \not| a$. Por el teorema de Fermat (5.65) tenemos que $a^{p-1} \equiv 1 \,\text{mód}\, p$. Multiplicando ambos miembros por a obtenemos que $a^p \equiv a \,\text{mód}\, p$.

2. Supongamos que $p|a$. En este caso se tiene que $p|a^n$ para todo natural n, en particular a^p es divisible por p y por consiguiente $a \equiv 0 \,\text{mód}\, p$ y $a^p \equiv 0 \,\text{mód}\, p$. Luego $a^p \equiv a \,\text{mód}\, p$.

□

Ejemplos 5.67. A continuación mostraremos dos aplicaciones del teorema de Fermat.

1. Hemos visto cómo calcular el resto de dividir dos números usando congruencias y sabemos que en algunos casos se requiere realizar muchos cálculos. El teorema de Fermat nos permite responder este tipo de preguntas más rápidamente. Queremos calcular el resto de dividir 2^{1991} entre 11. Observemos primero que el teorema de Fermat con $p = 11$ y $a = 2$ nos dice que

   $$2^{10} \equiv 1 \,\text{mód}\, 11.$$

   Como $2^{1990} = (2^{10})^{199}$ se tiene que $2^{1990} \equiv 1 \,\text{mód}\, 11$ y ya que $2^{1991} = 2 \cdot 2^{1990}$, entonces tenemos que $2^{1991} \equiv 2 \,\text{mód}\, 11$. Es decir, el resto de dividir 2^{1991} entre 11 es 2.

2. Veremos ahora que para todo entero n, se cumple que $n^7 - n$ es divisible por 42. Primero observemos que

   $$\begin{aligned} n^7 - n &= n(n^6 - 1) \\ &= n(n^3 - 1)(n^3 + 1) \\ &= n(n-1)(n^2 + n + 1)(n+1)(n^2 - n + 1) \\ &= (n-1)n(n+1)(n^2 + n + 1)(n^2 - n + 1). \end{aligned}$$

   De la última igualdad se tiene que $(n-1)n(n+1)$ divide a $n^7 - n$. Como $(n-1)n(n+1)$ es divisible por 2 y por 3 (¿por qué?) entonces 6 divide a $n^7 - n$ (¿por qué?). Para obtener que 42 divide a $n^7 - n$ bastaría entonces mostrar que 7 divide a $n^7 - n$ (¿por qué?). Para esto usaremos el teorema 5.66. En efecto, sabemos que $n^7 \equiv n \,\text{mód}\, 7$, esto quiere decir que $n^7 - n$ es divisible por 7.

□

Ejercicios 5.13

1. Indique cuáles de las siguientes afirmaciones son correctas y cuáles son falsas:
   (a) $18 \equiv 2 \,\text{mód}\, 5$ (b) $18 \equiv 2 \,\text{mód}\, 6$
   (c) $83 \equiv 3 \,\text{mód}\, 8$ (d) $4 \equiv 24 \,\text{mód}\, 4$
   (e) $5 \equiv 24 \,\text{mód}\, 5$ (f) $12345678 \equiv 6 \,\text{mód}\, 3$
   (g) $-7 \equiv 47 \,\text{mód}\, 9$ (h) $837896 \equiv 3 \,\text{mód}\, 11$.

2. Determine en cada caso para cuáles enteros n se cumple que:

   (a) $n(n+1)(n+2) \equiv 0 \,\text{mód}\, 3$
   (b) $4n + 2 \equiv 1 \,\text{mód}\, 7$
   (c) $4n + 3 \equiv 1 \,\text{mód}\, 8$
   (d) $2n \equiv 6 \,\text{mód}\, 2$.

3. Muestre que si $a \equiv b \,\text{mód}\, m$, entonces $a \equiv b \,\text{mód}\, k$ para todo k que sea un divisor de m.

4. *a*) Sea c un entero diferente de cero. Muestre que $a \equiv b \,\text{mód}\, 7$ si, y sólo si, $ca \equiv cb \,\text{mód}\, 7$.

   b) Sea c un entero diferente de cero. Muestre que $a \equiv b \,\text{mód}\, m$ si, y sólo si, $ca \equiv cb \,\text{mód}\, cm$.

5. Muestre que para todo entero $m \geq 0$ se cumple que $10^{2m+1} \equiv -1 \,\text{mód}\, 11$ y $10^{2m} \equiv 1 \,\text{mód}\, 11$.

6. Sea n un entero positivo. Considere el número $a = 12121212 \cdots 12$ donde 12 se repite n veces. Muestre que a es divisible por 11 si, y sólo si, n es divisible por 11.

7. Muestre los siguiente criterios de divisibilidad (*Sugerencia:* Imite lo hecho en el ejemplo 5.59):

   a) n es divisible por 2 si, y sólo si, el último dígito de n (en su representación decimal) es par.

   b) n es divisible por 5 si, y sólo si, el último dígito de n es 0 o 5.

   c) n es divisible por 9 si, y sólo si, la suma de sus dígitos es divisible por 9.

8. Sea n un natural. Muestre que 3^n y 9^n dejan el mismo resto al dividirlos por 6.

9. Sea n, m, a, b enteros positivos con $m > 1$ y $n \leq a$.

   a) Suponga que $b^n \equiv 1 \,\text{mód}\, m$ y que $a \equiv p \,\text{mód}\, n$ con $0 \leq p < n$. Muestre que $b^a \equiv b^p \,\text{mód}\, m$.

   b) Use (a) para determinar el último dígito de los siguientes números: 3^{36}, 7^{7^7}, 9^{9^9}, $7^{7^{7^7}}$.

10. Si hoy es viernes ¿Qué día será dentro de $6^{422} \cdot 8^{321}$ días?

11. Muestre que $x \equiv 1 \,\text{mód}\, 3$ si y sólo si alguna de las siguientes tres afirmaciones se cumple: (a) $x \equiv 1 \,\text{mód}\, 9$, (b) $x \equiv 4 \,\text{mód}\, 9$ (c) $x \equiv 7 \,\text{mód}\, 9$.

12. Muestre que si n es un entero entonces se cumple alguna de las siguientes tres afirmaciones: (a) $n^2 \equiv 0 \,\text{mód}\, 5$, (b) $n^2 \equiv 1 \,\text{mód}\, 5$, (c) $n^2 \equiv -1 \,\text{mód}\, 5$.

13. Resuelva las siguientes ecuaciones de congruencia:

    a) $12x \equiv 6 \,\text{mód}\, 13$

    b) $18x \equiv 1 \,\text{mód}\, 25$

    c) $11x \equiv 7 \,\text{mód}\, 84$

    d) $12x \equiv 6 \,\text{mód}\, 13$

    e) $13x \equiv 6 \,\text{mód}\, 140$.

14. Muestre lo dicho en 5.61: Si la ecuación $ax \equiv b \,\text{mód}\, m$ tiene una solución, entonces existe una solución entre 0 y $m-1$ (*Sugerencia:* El teorema 5.60 asegura que el conjunto solución es una clase de congruencia).

15. Pruebe que para todo primo $p > 2$ existen infinitos números naturales n tales que $p|2^n - 1$ (Sugerencia: Use el Teorema de Fermat 5.65).

16. Muestre que $15|n^5 - n$ (*Sugerencia:* Use 5.66).

17. Muestre que $15|(3n^5 + 5n^3 + 7n)$.

18. Para cualquier natural n se cumple que $1 + 2^n + 3^n + 4^n$ es divisible por 5 si y sólo si $4 \not| n$. (*Sugerencia:* Si n no es divisible por 4 entonces por el algoritmo de la división existen enteros r y k tal que $0 < r \leq 3$ y $n = 4k + r$. Considere los 3 casos posibles: $r = 1$, $r = 2$ y $r = 3$. Si $4|n$ use el teorema de Fermat).

19. Considere la siguiente sucesión de números definida recursivamente

$$x_{n+1} \equiv 23x_n \,\text{mód}\, 100.$$

    Sea $x_1 = 1$. Determine los primeros 10 términos de esta sucesión.

20. Sea $A_0 = \{n \in \mathbb{Z} : \ n \text{ es divisible por } 5\}$ y para cada $k \in \mathbb{P}$ sea $A_k = \{n + k : \ n \in A_0\}$.

    a) Enumere varios elementos de A_0, A_1, A_2, A_3, A_4, A_5, y A_6.

    b) Muestre que $A_0 = A_5$ y que $A_1 = A_6$.

    c) Generalice sus respuestas de la parte (b).

    d) Determine $\bigcup_{k=0}^{4} A_k$ y $\bigcup_{k=1}^{5} A_k$.

5.14. Ejercicios suplementarios del capítulo 5

1. Consideremos la sucesión

   $$1, 2, 2, 3, 3, 3, 4, 4, 4, 4, 5, 5, 5, 5, 5, \ldots$$

   cuyos términos son los enteros positivos consecutivos en orden creciente y en la cual el entero n se repite n veces. Halle el resto de dividir entre 5 el término 1997 de esta sucesión. (*Sugerencia:* Sea a_n la posición que ocupa el entero n la primera vez que aparece en la sucesión. Por ejemplo, tenemos que $a_1 = 1$, $a_2 = 2$, $a_3 = 4$, $a_4 = 7$, etc. Halle el término general de a_n).

2. Sean p y q enteros positivos tales que $2^p + 1 = q^2$. Muestre que $p = q = 3$.

3. Muestre que ningún entero de la forma $4^n + 1$ (con n un número natural) es divisible por 3.

4. Muestre que $mcd(n, n + 1) = 1$ para todo entero positivo n.

5. *a*) Muestre que a y $-a$ tienen los mismos divisores.

   b) Use la parte (a) para mostrar que para cada dos enteros no nulos a y b se cumple que $mcd(a, b) = mcd(-a, b) = mcd(-a, -b) = mcd(a, -b)$.

6. Enuncie y demuestre un criterio de divisibilidad por 18, 22, 30 y 90.

7. Se tienen dos números naturales a y b. Con ellos se obtienen cuatro números de la siguiente manera: (i) La suma de ellos. (ii) La diferencia entre el mayor y el menor entre ellos. (iii) El producto de ellos y (iv) El cociente entre el mayor y el menor de ellos. Los cuatro números obtenidos en (i), (ii), (iii) y (iv) se suman y se obtiene 243. Determine a y b.

8. Sean a y b enteros coprimos. Muestre que a^m y b^n son coprimos para todo natural n y m.

9. Sean a, b y c enteros. Pruebe que

   $$mcd(mcd(a, b), c) = mcd(a, mcd(b, c)) = mcd(a, b, c).$$

10. Pruebe que si $mcd(a, b) = 1$ entonces $mcd(a + b, a - b)$ es igual a 1 ó 2. (*Sugerencia:* Muestre que si c es un divisor común de $a + b$ y $a - b$ entonces x divide a 2. Recuerde que $mcd(ka, kb) = k \cdot mcd(a, b)$ cuando k es positivo.)

11. Use el teorema fundamental de la Aritmética para mostrar que si $mcd(a, b) = 1$, entonces $mcd(a^n, b^m) = 1$ para todo natural n y m.

12. Muestre por inducción que 8^n es de la forma $7k + 1$ para todo $n \in \mathbb{N}$.

13. Muestre que para todo $a, r \in \mathbb{N}$ existe un k tal que $ak + r$ no es primo.

14. Para probar la existencia de infinitos primos es suficiente conseguir una colección infinita de números coprimos dos a dos. En efecto, muestre que las siguientes proposiciones son equivalentes:

    a) Existe una sucesión $p_1, p_2, p_3, \cdots$ infinita de números primos.

    b) Existe una sucesión $q_1, q_2, q_3, \cdots$ infinita de números coprimos, es decir para cada i y j con $i \neq j$, $mcd(q_i, q_j) = 1$.

Índice alfabético

$(a_n)_n$, 77
$<$, 3
$A \setminus B$, 12
A^c, 14
$\square$, 2
$\Leftrightarrow$, 33
Π, 80
$\mathbb{Q}$, 2
$\mathbb{R}$, 3
Σ, 80
$\cap$, 11
$\cup$, 11
$\emptyset$, 7
$\exists$, 39
$\forall$, 38
$\in$, 1
$\leftrightarrow$, 23
$\leq$, 3
$a \equiv b \,\text{mód}\, m$, 144
$\mathbb{N}$, 2
$\neg$, 23
$\notin$, 1
$\not\subseteq$, 8
$\mathcal{P}(A)$, 8
$\rightarrow$, 23
$\triangle$, 12
$\subseteq$, 7
$\vee$, 23
$\wedge$, 23
$\mathbb{Z}$, 2
$n \not| m$, 101
$n|m$, 101

acotado superiormente, 72
adición, 36
ajedrez, 89
algebra Booleana, 51
algoritmo de Euclides, 122

base de la inducción, 86
Boole, 51

complemento de un conjunto, 14
conectivos lógicos, 22
conjunto de partes, 8
conjunto potencia, 8
conjunto universal, 14
conjunto vacío, 7
conjuntos disjuntos, 7
consecuencia lógica, 35
contradicción, 30
contraejemplo, 40, 60
contrapositiva, 34
coprimos, 127
coprimos dos a dos, 127
cota superior, 72
criba de Eratóstenes, 142
criterio de divisibilidad por 11, 150
criterio de divisibilidad por 3, 149
cuantificador existencial, 39
cuantificador universal, 38

De Morgan, 55
definición por comprensión, 2
definición por extensión, 1
demostración por inducción, 87
diagramas de Venn, 14
diferencia de conjuntos, 12
diferencia simétrica, 12
divisor común, 119
doble negación, 34

ecuación de recurrencia, 96
ecuación diofántica, 118
ecuación lineal de congruencia, 150

elemento, 1
etcétera, 5

fórmula proposicional, 29
factorial, 81
Fibonacci, 96

Gauss, 144

hipótesis, 24
hipótesis inductiva, 86

igualdad de conjuntos, 6
implicación, 34
implicación lógica, 35
intersección de conjuntos, 11

lógica, 21
lógica proposicional, 21
Leonardo de Pisa, 96
ley asociativa, 34, 51, 57
ley conmutativa, 34, 51
ley de De Morgan, 34, 55
ley de la idempotencia, 51
ley de la identidad, 51, 55
ley distributiva, 34, 51
ley distributiva generalizada, 54
leyes del álgebra de conjuntos, 51
locha, 64

máximo común divisor, 119
máximo de un conjunto, 72
mínimo común múltiplo, 138
mínimo de un conjunto, 69
miembro de un conjunto, 1
Modus Ponens, 36
Modus Tollens, 36

número compuesto, 101
número entero, 2
número impar, 5
número natural, 2
número par, 5
número primo, 101
número racional, 2
número real, 3

paso inductivo, 86
primos de Mersenne, 143
principio de buena ordenación, 70
principio de inducción completa, 93
principio de inducción fuerte, 93
propiedad transitiva, 47
proposición, 21
proposición atómica, 22
proposición compuesta, 22
proposición contrapositiva, 24
proposición contrarrecíproca, 24
proposición recíproca, 24
proposiciones lógicamente equivalentes, 33
prueba por casos, 34, 54

recursión, 96
reducción al absurdo, 64
relación de congruencia, 144

silogismo disyuntivo, 36
silogismo hipotético, 36
simplificación, 36
solución general de una ecuación, 133
solución particular de una ecuación, 133
subconjunto, 7
sucesión, 76
sucesión de Fibonacci, 96
sucesión finita, 79
sucesión recursiva, 96
sucesiones equivalentes, 78

tabla de verdad, 28, 29
tautología, 30
teorema, 66
teorema de Euclides, 141
teorema de Fermat, 153
tesis, 24

unión de conjuntos, 11
universo, 14

valor de verdad, 27
variables proposicionales, 29

Bibliografía

[1] K. Bogart. *Matemáticas discretas*. Editorial Limusa, Mexico, 1996.

[2] I. Copy and C. Cohen. *Introducción a la lógica*. Limusa, México, 2001. Quinta edición.

[3] A. Muñoz Garcia. *Lógica Simbólica Elemental*. Editorial Miro, Caracas, 1992.

[4] M. Gardner. *Máquinas lógicas y Diagramas*. Editorial Grijalbo S. A., Mexico, 1973.

[5] R. Johnsonbaugh. *Matemáticas discretas*. Grupo editorial Iberoamericano, Mexico, 1988.

[6] J. Leal. *Fundamentos de Álgebra I*. Notas mimeografiadas, Departamento de Matemáticas, Universidad de Los Andes, 1992.

[7] C. Miller, V. Heeren, and E. J. Hornsby. *Matemática: Razonamiento y Aplicaciones*. Addison Wesly Longman, 1999. Octava Edición.

[8] Y. Perelman. *El divertido juego de las matemáticas*. Círculo de Lectores, Ltda., Colombia, 1968.

[9] S. Rada. *Aritmética*. Editorial CENAMEC, Caracas, 1992.

[10] Malba Tahan. *El hombre que calculaba*. Venezuela.

[11] D. Velleman. *How to Prove it: A Structured Approach*. Cambridge University Press, London, 1994.

[12] K. Ross y C. Wright. *Matemáticas discretas*. Prentice Hall Hispanoamericana, Mexico, 1992. Segunda edición.