MATERIAL DE APOYO PARA EL PRIMER CURSO DE MATEMÁTICAS COMPUTACIONALES.

Ing. HUGO HUMBERTO MORALES PEÑA

MAESTRÍA EN ENSEÑANZA DE LAS MATEMÁTICAS
Línea de Matemáticas Computacionales

UNIVERSIDAD TECNOLÓGICA DE PEREIRA
FACULTAD DE CIENCIAS BÁSICAS
DEPARTAMENTO DE MATEMÁTICAS
Pereira, Risaralda
28 de Julio de 2010

Índice general

Capítulo 1

Introducción a la lógica matemática

1.1. Cálculo proposicional

Definición de proposición:

Una proposición es un enunciado declarativo que puede ser calificado sin ambigüedad como verdadero o falso. En este análisis no se tendrán en cuenta proposiciones que requieran una opinión individual y que por lo tanto, no pueden ser verdaderas o falsas.

Las siguientes declaraciones son ejemplos de proposiciones:

- Matemáticas Discretas es una materia que se evalúa en el Examen de Calidad de la Educación Superior (ECAES) en el programa académico de Ingeniería de Sistemas
- El promedio a nivel nacional en el ECAES de Ingeniería de Sistemas fue de 110.3 puntos en el año 2007
- El cuadernillo de inglés tenia 40 preguntas en el ECAES de Ingeniería de Sistemas del año 2008

Las siguientes declaraciones son ejemplos de lo que no es una proposición:

- Atlético Nacional es el mejor equipo del fútbol colombiano
- Álvaro Uribe ha sido el mejor presidente de los colombianos
- Los próximos juegos deportivos nacionales serán ganados por el departamento del Valle

Las proposiciones pueden considerarse como primitivas, ya que en realidad no se pueden descomponer en partes más simples.

Las proposiciones primitivas se utilizan con conectivos lógicos para formar proposiciones compuestas.

Los símbolos p, q, r, s, ... se utilizarán para denotar proposiciones, los cuales se llamarán variables proposicionales.

1.1.1. Conectivos proposicionales

Los conectivos proposicionales son también conocidos con el nombre de conectivos lógicos.

Los conectivos principales son:

- la negación, representada por el símbolo $\sim$
- la disyunción, representada por el símbolo $\vee$
- la conjunción, representada por el símbolo $\wedge$
- el condicional (o implicación), representada por el símbolo $\rightarrow$
- el bicondicional (o doble implicación), representada por el símbolo $\leftrightarrow$

Las tablas de verdad para estos conectivos son:

Tabla de verdad de la negación:

p	$\sim p$
V	F
F	V

Tabla de verdad de la disyunción:

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

Tabla de verdad de la conjunción:

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

Tabla de verdad del condicional:

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

Tabla de verdad del bicondicional:

p	q	$p \leftrightarrow q$
V	V	V
V	F	F
F	V	F
F	F	V

Dos proposiciones p y q son *equivalentes* cuando el bicondicional $p \leftrightarrow q$ es una proposición verdadera.

Ejemplo 1:

Se tienen las siguientes dos proposiciones:

- p : $\sqrt{2}$ es un número irracional
- q : un año bisiesto tiene 366 días

las dos proposiciones p y q son verdaderas, como $V \leftrightarrow V$ es verdadero, entonces las proposiciones p y q son equivalentes.

Ejemplo 2:

Se tienen las siguientes dos proposiciones:

- p : 2+3=7
- q : 4 es un número impar

las dos proposiciones p y q son falsas, como $F \leftrightarrow F$ es verdadero, entonces las proposiciones p y q son equivalentes.

1.1.2. Fórmulas bien formadas

Una fórmula es una sucesión finita de variables proposicionales, conectivos lógicos y paréntesis.

Una Fórmula Bien Formada (FBF), es, intuitivamente una fórmula coherente, con sentido gramatical.

Las FBF serán denotadas por los símbolos: A, B, C, A_1, B_1, C_1, ...

Definición:

Una FBF del cálculo proposicional es aquella fórmula que se ajusta a cualquiera de estos casos:

1. Toda variable proposicional aislada es una FBF
2. Si A es una FBF, entonces $\sim (A)$ es una FBF
3. Si A y B son FBF, entonces también lo son:
   - $(A) \wedge (B)$,
   - $(A) \vee (B)$,
   - $(A) \rightarrow (B)$, y
   - $(A) \leftrightarrow (B)$.
4. Una fórmula es bien formada si lo es como resultado de aplicar los casos 1, 2 y 3 un número finito de veces.

Ejemplo 3:

¿La fórmula $((p) \wedge (\sim (q))) \rightarrow ((\sim (\sim (p))) \leftrightarrow (q))$ es una fórmula bien formada?

Para determinar si la fórmula es bien formada, sea A_0 la fórmula que represente a ésta, si A_0 se puede obtener al aplicar un número finito de pasos los casos 1, 2 y 3 entonces la fórmula es bien formada, para esto se tiene:

$A_0 = ((p) \wedge (\sim (q))) \rightarrow ((\sim (\sim (p))) \leftrightarrow (q))$, como el conectivo principal de la fórmula es la implicación, entonces A_0 se puede representar como $A_0 = (A_1) \rightarrow (B_1)$ donde $A_1 = (p) \wedge (\sim (q))$ y $B_1 = (\sim (\sim (p))) \leftrightarrow (q)$. En el análisis de las fórmulas A_1 y B_1 se tiene:

- $A_1 = (p) \wedge (\sim (q))$, A_1 puede ser reescrita como $A_1 = (A_2) \wedge (B_2)$, con $A_2 = p$ y $B_2 = \sim (q)$, con $B_2 = \sim (B_3)$ y $B_3 = q$. Como A_2 y B_3 son variables proposicionales aisladas entonces éstas son FBF; como B_2 es la negación de una FBF entonces ésta también es una FBF; como la fórmula A_1 es la conjunción de las FBF A_2 y B_2 entonces A_1 es también una FBF.
- $B_1 = (\sim (\sim (p))) \leftrightarrow (q)$, B_1 puede ser reescrita como $B_1 = (A_4) \leftrightarrow (B_4)$, con $A_4 = \sim (\sim (p))$ y $B_4 = q$, como B_4 es una variable proposicional aislada entonces es una FBF. La fórmula A_4 puede ser reescrita como $A_4 = \sim (A_5)$ donde $A_5 = \sim (p)$ que puede ser reescrita como $A_5 = \sim (A_6)$ y $A_6 = p$, como A_6 es una variable proposicional aislada entonces es una FBF; A_5 es la negación de una FBF entonces ésta también es una FBF; A_4 es la negación de A_5 que es una FBF entonces A_4 también es una FBF. Como la fórmula B_1 es la doble implicación entre las FBF A_4 y B_4 entonces B_1 es también una FBF.

en el análisis anterior ya se obtuvo que A_1 y B_1 son FBF y como $A_0 = (A_1) \to (B_1)$ entonces A_0 es también una FBF.

1.1.3. Fórmulas lógicamente equivalentes (FLE)

Dos fórmulas A y B son lógicamente equivalentes, lo cual se indica en este trabajo como $A \Leftrightarrow B$, cuando tienen la misma tabla de verdad.

Ejemplo 4:

Se tienen las siguientes fórmulas $A = \sim (p \wedge \sim q)$ y $B = \sim p \vee q$, ¿son las fórmulas A y B lógicamente equivalentes?

Para dar respuesta a ésta pregunta se hará uso de las tablas de verdad, para lo cual se tiene:

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

como las columnas de la tabla que indican los valores para las fórmulas $\sim (p \wedge \sim q)$ y $\sim p \vee q$ son iguales entonces éstas fórmulas son lógicamente equivalentes.

1.1.4. Tautología

Cuando dos fórmulas A y B son lógicamente equivalentes, el bicondicional $A \leftrightarrow B$ es siempre verdadero. Cuando dos fórmulas A y B son lógicamente equivalentes entonces $A \leftrightarrow B$ es una tautología, según la definición siguiente:

Definición:

Si una FBF tiene siempre el valor verdadero independientemente de cada asignación particular de valores a sus variables, entonces esta fórmula es una tautología y se denota con V; si tal valor es siempre falso, entonces esta fórmula es una contradicción y se denota con F.

Ejemplo 5:

¿La fórmula $((p \to q) \wedge \sim p) \to (\sim q)$ es una tautología?

Para dar respuesta a esta pregunta se hará uso de las tablas de verdad, para lo cual se tiene:

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

la fórmula no es una tautología porque existe una combinación de asignación de valores de las variables proposicionales que hacen que la fórmula genere el valor falso, dicha asignación de valores es $p = F$ y $q = V$, lo cual se evidencia en la tercer fila de la tabla de verdad.

Una alternativa es indagar de forma indirecta la posibilidad de que alguna combinación de valores dé un valor F en la fórmula.

Manera alternativa:

El conectivo principal de la fórmula es una implicación ($\to$), la única posibilidad para que una implicación tome valor falso es cuando el antecedente es verdadero y el consecuente es falso

$$\underbrace{\underbrace{((p \to q) \wedge (\sim p))}_{V} \to \underbrace{(\sim q)}_{F}}_{F}$$

la única posibilidad para que el consecuente sea falso es cuando la variable proposicional q toma valor verdadero; tener en cuenta que la asignación de valor para la variable proposicional q aplica para toda la expresión

$$\underbrace{\underbrace{((p \to \underbrace{q}_{V}) \wedge (\sim p))}_{V} \to \underbrace{(\sim \underbrace{q}_{V})}_{F}}_{F}$$

la única posibilidad para que el antecedente sea verdadero es cuando la variable proposicional p toma valor falso; tener en cuenta que la asignación de valor para la variable proposicional p aplica para todas las ocurrencias de dicha variable en la expresión

$$\underbrace{\underbrace{((\underbrace{p}_{F} \to \underbrace{q}_{V}) \wedge (\sim \underbrace{p}_{F}))}_{V} \to \underbrace{(\sim \underbrace{q}_{V})}_{F}}_{F}$$

en este ejemplo utilizando la manera alternativa se concluye igualmente que la fórmula no es una tautología porque se logró determinar una asignación de valores para las variables proposicionales que hace que la fórmula tome el valor falso.

1.1.5. Leyes de la lógica

La siguiente tabla contiene las principales leyes de la lógica en el cálculo proposicional, donde A, B y C son fórmulas bien formadas. Para una mayor claridad con respecto al alcance de una negación en un fórmula bien formada en el cálculo proposicional, entonces se usará en la tabla y en el resto de ejercicios de la sección, la representación $\overline{A}$ en vez de $\sim A$, donde A es una fórmula bien formada.

Número	**Equivalencia Lógica**	**Nombre Ley**
1.	$\overline{\overline{A}} \Leftrightarrow A$	Ley de doble negación
2.	$\overline{A \vee B} \Leftrightarrow \overline{A} \wedge \overline{B}$	Ley de De Morgan
2'.	$\overline{A \wedge B} \Leftrightarrow \overline{A} \vee \overline{B}$	Ley de De Morgan
3.	$A \vee B \Leftrightarrow B \vee A$	Ley conmutativa
3'.	$A \wedge B \Leftrightarrow B \wedge A$	Ley conmutativa
4.	$A \vee (B \vee C) \Leftrightarrow (A \vee B) \vee C$	Ley asociativa
4'.	$A \wedge (B \wedge C) \Leftrightarrow (A \wedge B) \wedge C$	Ley asociativa
5.	$A \vee (B \wedge C) \Leftrightarrow (A \vee B) \wedge (A \vee C)$	Ley distributiva
5'.	$A \wedge (B \vee C) \Leftrightarrow (A \wedge B) \vee (A \wedge C)$	Ley distributiva
6.	$A \vee A \Leftrightarrow A$	Ley de idempotencia
6'.	$A \wedge A \Leftrightarrow A$	Ley de idempotencia
7.	$A \vee F \Leftrightarrow A$	Ley de identidad
7'.	$A \wedge V \Leftrightarrow A$	Ley de identidad
8.	$A \vee \overline{A} \Leftrightarrow V$	Ley inversa
8'.	$A \wedge \overline{A} \Leftrightarrow F$	Ley inversa
9.	$A \vee V \Leftrightarrow V$	Ley de dominación
9'.	$A \wedge F \Leftrightarrow F$	Ley de dominación
10.	$A \vee (A \wedge B) \Leftrightarrow A$	Ley de absorción
10'.	$A \wedge (A \vee B) \Leftrightarrow A$	Ley de absorción
11.	$(A \rightarrow B) \Leftrightarrow (\overline{B} \rightarrow \overline{A})$	Ley de transposición

1.1.6. Utilizando las leyes de la lógica proposicional

Ejemplo 6:

Simplificar la siguiente proposición compuesta $[(\overline{x} \wedge y) \vee (x \wedge \overline{y})] \rightarrow x$ utilizando las leyes de la lógica proposicional. En cada paso especificar la regla que se utilizó.

Utilizando las leyes de la lógica proposicional la simplificación es la siguiente:

$$
\begin{aligned}
&[(\overline{x} \wedge y) \vee (x \wedge \overline{y})] \rightarrow x \\
&\qquad \Longleftrightarrow \overline{[(\overline{x} \wedge y) \vee (x \wedge \overline{y})]} \vee x, \quad \text{equivalencia lógica de la implicación.} \\
&\qquad \Longleftrightarrow [\overline{(\overline{x} \wedge y)} \wedge \overline{(x \wedge \overline{y})}] \vee x, \quad \text{ley de De Morgan.} \\
&\qquad \Longleftrightarrow [(x \vee \overline{y}) \wedge (\overline{x} \vee y)] \vee x, \quad \text{ley de De Morgan y ley de doble negación.} \\
&\qquad \Longleftrightarrow [((x \vee \overline{y}) \wedge \overline{x}) \vee ((x \vee \overline{y}) \wedge y)] \vee x, \quad \text{ley distributiva.} \\
&\qquad \Longleftrightarrow [((x \wedge \overline{x}) \vee (\overline{x} \wedge \overline{y})) \vee ((x \wedge y) \vee (\overline{y} \wedge y))] \vee x, \quad \text{ley distributiva.} \\
&\qquad \Longleftrightarrow [(F \vee (\overline{x} \wedge \overline{y})) \vee ((x \wedge y) \vee F)] \vee x, \quad \text{ley inversa.} \\
&\qquad \Longleftrightarrow [(\overline{x} \wedge \overline{y}) \vee (x \wedge y)] \vee x, \quad \text{ley de identidad.} \\
&\qquad \Longleftrightarrow (\overline{x} \wedge \overline{y}) \vee ((x \wedge y) \vee x), \quad \text{ley asociativa.} \\
&\qquad \Longleftrightarrow (\overline{x} \wedge \overline{y}) \vee x \quad \text{ley de Absorción} \\
&\qquad \Longleftrightarrow (\overline{x} \vee x) \wedge (\overline{y} \vee x), \quad \text{ley distributiva.} \\
&\qquad \Longleftrightarrow V \wedge (\overline{y} \vee x), \quad \text{ley inversa} \\
&\qquad \Longleftrightarrow (\overline{y} \vee x), \quad \text{ley de identidad.} \\
&\qquad \Longleftrightarrow y \rightarrow x, \quad \text{equivalencia lógica de la implicación.}
\end{aligned}
$$

Se puede utilizar tablas de verdad, como mecanismo adicional, para verificar si el resultado obtenido en la simplificación es correcto. Es importante tener en cuenta que la validez del resultado de la simplificación, depende única y exclusivamente, del correcto uso de las leyes de la lógica proposicional, donde, en cada paso de la simplificación se garantizar que se tiene una proposición compuesta lógicamente equivalente a la proposición compuesta original.

x	y	$(\overline{x} \wedge y) \vee (x \wedge \overline{y})$	$[(\overline{x} \wedge y) \vee (x \wedge \overline{y})] \rightarrow x$	$y \rightarrow x$
V	V	F	V	V
V	F	V	V	V
F	V	V	F	F
F	F	F	V	V

Como se obtuvieron exactamente los mismos valores en las columnas de la tabla de

verdad correspondientes a $[(\overline{x} \wedge y) \vee (x \wedge \overline{y})] \rightarrow x$ y a $y \rightarrow x$ entonces las dos proposiciones compuestas son lógicamente equivalentes y la simplificación es correcta.

Ejemplo 7:

Utilizando las leyes de la lógica proposicional simplificar la siguiente proposición compuesta $[(p \vee q) \wedge (p \rightarrow q)] \ \vee \ [\overline{(p \vee q)} \wedge \overline{(p \rightarrow q)}]$.

Los pasos de la simplificación son los siguientes:

$[(p \vee q) \wedge (p \rightarrow q)] \ \vee \ [\overline{(p \vee q)} \wedge \overline{(p \rightarrow q)}]$

$\iff [(p \vee q) \wedge (\overline{p} \vee q)] \ \vee \ [\overline{(p \vee q)} \wedge \overline{(\overline{p} \vee q)}]$, equivalencia lógica implicación.

$\iff [(p \vee q) \wedge (\overline{p} \vee q)] \ \vee \ [(\overline{p} \wedge \overline{q}) \wedge (p \wedge \overline{q})]$, ley de De Morgan.

$\iff [(p \wedge \overline{p}) \vee q] \ \vee \ [(\overline{p} \wedge \overline{q}) \wedge (p \wedge \overline{q})]$, ley distributiva .

$\iff [F \vee q] \ \vee \ [(\overline{p} \wedge \overline{q}) \wedge (p \wedge \overline{q})]$, ley inversa.

$\iff [q] \ \vee \ [(\overline{p} \wedge \overline{q}) \wedge (p \wedge \overline{q})]$, ley de identidad.

$\iff q \ \vee \ [\ \overline{p} \wedge (\overline{q} \wedge p) \wedge \overline{q}\ ]$, ley asociativa.

$\iff q \ \vee \ [\ \overline{p} \wedge (p \wedge \overline{q}) \wedge \overline{q}\ ]$, ley conmutativa.

$\iff q \ \vee \ [(\ \overline{p} \wedge p) \wedge (\overline{q} \wedge \overline{q}\ )]$, ley asociativa.

$\iff q \ \vee \ [F \wedge (\overline{q} \wedge \overline{q}\ )]$, ley inversa.

$\iff q \ \vee \ F$, ley de dominación.

$\iff q$, ley de identidad.

1.1.7. Conectivo X-OR ($\bigotimes$)

El conectivo $\otimes$ de la lógica proposicional es llamado O Exclusivo o X-OR. Su tabla de verdad es:

p	q	$p \otimes q$
V	V	F
V	F	V
F	V	V
F	F	F

La siguiente equivalencia lógica representa al X-OR: $p \otimes q \Leftrightarrow (\overline{p} \wedge q) \vee (p \wedge \overline{q})$.

Ejemplo 8:

Determinar sin utilizar tablas de verdad si la proposición compuesta $\overline{(x \otimes y)} \rightarrow (x \vee \overline{y})$ es una tautología.

Haciendo uso de las leyes de la lógica proposicional, el análisis es el siguiente:

$$\begin{aligned}
\overline{(x \otimes y)} \to (x \vee \overline{y}) &\iff \overline{\overline{(x \otimes y)}} \vee (x \vee \overline{y}), \quad \text{equivalencia lógica de la implicación} \\
&\iff (x \otimes y) \vee (x \vee \overline{y}), \quad \text{ley de doble negación} \\
&\iff ((\overline{x} \wedge y) \vee (x \wedge \overline{y})) \vee (x \vee \overline{y}), \quad \text{equivalencia lógica del X-OR} \\
&\iff (\overline{x} \wedge y) \vee ((x \wedge \overline{y}) \vee (x \vee \overline{y})), \quad \text{ley asociativa} \\
&\iff (\overline{x} \wedge y) \vee (((x \wedge \overline{y}) \vee x) \vee \overline{y}), \quad \text{ley asociativa} \\
&\iff (\overline{x} \wedge y) \vee ((x) \vee \overline{y}), \quad \text{ley de absorción} \\
&\iff (\overline{x} \wedge y) \vee \overline{\overline{(x \vee \overline{y})}}, \quad \text{ley de doble negación} \\
&\iff (\overline{x} \wedge y) \vee \overline{(\overline{x} \wedge \overline{\overline{y}})}, \quad \text{ley de De Morgan} \\
&\iff (\overline{x} \wedge y) \vee \overline{(\overline{x} \wedge y)}, \quad \text{ley de doble negación} \\
&\iff V, \quad \text{ley inversa}
\end{aligned}$$

Queda demostrado que la proposición compuesta original es una tautología porque el valor obtenido como resultado de la simplificación es el V.

Ejemplo 9:

Demostrar utilizando las leyes de la lógica proposicional, que la proposición compuesta $\overline{\overline{(p \wedge q)} \vee (p \otimes q)}$ es lógicamente a la proposición compuesta $p \wedge q$.

La demostración se justifica con cada uno de los siguientes pasos:

$$\begin{aligned}
\overline{\overline{(p \wedge q)} \vee (p \otimes q)} &\iff \overline{\overline{(p \wedge q)}} \wedge \overline{(p \otimes q)}, \quad \text{ley de De Morgan} \\
&\iff (p \wedge q) \wedge \overline{(p \otimes q)}, \quad \text{ley de doble negación} \\
&\iff (p \wedge q) \wedge \overline{((p \wedge \overline{q}) \vee (\overline{p} \wedge q))}, \quad \text{equivalencia lógica del X-OR} \\
&\iff (p \wedge q) \wedge (\overline{(p \wedge \overline{q})} \wedge \overline{(\overline{p} \wedge q)}), \quad \text{ley de De Morgan} \\
&\iff (p \wedge q) \wedge ((\overline{p} \vee q) \wedge (p \vee \overline{q})), \quad \text{ley de De Morgan} \\
&\iff [(p \wedge q) \wedge (\overline{p} \vee q)] \wedge (p \vee \overline{q}), \quad \text{ley asociativa} \\
&\iff [((p \wedge q) \wedge \overline{p}) \vee ((p \wedge q) \wedge q)] \wedge (p \vee \overline{q}), \quad \text{ley distributiva} \\
&\iff [((q \wedge p) \wedge \overline{p}) \vee ((p \wedge q) \wedge q)] \wedge (p \vee \overline{q}), \quad \text{ley conmutativa} \\
&\iff [(q \wedge (p \wedge \overline{p})) \vee (p \wedge (q \wedge q))] \wedge (p \vee \overline{q}), \quad \text{ley asociativa} \\
&\iff [(q \wedge F) \vee (p \wedge q)] \wedge (p \vee \overline{q}), \quad \text{Leyes inversa y de idempotencia} \\
&\iff [F \vee (p \wedge q)] \wedge (p \vee \overline{q}), \quad \text{ley de dominación}
\end{aligned}$$

$$\iff (p \wedge q) \wedge (p \vee \overline{q}), \quad \text{ley de identidad}$$
$$\iff ((p \wedge q) \wedge p) \vee ((p \wedge q) \wedge \overline{q}), \quad \text{ley distributiva}$$
$$\iff (p \wedge (p \wedge q)) \vee ((p \wedge q) \wedge \overline{q}), \quad \text{ley conmutativa}$$
$$\iff ((p \wedge p) \wedge q) \vee (p \wedge (q \wedge \overline{q})), \quad \text{ley asociativa}$$
$$\iff (p \wedge q) \vee (p \wedge F), \quad \text{leyes idempotente e inversa}$$
$$\iff (p \wedge q) \vee F, \quad \text{ley de dominación}$$
$$\iff p \wedge q, \quad \text{ley de identidad}$$

1.1.8. Conectivo NOR (↓)

El conectivo NOR es un conectivo completo, en el sentido que, cualquier fórmula del cálculo proposicional puede ser escrita utilizando únicamente éste conectivo.

Mnemotecnicamente:

$$NOR \approx Not\ or \approx No\ o \approx \sim(p \vee q) \approx \overline{(p \vee q)} \approx p \not\vee q \approx p \downarrow q$$

Ejemplo 10:

Demostrar que el conectivo NOR es un conectivo completo.

Sugerencia: Para que el conectivo NOR sea un conectivo completo se debe presentar el equivalente de los siguientes conectivos principales utilizando únicamente el conectivo NOR:

- $\sim$
- $\vee$
- $\wedge$
- $\rightarrow$
- $\leftrightarrow$

Representación de la negación utilizando únicamente el NOR:

$\overline{p} \iff \overline{p \vee p}$, ley de idempotencia.

$\iff p \downarrow p$, equivalencia lógica NOR.

Representación de la disyunción utilizando únicamente el NOR:

$p \vee q \iff (p \vee q) \wedge (p \vee q)$, ley de idempotencia.

$\iff \overline{\overline{(p \vee q) \wedge (p \vee q)}}$, ley de la doble negación.

$\iff \overline{\overline{(p \vee q)} \vee \overline{(p \vee q)}}$, ley de De Morgan.

$\iff (p \downarrow q) \downarrow (p \downarrow q)$, equivalencia lógica NOR.

Representación de la conjunción utilizando únicamente el NOR:

$p \wedge q \iff \overline{\overline{(p \wedge q)}}$, ley de doble negación.

$\iff \overline{\overline{p} \vee \overline{q}}$, ley de De Morgan.

$\iff \overline{\overline{(p \vee p)} \vee \overline{(q \vee q)}}$, ley de idempotencia.

$\iff (p \downarrow p) \downarrow (q \downarrow q)$, equivalencia lógica NOR.

Representación de la implicación utilizando únicamente el NOR:

$p \to q \iff \overline{p} \vee q$, equivalencia lógica de la implicación.

$\iff (\overline{p} \downarrow q) \downarrow (\overline{p} \downarrow q)$, representación de la disyunción con el NOR.

$\iff ((p \downarrow p) \downarrow q) \downarrow ((p \downarrow p) \downarrow q)$, representación de la negación con el NOR.

Representación de la doble implicación utilizando únicamente el NOR:

$p \leftrightarrow q \iff (p \to q) \wedge (q \to p)$, equivalencia lógica de la doble implicación.

$\iff (\overline{p} \vee q) \wedge (\overline{q} \vee p)$, equivalencia lógica de la implicación.

$\iff \overline{\overline{(\overline{p} \vee q) \wedge (\overline{q} \vee p)}}$, ley de la doble negación.

$\iff \overline{\overline{(\overline{p} \vee q)} \vee \overline{(\overline{q} \vee p)}}$, ley de De Morgan.

$\iff (\overline{p} \downarrow q) \downarrow (\overline{q} \downarrow p)$, equivalencia lógica NOR.

$\iff (\overline{(\overline{p} \vee p)} \downarrow q) \downarrow (\overline{(\overline{q} \vee q)} \downarrow p)$, ley de idempotencia.

$\iff ((p \downarrow p) \downarrow q) \downarrow ((q \downarrow q) \downarrow p)$, equivalencia lógica NOR.

Ejemplo 11:

Representar la proposición $(p \wedge q) \to (q \vee r)$ sólo con el conectivo NOR ($\downarrow$)

Para resolver este ejercicio más fácilmente, primero se simplificará la proposición compuesta y luego sobre dicha simplificación se buscará la representación utilizando únicamente el conectivo NOR, para esto se tiene:

$(p \wedge q) \to (q \vee r) \iff \overline{(p \wedge q)} \vee (q \vee r)$, equivalencia lógica de la implicación.

$$\iff (\overline{p} \vee \overline{q}) \vee (q \vee r), \quad \text{ley de De Morgan.}$$
$$\iff \overline{p} \vee ((\overline{q} \vee q) \vee r), \quad \text{ley asociativa.}$$
$$\iff \overline{p} \vee (V \vee r), \quad \text{ley inversa.}$$
$$\iff \overline{p} \vee V, \quad \text{ley de dominación.}$$
$$\iff V, \quad \text{ley de dominación.}$$

Ahora se transformará el resultado de la simplificación utilizando únicamente el conectivo NOR

$$V \iff (\overline{p} \vee p), \text{ ley inversa.}$$
$$\iff (\overline{p} \vee p) \wedge (\overline{p} \vee p), \quad \text{ley de idempotencia.}$$
$$\iff \overline{\overline{(\overline{p} \vee p) \wedge (\overline{p} \vee p)}}, \quad \text{ley de doble negación.}$$
$$\iff \overline{\overline{(\overline{p} \vee p)} \vee \overline{(\overline{p} \vee p)}}, \quad \text{ley de De Morgan.}$$
$$\iff (\overline{p} \downarrow p) \downarrow (\overline{p} \downarrow p), \quad \text{equivalencia lógica NOR.}$$
$$\iff (\overline{(p \vee p)} \downarrow p) \downarrow (\overline{(p \vee p)} \downarrow p), \quad \text{ley de idempotencia.}$$
$$\iff (((p \downarrow p) \downarrow p) \downarrow ((p \downarrow p) \downarrow p)), \quad \text{equivalencia lógica NOR.}$$

Ejemplo 12:

Demostrar utilizando las leyes de la lógica proposicional que las proposiciones compuestas $\overline{(p \wedge \overline{q})} \vee (p \leftrightarrow q)$ y $((p \downarrow p) \downarrow q) \downarrow ((p \downarrow p) \downarrow q)$ son lógicamente equivalentes.

Los pasos que justifican la demostración son los siguientes:

$\overline{(p \wedge \overline{q})} \vee (p \leftrightarrow q)$

$$\iff (\overline{p} \vee q) \vee (p \leftrightarrow q), \quad \text{ley de De Morgan.}$$
$$\iff (\overline{p} \vee q) \vee ((p \rightarrow q) \wedge (q \rightarrow p)) \ , \quad \text{equivalencia lógica doble implicación.}$$
$$\iff (\overline{p} \vee q) \vee ((\overline{p} \vee q) \wedge (\overline{q} \vee p)), \quad \text{equivalencia lógica de la implicación.}$$
$$\iff \overline{p} \vee q, \quad \text{ley de absorción.}$$
$$\iff (\overline{p} \vee q) \wedge (\overline{p} \vee q), \quad \text{ley de la idempotencia.}$$
$$\iff \overline{\overline{(\overline{p} \vee q) \wedge (\overline{p} \vee q)}}, \quad \text{ley de la doble negación.}$$
$$\iff \overline{\overline{(\overline{p} \vee q)} \vee \overline{(\overline{p} \vee q)}}, \quad \text{ley de De Morgan.}$$
$$\iff (\overline{p} \downarrow q) \downarrow (\overline{p} \downarrow q), \quad \text{equivalencia lógica del NOR.}$$

$\iff (\overline{(p \vee p)} \downarrow q) \downarrow (\overline{(p \vee p)} \downarrow q)$, ley de idempotencia.

$\iff ((p \downarrow p) \downarrow q) \downarrow ((p \downarrow p) \downarrow q)$, equivalencia lógica del NOR.

1.1.9. Conectivo NAND ($\uparrow$)

El conectivo NAND es también un conectivo completo, en el sentido que, cualquier fórmula del cálculo proposicional puede ser escrita utilizando únicamente éste conectivo.

Mnemotecnicamente:

$NAND \approx Not\ AND \approx NO\ y \approx \sim(p \wedge q) \approx \overline{(p \wedge q)} \approx p \not\wedge q \approx p \uparrow q$

Ejemplo 13:

Demostrar que el conectivo NAND es un conectivo completo.

De forma similar como se demostró que el conectivo NOR es un conectivo completo, también se demuestra que el conectivo NAND es un conectivo completo, de esta forma se debe representar los conectivos $\sim$, $\vee$, $\wedge$, $\rightarrow$ y $\leftrightarrow$, utilizando únicamente el conectivo NAND.

Representación de la negación utilizando únicamente el NAND:

$\overline{p} \iff \overline{p \wedge p}$, ley de idempotencia

$\iff p \uparrow p$, equivalencia lógica de la NAND.

Representación de la disyunción utilizando únicamente el NAND:

$p \vee q \iff \overline{\overline{p \vee q}}$, ley de la doble negación.

$\iff \overline{\overline{p} \wedge \overline{q}}$, ley de De Morgan.

$\iff \overline{\overline{(p \wedge p)} \wedge \overline{(q \wedge q)}}$, ley de idempotencia.

$\iff (p \uparrow p) \uparrow (q \uparrow q)$, equivalencia lógica NAND.

Representación de la conjunción utilizando únicamente el NAND:

$p \wedge q \iff (p \wedge q) \vee (p \wedge q)$, ley de idempotencia.

$\iff \overline{\overline{(p \wedge q) \vee (p \wedge q)}}$, ley de doble negación.

$\iff \overline{\overline{(p \wedge q)} \wedge \overline{(p \wedge q)}}$, ley de De Morgan.

$\iff (p \uparrow q) \uparrow (p \uparrow q)$, equivalencia lógica NAND.

Representación de la implicación utilizando únicamente el NAND:

$p \to q \iff \overline{p} \vee q$, equivalencia lógica de la implicación.

$\iff \overline{\overline{(\overline{p} \vee q)}}$, ley de la doble negación.

$\iff \overline{(p \wedge \overline{q})}$, ley de De Morgan.

$\iff \overline{(p \wedge \overline{(q \wedge q)})}$, ley de idempotencia.

$\iff (p \uparrow (q \uparrow q))$, equivalencia lógica NAND.

Representación de la doble implicación utilizando únicamente el NAND:

$p \leftrightarrow q \iff (p \to q) \wedge (q \to p)$, equivalencia lógica de la doble implicación.

$\iff (\overline{p} \vee q) \wedge (\overline{q} \vee p)$, equivalencia lógica de la implicación.

$\iff ((\overline{p} \vee q) \wedge \overline{q}) \vee ((\overline{p} \vee q) \wedge p)$, ley distributiva.

$\iff ((\overline{p} \wedge \overline{q}) \vee (q \wedge \overline{q})) \vee ((\overline{p} \wedge p) \vee (q \wedge p))$, ley distributiva.

$\iff ((\overline{p} \wedge \overline{q}) \vee F) \vee (F \vee (q \wedge p))$, ley inversa.

$\iff ((\overline{p} \wedge \overline{q})) \vee ((q \wedge p))$, ley de identidad.

$\iff \overline{\overline{(\overline{p} \wedge \overline{q}) \vee (q \wedge p)}}$, ley de doble negación.

$\iff \overline{\overline{(\overline{p} \wedge \overline{q})} \wedge \overline{(q \wedge p)}}$, ley de De Morgan.

$\iff \overline{\overline{(\overline{(p \wedge p)} \wedge \overline{(q \wedge q)})} \wedge \overline{(q \wedge p)}}$, ley de idempotencia.

$\iff ((p \uparrow p) \uparrow (q \uparrow q)) \uparrow (q \uparrow p)$, equivalencia lógica NAND.

Ejemplo 14:

Representar la proposición $\overline{(p \vee q)} \otimes \overline{q}$ utilizando sólo con el conectivo NAND ($\uparrow$), y donde se utilice la mínima cantidad de estos.

Para utilizar la mínima cantidad de conectivos NAND, en necesario simplificar primero la proposición compuesta, para luego, sobre la simplificación buscar el equivalente uti-

lizando únicamente el conectivo NAND. De esta forma se tiene:

$$\begin{aligned}
\overline{(p \vee q) \otimes \overline{q}} &\iff \overline{\overline{((\overline{(p \vee q)} \wedge \overline{q}) \vee ((p \vee q) \wedge \overline{\overline{q}}))}}, \quad \text{equivalencia lógica del X-OR} \\
&\iff \overline{\overline{((\overline{(p \vee q)} \wedge \overline{q}) \vee ((p \vee q) \wedge q))}}, \quad \text{ley de doble negación} \\
&\iff \overline{\overline{(\overline{(p \vee q)} \wedge \overline{q})} \wedge \overline{((p \vee q) \wedge q)}}, \quad \text{ley de De Morgan} \\
&\iff \overline{\overline{(\overline{(p \vee q)} \wedge \overline{q})} \wedge \overline{(q)}}, \quad \text{ley de absorción} \\
&\iff (\overline{\overline{(\overline{(p \vee q)} \vee \overline{\overline{q}}\ )}} \wedge \overline{(q)}, \quad \text{ley de De Morgan} \\
&\iff ((p \vee q) \vee q) \wedge \overline{q}, \quad \text{ley de doble negación} \\
&\iff (p \vee (q \vee q)) \wedge \overline{q}, \quad \text{ley asociativa} \\
&\iff (p \vee q) \wedge \overline{q}, \quad \text{ley de idempotencia} \\
&\iff (q \wedge \overline{q}) \vee (p \wedge \overline{q}), \quad \text{ley distributiva} \\
&\iff F \vee (p \wedge \overline{q}), \quad \text{ley inversa} \\
&\iff p \wedge \overline{q}, \quad \text{ley de identidad} \\
&\iff (p \wedge \overline{q}) \vee (p \wedge \overline{q}), \quad \text{ley de idempotencia} \\
&\iff \overline{\overline{(p \wedge \overline{q}) \vee (p \wedge \overline{q})}}, \quad \text{ley de doble negación} \\
&\iff \overline{\overline{(p \wedge \overline{q})} \wedge \overline{(p \wedge \overline{q})}}, \quad \text{ley de De Morgan} \\
&\iff (p \uparrow \overline{q}) \uparrow (p \uparrow \overline{q}), \quad \text{equivalencia lógica del NAND} \\
&\iff (p \uparrow \overline{(q \wedge q)}) \uparrow (p \uparrow \overline{(q \wedge q)}), \quad \text{ley de idempotencia} \\
&\iff (p \uparrow (q \uparrow q)) \uparrow (p \uparrow (q \uparrow q)), \quad \text{equivalencia lógica del NAND}
\end{aligned}$$

1.1.10. Ejercicios

1. Determinar cuáles de las siguientes asignaciones de verdad a las proposiciones primitivas p, q, r y s hacen que la proposición compuesta $(p \wedge (q \vee r)) \rightarrow (r \wedge s)$ tome el valor falso.

   a) p=V, q=V, r=F, s=V
   b) p=V, q=V, r=F, s=F
   c) p=F, q=F, r=V, s=F
   d) p=V, q=F, r=V, s=V
   e) p=V, q=F, r=V, s=F
   f) p=F, q=F, r=F, s=F
   g) p=V, q=V, r=V, s=V

2. Identificar cuáles de las siguientes proposiciones compuestas son tautologías.

   a) $p \to ((\neg(r \wedge s) \vee (t \leftrightarrow (v \to (\neg w \vee q))) \vee (r \vee w)) \to p)$

   b) $(p \to q) \to p$

   c) $(p \to q) \leftrightarrow (\neg p \leftrightarrow \neg q)$

   d) $\neg(\neg(\neg(\neg p \vee p) \vee p) \vee p) \vee p$

   e) $(p \to (q \vee r)) \to ((p \to q) \vee (p \to r))$

3. Simplificar las siguientes proposiciones compuestas utilizando las leyes de la lógica proposicional. En cada paso de la simplificación registrar la regla que se utilizó.

   a) $p \to (p \to (p \to (\overline{p} \to (r \vee s))))$

   Respuesta: V

   b) $(\overline{p} \vee q) \wedge [(p \wedge \overline{q}) \vee (\overline{p} \wedge q)] \wedge (p \vee \overline{q})$

   Respuesta: F

   c) $(p \wedge \overline{q}) \vee (\overline{p} \wedge q) \vee [(\overline{p} \vee q) \wedge (p \vee \overline{q})]$

   Respuesta: V

   d) $(p \wedge q \wedge r) \vee (p \wedge t \wedge \overline{q}) \vee (p \wedge t \wedge r)$

   Respuesta: $p \wedge ((q \vee t) \wedge (r \vee (t \wedge \overline{q})))$

   e) $(p \wedge q \wedge r) \vee (p \wedge t \wedge \overline{q}) \vee (p \wedge \overline{t} \wedge r)$

   f) $(x \otimes y) \otimes x$

   Respuesta: y

   g) $\overline{(x \otimes y)} \to \overline{y}$

   Respuesta: $\overline{x \wedge y}$

   h) $(p \downarrow q) \otimes (p \uparrow q)$

   i) $(p \downarrow q) \downarrow (p \otimes q)$

   j) $(p \downarrow q) \uparrow (p \otimes q)$

   k) $(p \downarrow q) \leftrightarrow (p \uparrow q)$

   l) $((p \uparrow q) \uparrow p) \uparrow (q \uparrow q)$

   m) $((p \uparrow q) \downarrow p) \uparrow (q \downarrow q)$

   n) $(((p \uparrow q) \uparrow p) \uparrow q) \uparrow q$

   ñ) $(((p \downarrow q) \uparrow p) \downarrow q) \uparrow q$

   o) $((p \downarrow q) \downarrow p) \downarrow (q \downarrow q)$

   p) $((p \uparrow q) \downarrow p) \downarrow (q \uparrow q)$

   q) $(((p \downarrow q) \downarrow p) \downarrow q) \downarrow q$

   r) $(((p \uparrow q) \uparrow p) \downarrow q) \downarrow q$

4. Representar las siguientes proposiciones compuestas utilizando únicamente el conectivo NOR ($\downarrow$)

   a) $(p \vee \overline{q}) \wedge (\overline{p} \vee q)$

   b) $(\overline{p} \wedge \overline{q}) \vee (p \leftrightarrow q)$

   Respuesta: $p \leftrightarrow q \Leftrightarrow ((p \downarrow p) \downarrow q) \downarrow ((q \downarrow q) \downarrow p)$

   c) $(p \wedge \overline{q}) \vee (p \leftrightarrow q)$

   Respuesta: $q \rightarrow p \Leftrightarrow ((q \downarrow q) \downarrow p) \downarrow ((q \downarrow q) \downarrow p)$

   d) $(\overline{p} \wedge \overline{q}) \wedge (p \leftrightarrow q)$

   e) $(p \wedge \overline{q}) \wedge (p \leftrightarrow q)$

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

   Respuesta: $((p \downarrow p) \downarrow p) \downarrow ((p \downarrow p) \downarrow p)$

   g) $\overline{p \Leftrightarrow q}$

   h) $p \otimes q$

   i) $(\overline{p \otimes q}) \vee (\overline{p} \leftrightarrow q)$

   Respuesta: $(p \downarrow (p \downarrow p)) \downarrow (p \downarrow (p \downarrow p))$

5. Representar las siguientes proposiciones compuestas utilizando únicamente el conectivo NAND ($\uparrow$)

   a) $(p \wedge \overline{q}) \vee (\overline{p} \vee q)$

   Respuesta: $(p \uparrow p) \uparrow p$

   b) $(\overline{p} \wedge \overline{q}) \vee (p \leftrightarrow q)$

   c) $(p \wedge \overline{q}) \vee (p \leftrightarrow q)$

   Respuesta: $(p \uparrow (q \uparrow q)) \uparrow ((p \uparrow p) \uparrow (q \uparrow q)) \uparrow (p \uparrow q)$

   d) $(\overline{p} \wedge \overline{q}) \wedge (p \leftrightarrow q)$

   e) $(p \wedge \overline{q}) \wedge (p \leftrightarrow q)$

   f) $\overline{p \Leftrightarrow q}$

   g) $(\overline{p \wedge \overline{q}}) \vee (p \otimes q)$

   Respuesta: $p \uparrow (p \uparrow p)$

   h) $p \otimes q$

   Respuesta: $(p \uparrow (q \uparrow q)) \uparrow ((p \uparrow p) \uparrow q)$

   i) $(p \uparrow q) \wedge (p \otimes q)$

   j) $(p \uparrow q) \vee (p \otimes q)$

1.2. Reglas de inferencia

Las reglas de inferencia son utilizadas en la lógica proposicional, para demostrar que una conclusión se sigue lógicamente de un conjunto de hipótesis, al utilizar una serie de pasos que involucran reglas de inferencia y/o leyes de la lógica proposicional.

1.2.1. Tabla de reglas de inferencia

Regla de inferencia	Tautología	Nombre
$\begin{array}{l} p \\ \hline \therefore p \vee q \end{array}$	$p \rightarrow (p \vee q)$	Adicion
$\begin{array}{l} p \wedge q \\ \hline \therefore p \end{array}$	$(p \wedge q) \rightarrow p$	Simplifación
$\begin{array}{l} p \\ q \\ \hline \therefore p \wedge q \end{array}$	$[(p) \wedge (q)] \rightarrow (p \wedge q)$	Conjunción
$\begin{array}{l} p \\ p \rightarrow q \\ \hline \therefore q \end{array}$	$[p \wedge (p \rightarrow q)] \rightarrow q$	Modus Ponens
$\begin{array}{l} \neg q \\ p \rightarrow q \\ \hline \therefore \neg p \end{array}$	$[\neg q \wedge (p \rightarrow q)] \rightarrow \neg p$	Modus Tollens
$\begin{array}{l} p \rightarrow q \\ q \rightarrow r \\ \hline \therefore p \rightarrow r \end{array}$	$[(p \rightarrow q) \wedge (q \rightarrow r)] \rightarrow (p \rightarrow r)$	Silogismo Hipotético
$\begin{array}{l} p \vee q \\ \neg p \\ \hline \therefore q \end{array}$	$[(p \vee q) \wedge \neg p] \rightarrow q$	Silogismo Disyuntivo
$\begin{array}{l} p \vee q \\ \neg p \vee r \\ \hline \therefore q \vee r \end{array}$	$[(p \vee q) \wedge (\neg p \vee r)] \rightarrow (q \vee r)$	Resolucion

Ejemplo 15:

El siguiente razonamiento es un ejemplo de la regla de inferencia de adición:

"Antonio es una persona joven. Por lo tanto, Antonio es una persona joven o Antonio es una persona saludable".

A partir del enunciado del razonamiento se obtienen las proposiciones:

p : Antonio es una persona joven
q : Antonio es una persona saludable

El razonamiento puede ser reescrito ahora como la regla de inferencia de adición:

$$\frac{p}{\therefore p \vee q}$$

Ejemplo 16:

El siguiente razonamiento es un ejemplo de la regla de inferencia de simplificación:

"Antonio es una persona joven y Antonio es una persona saludable. Por lo tanto, Antonio es una persona joven".

A partir del enunciado del razonamiento se obtienen las proposiciones:

p : Antonio es una persona joven
q : Antonio es una persona saludable

El razonamiento puede ser reescrito ahora como la regla de inferencia de simplificación:

$$\frac{p \wedge q}{\therefore p}$$

Ejemplo 17:

El siguiente razonamiento es un ejemplo de la regla de inferencia de conjunción:

"Rosa es elegida presidenta de la junta de acción comunal. Elena ingresa a la junta de acción comunal. Por lo tanto, Rosa es elegida presidenta de la junta de acción comunal y Elena ingresa a la junta de acción comunal".

A partir del enunciado del razonamiento se obtienen las proposiciones:

p : Rosa es elegida presidenta de la junta de acción comunal
q : Elena ingresa a la junta de acción comunal

El razonamiento puede ser reescrito ahora como la regla de inferencia de conjunción:

p
q
$\therefore p \wedge q$

Ejemplo 18:

El siguiente razonamiento es un ejemplo de la regla de inferencia de Modus Ponens:

"Si Lina gana 100 millones de pesos en la lotería, entonces, José renunciará a su trabajo. Lina ganó 100 millones de pesos en la lotería. Por lo tanto, José renunciará a su trabajo".

A partir del enunciado del razonamiento se obtienen las proposiciones:

p : Lina gana 100 millones de pesos en la lotería
q : José renuncia a su trabajo

El razonamiento puede ser reescrito ahora como la regla de inferencia de Modus Ponens:

$p \rightarrow q$
p
$\therefore q$

Ejemplo 19:

El siguiente razonamiento es un ejemplo de la regla de inferencia de Modus Tollens:

"Si Lina gana 100 millones de pesos en la lotería, entonces, José renunciará a su trabajo. Se sabe que José no renunció a su trabajo. Por lo tanto, Lina no ganó 100 millones de pesos en la lotería".

A partir del enunciado del razonamiento se obtienen las proposiciones:

p : Lina gana 100 millones de pesos en la lotería
q : José renuncia a su trabajo

El razonamiento puede ser reescrito ahora como la regla de inferencia de Modus Tollens:

$p \rightarrow q$
$\neg q$
$\therefore \neg p$

Ejemplo 20:

El siguiente razonamiento es un ejemplo de la regla de inferencia de silogismo hipotético:

"Si hoy es un día lluvioso, entonces no debemos tener un asado hoy. Si no debemos tener un asado hoy, entonces debemos tener un asado mañana, Por lo tanto, si hoy es un día lluvioso, entonces debemos tener un asado mañana".

A partir del enunciado del razonamiento se obtienen las proposiciones:

p : Hoy es un día lluvioso

q : No debemos tener un asado hoy

r : Debemos tener el asado mañana

El razonamiento puede ser reescrito ahora como la regla de inferencia de silogismo hipotético:

$p \to q$
$q \to r$

$\therefore p \to r$

Ejemplo 21:

El siguiente razonamiento es un ejemplo de la regla de inferencia de silogismo disyuntivo:

"La billetera de Carlos está en su bolsillo o la billetera de Carlos está en la mesa. Se sabe que la billetera de Carlos no está en su bolsillo. Por lo tanto, la billetera de Carlos está en la mesa".

A partir del enunciado del razonamiento se obtienen las proposiciones:

p : La billetera de Carlos está en su bolsillo

q : La billetera de Carlos está en la mesa

El razonamiento puede ser reescrito ahora como la regla de inferencia de silogismo disyuntivo:

$p \vee q$
$\neg p$

$\therefore q$

1.2.2. Utilización de las reglas de inferencia para demostrar la validez de razonamientos

Ejemplo 22:

Determinar si el siguiente razonamiento es válido:

$\overline{g}$
$\overline{g} \rightarrow e$
$e \rightarrow k$
$k \rightarrow \overline{l}$
$\overline{l} \rightarrow m$
$m \rightarrow b$
$\therefore b$

En la solución de todos los ejemplos de esta sección, se numeran cada una de las hipótesis, para después poder referenciar a cada una de las éstas en las razones que justifican cada uno de los resultados en los pasos. Por ejemplo, para referenciar a la hipótesis 4 se utiliza H_4. De forma similar, para referenciar el resultado del paso i del análisis, se utilizará P_i.

La numeración de las hipótesis es la siguiente:

1. $\overline{g}$
2. $\overline{g} \rightarrow e$
3. $e \rightarrow k$
4. $k \rightarrow \overline{l}$
5. $\overline{l} \rightarrow m$
6. $m \rightarrow b$

   $\therefore b$

Los pasos, resultados y razones que se necesitan para demostrar la validez del razonamiento son los siguientes:

Pasos	**Resultados**	**Razones**
1.	e	Regla Modus Ponens entre H_1 e H_2
2.	k	Regla Modus Ponens entre P_1 e H_3
3.	$\overline{l}$	Regla Modus Ponens entre P_2 e H_4
4.	m	Regla Modus Ponens entre P_3 e H_5
5.	b	Regla Modus Ponens entre P_4 e H_6

Como la conclusión se obtiene a partir de las hipótesis y de la utilización de las reglas

de inferencia, entonces se concluye que el razonamiento es válido.

Ejemplo 23:

Mostrar o refutar que las hipótesis $p \to (q \to r)$, $\overline{q} \to \overline{p}$ y p implican la conclusión r.

El razonamiento se puede reescribir como:

1. $p \to (q \to r)$
2. $\overline{q} \to \overline{p}$
3. p

$\therefore r$

Los pasos y razones necesarios para obtener la conclusión a partir de las hipótesis, son:

Pasos	**Resultados**	**Razones**
1.	q	Regla Modus Tollens entre H_2 e H_3
2.	$q \to r$	Regla Modus Ponens entre H_1 e H_3
3.	r	Regla Modus Ponens entre P_1 y P_2

El razonamiento es válido porque la conclusión se obtiene a partir las hipótesis y del uso de algunas de las reglas de inferencia.

Ejemplo 24:

En el siguiente razonamiento ya se han enumerado las hipótesis, determinar su validez.

1. $p \to r$
2. $p \to q$

$\therefore p \to (r \wedge q)$

La justificación de la validez del razonamiento se apoya en los siguientes pasos, resultados y razones:

Pasos	**Resultados**	**Razones**
1.	$\overline{p} \vee r$	Equivalencia lógica de la implicación en H_1
2.	$\overline{p} \vee q$	Equivalencia lógica de la implicación en H_2
3.	$(\overline{p} \vee r) \wedge (\overline{p} \vee q)$	Regla de Conjunción entre P_1 y P_2
4.	$\overline{p} \vee (r \wedge q)$	Ley distributiva en P_3
5.	$p \to (r \wedge q)$	Equivalencia lógica de la implicación en P_4

Utilizando las leyes de la lógica, las reglas de inferencia y las hipótesis originales, se obtiene la conclusión del razonamiento, por lo tanto el razonamiento es válido.

Ejemplo 25:

Determinar si el siguiente razonamiento es válido. En el razonamiento las hipótesis ya están numeradas.

1. $p \to q$
2. $q \to s$
3. $r \to \overline{s}$
4. $\overline{p} \otimes r$

$\therefore \overline{r}$

Los pasos, resultados y razones necesarios para deducir la conclusión a partir de las hipótesis, el uso de las leyes de la lógica proposicional y del uso de las reglas de inferencia, son:

Pasos	**Resultados**	**Razones**
1.	$(p \wedge r) \vee (\overline{p} \wedge \overline{r})$	Equivalencia lógica del X-OR en H_4
2.	$p \to s$	Regla de Silogismo hipotético entre H_1 e H_2
3.	$\overline{r} \vee \overline{s}$	Equivalencia lógica de la implicación en H_3
4.	$\overline{s} \vee \overline{r}$	Ley conmutativa en P_3
5.	$s \to \overline{r}$	Equivalencia lógica de la implicación en P_4
6.	$p \to \overline{r}$	Regla de Silogismo Hipotético entre P_2 y P_5
7.	$\overline{p} \vee \overline{r}$	Equivalencia lógica de la implicación en P_6
8.	$\overline{(p \wedge r)}$	Ley de De Morgan en P_7
9.	$\overline{p} \wedge \overline{r}$	Regla de Silogismo Disyuntivo entre P_1 y P_8
10.	$\overline{r}$	Regla de simplificación en P_9

Se obtiene la conclusión, por lo tanto el razonamiento es válido.

Ejemplo 26:

Determinar si el siguiente razonamiento es válido:

$(p \wedge q) \vee r$
$r \to s$
$(p \vee s) \to \overline{t}$
$(q \vee s) \to u$

$\therefore \overline{u} \to \overline{t}$

La numeración de las hipótesis en el razonamiento es el siguiente:

1. $(p \wedge q) \vee r$
2. $r \to s$
3. $(p \vee s) \to \overline{t}$
4. $(q \vee s) \to u$

$\therefore \overline{u} \to \overline{t}$

La validez del razonamiento se obtiene con los siguientes pasos, resultados y razones:

Pasos	**Resultados**	**Razones**
1.	$(p \vee r) \wedge (q \vee r)$	Ley distributiva en H_1
2.	$p \vee r$	Regla de Simplificación del P_1
3.	$\overline{p} \to r$	Equivalencia lógica de la implicación del P_2
4.	$\overline{p} \to s$	Regla de Silogismo Hipotético entre P_3 e H_2
5.	$p \vee s$	Equivalencia lógica de la implicación del P_4
6.	$\overline{t}$	Regla Modus Ponens entre P_5 e H_3
7.	$q \vee r$	Regla de Simplificación del P_1
8.	$\overline{q} \to r$	Equivalencia lógica de la implicación del P_7
9.	$\overline{q} \to s$	Regla de Silogismo Hipotético entre P_8 e H_2
10.	$q \vee s$	Equivalencia lógica de la implicación del P_9
11.	u	Regla Modus Ponens entre P_{10} e H_4
12.	$u \vee \overline{t}$	Regla de Adición entre P_{11} y P_6
13.	$\overline{u} \to \overline{t}$	Equivalencia lógica de la implicación del P_{12}

Se obtiene la conclusión a partir de las hipótesis, de la aplicación de las leyes de la lógica proposicional y de reglas de inferencia. De esta forma la validez del razonamiento queda demostrada, pero, el resultado del paso número 12 a pesar de que es correcto no se ve muy "natural". Por este motivo la validez de este razonamiento se demostrará de nuevo en el capítulo 3 de Técnicas de Demostración en la subsección 3.2.2 de Técnica de Demostración por Contradicción, donde se obtiene una demostración más natural y aceptable para este razonamiento.

Ejemplo 27:

Mostrar o refutar que las hipótesis $q \vee p$, $\overline{p \vee \overline{r}}$, $r \to s$ y $(q \wedge s) \to (t \wedge s)$ implican la conclusión t.

El razonamiento se puede reescribir numerando las hipótesis de la siguiente forma:

1. $q \vee p$
2. $\overline{p \vee \overline{r}}$
3. $r \to s$
4. $\underline{(q \wedge s) \to (t \wedge s)}$

   $\therefore t$

Una forma correcta para establecer la validez del razonamiento es la siguiente:

Pasos	**Resultados**	**Razones**
1.	$\overline{p} \wedge r$	Ley de De Morgan en H_2
2.	$\overline{p}$	Regla de Simplificación del P_1
3.	r	Regla de Simplificación del P_1
4.	s	Regla Modus Ponens entre P_3 e H_3
5.	q	Regla de Silogismo disyuntivo entre P_2 e H_1
6.	$q \wedge s$	Regla de Conjunción entre P_5 y P_4
7.	$t \wedge s$	Regla Modus Ponens entre P_6 e H_4
8.	t	Regla de Simplificación del P_7

Se obtiene la conclusión del razonamiento a partir del conjunto de hipótesis, y del adecuado uso tanto, de las leyes de la lógica proposicional, como de las reglas de inferencia. Por lo tanto el razonamiento es correcto.

Ejemplo 28:

Determinar si el siguiente razonamiento es válido:

1. $u \to r$
2. $(r \wedge s) \to (p \vee t)$
3. $q \to (u \wedge s)$
4. $\underline{\overline{t}}$

   $\therefore q \to p$

Los pasos y razones que se necesitan para demostrar la validez del razonamiento son los siguientes:

Pasos	**Resultados**	**Razones**
1.	$\overline{(r \wedge s)} \vee (p \vee t)$	Equivalenca lógica de la implicación en H_2
2.	$(\overline{(r \wedge s)} \vee p) \vee t$	Ley asociativa en P_1
3.	$(\overline{(r \wedge s)} \vee p)$	Regla de Silogismo Disyuntivo entre P_2 e H_4
4.	$(\overline{r} \vee \overline{s}) \vee p$	Ley de De Morgan en P_3
5.	$\overline{r} \vee (\overline{s} \vee p)$	Ley asociativa en P_4
6.	$r \rightarrow (\overline{s} \vee p)$	Equivalenca lógica de la implicación en P_5
7.	$u \rightarrow (\overline{s} \vee p)$	Regla de Silogismo Hipotético entre H_1 y P_6
8.	$\overline{u} \vee (\overline{s} \vee p)$	Equivalenca lógica de la implicación en P_7
9.	$(\overline{u} \vee \overline{s}) \vee p$	Ley asociativa en P_8
10.	$\overline{(\overline{u} \vee \overline{s})} \rightarrow p$	Equivalenca lógica de la implicación en P_9
11.	$(u \wedge s) \rightarrow p$	Ley de De Morgan en P_{10}
12.	$q \rightarrow p$	Regla de Silogismo Hipotético entre H_3 y P_{11}

Se obtiene la conclusión a partir de las hipótesis, de la aplicación de las leyes de la lógica proposicional y de las reglas de inferencia, de esta forma queda demostrada la validez del razonamiento. Este ejemplo, también se demostrará de nuevo en el capítulo 3 de Técnicas de Demostración, utilizando una método diferente.

1.2.3. Ejercicios

1. Escribir cada uno de los siguientes argumentos en forma simbólica, después determine por reglas de inferencia si cada uno de éstos es válido:

   a) Si Carlos va a la carrera de autos, entonces Elena se enojará. Si Rafael juega cartas toda la noche, entonces Carmen se enojará. Si Elena o Carmen se enojan, le avisarán a Verónica (su abogado). Verónica no ha tenido noticias de estas dos clientes. En consecuencia, ni Carlos fue a la carrera ni Rafael jugó cartas toda la noche.

   b) Si Rosa María obtiene el puesto de supervisor y trabaja mucho, entonces obtendrá un aumento. Si obtiene el aumento, entonces comprará un auto nuevo. Ella no ha adquirido un auto nuevo. Por lo tanto, Rosa María no ha obtenido el puesto de supervisor o no ha trabajado mucho.

   c) Si la banda no pudiera tocar rock o las bebidas no llegasen a tiempo, entonces la fiesta de Año Nuevo tendría que cancelarse y Alicia se enojaría. Si la fiesta se cancelara, habría que devolver el dinero. No se devolvió el dinero. Por lo tanto, la banda pudo tocar rock.

   d) Si Tomás tiene 17 años, entonces es de la misma edad de Juana. Si José no tiene la misma edad de Tomás, entonces José tiene distinta edad que Juana. Tomás tiene 17 años y José tiene la misma edad que Juana. Por lo tanto, José tiene la misma edad que Tomás y Tomás tiene la misma edad que Juana.

e) Si es verdad que si llueve entonces los estudiantes se acuestan, entonces los estudiantes no estudian. Si los estudiantes aprueban el examen entonces o los estudiantes estudian o el examen es trivial. Si el examen es trivial, entonces los estudiantes son flojos. Es un hecho que los estudiantes aprueban el examen y no son flojos. Por lo tanto, llueve y los estudiantes no se acuestan.

f) Si el contrato es legal y Pérez entró en el contrato, entonces García ganará el pleito. O García no ganará el pleito o Pérez será responsable. Pérez no será responsable. Por lo tanto, o el contrato no es legal o Pérez no entró en el contrato.

2. Determinar si cada uno de los siguientes razonamientos es válido. Para cada uno de los pasos del análisis, indicar, que regla de inferencia o ley de la lógica proposicional se utilizó y sobre que hipótesis o resultados intermedios se aplicó.

a) $(\overline{q} \to \overline{p})$
$(q \to \overline{r})$
$\underline{(\overline{\overline{p} \wedge r})}$
$\therefore \overline{r}$

b) $\overline{\overline{(\overline{(p \wedge q)} \wedge \overline{r})}}$
$(\overline{r} \vee s)$
$((p \vee s) \to \overline{t})$
$\underline{((q \vee s) \to u)}$
$\therefore (t \to u)$

c) $\overline{\overline{r \wedge \overline{t}}}$
$\overline{q} \vee r$
$\overline{q} \to \overline{p}$
p
$\underline{\overline{q} \vee u \vee \overline{t}}$
$\therefore u$

d) p
$p \to q$
$r \to \overline{q}$
$\underline{s \vee r}$
$\therefore s \vee t$

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

f) $\overline{p} \leftrightarrow q$
$q \to r$
$\overline{r}$
$\therefore p$

g) $t \to (p \wedge s)$
$q \to \overline{p}$
$r \to \overline{s}$
$r \vee q$
$\therefore \overline{t}$

h) $(x = 5) \ \vee \ (x < y)$
$((x > 3) \ \vee \ (z < 2)) \to ((z < x) \ \vee \ (y = 1))$
$(x < y) \to (z < 2)$
$(x = 5) \to (x > 3)$
$(z < x) \to (x = 4)$
$(y = 1) \to \overline{((x > 3) \ \vee \ (z < 2))}$
$\therefore (x = 4)$

i) $(x > y) \ \vee \ (x < 6)$
$(x > y) \to (x > 4)$
$(x > 4) \to ((x = 5) \ \wedge \ (x < 7))$
$(x < 6) \to ((x = 5) \ \wedge \ (x < 7))$
$((x < 7) \ \wedge \ (x = 5)) \to ((z > x) \ \vee \ (y < z))$
$(x > y) \to \overline{((y < z) \ \vee \ (z > x))}$
$\therefore (x < 6)$

1.3. Lógica de predicados

El cálculo de predicados aparece gracias a la limitante de la lógica proposicional para representar situaciones como:

- Todo Hombre es mortal.
- Ningún número par divide a todos los números mayores o iguales a el.
- Juan ama a todas las mujeres hermosas.
- Existen personas menores de 30 años que sufren de hipertensión arterial.

Es necesario enriquecer a la lógica proposicional con elementos tales como:

- Funciones proposicionales (o predicados). Al ser funciones es necesario definir las variables de las funciones proposicionales y los dominios de dichas variables, que son conocidos con el nombre de universo del discurso.
- Cuantificadores universales y existenciales y el alcance de estos.

Esta lógica proposicional enriquecida es lo que se conoce como cálculo de predicados o lógica de predicados.

Es normal encontrar expresiones que involucran variables tales como:

- $x > 3$
- $x = y + 3$
- $x = y + z$

las cuales son frecuentemente encontradas en declaraciones matemáticas y en programas de computador.

Cuando los valores de las variables no son especificados, estas expresiones no son ni verdaderas ni falsas.

Ejemplo 29:

La expresión $x > 3$ se puede representar como $P(x) : x > 3$, donde la variable x es el sujeto de la expresión y "Es mayor que 3" es el predicado o propiedad que el sujeto de la expresión puede tener y que es representado por $P(x)$. La expresión $P(x)$ tomará el valor de verdad de la función proposicional P evaluada en x.

Una vez que le es asignado un valor a la variable x, la expresión $P(x)$ se convierte en una proposición y tiene un valor de verdad determinado.

Ejemplo 30:

Sea el predicado $P(x) : x > 3$, donde el universo del discurso (dominio de las x's) es el conjunto de los números naturales. ¿Cuáles son los valores de verdad de $P(2)$ y $P(6)$?

- $P(2) : 2 > 3$, como es falso que 2 sea mayor que 3 entonces $P(2)$ es Falso.
- $P(6) : 6 > 3$, como es verdadero que 6 sea mayor que 3 entonces $P(6)$ es Verdadero.

En general una expresión que involucra las n variables $x_1,\ x_2,\ x_3,\ \ldots,\ x_n$ puede ser denotada por $P(x_1,\ x_2,\ x_3,\ \ldots,\ x_n)$, de esta forma se deja en evidencia que un predicado puede estar definido en términos de más de una variable.

1.3.1. Cuantificador universal

La cuantificación universal de $P(x)$ es la proposición "para todo x del universo del discurso, $P(x)$", la cual es representada con la notación $\forall_x P(x)$. Aquí $\forall$ es llamado cuantificador universal.

Ejemplo 31:

Sea el predicado $V(x) : x$ es una vocal, donde el universo del discurso es el conjunto de letras del alfabeto español. ¿Cuál es la interpretación en palabras y el valor de verdad de la expresión $\forall_x V(x)$?

Para la expresión $\forall_x V(x)$ la interpretación en palabras es: "Toda letra del alfabeto español es una vocal", cuyo valor de verdad es falso, porque las letras consonantes no son vocales.

Ejemplo 32:

Representar la siguiente expresión en el cálculo de predicados: "Todo lo que brilla es oro".

Sean los predicados $B(x) : x$ brilla, $\quad O(x) : x$ es oro, donde el universo del discurso es el conjunto de metales; de esta forma la expresión "Todo lo que brilla es oro" se puede representar por: $\forall_x(B(x) \rightarrow O(x))$.

Ejemplo 33:

Representar por medio del cálculo de predicados la expresión: "Todo estudiante universitario en Colombia ha estudiado trigonometría".

Sea el predicado $P(x) : x$ ha estudiado trigonometría, donde el universo del discurso es el conjunto de los estudiantes universitarios colombianos. Entonces apoyados en el predicado anterior y en el cuantificador universal se tiene que la expresión: "Todo estudiante universitario en Colombia ha estudiado trigonometría" se representa con $\forall_x P(x)$.

La expresión anterior también se puede representar en cálculo de predicados de la siguiente forma: $\forall_x(U(x) \rightarrow T(x))$, donde el universo del discurso es el conjunto de todos los estudiantes colombianos, y se tienen los siguientes predicados:

- $U(x) :$ x es un estudiante universitario.
- $T(x) :$ x ha estudiado trigonometría.

Ejemplo 34:

Sea el predicado $Q(x) : x < 2$, donde el universo del discurso es el conjunto de los números reales. ¿Cuál es el valor de verdad de $\forall_x Q(x)$?

$Q(x)$ no es verdadera para todos los números reales x, por ejemplo $Q(4)$ es falsa, por lo tanto $\forall_x Q(x)$ es falsa.

Cuando todos los elementos del universo del discurso pueden ser listados, por ejemplo, $x_1,\ x_2,\ x_3,\ \ldots,\ x_n$ se tiene que el valor de verdad de $\forall_x P(x)$ es el mismo que el que se obtiene por la conjunción $P(x_1) \wedge P(x_2) \wedge P(x_3) \wedge \cdots \wedge P(x_n)$, de este modo $\forall_x P(x)$ solo es verdadero si todo $P(x_i)$ es verdadero, donde $1 \leq i \leq n$.

Ejemplo 35:

¿Cuál es el valor de verdad de $\forall_x P(x)$, donde se tiene el predicado $P(x) : x^2 < 10$ y el universo del discurso consiste del conjunto de los números entero positivos que no sobrepasen al 4?

La expresión $\forall_x P(x)$ toma el mismo valor de verdad que la conjunción de las proposiciones:

$$\begin{aligned} P(1) \wedge P(2) \wedge P(3) \wedge P(4) &\iff (1^2 < 10) \wedge (2^2 < 10) \wedge (3^2 < 10) \wedge (4^2 < 10) \\ &\iff (1 < 10) \wedge\ (4 < 10)\ \wedge\ (9 < 10) \wedge (16 < 10) \\ &\iff \quad (V_o) \quad \wedge \quad (V_o) \quad \wedge \quad (V_o) \quad \wedge \quad (F_o) \\ &\iff \quad F_o \end{aligned}$$

Entonces se tiene que $\forall_x P(x)$ es falsa en éste universo del discurso.

1.3.2. Cuantificador existencial

La cuantificación existencial de $P(x)$ es la proposición "Existe un x del universo del discurso tal que $P(x)$". La notación $\exists_x P(x)$ denota la cuantificación existencial de $P(x)$. Aquí $\exists$ es llamado el cuantificador existencial. La expresión $\exists_x P(x)$ es también expresada como: "Hay un x tal que $P(x)$", "hay al menos un x tal que $P(x)$" o "Para algún x, $P(x)$".

Ejemplo 36:

Sea el predicado $V(x) : x$ es una vocal, donde el universo del discurso es el conjunto de letras del alfabeto español. ¿Cuál es la interpretación en palabras y el valor de verdad de la expresión $\exists_x V(x)$?

Para la expresión $\exists_x V(x)$ la interpretación en palabras es: "Algunas letras del alfabeto español son vocales", cuyo valor de verdad es cierto.

Ejemplo 37:

Sea el predicado $Q(x) : \ x = x + 1$, ¿Cuál es el valor de verdad de $\exists_x Q(x)$ donde el universo del discurso es el conjunto de los números reales?

Como $Q(x)$ es falsa para todo número real x entonces $\exists_x Q(x)$ es falsa.

Cuando todos los elementos del universo del discurso pueden ser listados, por ejemplo $x_1,\ x_2,\ x_3,\ \ldots,\ x_n$, se tiene que el valor de verdad de $\exists_x P(x)$ es el mismo que el que se obtiene por la disyunción $P(x_1) \vee P(x_2) \vee P(x_3) \vee \cdots \vee P(x_n)$; de este modo $\exists_x P(x)$ es verdadero cuando al menos un solo $P(x_i)$ es verdadero, donde $1 \leq i \leq n$.

Ejemplo 38:

¿Cuál es el valor de verdad de $\exists_x P(x)$, donde se tiene el predicado $P(x) : x^2 > 10$ y el universo del discurso consiste del conjunto de los números entero positivos que no sobrepasen al 4?

La expresión $\exists_x P(x)$ toma el mismo valor de verdad que la disyunción de las proposiciones:

$$\begin{aligned} P(1) \vee P(2) \vee P(3) \vee P(4) &\iff (1^2 > 10) \vee (2^2 > 10) \vee (3^2 > 10) \vee (4^2 > 10) \\ &\iff (1 > 10) \ \vee \ (4 > 10) \vee (9 > 10) \ \vee (16 > 10) \\ &\iff \quad (F_o) \quad \vee \quad (F_o) \quad \vee \quad (F_o) \quad \vee \quad (V_o) \\ &\iff \quad V_o \end{aligned}$$

Entonces se tiene que $\exists_x P(x)$ es verdadera en éste universo del discurso.

Ejemplo 39:

Se tienen los siguientes predicados $C(x)$: x tiene un computador, $A(x,\ y)$: x y y son amigos. El universo del discurso para las variables de los predicados es el conjunto de estudiantes de la institución. El significado en palabras de la expresión: $\forall_x(C(x) \vee \exists_y(C(y) \wedge A(x,\ y)))$, es: "Todo estudiante de la institución tiene computador o es amigo de algún estudiante de la institución que tiene computador".

Ejemplo 40:

Se tiene el siguiente predicado $S(x,\ y)$: $x+y=0$, donde el universo del discurso de las variables del predicado es el conjunto de los números reales. El significado en palabras de la expresión: $\forall_x\exists_y S(x,\ y)$, es: "Para cada número real x existe un número real y tal que la suma de x y y es igual a cero".

Ejemplo 41:

Sea el predicado $T(x,\ y)$: $x \geq y$, donde el universo del discurso es $x,\ y \in \{1,\ 2,\ 3,\ 4,\ 5\}$.

A continuación se presentan las interpretaciones en palabras y los valores de verdad de algunas de las formas como se puede cuantificar el predicado $T(x,\ y)$

- Para la expresión $\forall_x\forall_y T(x,\ y)$ la interpretación en palabras es: "Todo número entre 1 y 5 es mayor o igual a todo número entre 1 y 5", cuyo valor de verdad es falso.

- Para la expresión $\forall_x\exists_y T(x,\ y)$ la interpretación en palabras es: " Todo número entre 1 y 5 es mayor o igual a algún número entre 1 y 5", cuyo valor de verdad es cierto.

- Para la expresión $\exists_x\forall_y T(x,\ y)$ la interpretación en palabras es: "Existe un número entre 1 y 5 que es mayor o igual a todos los números entre 1 y 5", cuyo valor de verdad es cierto.

- Para la expresión $\exists_x\exists_y T(x,\ y)$ la interpretación en palabras es: "Existe un número entre 1 y 5 que es mayor o igual a algún número entre 1 y 5", cuyo valor de verdad es cierto.

- Para la expresión $\forall_y\exists_x T(x,\ y)$ la interpretación en palabras es: "Todo número entre 1 y 5 es menor o igual a algún número entre 1 y 5", cuyo valor de verdad es cierto.

- Para la expresión $\exists_x\forall_y T(y,\ x)$ la interpretación en palabras es: "Existe un número entre 1 y 5 que es menor o igual a todo número entre 1 y 5", cuyo valor de verdad es cierto.

1.3.3. Variables ligadas

Cuando un cuantificador es usado sobre la variable x, o cuando le es asignado un valor a dicha variable, se dice que la ocurrencia de la variable está ligada. Una ocurrencia de una variable que no está ligada por un cuantificador o no le ha sido asignada un valor particular se dice que es libre.

Todas las variables que aparecen en una función proposicional deben estar ligadas para que dicha función proposicional sea transformada en una proposición. Esto se puede realizar usando una combinación de cuantificadores universales, cuantificadores existenciales y la asignación de valores a las variables.

1.3.4. Alcance de un cuantificador

La parte de una expresión lógica para la cual un cuantificador es aplicado es llamado el alcance del cuantificador, adicionalmente, una variable también es libre si está fuera del alcance de todos los cuantificadores en la fórmula donde aparece dicha variable.

Ejemplo 42:

Se tiene el siguiente predicado $M(x,\ y) : x > y$, donde el universo del discurso es el conjunto de los números naturales. En la expresión $\exists_x M(x,\ y)$ la variable x está ligada por el cuantificador existencial, mientras que la variable y está libre porque no está ligada por un cuantificador y no le ha sido asignado ningún valor.

Ejemplo 43:

Sea la siguiente expresión del cálculo de predicados: $\forall_x[\exists_y(P(x,y) \wedge Q(x,y)) \rightarrow R(x)]$, los diferentes alcances de los cuantificadores son presentados en la siguiente expresión:

$$\underbrace{\forall_x\,[\exists_y\,\underbrace{(P(x,\ y) \wedge Q(x,\ y))}_{Alcance\ de\ \exists_y} \rightarrow R(x)]}_{Alcance\ de\ \forall_x}$$

en la expresión no hay ninguna variable libre, todas están ligadas.

Ejemplo 44:

Sean los predicados $M(x,\ y) : x \leq y, \quad I(x,\ y) : x + y = 10$, el universo del discurso de las variables de los predicados es el conjunto de los números enteros. ¿En la siguiente expresión del cálculo de predicados $\forall_x(\exists_y M(x,\ y) \wedge I(x,\ y))$ todas las ocurrencias de la variable y están ligadas?

Según la expresión, la variable y en el predicado $I(x,\ y)$ no está ligada porque el alcance del cuantificador existencial es únicamente el predicado $M(x,\ y)$.

Ejemplo 45:

Sea el siguiente predicado $M(x,\ y):\ x < y$, donde el universo del discurso es el conjunto de los números enteros ($\mathbb{Z}$). ¿Cuál es la interpretación en palabras y el valor de verdad de $\forall_x \exists_x M(x,\ x)$?.

La interpretación en palabras de $\forall_x \exists_x M(x,\ x)$ es: "Para todo número entero dicho número es estrictamente menor que el mismo", el valor de verdad de esta interpretación es falso.

El ejemplo anterior deja en evidencia un serio problema que se puede presentar en el cálculo de predicados, donde la misma variable x es cuantificada de forma diferente bajo el alcance de la misma variable para otro cuantificador, esto siempre se debe evitar.

Ejemplo 46:

Para el predicado y el universo del discurso del ejemplo anterior, ¿Cuál es la interpretación en palabras y el valor de verdad de $\exists_y \forall_x P(x,\ y)$?

La interpretación en palabras de $\exists_y \forall_x P(x,\ y)$ es: "Existe un número entero que es mayor que todos los números enteros", cuyo valor de verdad es falso porque los números enteros no están acotados superiormente.

Ejemplo 47:

Sea el predicado $N(x,\ y):\ x \leq y,$ donde el universo del discurso es el conjunto de los números naturales ($\mathbb{N}$). ¿Cuál es la interpretación en palabras y el valor de verdad de $\exists_x \forall_y N(x,\ y)$?

La interpretación en palabras de $\exists_x \forall_y N(x,\ y)$ es: "Existe un número natural que es menor o igual a todos los números naturales", cuyo valor de verdad es cierto porque los números naturales están acotados inferiormente, dicho número es el cero.

1.3.5. Negaciones y cuantificadores

Es normal tener la negación de una expresión cuantificada, por ejemplo la negación de la siguiente expresión: "Todo estudiante universitario colombiano ha estudiado trigonometría" sería : "No es el caso que cada estudiante universitario colombiano ha estudiado trigonometría", o "Hay algún estudiante universitario en Colombia que no ha estudiado trigonometría".

Si se tiene el predicado $P(x)$: x ha estudiado trigonometría, donde el universo del discurso son los estudiantes universitarios colombianos, entonces $\neg \forall_x (P(x)) = \exists_x (\neg P(x))$.

Ejemplo 48:

¿Cuál es la negación de la siguiente expresión: "Hay un político honesto"?

Sea el predicado $H(x) : x$ es honesto, donde el universo del discurso es el conjunto de los políticos, la expresión: "Hay un político honesto" puede ser representada por $\exists_x H(x)$, luego la negación es $\neg\exists_x H(x)$ que significa: "Ningún político es honesto", o que puede también ser visto como: $\forall_x \neg H(x)$ que significa: "Todo político es deshonesto".

Ejemplo 49:

¿Cuál es la negación de la siguiente expresión $\forall_x(x^2 \geq x)$?, donde el universo del discurso es el conjunto de los números enteros.

Primero que todo el significado en palabras de la expresión $\forall_x(x^2 \geq x)$ es: "el cuadrado de cualquier número entero x es mayor o igual al número entero x", ahora la negación de la expresión es: $\neg\forall_x(x^2 \geq x) = \exists_x \neg(x^2 \geq x) = \exists_x(x^2 < x)$, donde el significado en palabras de la expresión $\neg\forall_x(x^2 \geq x)$ es: "no es cierto que el cuadrado de cualquier número entero x es mayor o igual a número entero x". El significado en palabras de la expresión $\exists_x \neg(x^2 \geq x)$ es: "existe algún número entero x para el cual no se cumple que el cuadrado del número entero x sea mayor o igual al número entero x". Por último, el significado en palabras de la expresión $\exists_x(x^2 < x)$ es: "existe algún número entero x para el cual se cumple que el cuadrado del número entero x es menor al número entero x".

1.3.6. Ejercicios

1. Se definen los siguientes predicados con sus símbolos. Escriba cada enunciado simbólicamente. Hacer uso de los cuantificadores adecuados.
   D(x): "x es un día", S(x): "x es soleado", L(x): "x es lluvioso"

   a) Todos los días son soleados

   b) Algunos días son lluviosos

   c) Todo día que es soleado no es lluvioso

   d) Algunos días son soleados y lluviosos

   e) Ningún día es soleado y lluvioso a la vez

   f) Solo es día soleado el día lluvioso

2. Si A(x): "x es un automóvil", R(x): "x es rápido", L(x): "x es lento". Escriba cada enunciado simbólicamente. Atención a los cuantificadores.

   a) Algunos automóviles son rápidos y lentos.

   b) Algunos automóviles son rápidos.

   c) Ningún automóvil es lento y rápido a la vez.

d) Todos los automóviles son lentos.

e) Solo es automóvil rápido el automóvil lento.

f) Todo automóvil que es rápido no es lento.

3. Escriba cada enunciado simbólicamente en la lógica de predicados.

a) Todos los pájaros cantores vuelan.

b) Algún pájaro cantor no vuela.

c) No hay pájaros grandes que se alimenten de néctar.

d) Perro no come perro.

e) Hijo de tigre sale pintado.

f) Algunos leones no toman café.

g) Todos los peces, excepto los tiburones, son amables con los niños.

h) Cualquier caballo que es manso está bien entrenado.

i) Las serpientes son reptiles.

j) Ningún automóvil que tenga más de diez años será reparado si está seriamente dañado.

k) Ningún abrigo es impermeable a menos que haya sido especialmente tratado.

l) Nadie sino los valientes merecen a la bella.

m) Algunos senadores son o desleales o mal aconsejados.

n) Sólo los ejecutivos tienen secretaria.

ñ) Existe un entero que es mayor que 100 que es una potencia de 2.

o) El sucesor de un número es un número.

p) Para todo número natural, existe un número que es su inmediato sucesor.

q) Para todo número natural diferente de cero, existe un número natural que es su inmediato predecesor.

r) Todo número racional es un número real.

s) Existe un número que es un primo.

t) Para todo número x, existe un número y tal que x <y.

u) Algunos números naturales son pares.

v) Todo elemento $n \neq 1$ de $\mathbb{N}$ es el siguiente de algún otro elemento de $\mathbb{N}$.

w) Si $n,\ m \in \mathbb{N}$ y $m > n$ para todo $p \in \mathbb{N}$ entonces $m \cdot p > n \cdot p$

4. Sea $T(x,\ y)$: "x es mas alto que y". El dominio consta de 5 estudiantes: Lina, que mide 1.55 cm, Federnam, que mide 1.70 cm, Francisco que mide 1.64 cm, Isabel, que mide 1.60 cm y Alexander, quien mide 1.68 cm. Escriba cada proposición con palabras e indique si es verdadera o falsa.

a) $\forall_x \forall_y T(x,\ y)$.

b) $\forall_x \exists_y T(x,\ y)$.

c) $\exists_x \forall_y T(x,\ y)$.

d) $\exists_x \exists_y T(x,\ y)$.

e) $\forall_y \exists_x T(x,\ y)$.

f) $\exists_x \forall_y T(y,\ x)$.

5. Si L(x, y): "x ama a y", H(x): "x es joven", M(x): "x es un hombre", W(x): es una mujer, P(x): "x es hermosa", j: "Juan", k: "Katherine", Escriba el equivalente en español de los siguientes enunciados simbólicos:

   a) $(\forall x)(M(x) \to H(x))$

   b) $(\forall x)[W(x) \to (\forall y)(L(x,\ y) \to M(y) \wedge H(y))]$

   c) $(\exists x)(M(x) \wedge H(x) \wedge L(x,\ k))$

   d) $(\forall x)(W(x) \wedge P(x) \to L(j,\ x))$

6. Sea P(x, y): "x es el padre de y", donde el dominio de x y y son los seres humanos del mundo.

   a) Representar el predicado A(x, z): "x es el abuelo de z", utilizando el predicado P y los cuantificadores si son necesarios.

   b) Representar el predicado H(y, z): "y es hermano de z", utilizando el predicado P y los cuantificadores si son necesarios.

   c) Representar el predicado T(z, y): "z es el tío de y", utilizando los predicados P y H (solución del item anterior) y los cuantificadores si son necesarios.

7. Sea el siguiente dominio $D = \{a,\ b\}$ para el predicado P que toma los siguientes valores de verdad para la combinación de valores del dominio:

P(a,a)	P(a,b)	P(b,a)	P(b,b)
V	F	F	V

   Determine los valores de verdad para:

   a) $(\forall x)(\exists y)P(x,\ y)$

   b) $(\forall x)(\forall y)P(x,\ y)$

   c) $(\exists x)(\forall y)P(x,\ y)$

   d) $(\exists y) \sim P(x,\ y)$

   e) $(\forall x)P(x,\ x)$

8. Sean los siguientes predicados:

- $P(x)$: x es primate
- $A(x)$: x es arbóreo
- $R(x)$: x es roedor

Escribir en palabras el significado de la siguiente expresión:

a) $\exists x(P(x) \wedge A(x)) \ \wedge \ \exists x(R(x) \wedge A(x))$
b) $\exists x(P(x) \wedge A(x)) \ \wedge \ \exists x((\sim R(x)) \wedge A(x))$
c) $\forall x((P(x) \wedge A(x)) \rightarrow R(x))$
d) $\forall x(R(x) \rightarrow (P(x) \vee A(x)))$

9. Sean los siguientes predicados:

- $O(x)$: x es un organismo
- $M(x)$: x es molusco
- $D(x)$: x es doméstico

Escribir en palabras el significado de la siguiente expresión:

a) $(\exists x(O(x) \wedge D(x))) \ \wedge \ (\exists x(O(x) \wedge M(x))) \ \wedge \ (\sim \exists x(O(x) \wedge D(x) \wedge M(x)))$
b) $\forall x(M(x) \rightarrow O(x))$
c) $\forall x(D(x) \rightarrow O(x))$
d) $\sim \exists x((O(x) \wedge M(x)) \rightarrow D(x))$

Capítulo 2

Sucesiones y sumatorias

2.1. Funciones piso y techo

Definición: La función piso asigna al número real x el entero más grande que sea menor o igual a x. La función piso de x se denota por $\lfloor x \rfloor$.

Ejemplo 1:

- $\lfloor \frac{1}{2} \rfloor = 0$
- $\lfloor -\frac{1}{2} \rfloor = -1$
- $\lfloor 3{,}00000001 \rfloor = 3$
- $\lfloor 4{,}99999999 \rfloor = 4$
- $\lfloor -3{,}78 \rfloor = -4$
- $\lfloor 3{,}78 \rfloor = 3$

Definición: La función techo asigna al número real x el entero más pequeño que sea mayor o igual a x. La función techo de x se denota por $\lceil x \rceil$.

Ejemplo 2:

- $\lceil \frac{1}{2} \rceil = 1$
- $\lceil -\frac{1}{2} \rceil = 0$
- $\lceil 3{,}00000001 \rceil = 4$
- $\lceil 4{,}99999999 \rceil = 5$
- $\lceil -3{,}78 \rceil = -3$
- $\lceil 3{,}78 \rceil = 4$

2.1.1. Propiedades de las funciones piso y techo

En las siguientes propiedades $n \in \mathbb{Z}$ y $x \in \mathbb{R}$.

1. *a)* $\lfloor x \rfloor = n$ si y solo si $n \leq x < n + 1$
   b) $\lceil x \rceil = n$ si y solo si $n - 1 < x \leq n$
   c) $\lfloor x \rfloor = n$ si y solo si $x - 1 < n \leq x$

d) $\lceil x \rceil = n$ si y solo si $x \leq n < x + 1$

2. $x - 1 < \lfloor x \rfloor \leq x \leq \lceil x \rceil < x + 1$

3. *a)* $\lfloor -x \rfloor = -\lceil x \rceil$
   b) $\lceil -x \rceil = -\lfloor x \rfloor$

4. *a)* $\lfloor x + n \rfloor = \lfloor x \rfloor + n$
   b) $\lceil x + n \rceil = \lceil x \rceil + n$

Ejemplo 3:

Probar que si x es un número real, entonces $\lfloor 2x \rfloor = \lfloor x \rfloor + \lfloor x + \frac{1}{2} \rfloor$.

Sea $x = n + \epsilon$, donde n representa la parte entera del número x y ϵ representa la parte decimal.

Se presentan dos casos, cuando $\epsilon < \frac{1}{2}$ y cuando $\epsilon \geq \frac{1}{2}$. En análisis de cada uno de los casos es el siguiente:

- Caso donde $\epsilon < \frac{1}{2}$:

  $\lfloor 2(n + \epsilon) \rfloor = \lfloor 2n + 2\epsilon \rfloor$, como $2\epsilon < 1$, entonces $\lfloor 2n + 2\epsilon \rfloor = 2n$

  $$\lfloor n + \epsilon \rfloor + \Big\lfloor n + \underbrace{\epsilon + \frac{1}{2}}_{menor\ que\ 1} \Big\rfloor = n + n = 2n$$

  Por lo tanto $\lfloor 2x \rfloor = \lfloor x \rfloor + \lfloor x + \frac{1}{2} \rfloor = 2n$

- Caso donde $\epsilon \geq \frac{1}{2}$:

  $$\lfloor 2(n + \epsilon) \rfloor = \lfloor 2n + \underbrace{2\epsilon}_{mayor\ o\ igual\ que\ 1} \rfloor = 2n + 1$$

  $$\lfloor n + \epsilon \rfloor + \Big\lfloor n + \underbrace{\epsilon + \frac{1}{2}}_{mayor\ o\ igual\ que\ 1} \Big\rfloor = n + n + 1 = 2n + 1$$

  Por lo tanto $\lfloor 2x \rfloor = \lfloor x \rfloor + \lfloor x + \frac{1}{2} \rfloor = 2n + 1$

Como se cumplen los dos casos, entonces queda demostrado que $\lfloor 2x \rfloor = \lfloor x \rfloor + \lfloor x + \frac{1}{2} \rfloor$.

2.2. Sucesiones

Las sucesiones son usadas para representar listas ordenadas de elementos.

Definición: Una sucesión es una función del conjunto de los números naturales o del conjunto de los números enteros positivos a un conjunto S. Se usa la notación S_n para denotar la imagen del número n en el conjunto S, de esta misma forma, S_n representa al término ubicado en la posición n de la sucesión. Se usa la notación $\{S_n\}$ para denotar todo el rango de la función. Las sucesiones son descritas listando los términos de la sucesión en el orden como se va incrementando el subíndice.

Ejemplo 4:

Considerar la sucesión $\{S_n\}$, donde $S_n = \dfrac{n}{2^n}$.

Los elementos de la sucesión, comenzando en S_1, son:

$S_1 = \dfrac{1}{2^1}$

$S_2 = \dfrac{2}{2^2}$

$S_3 = \dfrac{3}{2^3}$

$S_4 = \dfrac{4}{2^4}$

$S_5 = \dfrac{5}{2^5}$

$\vdots$

$S_n = \dfrac{n}{2^n}$

de esta forma se tiene que la lista de términos de la sucesión es:

$$\frac{1}{2^1}\,,\frac{2}{2^2}\,,\,\frac{3}{2^3}\,,\,\frac{4}{2^4}\,,\,\frac{5}{2^5}\,,\,\ldots\,,\,\frac{n}{2^n}$$

Definición: Una progresión aritmética es una sucesión de la forma:

$$a,\ a+d,\ a+2\cdot d,\ a+3\cdot d,\ \ldots,\ a+n\cdot d$$

donde el término inicial a y la diferencia común d son números reales.

Ejemplo 5:

La sucesión $\{S_n\}$ con $S_n = 1+2\cdot n$ es una progresión aritmética con término inicial $a = 1$ y diferencia común $d = 2$.

Los elementos de la sucesión, comenzando en $n = 0$, son:

$S_0 = 1 + 2\cdot 0 = 1 + 0 = 1$

$S_1 = 1 + 2 \cdot 1 = 1 + 2 = 3$
$S_2 = 1 + 2 \cdot 2 = 1 + 4 = 5$
$S_3 = 1 + 2 \cdot 3 = 1 + 6 = 7$
$S_4 = 1 + 2 \cdot 4 = 1 + 8 = 9$
$\vdots$
$S_n = 1 + 2 \cdot n$

de esta forma se tiene que la lista de términos de la sucesión es la lista de los números enteros positivos impares: $1,\ 3,\ 5,\ 7,\ 9,\ \ldots\ ,\ 1 + 2 \cdot n$.

Ejemplo 6:

Encontrar una fórmula para generar el n-ésimo término de la sucesión que tiene los primeros seis términos siguientes: 1, 5, 9, 13, 17 y 21.

Entre un par de términos consecutivos de la sucesión hay una diferencia constante de 4, se tiene como primer término de la sucesión al número 1, por este motivo la sucesión 1, 5, 9, 13, 17, 21, ..., es una progresión aritmética con primer término $a = 1$ y diferencia constante $d = 4$.

La forma como se generan los primeros seis términos de la sucesión por medio de la progresión aritmética es:

$a + 0 \cdot d,$	$a + 1 \cdot d,$	$a + 2 \cdot d,$	$a + 3 \cdot d,$	$a + 4 \cdot d,$	$a + 5 \cdot d$
$1 + 0 \cdot 4,$	$1 + 1 \cdot 4,$	$1 + 2 \cdot 4,$	$1 + 3 \cdot 4,$	$1 + 4 \cdot 4,$	$1 + 5 \cdot 4$
$1 + 0,$	$1 + 4,$	$1 + 8,$	$1 + 12,$	$1 + 16,$	$1 + 20$
$1,$	$5,$	$9,$	$13,$	$17,$	21

Definición: Una progresión geométrica es una sucesión de la forma:

$$a,\ a \cdot r,\ a \cdot r^2,\ a \cdot r^3,\ \ldots\ ,\ a \cdot r^n$$

donde el término inicial a y la razón constante r son números reales.

Ejemplo 7:

La sucesión $\{S_n\}$ con $S_n = 2^n$ es una progresión geométrica con término inicial $a = 1$ y razón constante $r = 2$.

Los elementos de la sucesión, comenzando en $n = 0$, son:

$S_0 = 2^0 = 1$
$S_1 = 2^1 = 2$
$S_2 = 2^2 = 4$
$S_3 = 2^3 = 8$
$S_4 = 2^4 = 16$

$\vdots$
$S_n = 2^n$

de esta forma se tiene que la lista de términos de la sucesión es:

$$1,\ 2,\ 4,\ 8,\ 16,\ \ldots\ ,\ 2^n$$

Ejemplo 8:

La sucesión $\{S_n\}$ con $S_n = 2 \cdot 3^n$ es una progresión geométrica con término inicial $a = 2$ y razón constante $r = 3$.

Los elementos de la sucesión, comenzando en $n = 0$, son:

$S_0 = 2 \cdot 3^0 = 2 \cdot 1 = 2$
$S_1 = 2 \cdot 3^1 = 2 \cdot 3 = 6$
$S_2 = 2 \cdot 3^2 = 2 \cdot 9 = 18$
$S_3 = 2 \cdot 3^3 = 2 \cdot 27 = 54$
$S_4 = 2 \cdot 3^4 = 2 \cdot 81 = 162$
$\vdots$
$S_n = 2 \cdot 3^n$

de esta forma se tiene que la lista de términos de la sucesión es:

$$2,\ 6,\ 18,\ 54,\ 162,\ \ldots\ ,\ 2 \cdot 3^n$$

2.3. Sucesiones especiales de números

Cuando es difícil deducir una posible fórmula para generar el n-ésimo términos de una sucesión, entonces, las siguientes son algunas de las preguntas que se deben formular:

- ¿La sucesión tiene siempre el mismo término?
- ¿Los términos son obtenidos de términos previos y la suma de alguna cantidad o los términos son obtenidos de una cantidad que depende de la posición en la sucesión?
- ¿Los términos son obtenidos de términos previos y la multiplicación de alguna cantidad o los términos son obtenidos de una cantidad que depende de la posición en la sucesión?
- ¿Los términos son obtenidos por la combinación de términos en una cierta forma?
- ¿Hay ciclos entre los términos de la sucesión?

Ejemplo 9:

Encontrar una fórmula para generar el n-ésimo término de la sucesión que tiene los primeros 10 términos siguientes: 3, 9, 15, 21, 27, 33, 39, 45, 51 y 57.

Para la sucesión de este ejemplo aplica la pregunta: "¿Los términos son obtenidos de términos previos y la suma de alguna cantidad o los términos son obtenidos de una cantidad que depende de la posición en la sucesión?".

Con respecto a la primera opción de la pregunta la siguiente fórmula recursiva permite generar el n-ésimo término de la sucesión:

$S_1 = 3$
$S_n = S_{n-1} + 6$, para $n \geq 2$.

Con respecto a la segunda opción de la pregunta se puede determinar que el n-ésimo término de la sucesión únicamente depende de su posición, ya que la sucesión es una progresión aritmética, donde el primer término es $a = 3$ y la diferencia común entre dos términos consecutivos de la sucesión es $d = 6$, por lo tanto la fórmula que genera el n-ésimo término de la sucesión es:

$S_n = 3 + n \cdot 6$, para $n \geq 0$.

Ejemplo 10:

Encontrar una fórmula para generar el n-ésimo término de la sucesión que tiene los primeros cinco términos siguientes: 1, $\frac{2}{3}$, $\frac{4}{9}$, $\frac{8}{27}$ y $\frac{16}{81}$

Para la sucesión de este ejemplo aplica la pregunta: "¿Los términos son obtenidos de términos previos y la multiplicación de alguna cantidad o los términos son obtenidos de una cantidad que depende de la posición en la sucesión?".

Con respecto a la primera opción de la pregunta la siguiente fórmula recursiva permite generar el n-ésimo término de la sucesión:

$S_1 = 1$
$S_n = \frac{2}{3} \cdot S_{n-1}$, para $n \geq 2$.

Con respecto a la segunda opción de la pregunta se puede determinar que el n-ésimo término de la sucesión únicamente depende de su posición, ya que la sucesión es una progresión geométrica, donde el primer término es $a = 1$ y la razón constante entre dos términos consecutivos de la sucesión es $r = \frac{2}{3}$, por lo tanto la fórmula que genera el n-ésimo término de la sucesión es:

$S_n = 1 \cdot \left(\frac{2}{3}\right)^n = \left(\frac{2}{3}\right)^n$, para $n \geq 0$.

Ejemplo 11:

Encontrar una fórmula para generar el n-ésimo término de la sucesión que tiene los primeros seis términos siguientes: 1, 3, 6, 10, 15, 21, ...

Para la sucesión de este ejemplo aplica la pregunta: "¿Los términos son obtenidos de términos previos y la suma de alguna cantidad o los términos son obtenidos de una cantidad que depende de la posición en la sucesión?".

Con respecto a la primera opción de la pregunta la siguiente fórmula recursiva permite generar el n-ésimo término de la sucesión:

$S_1 = 1$
$S_n = S_{n-1} + n$, para $n \geq 2$.

Con respecto a la segunda opción de la pregunta se puede determinar que el n-ésimo término de la sucesión únicamente depende de su posición de la siguiente forma:

$S_n = \frac{n(n+1)}{2}$, para $n \geq 1$.

Ejemplo 12:

Encontrar una fórmula para generar el n-ésimo término de la sucesión que tiene los primeros seis términos siguientes: 1, 1, 2, 6, 24, 120, ...

Para la sucesión de este ejemplo aplica la pregunta: "¿Los términos son obtenidos de términos previos y la multiplicación de alguna cantidad o los términos son obtenidos de una cantidad que depende de la posición en la sucesión?".

Con respecto a la primera opción de la pregunta la siguiente fórmula recursiva permite generar el n-ésimo término de la sucesión:

$S_0 = 1$
$S_n = n \cdot S_{n-1}$, para $n \geq 1$.

Con respecto a la segunda opción de la pregunta se puede determinar que el n-ésimo término de la sucesión únicamente depende de su posición de la siguiente forma:

$S_n = n!$, donde $n \geq 0$

Ejemplo 13:

Encontrar una fórmula para generar el n-ésimo término de la sucesión que tiene los primeros 16 términos siguientes: 1, 2, 2, 2, 3, 3, 3, 3, 3, 4, 4, 4, 4, 4, 4 y 4.

Para la sucesión de este ejemplo aplica la segunda opción de la pregunta: "¿Los términos son obtenidos de términos previos y la suma de alguna cantidad o los términos son obtenidos de una cantidad que depende de la posición en la sucesión?". Se puede

determinar que el n-ésimo término de la sucesión únicamente depende de su posición de la siguiente forma:

$S_n = \lceil \sqrt{n} \rceil$, para $n \geq 1$.

Ejemplo 14:

Encontrar una fórmula para generar el n-ésimo término de la sucesión que tiene los primeros 15 términos siguientes: 1, 1, 1, 2, 2, 2, 2, 2, 3, 3, 3, 3, 3, 3 y 3.

Para la sucesión de este ejemplo aplica la segunda opción de la pregunta: "¿Los términos son obtenidos de términos previos y la suma de alguna cantidad o los términos son obtenidos de una cantidad que depende de la posición en la sucesión?". Se puede determinar que el n-ésimo término de la sucesión únicamente depende de su posición de la siguiente forma:

$S_n = \lfloor \sqrt{n} \rfloor$, para $n \geq 1$.

Ejemplo 15:

Encontrar una fórmula para generar el n-ésimo término de la sucesión que tiene los primeros 10 términos siguientes: 2, 7, 24, 77, 238, 723, 2180, 6553, 19674 y 59039.

Para la sucesión de este ejemplo aplica la pregunta: "¿Los términos son obtenidos por la combinación de términos en una cierta forma?".

El n-ésimo término de la sucesión depende del resultado de una potencia de 3 menos una cantidad especifica con respecto a la posición del término en la sucesión. La fórmula es la siguiente:

$S_n = 3^n - n$, para $n \geq 1$.

Ejemplo 16:

Encontrar una fórmula para generar el n-ésimo término de la sucesión que tiene los primeros nueve términos siguientes: 0, 1, 1, 0, 1, 1, 0, 1, 1, ...

Para la sucesión de este ejemplo aplica la pregunta: "¿Hay ciclos entre los términos de la sucesión?".

De forma cíclica los elementos 0, 1 y 1 se siguen presentado en la sucesión. Una fórmula que garantiza la generación cíclica de los términos es la siguiente:

$S_0 = 0$
$S_1 = 1$
$S_2 = 1$
$S_n = S_{(n \mod 3)}$, para $n \geq 3$.

Se debe tener en cuenta que n *mod* 3 es el residuo de la división entera entre n y 3, donde los únicos posibles residuos que se pueden obtener al dividir el número entero positivo n por 3 son: 0, 1 y 2.

2.4. Sumatorias

La notación de sumatoria es usada para representar la suma de los términos S_m, S_{m+1}, S_{m+2}, ..., S_n de la sucesión $\{S_n\}$.

Se usa la notación $\sum_{i=m}^{n} S_i$ para representar $S_m + S_{m+1} + S_{m+2} + \cdots + S_n$.

Ejemplo 17:

La suma de los primeros 50 términos de la sucesión $\{S_n\}$ donde el n-ésimo término de la sucesión está definido por $S_n = \frac{n}{2^n}$ puede ser representada por medio de sumatorias como:

$$\sum_{i=1}^{50} \frac{i}{2^i} = \frac{1}{2^1} + \frac{2}{2^2} + \frac{3}{2^3} + \frac{4}{2^4} + \cdots + \frac{50}{2^{50}}$$

Ejemplo 18:

¿Cuál es el resultado que se obtiene de $\sum_{i=1}^{8} i$?

El resultado es el siguiente: $\sum_{i=1}^{8} i = 1 + 2 + 3 + 4 + 5 + 6 + 7 + 8 = 36$.

Teorema:

$\sum_{i=1}^{n} i = 1 + 2 + 3 + \cdots + n = \frac{n(n+1)}{2}$, para $n \in \mathbb{Z}^+$.

Demostración:

Sea $S = 1 + 2 + 3 + \cdots + n$, como el orden de los sumandos no altera el resultado entonces $S = n + (n-1) + (n-2) + \cdots + 1$

$$\begin{array}{rccccccccc} S = & 1 & + & 2 & + & 3 & + & \cdots & + & n \\ S = & n & + & (n-1) & + & (n-2) & + & \cdots & + & 1 \\ \hline 2S = & \underbrace{(n+1)} & + & (n+1) & + & (n+1) & + & \cdots & + & (n+1) \\ & & & & & n \text{ veces} & & & & \end{array}$$

$$2S = n(n+1)$$

$$S = \frac{n(n+1)}{2}$$

Como S es igual a $1+2+3+\cdots+n$ entonces $1+2+3+\cdots+n = \frac{n(n+1)}{2}$, para $n \in \mathbb{Z}^+$.

Ejemplo 19:

Obtener una fórmula que sea la solución de la siguiente suma de términos:

$2+4+6+8+\cdots+2\cdot n$, para $n \in \mathbb{Z}^+$.

$$\begin{aligned} 2 + 4 + 6 + 8 + \cdots + 2\cdot n &= 2\cdot 1 + 2\cdot 2 + 2\cdot 3 + 2\cdot 4 + \cdots + 2\cdot n \\ &= 2\cdot(1 + 2 + 3 + 4 + \cdots + n) \\ &= 2\cdot\left(\sum_{i=1}^{n} i\right) \\ &= 2\cdot\left(\frac{n(n+1)}{2}\right) \\ &= n(n+1) \end{aligned}$$

Por lo tanto $\sum_{i=1}^{n} 2\cdot i \;=\; 2+4+6+8+\cdots+2\cdot n \;=\; n(n+1)$

Ejemplo 20:

Obtener una fórmula que sea la solución de la siguiente suma de términos:

$1+3+5+7+\cdots+2n-1$, para $n \in \mathbb{Z}^+$.

$$\begin{aligned} 1+3+5+\cdots+2\cdot n-1 &= 2\cdot 1-1 + 2\cdot 2-1 + 2\cdot 3-1 + \cdots + 2\cdot n-1 \\ &= (2\cdot 1 + 2\cdot 2 + 2\cdot 3 +\cdots+ 2\cdot n) - (\underbrace{1+1+1+\cdots+1}_{n \text{ veces}}) \\ &= 2\cdot(1+2+3+4+\cdots+n) - n \\ &= 2\cdot\left(\sum_{i=1}^{n} i\right) - n \\ &= 2\cdot\left(\frac{n(n+1)}{2}\right) - n \\ &= n(n+1) - n \\ &= n^2 + n - n \end{aligned}$$

$$= \ n^2$$

Por lo tanto $\sum_{i=1}^{n}(2 \cdot i \ - \ 1) \ = \ 1+3+5+\cdots+2 \cdot n-1 \ = \ n^2$.

A continuación se presenta otra forma alternativa de obtener la solución de la suma de términos.

Sea $S = 1+3+5+\cdots+2n-1$, como el orden de los sumandos no altera el resultado entonces $S = (2n-1)+(2n-3)+(2n-5)+\cdots+1$

$$\begin{array}{rccccccc} S = & 1 & + & 3 & + & 5 & +\cdots+ & 2n-1 \\ S = & (2n-1) & + & (2n-3) & + & (2n-5) & +\cdots+ & 1 \\ \hline 2S = & \underbrace{(2n) \quad + \quad (2n) \quad + \quad (2n) \quad +\cdots+ \quad (2n)}_{n \ veces} & & & & & & \end{array}$$

$$2S = n(2n)$$

$$S = n^2$$

Como S es igual a $1+3+5+\cdots+2n-1$ entonces $1+3+5+\cdots+2n-1 = n^2$, para $n \in \mathbb{Z}^+$.

Teorema:

Si a y r son números reales con $r \neq 0$, entonces:

$$\sum_{i=0}^{n} a \cdot r^i = \begin{cases} a \cdot (n+1) & si \ \ r = 1 \\ \dfrac{a \cdot r^{n+1} - a}{r-1} & si \ \ r \neq 1 \end{cases}$$

Demostración:

Se debe demostrar cada uno de los dos casos del teorema de forma independiente, si los dos casos se cumplen entonces queda demostrada la validez del teorema

- **Caso donde** $r = 1$

  $$\sum_{i=0}^{n} a \cdot 1^i = \sum_{i=0}^{n} a \cdot 1 = \sum_{i=0}^{n} a = \underbrace{a+a+a+a+\cdots+a}_{n+1 \ \ veces} = a \cdot (n+1).$$

  Queda demostrado el caso.

- **Caso donde** $r \neq 1$

  Sea $S = a + a \cdot r + a \cdot r^2 + a \cdot r^3 + \cdots + a \cdot r^n$, al multiplicar a ambos lados de la igualdad por $-r$ se sigue conservando la igualdad, donde se obtiene: $-S \cdot r = -a \cdot r - a \cdot r^2 - a \cdot r^3 - a \cdot r^4 - \cdots - a \cdot r^{n+1}$, al sumar ambas igualdades se tiene:

$$\begin{array}{rccccccccccc} S = & a & + & a \cdot r & + & a \cdot r^2 & + & a \cdot r^3 & + \cdots + & a \cdot r^n & & \\ -S \cdot r = & & - & a \cdot r & - & a \cdot r^2 & - & a \cdot r^3 & - \cdots - & a \cdot r^n & - & a \cdot r^{n+1} \\ \hline S - S \cdot r = & a & & & & & & & & & - & a \cdot r^{n+1} \end{array}$$

$$S \cdot (1 - r) = a - a \cdot r^{n+1}$$

$$S = \frac{a - a \cdot r^{n+1}}{1 - r}$$

$$S = \frac{-1}{-1} \cdot \frac{a - a \cdot r^{n+1}}{1 - r}$$

$$S = \frac{-a + a \cdot r^{n+1}}{-1 + r}$$

$$S = \frac{a \cdot r^{n+1} - a}{r - 1}$$

  Como S es igual a $a + a \cdot r + a \cdot r^2 + a \cdot r^3 + \cdots + a \cdot r^n$ entonces $a + a \cdot r + a \cdot r^2 + a \cdot r^3 + \cdots + a \cdot r^n = \dfrac{a \cdot r^{n+1} - a}{r - 1}$, para $n \in \mathbb{Z}^+$.

  Queda demostrado el caso.

Como se cumplen todos los casos del teorema entonces queda demostrada la validez del teorema de la suma de términos de la serie o progresión geométrica.

Ejemplo 21:

Obtener una fórmula que sea la solución de la siguiente suma de términos:

$\sum_{i=1}^{n} i \cdot 2^i = 1 \cdot 2^1 + 2 \cdot 2^2 + 3 \cdot 2^3 + 4 \cdot 2^4 + \cdots + n \cdot 2^n$, para $n \in \mathbb{Z}^+$.

Los términos que se están sumando no pertenecen originalmente a una serie geométrica, pero se puede hacer un manejo de los términos para que la solución de la sumatoria de términos de la serie geométrica pueda ser utilizada. El manejo es el siguiente:

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

$$
\begin{aligned}
&= (2^1) \ + \ (2^2 + 2^2) \ + \ (2^3 + 2^3 + 2^3) \ + \cdots + \ (\underbrace{2^n + 2^n + 2^n + \cdots + 2^n}_{n \quad veces}) \\
&= (2^1 + 2^2 + 2^3 + \cdots + 2^n) \ + \ (2^2 + 2^3 + \cdots + 2^n) \ + \cdots + \ (2^n) \\
&= \sum_{i=1}^{n} 2^i \ + \ \sum_{i=2}^{n} 2^i \ + \ \sum_{i=3}^{n} 2^i \ + \cdots + \ \sum_{i=n}^{n} 2^i \\
&= \left(\sum_{i=0}^{n} 2^i \ - \ \sum_{i=0}^{0} 2^i \right) \ + \ \left(\sum_{i=0}^{n} 2^i \ - \ \sum_{i=0}^{1} 2^i \right) \ + \cdots + \ \left(\sum_{i=0}^{n} 2^i \ - \ \sum_{i=0}^{n-1} 2^i \right) \\
&= n \sum_{i=0}^{n} 2^i \ - \ \left(\sum_{i=0}^{0} 2^i \ + \ \sum_{i=0}^{1} 2^i \ + \cdots + \ \sum_{i=0}^{n-1} 2^i \right) \\
&= n \cdot (2^{n+1} \ - \ 1) \ - \ \big((2^1 - 1) \ + \ (2^2 \ - \ 1) \ + \ (2^3 \ - \ 1) \ + \cdots + \ (2^n \ - \ 1) \big) \\
&= n \cdot (2^{n+1} \ - \ 1) \ - \ \big((2^1 \ + \ 2^2 \ + \ 2^3 \ + \cdots + \ 2^n) \ - \ n \big) \\
&= n \cdot (2^{n+1} \ - \ 1) \ - \ \big(- n \ + \ (2^1 \ + \ 2^2 \ + \ 2^3 \ + \cdots + \ 2^n) \big) \\
&= n \cdot (2^{n+1} \ - \ 1) \ - \ \left(- n \ + \ \left(\sum_{i=1}^{n} 2^i \right) \right) \\
&= n \cdot (2^{n+1} \ - \ 1) \ - \ \left(- n \ + \ \left(\sum_{i=0}^{n} 2^i \ - \ \sum_{i=0}^{0} 2^i \right) \right) \\
&= n \cdot (2^{n+1} \ - \ 1) \ - \ \big(- n \ + \ \big((2^{n+1} - 1) \ - \ 1 \big) \big) \\
&= n \cdot (2^{n+1} \ - \ 1) \ - \ (-n \ + \ 2^{n+1} \ - \ 2) \\
&= n \cdot 2^{n+1} \ - \ n \ + \ n \ - \ 2^{n+1} \ + \ 2 \\
&= n \cdot 2^{n+1} \ - \ 2^{n+1} \ + \ 2 \\
&= (n-1) \cdot 2^{n+1} \ + \ 2
\end{aligned}
$$

Por lo tanto $\sum_{i=1}^{n} i \cdot 2^i = (n-1) \cdot 2^{n+1} \ + \ 2$.

2.4.1. Fórmulas de sumatorias útiles:

Las siguientes son algunas de las sumatorias más importantes (o más utilizadas) en Matemáticas Computacionales junto con su solución. Esta información será de gran importancia en el Capítulo 4 de Relaciones de Recurrencia, cuando se trabaje en la sección 4.1 el Método de Iteración

- $\sum_{i=1}^{n} i = \frac{n}{2}(n+1)$, para $n \in \mathbb{Z}^+$.
- $\sum_{i=1}^{n} i^2 = \frac{n(n+1)(2n+1)}{6}$, para $n \in \mathbb{Z}^+$.

- $\sum_{i=1}^{n} i^3 = \frac{n^2(n+1)^2}{4}$, para $n \in \mathbb{Z}^+$.
- $\sum_{i=1}^{n} i^4 = \frac{n(n+1)(2n+1)(3n^2+3n-1)}{30}$, para $n \in \mathbb{Z}^+$.
- $\sum_{i=0}^{n} a \cdot r^i = \frac{ar^{n+1}-a}{r-1}$, donde $r \neq 0$, $r \neq 1$ y $n \in \mathbb{N}$.
- Si $|r| < 1$ y $r \neq 0$, entonces $\sum_{i=0}^{\infty} a \cdot r^i = \frac{a}{1-r}$, para $i \in \mathbb{N}$.
- $\sum_{i=1}^{n} i \cdot 2^i = (n-1)2^{n+1} + 2$, para $n \in \mathbb{Z}^+$.
- $\sum_{i=1}^{n} \frac{i}{2^i} = 2 - \frac{n+2}{2^n}$, para $n \in \mathbb{Z}^+$.

2.5. Ejercicios

1. Determinar el valor generado por la expresión:

$$\left\lfloor 1{,}3 * \left(\left\lceil \sqrt{\left\lceil 2{,}7 * \left(\left\lfloor \sqrt{\left\lfloor \sqrt{39652} \right\rfloor} \right\rfloor \right)^3 \right\rceil} \right\rceil \right) \right\rfloor$$

2. Probar o refutar que $\lfloor x \rfloor + \lfloor y \rfloor + \lfloor x+y \rfloor \leq \lfloor 2x \rfloor + \lfloor 2y \rfloor$, $x,\ y \in \mathbb{R}$

3. Producir los 17 primeros términos que se generan con las fórmulas de los siguientes items, donde *Min* es una función que devuelve el mínimo de dos valores, y *mod* es la función modulo que es equivalente al residuo de la división entera entre dos números enteros.

   Explicar en palabras la forma que toma la sucesión que se genera.

   a) $S(0) = 1$
   $S(n) = S(n-1) + (Min(2^{n \ mod \ 3}, 2^{(n-1) \ mod \ 3}))\ mod\ 2$, para $n \in \mathbb{Z}^+$.

   b) $S(0) = 1$
   $S(n) = S(n-1) + (Min(2^{n \ mod \ 4}, 2^{(n-1) \ mod \ 4}))\ mod\ 2$, para $n \in \mathbb{Z}^+$.

   c) $S(0) = 1$
   $S(n) = S(n-1) + (Min(2^{n \ mod \ 5}, 2^{(n-1) \ mod \ 5}))\ mod\ 2$, para $n \in \mathbb{Z}^+$.

   d) $S(0) = 1$
   $S(n) = S(n-1) + (Min(3^{n \ mod \ 5}, 3^{(n-1) \ mod \ 5}))\ mod\ 3$, para $n \in \mathbb{Z}^+$.

4. Encontrar una fórmula para generar el n-ésimo término de cada una de las sucesión que tienen los primeros términos:

a) 2, 4, 6, 10, 16, 26, 42, ...

b) 0, 1, 1, 2, 4, 7, 13, 24, 44, 81, ...

c) 1, 2, 3, 10, 20, 30, 100, 200, 300, ...

d) 2^1, 3^1, 2^2, 3^2, 2^4, 3^4, 2^8, 3^8, 2^{16}, 3^{16}, ...

5. Para cada uno de los siguientes items, ¿Cuál es la fórmula que representa el resultado de la suma de términos?

a) $1 \cdot \frac{1}{4} + 4 \cdot \frac{5}{4} + 9 \cdot \frac{9}{4} + \ldots + n^2 \cdot (n - \frac{3}{4})$, donde $n \in \mathbb{Z}^+$.

b) $1 \cdot \frac{1}{2} + 2 \cdot \frac{3}{2} + \ldots + n \cdot (n - \frac{1}{2})$, donde $n \in \mathbb{Z}^+$.

c) $1 \cdot \frac{1}{5} + 2 \cdot \frac{16}{5} + 3 \cdot \frac{41}{5} + \ldots + n \cdot (n^2 - \frac{4}{5})$, donde $n \in \mathbb{Z}^+$.

d) $\frac{3}{2} + \frac{14}{4} + \frac{45}{8} + \frac{124}{16} + \ldots + (2n - \frac{n}{2^n})$, donde $n \in \mathbb{Z}^+$.

e) $1 + 4 + 7 + 10 + 13 + \ldots + (3n - 2)$, donde $n \in \mathbb{Z}^+$.

f) $1 + 5 + 9 + 13 + 17 + \ldots + (4n - 3)$, donde $n \in \mathbb{Z}^+$.

g) $1(2) + 2(3) + 3(4) + 4(5) + \ldots + n(n + 1)$, donde $n \in \mathbb{Z}^+$.

h) $1 \cdot \frac{2}{3} + 2 \cdot \frac{5}{3} + \ldots + n \cdot (n - \frac{1}{3})$, donde $n \in \mathbb{Z}^+$.

i) $0 + 3 + 8 + \ldots + (n^2 - 1)$, donde $n \in \mathbb{Z}^+$.

j) $0 + 7 + 26 + \ldots + (n^3 - 1)$, donde $n \in \mathbb{Z}^+$.

k) $1^2 + 3^2 + 5^2 + \ldots + (2n - 1)^2$, donde $n \in \mathbb{Z}^+$.

l) $3^2 + 4^2 + 5^2 + 6^2 + \ldots + (n + 2)^2$?, donde $n \in \mathbb{Z}^+$.

m) $1^2 + 4^2 + 7^2 + 10^2 + \ldots + (3n - 2)^2$?, donde $n \in \mathbb{Z}^+$.

n) $4^2 + 7^2 + 10^2 + 13^2 + \ldots + (3n + 1)^2$?, donde $n \in \mathbb{Z}^+$.

ñ) $5^2 + 8^2 + 11^2 + 14^2 + \ldots + (3n + 2)^2$?, donde $n \in \mathbb{Z}^+$.

o) $5^3 + 8^3 + 11^3 + 14^3 + \ldots + (3n + 2)^3$?, donde $n \in \mathbb{Z}^+$.

p) $3^3 + 4^3 + 5^3 + 6^3 + \ldots + (n + 2)^3$?, donde $n \in \mathbb{Z}^+$.

q) $1^3 + 4^3 + 7^3 + 10^3 + \ldots + (3n - 2)^3$?, donde $n \in \mathbb{Z}^+$.

r) $4^3 + 7^3 + 10^3 + 13^3 + \ldots + (3n + 1)^3$?, donde $n \in \mathbb{Z}^+$.

Capítulo 3

Técnicas de demostración

3.1. Técnica de demostración directa.

La técnica de demostración directa es tradicionalmente la más utilizada en matemáticas, en ésta técnica se parte de la hipótesis **(H)** para llegar a la conclusión **(C)**, $H \to C$.

Definición: El número entero n es par si existe un número entero k tal que $n = 2k$ y n es un número entero impar si existe un número entero k tal que $n = 2k + 1$.

Ejemplo 1:

Utilizando la técnica de demostración directa, demostrar que si n es un número entero impar, entonces n^2 es un número entero impar.

En la técnica de demostración directa para este ejemplo se tiene que la hipótesis es: "n es un número entero impar" y que la conclusión es: "n^2 es un número entero impar".

Para demostrar que $Hipótesis \to Conclusión$, entonces se considera que la hipótesis es verdadera y se termina demostrando que la conclusión también es verdadera.

Si n es un número entero impar entonces, $n = 2k + 1$, donde $k \in \mathbb{Z}$. Por lo tanto se tiene que:

$$\begin{aligned} n^2 &= (2k+1)^2 \\ &= 4k^2 + 4k + 1 \\ &= 2(2k^2 + 2k) + 1 \\ &= 2t + 1, \text{ donde } t = 2k^2 + 2k \ \text{ y } t \in \mathbb{Z} \end{aligned}$$

Por tanto como n^2 es de la forma $2t+1$ la cual es la representación de un número entero impar, por lo tanto, se ha demostrado de forma directa que: "si n es un número entero

impar, entonces n^2 es un número entero impar" porque se partió de la hipótesis y se alcanzó la conclusión.

Ejemplo 2:

Demostrar que la suma de n enteros positivos consecutivos cualesquiera es divisible por n solo cuando n es un número entero impar positivo.

Sea m un número entero positivo ($m \in \mathbb{Z}^+$), m es el primer número de la secuencia de n números enteros consecutivos que se van a tomar, de esta forma se tiene:

$$\underbrace{m + (m+1) + (m+2) + \cdots + (m + (n-1))}_{n \text{ enteros positivos consecutivos}}$$

$$= \underbrace{(m + m + m + \cdots + m)}_{n \text{ veces}} \; + \; (0 + 1 + 2 + \cdots + (n-1))$$

$$= n(m) \; + \; (1 + 2 + \cdots + (n-1))$$

$$= n(m) \; + \; \frac{(n-1)(n)}{2}$$

$$= n\left[m + \frac{n-1}{2}\right]$$

$$= n \cdot x, \quad \text{donde } x = m + \frac{n-1}{2}$$

Ahora para que $n \cdot x$ sea divisible por n se necesita que x sea un número entero, esto se logra siempre y cuando el número n sea un entero impar porque al restarle el uno se obtiene un número par que al dividirlo por dos genera un número entero, la suma del entero m con el entero que es el resultado de la fracción genera como resultado un número entero. De esta forma queda demostrado que la suma de n enteros positivos consecutivos cualesquiera es divisible por n solo cuando n es un número entero impar positivo.

Definición: El número real r es número racional si existe un número entero[1] p y un número entero positivo[2] q, tales que $r = \frac{p}{q}$. Un número real r que no es racional es entonces un número irracional.

Ejemplo 3:

Demostrar utilizando la técnica de demostración directa que la suma de dos números racionales es un número racional.

[1]Recordar que el conjunto de los números enteros es $\mathbb{Z} = \{ \ldots, -3, -2, -1, 0, 1, 2, 3, \ldots \}$.
[2]Recordar que el conjunto de los números enteros positivos es $\mathbb{Z}^+ = \{ 1, 2, 3, 4, 5, \ldots \}$.

El enunciado: "la suma de dos números racionales es un número racional", puede ser reescrito como: "Si r y s son números racionales, entonces, la suma de r y s da como resultado un número racional".

En la técnica de demostración directa para este ejemplo se tiene que la hipótesis es: "r y s son números racionales", la conclusión es: "la suma de r y s da como resultado un número racional".

Para demostrar que $Hipótesis \rightarrow Conclusión$, entonces se considera que la hipótesis es verdadera y se termina demostrando que la conclusión también es verdadera.

Si r y s son números reales racionales entonces, $r = \dfrac{p}{q}$ y $s = \dfrac{t}{u}$, donde $p,\ t \in \mathbb{Z}$ y $q,\ u \in \mathbb{Z}^+$. Por lo tanto se tiene que:

$$r + s = \frac{p}{q} + \frac{t}{u} = \frac{p \cdot u\ +\ q \cdot t}{q \cdot u} = \frac{m}{n}$$

donde $m = p \cdot u\ +\ q \cdot t$, como los números enteros positivos están contenidos en los números enteros, entonces, la multiplicación de números enteros positivos y números enteros da como resultado un número entero, también sucede lo mismo con la suma de números enteros y números enteros positivos, por este motivo $m \in \mathbb{Z}$.

Adicionalmente, $n = q \cdot u$, como la multiplicación de números enteros positivos da como resultado un número entero positivo, entonces $n \in \mathbb{Z}^+$.

Por tanto como $r + s$ es de la forma m/n la cual es la representación de un número racional, por lo tanto, se ha logrado demostrar de forma directa que: "Si r y s son números racionales, entonces, la suma de r y s da como resultado un número racional", porque se a partir de la hipótesis se dedujo la conclusión.

3.2. Técnica de demostración indirecta

Muchas veces al intentar una demostración directa del resultado $H \rightarrow C$ (hipótesis entonces conclusión) se presentan dificultades o carencias de información tales, que se opta por establecer la validez del mismo demostrando la validez de una fórmula lógicamente equivalente con $H \rightarrow C$. En este caso se habla de una demostración indirecta. También se intenta a veces una demostración indirecta bien porque se presienten menos dificultades o bien porque las hipótesis que para el efecto se adoptan proporcionan más información que las que se utilizan en una demostración directa.

3.2.1. Técnica de demostración por contra-recíproca

La primer técnica de demostración indirecta es conocida con el nombre de técnica de demostración por contra-recíproca o también es conocida con el nombre de técnica

de demostración por contra-posición. Utiliza la equivalencia lógica:

$$(H \to C) \iff (\neg C \to \neg H)$$

y consiste en demostrar la validez de la implicación $\neg C \to \neg H$ con lo cual queda demostrado la validez de la implicación original $H \to C$ gracias a la equivalencia lógica.

Se explicará mucho mejor la técnica de demostración con el siguiente ejemplo:

Ejemplo 4:

Demostrar utilizando la técnica de demostración por contra-recíproca que si el producto de dos números enteros es par entonces uno por lo menos de los dos números enteros es par.

La representación del resultado en la forma $H \to C$ es la siguiente:

"Si $m \cdot n$ es par, entonces m es par o n es par".

La representación del resultado en la forma $\neg C \to \neg H$ es la siguiente:

"Si m es impar y n es impar, entonces $m \cdot n$ es impar".

Como m y n son números enteros impares entonces tienen la representación $m = 2t + 1$ y $n = 2s + 1$ para números enteros t y s, por lo tanto:

$$\begin{aligned} m \cdot n &= (2t+1) \cdot (2s+1) \\ &= 4ts + 2t + 2s + 1 \\ &= 2(2ts + t + s) + 1 \\ &= 2r + 1, \text{ donde } r = 2ts + t + s \end{aligned}$$

de esta forma queda demostrado que $m \cdot n$ es un número entero impar. Al demostrar la validez de $\neg C \to \neg H$ también queda demostrada la validez de $H \to C$, por lo tanto es cierto que "si el producto de dos números enteros es par entonces uno por lo menos de los dos números enteros es par."

Ejemplo 5:

Demostrar utilizando la técnica de demostración por contra-recíproca que si $3n + 2$ es un número entero impar, entonces n es un número entero impar.

La representación del resultado en la forma $H \to C$ es la siguiente:

"Si $3n + 2$ es un número entero impar, entonces n es un número entero impar".

La representación del resultado en la forma $\neg C \to \neg H$ es la siguiente:

"Si n es un número entero par, entonces $3n + 2$ es un número entero par".

Como n es un número entero par entonces tienen la representación $n = 2t$ para algún número entero t, por lo tanto:

$$\begin{aligned} 3n + 2 &= 3(2t) + 2 \\ &= 2(3t) + 2 \\ &= 2(3t + 1) \\ &= 2r, \text{ donde } r = 3t + 1 \end{aligned}$$

de esta forma queda demostrado que $3n + 2$ es un número entero par. Al demostrar la validez de $\neg C \rightarrow \neg H$ también queda demostrada la validez de $H \rightarrow C$, por lo tanto es cierto que "Si $3n + 2$ es un número entero impar, entonces n es un número entero impar".

3.2.2. Técnica de demostración por contradicción.

La segunda técnica de demostración indirecta es conocida con el nombre de técnica de demostración por contradicción o también conocida con el nombre de técnica de demostración por reducción al absurdo.

La técnica de demostración por contradicción sirve para ayudar a definir si un razonamiento es válido o no (si una conclusión se obtiene a partir de un conjunto de hipótesis).

Si un razonamiento es valido es porque siempre que las hipótesis sean verdaderas la conclusión también es verdadera, de esta forma la implicación $H \rightarrow C$ nunca tomará un valor falso y se presentará la equivalencia lógica: $(H \rightarrow C) \Longleftrightarrow V_o$, donde se sigue teniendo una equivalencia lógica si se niegan ambos lados de la equivalencia, de esta forma se tiene el siguiente análisis que justifica la utilización de la técnica de demostración:

$$\begin{aligned} \overline{(H \rightarrow C)} &\Longleftrightarrow \overline{V_o} \\ \overline{(\overline{H} \vee C)} &\Longleftrightarrow F_o \\ (H \wedge \overline{C}) &\Longleftrightarrow F_o \end{aligned}$$

a partir de la equivalencia anterior está establecida la validez de la técnica de demostración, donde se supone la negación de la conclusión como otra hipótesis más del razonamiento y el objetivo es llegar a una contradicción (valor F_o) como conclusión a partir del nuevo conjunto de hipótesis.

Ejemplo 6:

Demostrar utilizando la técnica de demostración por contradicción que si $3n + 2$ es un número entero impar, entonces n es un número entero impar.

La representación del resultado en la forma $H \rightarrow C$ es la siguiente:

"Si $3n + 2$ es un número entero impar, entonces n es un número entero impar".

La representación del resultado en la forma $H \wedge \neg C$ es la siguiente:

"$3n + 2$ es un número entero impar **y** n es un número entero par".

La representación del resultado en la forma $\neg C \wedge H$ es la siguiente:

"n es un número entero par **y** $3n + 2$ es un número entero impar".

Como n es un número entero par entonces tienen la representación $n = 2t$ para algún número entero t, por lo tanto:

$$\begin{aligned} 3n + 2 &= 3(2t) + 2 \\ &= 2(3t) + 2 \\ &= 2(3t + 1) \\ &= 2r, \text{ donde } r = 3t + 1 \end{aligned}$$

se deduce que "$3n+2$ es un número entero par" lo cual se contradice con la hipótesis que afirma que "$3n + 2$ es un número entero impar", de esta forma se obtiene el valor falso (F_o). Al llegar a una contradicción con el método de demostración por contradicción entonces queda demostrada la validez de $H \to C$, por lo tanto es cierto que "Si $3n + 2$ es un número entero impar, entonces n es un número entero impar".

Ejemplo 7:

Determinar si el siguiente razonamiento es valido:

1. $(p \wedge q) \vee r$
2. $r \to s$
3. $(p \vee s) \to \overline{t}$
4. $(q \vee s) \to u$

$\therefore \overline{u} \to \overline{t}$

Ya se demostró la validez de éste razonamiento en el Capítulo 1 de Introducción a la Lógica Matemática, sección 1.2 de Reglas de Inferencia, ahora se va a utilizar la técnica de demostración por contradicción para demostrar de nuevo la validez de dicho razonamiento, para esto se tiene el nuevo conjunto de hipótesis y la nueva conclusión:

1. $(p \wedge q) \vee r$
2. $r \to s$
3. $(p \vee s) \to \overline{t}$
4. $(q \vee s) \to u$
5. $\overline{\overline{u} \to \overline{t}}$

$\therefore F_o$

	Pasos	**Razones**
1.	$(p \vee r) \wedge (q \vee r)$	Equivalencia Lógica H_1
2.	$p \vee r$	Ley de simplificación del P_1
3.	$\overline{\overline{\overline{u}} \vee \overline{t}}$	Equivalencia Lógica H_5
4.	$\overline{u} \wedge t$	Equivalencia Lógica P_3
5.	t	Ley de simplificación del P_4
6.	$\overline{r} \vee s$	Equivalencia Lógica H_2
7.	$p \vee s$	Ley de resolución entre P_2 y P_6
8.	$\overline{t}$	Ley Modus Ponens entre P_7 e H_3
9.	$t \wedge \overline{t}$	Ley de conjunción entre P_5 y P_8
10.	F_o	Equivalencia Lógica P_9

Como se obtiene una contradicción (F_o) entonces queda demostrada la validez del razonamiento original por medio del uso de la técnica de demostración por contradicción.

Ejemplo 8:

Determinar si el siguiente razonamiento es valido:

1. $u \rightarrow r$
2. $(r \wedge s) \rightarrow (p \vee t)$
3. $q \rightarrow (u \wedge s)$
4. $\overline{t}$

$\therefore q \rightarrow p$

Ya se demostró la validez de éste razonamiento en el Capítulo 1 de Introducción a la Lógica Matemática, sección 1.2 de Reglas de Inferencia, ahora se va a utilizar la técnica de demostración por contradicción para demostrar de nuevo la validez de dicho razonamiento, para esto se tiene el nuevo conjunto de hipótesis y la nueva conclusión:

1. $u \rightarrow r$
2. $(r \wedge s) \rightarrow (p \vee t)$
3. $q \rightarrow (u \wedge s)$
4. $\overline{t}$
5. $\overline{q \rightarrow p}$

$\therefore F_o$

	Pasos	**Razones**
1.	$\overline{\overline{q} \vee p}$	Equivalenca Lógica H_5
2.	$q \wedge \overline{p}$	Equivalenca Lógica P_1
3.	q	Ley de Simplificación P_2
4.	$\overline{p}$	Ley de Simplificación P_2
5.	$\overline{p} \wedge \overline{t}$	Ley de Conjunción entre P_4 e H_4
6.	$\overline{p \vee t}$	Equivalenca Lógica P_5
7.	$u \wedge s$	Ley Modus Ponens entre P_3 e H_3
8.	$\overline{r \wedge s}$	Ley Modus Tollens entre P_6 e H_2
9.	$\overline{r} \vee \overline{s}$	Equivalenca Lógica P_8
10.	$\overline{u} \vee r$	Equivalenca Lógica H_1
11.	$\overline{u} \vee \overline{s}$	Ley de Resolución entre P_{10} y P_9
12.	$\overline{u \wedge s}$	Equivalenca Lógica P_{11}
13.	$(u \wedge s) \wedge \overline{(u \wedge s)}$	Ley de Conjunción entre P_7 y P_{12}
14.	F_o	Equivalenca Lógica P_{13}

Como se obtiene una contradicción (F_o) entonces queda demostrada la validez del razonamiento original por medio del uso de la técnica de demostración por contradicción.

3.3. Técnica de demostración por disyunción de casos

Para probar una implicación de la forma $(p_1 \vee p_2 \vee p_3 \vee \cdots \vee p_n) \rightarrow q$ se utiliza la siguiente equivalencia lógica $(p_1 \rightarrow q) \wedge (p_2 \rightarrow q) \wedge (p_3 \rightarrow q) \wedge \cdots \wedge (p_n \rightarrow q)$, la cual se obtiene de la siguiente forma:

$(p_1 \vee p_2 \vee p_3 \vee \cdots \vee p_n) \rightarrow q$

$\iff \overline{(p_1 \vee p_2 \vee p_3 \vee \cdots \vee p_n)} \vee q$, Equivalencia Lógica de la implicación.

$\iff (\overline{p_1} \wedge \overline{p_2} \wedge \overline{p_3} \wedge \cdots \wedge \overline{p_n}) \vee q$, Ley de De Morgan.

$\iff (\overline{p_1} \vee q) \wedge (\overline{p_2} \vee q) \wedge (\overline{p_3} \vee q) \wedge \cdots \wedge (\overline{p_n} \vee q)$, Ley Distributiva.

$\iff (p_1 \rightarrow q) \wedge (p_2 \rightarrow q) \wedge (p_3 \rightarrow q) \wedge \cdots \wedge (p_n \rightarrow q)$, Eq. Lógica de la implicación.

La equivalencia lógica evidencia que la implicación original con una hipótesis que se forma de la disyunción de las proposiciones p_1, p_2, p_3, ..., p_n puede ser probado al demostrar individualmente cada una de las n implicaciones $p_i \rightarrow q$, para $1 \leq i \leq n$.
La única forma para que se cumpla la implicación original es cuando se cumplen absolutamente todas las implicaciones $p_1 \rightarrow q$, $p_2 \rightarrow q$, $p_3 \rightarrow q$, $\cdots$, $p_n \rightarrow q$.

Ejemplo 9:

Probar o refutar utilizando el método de demostración por disyunción de casos que $n(n^2+5)$ es divisible por 6, para $n \in \mathbb{N}$.

Cualquier número natural n está en alguno de los siguientes seis casos, donde $k \in \mathbb{N}$:

- caso 1: $n = 6k$, el número n es un múltiplo de seis.
- caso 2: $n = 6k+1$, el número n es un múltiplo de seis más uno.
- caso 3: $n = 6k+2$, el número n es un múltiplo de seis más dos.
- caso 4: $n = 6k+3$, el número n es un múltiplo de seis más tres.
- caso 5: $n = 6k+4$, el número n es un múltiplo de seis más cuatro.
- caso 6: $n = 6k+5$, el número n es un múltiplo de seis más cinco.

Ahora se tienen que demostrar cada uno de los seis casos, para lo cual se tiene:

caso 1: $n = 6k$:

$$\begin{aligned} n(n^2+5) &= 6k((6k)^2+5) \\ &= 6k(36k^2+5) \\ &= 6(36k^3+5k) \\ &= 6z, \text{ donde } z = 36k^3+5k \text{ y } z \in \mathbb{N}. \end{aligned}$$

Se cumple el caso 1, porque cualquier número que es múltiplo de 6 también es divisible por 6.

caso 2: $n = 6k+1$:

$$\begin{aligned} n(n^2+5) &= (6k+1)((6k+1)^2+5) \\ &= (6k+1)(36k^2+12k+1+5) \\ &= (6k+1)(36k^2+12k+6) \\ &= (6k+1)\cdot 6 \cdot (6k^2+2k+1) \\ &= 6\cdot(6k+1)(6k^2+2k+1) \\ &= 6z \text{ donde } z = (6k+1)(6k^2+2k+1) \text{ y } z \in \mathbb{N}. \end{aligned}$$

Se cumple el caso 2, porque cualquier número que es múltiplo de 6 también es divisible por 6.

caso 3: $n = 6k + 2$:

$$\begin{aligned} n(n^2+5) &= (6k+2)((6k+2)^2+5) \\ &= (6k+2)(36k^2+24k+4+5) \\ &= (6k+2)(36k^2+24k+9) \\ &= 2\cdot(3k+1)\cdot 3\cdot(12k^2+8k+3) \\ &= 2\cdot 3\cdot(3k+1)(12k^2+8k+3) \\ &= 6\cdot(3k+1)(12k^2+8k+3) \\ &= 6z, \text{ donde } z = (3k+1)(12k^2+8k+3) \text{ y } z \in \mathbb{N}. \end{aligned}$$

Se cumple el caso 3, porque cualquier número que es múltiplo de 6 también es divisible por 6.

caso 4: $n = 6k + 3$:

$$\begin{aligned} n(n^2+5) &= (6k+3)((6k+3)^2+5) \\ &= (6k+3)(36k^2+36k+9+5) \\ &= (6k+3)(36k^2+36k+14) \\ &= 3\cdot(2k+1)\cdot 2\cdot(18k^2+18k+7) \\ &= 3\cdot 2\cdot(2k+1)(18k^2+18k+7) \\ &= 6\cdot(2k+1)(18k^2+18k+7) \\ &= 6z, \text{ donde } z = (2k+1)(18k^2+18k+7) \text{ y } z \in \mathbb{N}. \end{aligned}$$

Se cumple el caso 4, porque cualquier número que es múltiplo de 6 también es divisible por 6.

caso 5: $n = 6k + 4$

$$\begin{aligned} n(n^2+5) &= (6k+4)((6k+4)^2+5) \\ &= (6k+4)(36k^2+48k+16+5) \\ &= (6k+4)(36k^2+48k+21) \\ &= 2\cdot(3k+2)\cdot 3\cdot(12k^2+16k+7) \\ &= 2\cdot 3\cdot(3k+2)(12k^2+16k+7) \\ &= 6\cdot(3k+2)(12k^2+16k+7) \\ &= 6z, \text{ donde } z = (3k+2)(12k^2+16k+7) \text{ y } z \in \mathbb{N}. \end{aligned}$$

Se cumple el caso 5, porque cualquier número que es múltiplo de 6 también es

divisible por 6.

caso 6: $n = 6k + 5$:

$$\begin{aligned} n(n^2+5) &= (6k+5)((6k+5)^2+5) \\ &= (6k+5)(36k^2+60k+25+5) \\ &= (6k+5)(36k^2+60k+30) \\ &= (6k+5)\cdot 6\cdot(6k^2+10k+5) \\ &= 6\cdot(6k+5)(6k^2+10k+5) \\ &= 6z, \text{ donde } z = (6k+5)(6k^2+10k+5) \text{ y } z \in \mathbb{N}. \end{aligned}$$

Se cumple el caso 6, porque cualquier número que es múltiplo de 6 también es divisible por 6.

Como se cumplen todos los seis casos entonces queda demostrado utilizando la técnica de demostración por disyunción de casos que $n(n^2+5)$ es divisible por 6, para $n \in \mathbb{N}$.

Ejemplo 10:

Probar o refutar que el cuadrado de todo número natural, es un múltiplo de 5, ó difiere de un múltiplo de 5 en 1.

Cualquier número natural n está en alguno de los siguientes cinco casos, donde $m \in \mathbb{N}$:

- caso 1: $n = 5m$, el número n es un múltiplo de cinco.
- caso 2: $n = 5m + 1$, el número n es un múltiplo de cinco más uno.
- caso 3: $n = 5m + 2$, el número n es un múltiplo de cinco más dos.
- caso 4: $n = 5m + 3$, el número n es un múltiplo de cinco más tres.
- caso 5: $n = 5m + 4$, el número n es un múltiplo de cinco más cuatro.

Ahora se tienen que demostrar cada uno de los cinco casos, para lo cual se tiene:

- caso 1: $n = 5m$:

  $$\begin{aligned} n^2 &= (5m)^2 \\ &= 5^2m^2 \\ &= 5(5m^2) \\ &= 5\cdot z, \text{ donde } z = 5m^2 \text{ y } z \in \mathbb{N}. \end{aligned}$$

  Se cumple el caso 1, porque el número que se obtiene es un múltiplo de cinco.

- caso 2: $n = 5m + 1$:

  $n^2 = (5m + 1)^2$

  $= 5^2m^2 + 2 \cdot 5m + 1$

  $= 5(5m^2 + 2m) + 1$

  $= 5 \cdot z + 1$, donde $z = 5m^2 + 2m$ y $z \in \mathbb{N}$.

  Se cumple el caso 2, porque el número que se obtiene es un múltiplo de cinco más uno.

- caso 3: $n = 5m + 2$:

  $n^2 = (5m + 2)^2$

  $= 5^2m^2 + 2 \cdot 5 \cdot 2m + 4$

  $= 5^2m^2 + 5 \cdot 4m + 5 - 1$

  $= 5(5m^2 + 4m + 1) - 1$

  $= 5z - 1$, donde $z = 5m^2 + 4m + 1$ y $z \in \mathbb{N}$.

  Se cumple el caso 3, porque el número que se obtiene es un múltiplo de cinco menos uno.

- caso 4: $n = 5m + 3$:

  $n^2 = (5m + 3)^2$

  $= 5^2m^2 + 2 \cdot 5 \cdot 3m + 9$

  $= 5^2m^2 + 5 \cdot 2 \cdot 3m + 10 - 1$

  $= 5(5m^2 + 6m + 2) - 1$

  $= 5z - 1$, donde $z = 5m^2 + 6m + 2$ y $z \in \mathbb{N}$.

  Se cumple el caso 4, porque el número que se obtiene es un múltiplo de cinco menos uno.

- caso 5: $n = 5m + 4$:

  $n^2 = (5m + 4)^2$

  $= 5^2m^2 + 2 \cdot 5 \cdot 4m + 16$

  $= 5^2m^2 + 5 \cdot 2 \cdot 4m + 15 + 1$

  $= 5(5m^2 + 8m + 3) + 1$

$= 5z + 1$, donde $z = 5m^2 + 8m + 3$ y $z \in \mathbb{N}$.

Se cumple el caso 5, porque el número que se obtiene es un múltiplo de cinco más uno.

Como se cumplen todos los cinco casos entonces queda demostrado utilizando la técnica de demostración por disyunción de casos que el cuadrado de todo número natural, es un múltiplo de 5, ó difiere de un múltiplo de 5 en 1.

Ejemplo 11:

Probar o refutar que $n^2 - 1$ es divisible por 8 para los números enteros impares.

Cualquier número entero n está en alguno de los siguientes ocho casos, donde $k \in \mathbb{Z}$:

- caso 1: $n = 8k$, el número n es un múltiplo de ocho.
- caso 2: $n = 8k + 1$, el número n es un múltiplo de ocho más uno.
- caso 3: $n = 8k + 2$, el número n es un múltiplo de ocho más dos.
- caso 4: $n = 8k + 3$, el número n es un múltiplo de ocho más tres.
- caso 5: $n = 8k + 4$, el número n es un múltiplo de ocho más cuatro.
- caso 6: $n = 8k + 5$, el número n es un múltiplo de ocho más cinco.
- caso 7: $n = 8k + 6$, el número n es un múltiplo de ocho más seis.
- caso 8: $n = 8k + 7$, el número n es un múltiplo de ocho más siete.

En el análisis sólo se consideraran los casos 2, 4, 6 y 8 porque estos son los que representan a los números enteros impares. Para la demostración de estos cuatro casos se tiene:

caso 2: $n = 8k + 1$:

$$\begin{aligned} n^2 - 1 &= (8k+1)^2 - 1 \\ &= 64k^2 + 16k + 1 - 1 \\ &= 8(8k^2 + 2k) \\ &= 8z, \text{ donde } z = 8k^2 + 2k \text{ y } z \in \mathbb{N} \end{aligned}$$

Se cumple el caso 2, porque cualquier número que es múltiplo de 8 también es divisible por 8.

caso 4: $n = 8k + 3$:

$$\begin{aligned} n^2 - 1 &= (8k+3)^2 - 1 \\ &= 64k^2 + 48k + 9 - 1 \\ &= 64k^2 + 48k + 8 \\ &= 8(8k^2 + 6k + 1) \\ &= 8z, \text{ donde } z = 8k^2 + 6k + 1 \text{ y } z \in \mathbb{N} \end{aligned}$$

Se cumple el caso 4, porque cualquier número que es múltiplo de 8 también es divisible por 8.

caso 6: $n = 8k + 5$:

$$\begin{aligned} n^2 - 1 &= (8k+5)^2 - 1 \\ &= 64k^2 + 80k + 25 - 1 \\ &= 64k^2 + 80k + 24 \\ &= 8(8k^2 + 10k + 3) \\ &= 8z, \text{ donde } z = 8k^2 + 10k + 3 \text{ y } z \in \mathbb{N} \end{aligned}$$

Se cumple el caso 6, porque cualquier número que es múltiplo de 8 también es divisible por 8.

caso 8: $n = 8k + 7$:

$$\begin{aligned} n^2 - 1 &= (8k+7)^2 - 1 \\ &= 64k^2 + 8(14)k + 49 - 1 \\ &= 64k^2 + 8(14)k + 48 \\ &= 8(8k^2 + 14k + 6) \\ &= 8z, \text{ donde } z = 8k^2 + 14k + 6 \text{ y } z \in \mathbb{N} \end{aligned}$$

Se cumple el caso 8, porque cualquier número que es múltiplo de 8 también es divisible por 8.

Como se cumplen todos los cuatro casos que representan números enteros impares, entonces queda demostrado utilizando la técnica de demostración por disyunción de casos que $n^2 - 1$ es divisible por 8 para todo n que es un número entero impar.

3.4. Técnica de demostración por contraejemplo

La técnica de demostración por contraejemplo es utilizada para demostrar que un argumento que se intuye que no es válido realmente no es válido. La técnica de demostración por contraejemplo no sirve para demostrar validez, únicamente sirve para

demostrar falsedad, por este motivo el hecho de no encontrar un contraejemplo no garantiza la validez del argumento, en dicho caso se debe utilizar alguna de las técnicas de demostración de éste capítulo que sirva para demostrar validez.

Ejemplo 12:

Demostrar o refutar si el siguiente razonamiento es valido:

1. $p \rightarrow (q \ \rightarrow r)$
2. $q \rightarrow (p \rightarrow r)$

$\therefore (p \vee q) \rightarrow r$

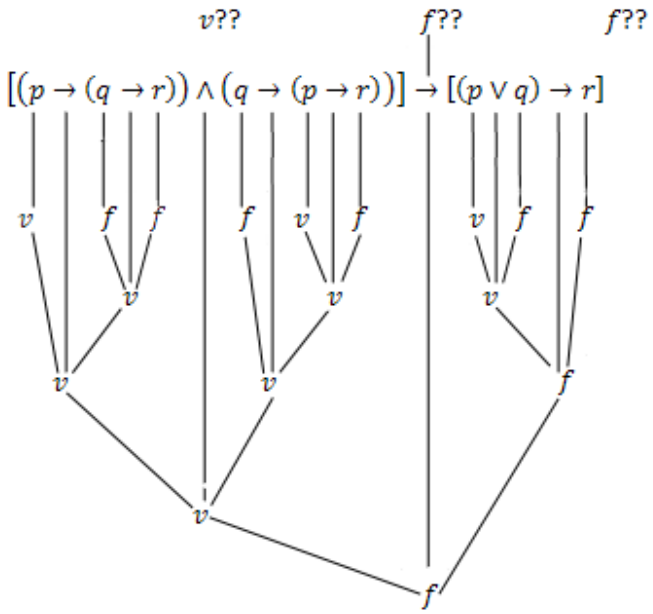
Para este ejemplo primero que todo se va a tratar de determinar la validez del razonamiento por medio de la técnica de demostración directa al hacer uso de las dos hipótesis, de equivalencias lógicas y de reglas de inferencia para llegar a la conclusión, de esta forma se tiene:

	Pasos	**Razones**
1.	$\overline{p} \vee (\overline{q} \vee r)$	Equivalencia Lógica de H_1
2.	$\overline{q} \vee (\overline{p} \vee r)$	Equivalencia Lógica del P_1
3.	$q \rightarrow (p \rightarrow r)$	Equivalencia Lógica del P_2
4.	$(q \rightarrow (p \rightarrow r)) \wedge (q \rightarrow (p \rightarrow r))$	Ley de conjunción entre P_3 e H_2
5.	$q \rightarrow (p \rightarrow r)$	Equivalencia Lógica del P_4

No se llego a la conclusión, esto indica que "posiblemente" el razonamiento no es correcto, como se intuye que el razonamiento no es válido entonces se va a buscar una asignación de valores de verdad para las variables proposicionales que hagan que todas las hipótesis sean verdaderas y la conclusión sea falsa, para esto se debe tener en cuenta que el razonamiento puede ser representado de forma equivalente por la expresión:

$$[(p \rightarrow (q \ \rightarrow r)) \ \wedge \ (q \rightarrow (p \rightarrow r))] \ \rightarrow \ [(p \vee q) \rightarrow r]$$

donde si todas las hipótesis son verdaderas entonces el antecedente de la implicación sería verdadero y si la conclusión es falsa entonces el consecuente de la implicación sería falso los que llevaría a que la implicación fuera falsa, o dicho de forma equivalente, lo que haría que el razonamiento sea falso. En la exploración de la posible asignación de valores de verdad para las variables proposicionales que hagan que el razonamiento sea falso se tiene:



en consecuencia, la asignación de los valores $p : V_o$, $q : F_o$, $r : F_o$, hacen que el razonamiento sea falso, por lo tanto dicha asignación de valores son un contraejemplo de la validez del razonamiento.

Ejemplo 13:

¿Es posible probar que $\binom{2n}{n} = 2\binom{n}{2} + n^2$, para $n \in \mathbb{Z}^+$ donde $n \geq 2$?.

Como dato anecdótico al autor, en un examen de Matemáticas Discretas en la Maestría, se le pidió que demostrara dicho ejercicio, cuando se pide que se demuestre se sobre entiende que es cierta la fórmula, por éste motivo durante aproximadamente tres horas trato de multiples formas de demostrar la validez de dicha fórmula, pero no lo logro. Existía la posibilidad de que le hubieran pedido que demostrara algo que no se podía demostrar, por este motivo utilizó la técnica de demostración por contraejemplo para demostrar que la fórmula era falsa, lo que se hizo fue evaluar la fórmula a partir de números enteros positivos mayores o iguales a dos para ver si se cumple o no, para esto se tiene:

Evaluación de la fórmula en $n = 2$:

$$\begin{aligned}
\binom{2(2)}{2} &= 2\binom{2}{2} + 2^2 \\
\binom{4}{2} &= 2\binom{2}{2} + 2^2 \\
\frac{4!}{(4-2)! \cdot 2!} &= 2\left[\frac{2!}{(2-2)! \cdot 2!}\right] + 4
\end{aligned}$$

$$\begin{aligned}
\frac{4!}{2!\cdot 2!} &= 2\left[\frac{2!}{0!\cdot 2!}\right]+4\\
\frac{4\cdot 3\cdot 2!}{2!\cdot 2!} &= 2\left[\frac{2!}{0!\cdot 2!}\right] + 4\\
\frac{4\cdot 3}{2!} &= 2\left[\frac{1}{0!}\right] + 4\\
\frac{4\cdot 3}{2} &= 2\left[\frac{1}{1}\right] + 4\\
6 &= 2+4\\
6 &= 6
\end{aligned}$$

La fórmula se cumple para $n = 2$

Evaluación de la fórmula en $n = 3$:

$$\begin{aligned}
\binom{2(3)}{3} &= 2\binom{3}{2}+3^2\\
\binom{6}{3} &= 2\binom{3}{2}+3^2\\
\frac{6!}{(6-3)!\cdot 3!} &= 2\left[\frac{3!}{(3-2)!\cdot 2!}\right] + 9\\
\frac{6!}{3!\cdot 3!} &= 2\left[\frac{3!}{1!\cdot 2!}\right]+9\\
\frac{6\cdot 5\cdot 4\cdot 3!}{3!\cdot 3!} &= 2\left[\frac{3\cdot 2!}{1!\cdot 2!}\right] + 9\\
\frac{6\cdot 5\cdot 4}{3!} &= 2\left[\frac{3}{1!}\right] + 9\\
\frac{6\cdot 5\cdot 4}{6} &= 2\left[\frac{3}{1}\right] + 9\\
\frac{5\cdot 4}{1} &= 2\big[3\big] + 9\\
20 &= 6+9\\
20 &= 15
\end{aligned}$$

La fórmula no se cumple para $n = 3$.

Como se encontrón un valor de n para el cual no se cumple la fórmula, entonces queda demostrado por contra ejemplo que la fórmula es falsa.

3.5. Técnica de demostración por inducción matemática

La técnica de demostración por inducción matemática es utilizada para probar proposiciones de la forma $\forall_n p(n)$, donde el universo del discurso es el conjunto de los números naturales ($\mathbb{N}$).

Una demostración por la técnica de inducción matemática consiste de tres pasos:

Paso base:

se demuestra la validez de la proposición p evaluada en el caso base, donde dicho caso base puede ser un cero o un uno dependiendo del punto de partida o condición inicial del problema que se está demostrando.

Paso inductivo (o hipótesis de inducción):

se asume que es verdadera la proposición p evaluada en un número natural k.

Paso post-inductivo:

apoyados en la suposición de validez de la proposición $p(k)$ se demuestra la validez de la proposición $p(k+1)$, es decir, $p(k) \rightarrow p(k+1)$.

Cuando se cumplen los tres casos de la técnica por inducción matemática, entonces se ha demostrado que la proposición $p(n)$ es verdadero para todo número natural n, es decir, se ha demostrado que $\forall_n p(n)$ es verdadero.

Ejemplo 14:

Probar o refutar utilizando la técnica de demostración por inducción matemática que:

$$\sum_{i=1}^{n} i = 1 + 2 + 3 + \ldots + n = \frac{n(n+1)}{2}, \text{ para } \; n \in \mathbb{Z}^+$$

Para el desarrollo de la demostración considere que se tiene la proposición

$$p(n) = \sum_{i=1}^{n} i = 1 + 2 + 3 + \ldots + n = \frac{n(n+1)}{2}, \;\; \text{donde} \;\; n \in \mathbb{Z}^+$$

Recordar que una proposición sólo puede tomar de forma precisa el valor verdadero (V_o) o el valor falso (F_o), nada más. Ahora se consideran los tres pasos de la técnica por inducción matemática:

Paso base n = 1:

$$p(1) = \underbrace{\sum_{i=1}^{1} i = 1}_{\text{resultado a partir de la sumatoria de términos}} = \underbrace{\frac{1(1+1)}{2} = 1}_{\text{resultado a partir de la fórmula}}$$

como se obtiene el mismo resultado en la sumatoria de términos y en la fórmula que es la solución de la sumatoria entonces la proposición $p(1)$ es verdadera y la demostración continua en el paso inductivo.

Paso inductivo n = k:

$p(k) = \sum_{i=1}^{k} i = 1 + 2 + 3 + \ldots + k = \frac{k(k+1)}{2}$, se asume que la proposición $p(k)$ es verdadera, esto quiere decir, que se asume que se cumple la siguiente igualdad $1 + 2 + 3 + \ldots + k = \frac{k(k+1)}{2}$.

Paso post-inductivo n = k + 1:

$$p(k+1) = \sum_{i=1}^{k+1} i = \underbrace{1 + 2 + 3 + \ldots + k}_{\substack{\text{Se reemplaza por su equivalente} \\ \text{en el paso inductivo}}} + (k+1) = \frac{(k+1)(k+2)}{2}$$

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

$$(k+1)\big[\frac{k}{2} + 1\big] = \frac{(k+1)(k+2)}{2}$$

$$(k+1)\big[\frac{k+2}{2}\big] = \frac{(k+1)(k+2)}{2}$$

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

Se cumple la igualdad, por lo tanto la proposición $p(k+1)$ es verdadera, como se cumplen los tres pasos de técnica de demostración por inducción matemática entonces queda demostrada la validez de la solución de la sumatoria originalmente planteada.

Ejemplo 15:

Probar o refutar utilizando la técnica de demostración por inducción matemática que:

$$\sum_{i=1}^{n} i^2 = 1^2 + 2^2 + 3^2 + \ldots + n^2 = \frac{n(n+1)(2n+1)}{6}, \text{ para } n \in \mathbb{Z}^+$$

Para el desarrollo de la demostración considerar que se tiene la proposición

$$p(n) = \sum_{i=1}^{n} i^2 = 1^2 + 2^2 + 3^2 + \ldots + n^2 = \frac{n(n+1)(2n+1)}{6}, \quad \text{donde} \quad n \in \mathbb{Z}^+$$

La proposición $p(n)$ tomará el valor verdadero (V_o) o falso (F_o) dependiendo de si se cumple o no la igualdad $\sum_{i=1}^{n} i^2 = \frac{n(n+1)(2n+1)}{6}$. Ahora se consideran los tres pasos de la técnica por inducción matemática:

Paso base n = 1:

$$p(1) = \underbrace{\sum_{i=1}^{1} i^2 = 1^2 = 1}_{\textit{resultado a partir de la sumatoria de términos}} = \underbrace{\frac{1(1+1)(2(1)+1)}{6} = \frac{1(2)(3)}{6} = 1}_{\textit{resultado a partir de la fórmula}}$$

como se obtiene el mismo resultado en la sumatoria de términos y en la fórmula que es la solución de la sumatoria entonces la proposición $p(1)$ es verdadera y la demostración continua en el paso inductivo.

Paso inductivo n = k:

$p(k) = \sum_{i=1}^{k} i^2 = 1^2+2^2+3^2+\ldots+k^2 = \frac{k(k+1)(2k+1)}{6}$, se asume que la proposición $p(k)$ es verdadera, esto quiere decir, que se asume que se cumple la siguiente igualdad $1^2 + 2^2 + 3^2 + \ldots + k^2 = \frac{k(k+1)(2k+1)}{6}$.

Paso post-inductivo n = k + 1:

$$p(k+1) = \sum_{i=1}^{k+1} i^2 = \underbrace{1^2 + 2^2 + 3^2 + \ldots + k^2}_{\substack{\textit{Se reemplaza por su equivalente} \\ \textit{en el paso inductivo}}} + (k+1)^2 = \frac{(k+1)(k+1+1)(2(k+1)+1)}{6}$$

$$\frac{k(k+1)(2k+1)}{6} + (k+1)^2 = \frac{(k+1)(k+2)(2k+2+1)}{6}$$

$$(k+1)\left[\frac{k(2k+1)}{6} + (k+1)\right] = \frac{(k+1)(k+2)(2k+3)}{6}$$

$$(k+1)\left[\frac{k(2k+1) \ + \ 6(k+1)}{6}\right] = \frac{(k+1)(k+2)(2k+3)}{6}$$

$$(k+1)\left[\frac{2k^2 \ + \ k \ + \ 6k \ + \ 6}{6}\right] = \frac{(k+1)(k+2)(2k+3)}{6}$$

$$(k+1)\left[\frac{2k^2 \ + \ 7k \ + \ 6}{6}\right] = \frac{(k+1)(k+2)(2k+3)}{6}$$

hace falta averiguar a que es igual la ecuación cuadrática $2k^2 + 7k + 6 = 0$, para esto se debe recordar primero la fórmula general para este fin, la cual es:

$$k = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}$$

en la ecuación cuadrática que estamos trabajando se tiene que $a = 2$, $b = 7$ y $c = 6$, al reemplazar en la fórmula se tiene:

$$k = \frac{-7 \pm \sqrt{7^2 - (4)(2)(6)}}{2 \cdot 2} = \frac{-7 \pm \sqrt{49 - 48}}{4} = \frac{-7 \pm \sqrt{1}}{4} = \frac{-7 \pm 1}{4}$$

de donde se obtienen las raíces reales distintas

- $k = \dfrac{-7 - 1}{4} = -\dfrac{8}{4} = -2, \quad k = -2, \quad k + 2 = 0$
- $k = \dfrac{-7 + 1}{4} = -\dfrac{6}{4} = -\dfrac{3}{2}, \quad k = -\dfrac{3}{2}, \quad 2k + 3 = 0$

a partir de las soluciones de la ecuación cuadrática se tiene que

$$2k^2 + 7k + 6 = (k + 2)(2k + 3)$$

ahora continuando con la demostración del paso post-inductivo se tiene:

$$(k+1)\left[\frac{(k+2)(2k+3)}{6}\right] = \frac{(k+1)(k+2)(2k+3)}{6}$$

$$\frac{(k+1)(k+2)(2k+3)}{6} = \frac{(k+1)(k+2)(2k+3)}{6}$$

Se cumple la igualdad, por lo tanto la proposición $p(k + 1)$ es verdadera, como se cumplen los tres pasos de técnica de demostración por inducción matemática entonces queda demostrada la validez de la solución de la sumatoria originalmente planteada.

Ejemplo 16:

Demostrar utilizando la técnica de inducción matemática que:

$$\sum_{i=1}^{n} i^3 = 1^3 + 2^3 + 3^3 + \ldots + n^3 = \left(\frac{n(n+1)}{2}\right)^2, \text{ para } \; n \in \mathbb{Z}^+$$

Para el desarrollo de la demostración considerar que se tiene la proposición

$$p(n) = \sum_{i=1}^{n} i^3 = 1^3 + 2^3 + 3^3 + \ldots + n^3 = \left(\frac{n(n+1)}{2}\right)^2, \text{ para } \; n \in \mathbb{Z}^+$$

la proposición $p(n)$ tomará el valor verdadero (V_o) o falso (F_o) dependiendo de si se cumple o no la igualdad $\sum_{i=1}^{n} i^3 = \left(\frac{n(n+1)}{2}\right)^2$. Ahora se consideran los tres pasos de la técnica por inducción matemática:

Paso base n = 1:

$$p(1) = \underbrace{\sum_{i=1}^{1} i^3 = 1^3 = 1}_{\textit{resultado a partir de la sumatoria de términos}} = \underbrace{\left(\frac{1(1+1)}{2}\right)^2 = \left(\frac{1(2)}{2}\right)^2 = 1^2 = 1}_{\textit{resultado a partir de la fórmula}}$$

como se obtiene el mismo resultado en la sumatoria de términos y en la fórmula que es la solución de la sumatoria entonces la proposición $p(1)$ es verdadera y la demostración continua en el paso inductivo.

Paso inductivo n = k:

$p(k) = \sum_{i=1}^{k} i^3 = 1^3 + 2^3 + 3^3 + \ldots + k^3 = \left(\frac{k(k+1)}{2}\right)^2$, se asume que la proposición $p(k)$ es verdadera, esto quiere decir, que se asume que se cumple la siguiente igualdad $1^3 + 2^3 + 3^3 + \ldots + k^3 = \left(\frac{k(k+1)}{2}\right)^2$.

Paso post-inductivo n = k + 1:

$$p(k+1) = \sum_{i=1}^{k+1} i^3 = \underbrace{1^3 + 2^3 + 3^3 + \ldots + k^3}_{\substack{\textit{Se reemplaza por su equivalente} \\ \textit{en el paso inductivo}}} + (k+1)^3 = \left(\frac{(k+1)(k+1+1)}{2}\right)^2$$

$$\left(\frac{k(k+1)}{2}\right)^2 + (k+1)^3 = \left(\frac{(k+1)(k+2)}{2}\right)^2$$

$$\frac{k^2(k+1)^2}{4} + (k+1)^3 = \left(\frac{(k+1)(k+2)}{2}\right)^2$$

$$(k+1)^2\left[\frac{k^2}{4} + \frac{4(k+1)}{4}\right] = \left(\frac{(k+1)(k+2)}{2}\right)^2$$

$$(k+1)^2\left[\frac{k^2+4k+4}{4}\right] = \left(\frac{(k+1)(k+2)}{2}\right)^2$$

$$(k+1)^2\left[\frac{(k+2)^2}{2^2}\right] = \left(\frac{(k+1)(k+2)}{2}\right)^2$$

$$\frac{(k+1)^2(k+2)^2}{2^2} = \left(\frac{(k+1)(k+2)}{2}\right)^2$$

$$\left(\frac{(k+1)(k+2)}{2}\right)^2 = \left(\frac{(k+1)(k+2)}{2}\right)^2$$

Se cumple la igualdad, por lo tanto la proposición $p(k+1)$ es verdadera, como se cumplen los tres pasos de técnica de demostración por inducción matemática entonces queda demostrada la validez de la solución de la sumatoria originalmente planteada.

Ejemplo 17:

Demostrar utilizando la técnica de inducción matemática que:

$$\sum_{i=1}^{n} \frac{i}{2^i} = \frac{1}{2^1} + \frac{2}{2^2} + \frac{3}{2^3} + \ldots + \frac{n}{2^n} = 2 - \frac{n+2}{2^n}, \text{ para } n \in \mathbb{Z}^+$$

Para el desarrollo de la demostración considerar que se tiene la proposición

$$p(n) = \sum_{i=1}^{n} \frac{i}{2^i} = \frac{1}{2^1} + \frac{2}{2^2} + \frac{3}{2^3} + \ldots + \frac{n}{2^n} = 2 - \frac{n+2}{2^n}, \text{ para } n \in \mathbb{Z}^+$$

la proposición $p(n)$ tomará el valor verdadero (V_o) o falso (F_o) dependiendo de si se cumple o no la igualdad $\sum_{i=1}^{n} \frac{i}{2^i} = 2 - \frac{n+2}{2^n}$. Ahora se consideran los tres pasos de la técnica por inducción matemática:

Paso base n = 1:

$$p(1) = \underbrace{\sum_{i=1}^{1} \frac{i}{2^i} = \frac{1}{2^1} = \frac{1}{2}}_{\textit{resultado a partir de la sumatoria de términos}} = \underbrace{2 - \frac{1+2}{2^1} = 2 - \frac{3}{2} = \frac{4-3}{2} = \frac{1}{2}}_{\textit{resultado a partir de la fórmula}}$$

como se obtiene el mismo resultado en la sumatoria de términos y en la fórmula que es la solución de la sumatoria entonces la proposición $p(1)$ es verdadera y la demostración continua en el paso inductivo.

Paso inductivo n = k:

$p(k) = \sum_{i=1}^{k} \frac{i}{2^i} = \frac{1}{2^1} + \frac{2}{2^2} + \frac{3}{2^3} + \ldots + \frac{k}{2^k} = 2 - \frac{k+2}{2^k}$, se asume que la proposición $p(k)$ es verdadera, esto quiere decir, que se supone que se cumple la siguiente igualdad $\frac{1}{2^1} + \frac{2}{2^2} + \frac{3}{2^3} + \ldots + \frac{k}{2^k} = 2 - \frac{k+2}{2^k}$.

Paso post-inductivo $\mathbf{n = k + 1}$:

$$p(k+1) = \sum_{i=1}^{k+1} \frac{i}{2^i} = \underbrace{\frac{1}{2} + \frac{2}{2^2} + \frac{3}{2^3} + \ldots + \frac{k}{2^k}}_{\text{Se reemplaza por su equivalente en el paso inductivo}} + \frac{k+1}{2^{k+1}} = 2 - \frac{k+1+2}{2^{k+1}}$$

$$2 - \frac{k+2}{2^k} + \frac{k+1}{2^{k+1}} = 2 - \frac{k+3}{2^{k+1}}$$

$$2 - \left(\frac{k+2}{2^k} \cdot \frac{2}{2}\right) + \frac{k+1}{2^{k+1}} = 2 - \frac{k+3}{2^{k+1}}$$

$$2 - \frac{2k+4}{2^{k+1}} + \frac{k+1}{2^{k+1}} = 2 - \frac{k+3}{2^{k+1}}$$

$$2 - \left[\frac{2k+4}{2^{k+1}} - \frac{k+1}{2^{k+1}}\right] = 2 - \frac{k+3}{2^{k+1}}$$

$$2 - \left[\frac{2k+4 \ - \ (k+1)}{2^{k+1}}\right] = 2 - \frac{k+3}{2^{k+1}}$$

$$2 - \left[\frac{2k \ + \ 4 \ - \ k \ - \ 1)}{2^{k+1}}\right] = 2 - \frac{k+3}{2^{k+1}}$$

$$2 - \left[\frac{k \ + \ 3}{2^{k+1}}\right] = 2 - \frac{k+3}{2^{k+1}}$$

$$2 - \frac{k+3}{2^{k+1}} = 2 - \frac{k+3}{2^{k+1}}$$

Se cumple la igualdad, por lo tanto la proposición $p(k+1)$ es verdadera, como se cumplen los tres pasos de técnica de demostración por inducción matemática entonces queda demostrada la validez de la solución de la sumatoria originalmente planteada.

Ejemplo 18:

Demostrar por la técnica de inducción matemática que:

$$\sum_{i=1}^{n} \frac{2}{i(i+1)} = \frac{2}{1(2)} + \frac{2}{2(3)} + \frac{2}{3(4)} + \ \ldots \ + \frac{2}{n(n+1)} = 2 - \frac{2}{n+1}, \text{ para } \ n \in \mathbb{Z}^+$$

Para el desarrollo de la demostración considerar que se tiene la proposición

$$p(n) = \sum_{i=1}^{n} \frac{2}{i(i+1)} = \frac{2}{1(2)} + \frac{2}{2(3)} + \frac{2}{3(4)} + \ldots + \frac{2}{n(n+1)} = 2 - \frac{2}{n+1}$$

la proposición $p(n)$ tomará el valor verdadero (V_o) o falso (F_o) dependiendo de si se cumple o no la igualdad $\sum_{i=1}^{n} \frac{2}{i(i+1)} = 2 - \frac{2}{n+1}$. Ahora se consideran los tres pasos de la técnica por inducción matemática:

Paso base n = 1:

$$p(1) = \underbrace{\sum_{i=1}^{1} \frac{2}{i(i+1)} = \frac{2}{1(2)} = 1}_{\textit{resultado a partir de la sumatoria de términos}} \qquad = \underbrace{2 - \frac{2}{1+1} = 2 - \frac{2}{2} = 2 - 1 = 1}_{\textit{resultado a partir de la fórmula}}$$

como se obtiene el mismo resultado en la sumatoria de términos y en la fórmula que es la solución de la sumatoria entonces la proposición $p(1)$ es verdadera y la demostración continua en el paso inductivo.

Paso inductivo n = k:

$p(k) = \sum_{i=1}^{k} \frac{2}{i(i+1)} = \frac{2}{1(2)} + \frac{2}{2(3)} + \frac{2}{3(4)} + \ldots + \frac{2}{k(k+1)} = 2 - \frac{2}{k+1}$, se asume que la proposición $p(k)$ es verdadera, esto quiere decir, que se supone que se cumple la siguiente igualdad $\frac{2}{1(2)} + \frac{2}{2(3)} + \frac{2}{3(4)} + \ldots + \frac{2}{k(k+1)} = 2 - \frac{2}{k+1}$.

Paso post-inductivo n = k + 1:

$$p(k+1) = \sum_{i=1}^{k+1} \frac{2}{i(i+1)} = \underbrace{\frac{2}{1(2)} + \ldots + \frac{2}{k(k+1)}}_{\substack{\textit{Se reemplaza por su equivalente} \\ \textit{en el paso inductivo}}} + \frac{2}{(k+1)(k+2)} = 2 - \frac{2}{k+1+1}$$

$$2 - \frac{2}{k+1} + \frac{2}{(k+1)(k+2)} = 2 - \frac{2}{k+2}$$

$$2 - \frac{2}{k+1}\left(1 - \frac{1}{k+2}\right) = 2 - \frac{2}{k+2}$$

$$2 - \frac{2}{k+1}\left(\frac{k+2-1}{k+2}\right) = 2 - \frac{2}{k+2}$$

$$2 - \frac{2}{k+1}\left(\frac{k+1}{k+2}\right) = 2 - \frac{2}{k+2}$$

$$2 - \frac{2}{k+2} = 2 - \frac{2}{k+2}$$

Se cumple la igualdad, por lo tanto la proposición $p(k+1)$ es verdadera, como se cumplen los tres pasos de técnica de demostración por inducción matemática entonces queda demostrada la validez de la solución de la sumatoria originalmente planteada.

Ejemplo 19:

Demostrar por la técnica de inducción matemática que $7^n - 2^n$ es múltiplo de 5, para $n \in \mathbb{N}$.

Para el desarrollo de la demostración considerar que se tiene la proposición $p(n) = 7^n - 2^n = 5 \cdot p$, para $p \in \mathbb{N}$. La proposición $p(n)$ tomará el valor verdadero (V_o) o falso (F_o) dependiendo de si se cumple o no que $7^n - 2^n$ es múltiplo de 5. Ahora se consideran los tres pasos de la técnica por inducción matemática:

Paso base n = 0:

$p(0) = 7^0 - 2^0 = 1 - 1 = 0 = 5(0)$

la proposición $p(0)$ es verdadera porque al evaluar $7^0 - 2^0$ se obtiene como resultado el número 0 el cual es múltiplo de 5.

Paso inductivo n = k:

$p(k) = 7^k - 2^k = 5 \cdot m$, para $m \in \mathbb{Z}^+$. Se asume que la proposición $p(k)$ es verdadera, esto quiere decir, que $7^k - 2^k$ da como resultado un número entero múltiplo de 5.

Paso post-inductivo n = k + 1:

$$p(k+1) = 7^{k+1} - 2^{k+1} = 5 \cdot r$$

$$7 \cdot 7^k - 2 \cdot 2^k = 5 \cdot r$$

$$(5+2) \cdot 7^k - 2 \cdot 2^k = 5 \cdot r$$

$$5 \cdot 7^k + 2 \cdot 7^k - 2 \cdot 2^k = 5 \cdot r$$

$$5 \cdot 7^k + 2 \cdot \underbrace{(7^k - 2^k)}_{\substack{\textit{Se reemplaza por} \\ \textit{su equivalente en} \\ \textit{el paso inductivo}}} = 5 \cdot r$$

$$5 \cdot 7^k + 2 \cdot (5m) = 5 \cdot r$$

$$5 \cdot (7^k + 2m) = 5 \cdot r$$

$$5 \cdot r = 5 \cdot r, \text{ donde } r = 7^k + 2m$$

Se cumple la igualdad, por lo tanto la proposición $p(k+1)$ es verdadera, como se cumplen los tres pasos de la técnica de demostración por inducción matemática entonces queda demostrada la validez de que cuando se evalúa la expresión $7^n - 2^n$ para $n \in \mathbb{N}$ se obtiene como resultado un número natural que es múltiplo de 5.

Ejemplo 20:

Demostrar utilizando la técnica de inducción matemática que:

$$\binom{n}{0} + \binom{n}{1} + \binom{n}{2} + \cdots + \binom{n}{n-1} + \binom{n}{n} = 2^n, \quad \text{donde} \quad n \in \mathbb{N}$$

Esta demostración es importante hacerla porque será utilizada en el Capítulo de Conjuntos, cuando se trabaje la cardinalidad del conjunto potencia de un conjunto A.

Para la demostración primero se debe recordar el Triángulo de Pascal, el cual es:

$$\begin{array}{ccccccccccccc}
 & & & & & & 1 & & & & & & \\
 & & & & & 1 & & 1 & & & & & \\
 & & & & 1 & & 2 & & 1 & & & & \\
 & & & 1 & & 3 & & 3 & & 1 & & & \\
 & & 1 & & 4 & & 6 & & 4 & & 1 & & \\
 & 1 & & 5 & & 10 & & 10 & & 5 & & 1 & \\
1 & & 6 & & 15 & & 20 & & 15 & & 6 & & 1 \\
\vdots & & & & & & \vdots & & & & & & \vdots
\end{array}$$

En el Triángulo de Pascal se evidencian las siguientes reglas de generación:

- Únicamente el número uno está en la cúspide y en los lados del triángulo.
- Los números internos del triángulo se obtienen al sumar los dos números más cercanos a este en el nivel inmediatamente superior.

El Triángulo de Pascal también se puede generar utilizando el combinatorio de la siguiente forma:

$$\begin{array}{ccccccccccccc}
 & & & & & & \binom{0}{0} & & & & & & \\
 & & & & & \binom{1}{0} & & \binom{1}{1} & & & & & \\
 & & & & \binom{2}{0} & & \binom{2}{1} & & \binom{2}{2} & & & & \\
 & & & \binom{3}{0} & & \binom{3}{1} & & \binom{3}{2} & & \binom{3}{3} & & & \\
 & & \binom{4}{0} & & \binom{4}{1} & & \binom{4}{2} & & \binom{4}{3} & & \binom{4}{4} & & \\
 & \binom{5}{0} & & \binom{5}{1} & & \binom{5}{2} & & \binom{5}{3} & & \binom{5}{4} & & \binom{5}{5} & \\
\binom{6}{0} & & \binom{6}{1} & & \binom{6}{2} & & \binom{6}{3} & & \binom{6}{4} & & \binom{6}{5} & & \binom{6}{6} \\
\vdots & & & & & & \vdots & & & & & & \vdots
\end{array}$$

Al "cruzar" las dos formas de generar el Triángulo de Pascal se obtiene la siguiente definición recursiva que sirve para calcular n combinado r, donde $n,\ r \in \mathbb{N}$:

$$\binom{n}{r} = \begin{cases} 1 & si \quad r = 0 \\ 1 & si \quad n = r \\ \binom{n-1}{r-1} + \binom{n-1}{r} & si \quad n > r \geq 1 \end{cases}$$

Para el desarrollo de la demostración considerar que se tiene la proposición

$$p(n) = \sum_{i=0}^{n} \binom{n}{i} = \binom{n}{0} + \binom{n}{1} + \binom{n}{2} + \cdots + \binom{n}{n-1} + \binom{n}{n} = 2^n, \text{ para } \ n \in \mathbb{N}$$

la proposición $p(n)$ tomará el valor verdadero (V_o) o falso (F_o) dependiendo de si se cumple o no la igualdad $\sum_{i=0}^{n} \binom{n}{i} = 2^n$. Ahora se consideran los tres pasos de la técnica por inducción matemática:

Paso base n = 0:

$$p(0) = \underbrace{\sum_{i=0}^{0} \binom{0}{i} = \binom{0}{0} = \frac{0!}{0! \cdot 0!} = \frac{1}{1 \cdot 1} = 1}_{\textit{resultado a partir de la sumatoria de términos}} = \underbrace{2^0 = 1}_{\textit{resultado a partir de la fórmula}}$$

como se obtiene el mismo resultado en la sumatoria de términos y en la fórmula que es la solución de la sumatoria entonces la proposición $p(0)$ es verdadera y la demostración continua en el paso inductivo.

Paso inductivo n = k:

$$p(k) = \sum_{i=0}^{k} \binom{k}{i} = \binom{k}{0} + \binom{k}{1} + \binom{k}{2} + \cdots + \binom{k}{k-1} + \binom{k}{k} = 2^k,$$

se asume que la proposición $p(k)$ es verdadera, esto quiere decir, que se supone que se cumple la siguiente igualdad:

$$\binom{k}{0} + \binom{k}{1} + \binom{k}{2} + \cdots + \binom{k}{k-1} + \binom{k}{k} = 2^k.$$

Paso post-inductivo n = k + 1:

$$p(k+1) = \sum_{i=0}^{k+1} \binom{k+1}{i} = \binom{k+1}{0} + \binom{k+1}{1} + \cdots + \binom{k+1}{k} + \binom{k+1}{k+1} = 2^{k+1}$$

Apoyados en la definición recursiva se tiene que:

$$\binom{k+1}{0} = \binom{k}{0} = 1$$
$$\binom{k+1}{1} = \binom{k}{0} + \binom{k}{1}$$
$$\binom{k+1}{2} = \binom{k}{1} + \binom{k}{2}$$
$$\binom{k+1}{3} = \binom{k}{2} + \binom{k}{3}$$
$$\vdots$$
$$\binom{k+1}{k} = \binom{k}{k-1} + \binom{k}{k}$$
$$\binom{k+1}{k+1} = \binom{k}{k} = 1$$

de esta forma se tiene que:

$$\underbrace{\binom{k}{0}}_{\binom{k+1}{0}} + \Big[\underbrace{\binom{k}{0} + \binom{k}{1}}_{\binom{k+1}{1}}\Big] + \Big[\underbrace{\binom{k}{1} + \binom{k}{2}}_{\binom{k+1}{2}}\Big] + \cdots + \Big[\underbrace{\binom{k}{k-1} + \binom{k}{k}}_{\binom{k+1}{k}}\Big] + \underbrace{\binom{k}{k}}_{\binom{k+1}{k+1}} = 2^{k+1}$$

$$\Big[\binom{k}{0} + \binom{k}{0}\Big] + \Big[\binom{k}{1} + \binom{k}{1}\Big] + \Big[\binom{k}{2} + \binom{k}{2}\Big] + \cdots + \Big[\binom{k}{k} + \binom{k}{k}\Big] = 2^{k+1}$$

$$2\binom{k}{0} + 2\binom{k}{1} + 2\binom{k}{2} + \cdots + 2\binom{k}{k} = 2^{k+1}$$

$$2\Big[\underbrace{\binom{k}{0} + \binom{k}{1} + \binom{k}{2} + \cdots + \binom{k}{k}}\Big] = 2^{k+1}$$

Se reemplaza por su equivalente en el paso inductivo

$$2\big[2^k\big] = 2^{k+1}$$

$$2^{k+1} = 2^{k+1}$$

Se cumple la igualdad, por lo tanto la proposición $p(k+1)$ es verdadera, como se cumplen los tres pasos de técnica de demostración por inducción matemática entonces queda demostrada la validez de la solución de la sumatoria originalmente planteada.

3.6. Ejercicios

1. Probar o refutar cada uno de los siguientes ítems utilizando alguno de los métodos de demostración:

   a) La suma de dos números enteros pares es un entero par.

   b) La suma de dos números enteros impares es un entero par.

   c) La suma de un número entero impar con un número entero par es un número entero impar.

   d) Si el producto de dos números enteros es par, entonces alguno de los dos números que se esta multiplicando es par.

   e) Si el producto de dos números enteros es impar, entonces los dos números que se esta multiplicando son impares.

   f) El cuadrado de todo número entero es un número entero no negativo.

   g) Si el cuadrado de n no es divisible por 2 entonces n no es divisible por 2.

   h) Si un número entero es divisible por 4 entonces es divisible por 2.

   i) Si n es un entero positivo, entonces n es par si y únicamente si $7n+4$ es par.

   j) La suma de cualquier número entero n con n^2 es par.

   k) Si n es un número entero y n^3+1 es impar, entonces n es par.

   l) Si n es un número entero y n^3+5 es par, entonces n es impar.

   m) Si n es un número entero y $3n+2$ es par, entonces n es par.

   n) $\binom{n}{r} + 2\binom{n}{r-1} + \binom{n}{r-2} = \binom{n+2}{r}$, para $n \geq r \geq 2$

   ñ) $\binom{n}{0} + \binom{n+1}{1} + \binom{n+2}{2} + \cdots + \binom{n+r-1}{r-1} + \binom{n+r}{r} = \binom{n+r+1}{r}$

   donde n, r son números enteros positivos.

   o) p
   $p \vee q$
   $\underline{q \to (r \to s)\ t \to r}$
   $\therefore \neg s \to \neg t$

   p) $p \to q$
   $q \to s$
   $r \to \neg s$
   $\underline{\neg p \otimes r}$
   $\therefore \neg p$

   q) La suma de 4 enteros positivos consecutivos cualquiera es divisible por 4.

   r) La suma de 5 enteros positivos consecutivos cualquiera es divisible por 9.

2. Probar o refutar cada uno de los siguientes ítems utilizando el método de demostración por casos:

   a) El producto de cualesquiera 3 enteros positivos consecutivos es divisible por 6.

   b) El producto de cualesquiera 4 enteros positivos consecutivos es divisible por 12.

   c) La diferencia entre los cuadrados de dos números enteros impares es divisible por 8. La demostración se tiene que cumplir para cualquier pareja de números enteros impares.

   d) $n(n^2+5)$ es divisible por 3, para $n \in \mathbb{Z}^+$, $n \geq 1$

   e) El cuadrado de cualquier número entero positivo finaliza con un 0, 1, 4, 5, 6 o 9. (Ayuda: Sea $n = 10k + j$ donde $j = 0,\ 1,\ ...,\ 9$). Probar si es necesario cada uno de los diez casos y concluir.

   f) El cubo de cualquier número entero positivo finaliza con un 0, 1, 2, 4, 5, 6, 7 u 8. (Ayuda: Sea $n = 10k + j$ donde $j = 0,\ 1,\ ...,\ 9$). Probar si es necesario cada uno de los diez casos y concluir.

   g) El cuadrado de todo número entero, es un múltiplo de 3, ó difiere de un múltiplo de 3 en 1.

   h) El cuadrado de todo número entero, es un múltiplo de 4, ó difiere de un múltiplo de 4 en 1.

3. Probar o refutar cada uno de los siguientes ítems utilizando el método de demostración por Inducción Matemática:

   a) $1(2) + 2(3) + 3(4) + 4(5) + \ldots + n(n+1) = \frac{n(n+1)(n+2)}{3}$, para $n \in \mathbb{Z}^+$, $n \geq 1$.

   b) $0 + 3 + 8 + \ldots + (n^2 - 1) = \frac{n(2n+5)(n-1)}{6}$, para $n \in \mathbb{Z}^+$, $n \geq 1$.

   c) $0 + 7 + 26 + \ldots + (n^3 - 1) = \frac{n(n(n+1)^2 - 4)}{4}$, para $n \in \mathbb{Z}^+$, $n \geq 1$.

   d) $1 \cdot \frac{2}{3} + 2 \cdot \frac{5}{3} + \ldots + n \cdot (n - \frac{1}{3}) = \frac{n^2(n+1)}{3}$, para $n \in \mathbb{Z}^+$, $n \geq 1$.

   e) $3 + 6 + 20 + \ldots + (n(n!) + 2) = (n+1)! + 2n - 1$, para $n \in \mathbb{Z}^+$, $n \geq 1$.

   f) $1^2 + 3^2 + 5^2 + \ldots + (2n-1)^2 = \frac{n(2n-1)(2n+1)}{3}$, para $n \in \mathbb{Z}^+$, $n \geq 1$.

   g) $1 \cdot 2^1 + 2 \cdot 2^2 + 3 \cdot 2^3 + 4 \cdot 2^4 + \ldots + n \cdot 2^n = 2^{n+1}(n-1) + 2$, para $n \in \mathbb{Z}^+$, $n \geq 1$.

   h) $\frac{3}{1(3)} + \frac{3}{3(5)} + \frac{3}{5(7)} + \frac{3}{7(9)} + \ldots + \frac{3}{(2n-1)(2n+1)} = \frac{3n}{2n+1}$, para $n \in \mathbb{Z}^+$, $n \geq 1$.

   i) $\frac{1}{1(2)} + \frac{1}{2(3)} + \frac{1}{3(4)} + \frac{1}{4(5)} + \ldots + \frac{1}{n(n+1)} = \frac{n}{n+1}$, para $n \in \mathbb{Z}^+$, $n \geq 1$.

   j) $1^4 + 2^4 + 3^4 + 4^4 + \ldots + n^4 = \frac{n(n+1)(2n+1)(3n^2+3n-1)}{30}$, para $n \in \mathbb{Z}^+$, $n \geq 1$.

k) $1 + \frac{1}{2} + \frac{1}{4} + \ldots + \frac{1}{2^n} < 2,$ para $n \geq 0$.

Ayuda:

Probar que $1 + \frac{1}{2} + \frac{1}{4} + \ldots + \frac{1}{2^n} = 2 - \frac{1}{2^n}$, para $n \geq 0$, con lo cual se sigue que: $1 + \frac{1}{2} + \frac{1}{4} + \ldots + \frac{1}{2^n} < 2$, para $n \geq 0$.

l) $11^n - 6$ es divisible por 5, para $n \in \mathbb{Z}^+$, $n \geq 1$.

m) $3^{2n} + 7$ es divisible por 8, para $n \in \mathbb{Z}^+$, $n \geq 1$.

n) $n^3 - n$ es divisible por 3, para $n \in \mathbb{Z}^+$, $n \geq 1$.

Capítulo 4

Relaciones de recurrencia

A menudo es posible encontrar relaciones entre los elementos de una sucesión. Estas relaciones se llaman relaciones de recurrencia.

Una relación de recurrencia para una sucesión a_o, a_1, a_2, ..., a_n es una ecuación que relaciona a_n con alguno (o algunos) de sus antecesores a_o, a_1, a_2, ..., a_{n-1} y la suma o multiplicación de alguna cantidad.

Ejemplo 1:

En el ejemplo 9 del Capítulo 2 de Sucesiones y Sumatorias se pide que se genere una fórmula para calcular el n-ésimo término de la sucesión que tiene los primeros 10 términos siguientes: 3, 9, 15, 21, 27, 33, 39, 45, 51 y 57. La fórmula que se obtuvo en este ejemplo es:

$S_1 = 3$
$S_n = S_{n-1} + 6$, para $n \geq 2$, $n \in \mathbb{Z}^+$

esta fórmula es una relación de recurrencia, con la cual se indica que el término ubicado en la posición n de la sucesión se obtiene al relacionar el término que se encuentra en la sucesión en la posición $n - 1$ con la suma del número 6.

¿Cuántos llamados recursivos son necesarios en la fórmula anterior para calcular el elemento que se encuentra en la posición un millón de la sucesión?

Son necesarios un millón de llamados recursivos, y en cada llamado recursivo a excepción del caso base, es realizada una suma. La fórmula recursiva o relación de recurrencia anterior, es correcta para calcular el n-ésimo término de la sucesión, pero, tiene un costo computacional muy alto; por este motivo es fundamental determinar fórmulas sin recursividad para generar el n-ésimo término de la sucesión. La solución de relaciones de recurrencia permite generar a partir de la relación de recurrencia una fórmula sin recursividad, que permite generar el mismo valor n-ésimo de la sucesión.

La fórmula $S_n = 3 + 6 * (n - 1)$, para $n \in \mathbb{Z}^+$, es la solución de la relación de recurrencia, y para calcular el elemento ubicado en la posición n de la sucesión, sólo necesita realizar tres operaciones (una resta, una multiplicación y una suma) independientemente del valor de n.

En los ejercicios de la siguiente sección se presentan las relaciones de recurrencia que permiten generar de forma recursiva el n-ésimo término de una sucesión y se pide que utilizando el método de iteración se obtenga una fórmula que permita generar el mismo n-ésimo término de la sucesión sin necesidad de consultar términos previos en la sucesión, para de ésta forma evitar el costo computacional de la recursividad.

4.1. Método de Iteración

En la serie de ejercicios de esta sección se utilizará el Método de Iteración para resolver las relaciones de recurrencia de primer orden no homogéneas, el método consiste en comenzar en el caso base de la relación de recurrencia y utilizarlo para definir sin recursividad el caso que sigue después del caso base, y así sucesivamente se itera tantas veces como sea necesario, hasta lograr determinar cuál es la sumatoria o sumatorias "ocultas" que sirven para solucionar la relación de recurrencia sin utilizar recursividad.

Después de tener la sumatoria o sumatorias para la relación de recurrencia evaluada en un valor n, estas (o esta) son resueltas y de esta forma se obtiene la solución de la relación de recurrencia.

Por último el método de demostración por inducción matemática puede ser utilizado para ratificar o refutar que la solución de la relación de recurrencia es correcta.

Ejemplo 2:

Resolver la siguiente relación de recurrencia:

$P(1) = 1$

$P(n) = P(n-1) \ + \ n$, para $\ n > 1$

Utilizando el método de iteración se tiene:

$P(1) = 1$

$P(2) = P(1) \ + \ 2 = 1 \ + \ 2$
no dar el resultado de $1 \ + \ 2$ sino dejar indicada la suma de términos para no desaparecer la sumatoria.

$P(3) = P(2) + 3 = 1 + 2 + 3$

$P(4) = P(3) + 4 = 1 + 2 + 3 + 4$

$P(5) = P(4) + 5 = 1 + 2 + 3 + 4 + 5$

Se itera tantas como se considere necesario hasta que se identifique cual es la sumatoria oculta. En estos momentos debe ser evidente que:

$P(n) = 1 + 2 + 3 + 4 + \ldots + n$

de esta forma se detecta que la sumatoria oculta que resuelve la relación de recurrencia sin recursividad es $\sum_{i=1}^{n} i = 1 + 2 + \ldots + n$

la cual tiene solución $\frac{n(n+1)}{2}$. Por lo tanto $P(n) = \sum_{i=1}^{n} i = \frac{n(n+1)}{2}$. De esta forma la solución de la relación de recurrencia es $P(n) = \frac{n(n+1)}{2}$ para $n \geq 1$

Ahora se va a utilizar el método de demostración por inducción matemática para ratificar que la solución obtenida de la relación de recurrencia es correcta.

Caso base $n = 1$

n toma el valor de 1 porque este es el valor con el cuál termina la recursividad en la relación de recurrencia, o dicho en otras palabras, para n=1, esta definido el caso base de la relación de recurrencia.

$$\underbrace{P(1) = 1}_{\textit{Caso base de la R.R.}} = \underbrace{\frac{1(2)}{2} = 1}_{\textit{Solución de la relación de recurrencia evaluada en } 1}$$

Como se cumple la igualdad entre el caso base de la relación de recurrencia y la solución de la relación de recurrencia evaluada en $n = 1$, entonces la demostración continua en el caso inductivo.

Caso inductivo n=k:

Se asume como cierta la solución de la relación de recurrencia evaluada en k, donde $k \in \mathbb{Z}^+$ para $k > 1$

$$P(k) = \frac{k(k+1)}{2}$$

Caso post-inductivo $n = k + 1$:

en este caso se recuerda el paso recursivo de la relación de recurrencia donde

$P(n) = P(n-1) \ + \ n$, reemplazando n por $k+1$ se tiene:

$P(k+1) = P(k+1-1) \ + \ k+1$

$P(k+1) = P(k) \ + \ (k \ + \ 1)$

donde $P(k+1)$ y $P(k)$ se reemplazan por su equivalente en el caso inductivo evaluado en $k+1$ y k respectivamente

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

$$\begin{aligned}\frac{(k+1)(k+2)}{2} &= (k+1)\left[\frac{k}{2} \ + \ 1\right] \\ &= (k+1)\left[\frac{k}{2} \ + \ \frac{2}{2}\right] \\ &= (k+1)\left[\frac{k+2}{2}\right] \\ &= \frac{(k+1)(k+2)}{2}\end{aligned}$$

Como efectivamente se llegó a la igualdad, entonces, se ratifica que la solución de la relación de recurrencia obtenida por el método de iteración es correcta.

Ejemplo 3:

Resolver la siguiente relación de recurrencia:

$P(1) = 2$

$P(n) = P(n-1) \ + \ n \cdot 2^n$, para $n > 1$

Utilizando el método de iteración se tiene:

$P(1) = 2$

$P(2) = P(1) \ + \ 2 \cdot 2^2 = 2 \ + \ 2 \cdot 2^2 = 1 \cdot 2^1 \ + \ 2 \cdot 2^2$

recordar que no se calculan las potencias ni se hacen las multiplicaciones, ni se hacen las sumas porque se desaparecería la sumatoria "oculta" que está debajo de la relación de recurrencia. Retomando el método iterativo se tiene:

$P(3) = P(2) \ + \ 3 \cdot 2^3 = 1 \cdot 2^1 \ + \ 2 \cdot 2^2 \ + \ 3 \cdot 2^3$

$P(4) = P(3) \ + \ 4 \cdot 2^4 = 1 \cdot 2^1 \ + \ 2 \cdot 2^2 \ + \ 3 \cdot 2^3 \ + \ 4 \cdot 2^4$

$\vdots$

$P(n) = 1 \cdot 2^1 \ + \ 2 \cdot 2^2 \ + \ 3 \cdot 2^3 \ + \ldots + \ n \cdot 2^n$

lo que se hizo en el paso anterior fue dejar de iterar porque ya se identificó la sumatoria y generalizar esta cuando la relación de recurrencia P es evaluada en "n".

Como $P(n) = \sum_{i=1}^{n} i \cdot 2^i$ entonces la solución de la relación de recurrencia es la solución de la sumatoria. Tomando la solución de dicha sumatoria de la sección de "Sumatorias Especiales" se tiene que $P(n) = \sum_{i=1}^{n} i \cdot 2^i = (n-1) \cdot 2^{n+1} + 2$, por lo tanto la solución de la relación de recurrencia es $P(n) = (n-1) \cdot 2^{n+1} + 2$, para $n \geq 1$.

Ahora se utilizará el método de demostración por inducción matemática para ratificar la validez de la solución de la relación de recurrencia, por lo tanto se tiene:

Caso base $n = 1$:

$$\underbrace{P(1) = 2}_{\textit{caso base de la R.R.}} = \underbrace{(1-1) \cdot 2^{1+1} + 2 = 0 \cdot 2^2 + 2 = 0 + 2 = 2}_{\textit{Solución de la relación de recurrencia evaluada en 1}}$$

Como se cumple la igualdad, entonces sigue la demostración con el caso inductivo.

Caso inductivo n=k:

Se asume como cierta la solución de la relación de recurrencia evaluada en k, donde $k \in \mathbb{Z}^+$ para $k > 1$

$P(k) = (k-1) \cdot 2^{k+1} + 2$

Caso post-inductivo $n = k + 1$:

Recordar el paso recursivo de la relación de recurrencia:

$P(n) = P(n-1) + n \cdot 2^n$, reemplazando n por $k+1$ se tiene:

$P(k+1) = P(k+1-1) + (k+1) \cdot 2^{k+1}$

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

donde $P(k+1)$ y $P(k)$ se reemplazan por su equivalente en el caso inductivo evaluado en $k+1$ y k respectivamente.

$$\underbrace{(k+1-1) \cdot 2^{k+1+1} + 2}_{P(k+1)} = \underbrace{(k-1) \cdot 2^{k+1} + 2}_{P(k)} + (k+1) \cdot 2^{k+1}$$

$$\begin{aligned} k \cdot 2^{k+2} + 2 &= (k-1+k+1) \cdot 2^{k+1} + 2 \\ &= (2k) \cdot 2^{k+1} + 2 \\ &= k \cdot 2^{k+2} + 2 \end{aligned}$$

Como se llegó a una igualdad, entonces, se ratifica que la solución de la relación de recurrencia obtenida por el método de iteración es correcta.

Ejemplo 4:

Resolver la siguiente relación de recurrencia:

$P(1) = 1$

$P(n) = 2P(n-1) \ + \ 1$, para $n > 1$

Por el método de iteración se tiene:

$P(1) = 1$

$P(2) = 2P(1) \ + \ 1 = 2(1) \ + \ 1 = 2^1 \ + \ 2^0$

$P(3) = 2P(2) \ + \ 1 = 2(2^1 \ + \ 2^0) \ + \ 1 = 2^2 \ + \ 2^1 \ + \ 2^0$

$P(4) = 2P(3) \ + \ 1 = 2(2^2 \ + \ 2^1 \ + \ 2^0) \ + \ 1 = 2^3 \ + \ 2^2 \ + \ 2^1 \ + \ 2^0$

$\vdots$

$P(n) = 2^{n-1} \ + \ 2^{n-2} \ + \ldots + \ 2^1 + \ 2^0$

$P(n) = 2^0 \ + \ 2^1 \ + \ldots + \ 2^{n-1}$

Como $P(n) = \sum_{i=0}^{n-1} 2^i$ entonces la solución de la relación de recurrencia es la solución de la suma de términos de la serie geométrica con primer término $a = 2^0 = 1$, razón constante $r = 2$ y potencia más grande igual a $n-1$ tomando la solución de dicha sumatoria de la sección de "Sumatorias Especiales" se tiene que

$$P(n) = \sum_{i=0}^{n-1} 2^i = \frac{a \ \cdot \ r^{(potencia \ más \ grande)+1} \ - \ a}{r \ - \ 1} = \frac{1 \ \cdot \ 2^{(n-1)+1} \ - \ 1}{2 \ - \ 1} = 2^n - 1$$

por lo tanto la solución de la relación de recurrencia es $P(n) = 2^n - 1$, para $n \geq 1$.

Si se quiere ratificar o refutar la solución obtenida para la relación de recurrencia, entonces se puede utilizar el método de demostración por inducción matemática.

Ejemplo 5:

Resolver la siguiente relación de recurrencia:

$P(1) = 2$

$P(n) = 2P(n-1) \ + \ 3^n \ - \ 1$, para $n \geq 2$

La diferencia de este ejemplo con los anteriores, radica en la cantidad de términos independientes que se encuentran en el caso recursivo, donde se tiene que al llamado

recursivo se le suma $3^n - 1$. Cada uno de los términos independientes genera su propia suma de términos.

Utilizando el método de iteración se tiene:

$$P(1) = 2$$

$$P(2) = 2P(1) + 3^2 - 1 = 2(2) + 3^2 - 1 = 2^2 + 3^2 - 1$$

$$\begin{aligned} P(3) &= 2P(2) + 3^3 - 1 = 2\big(2^2 + 3^2 - 1\big) + 3^3 - 1 \\ &= \big(2^3 + 2 \cdot 3^2 - 2\big) + 3^3 - 1 \\ &= \big(2^3 + 2^1 \cdot 3^2 - 2^1\big) + 2^0 \cdot 3^3 - 2^0 \\ &= \big(2^3\big) + \big(2^1 \cdot 3^2 + 2^0 \cdot 3^3\big) - \big(2^1 + 2^0\big) \end{aligned}$$

$$\begin{aligned} P(4) &= 2P(3) + 3^4 - 1 = 2\Big(\big(2^3\big) + \big(2^1 \cdot 3^2 + 2^0 \cdot 3^3\big) - \big(2^1 + 2^0\big)\Big) + 3^4 - 1 \\ &= \Big(\big(2^4\big) + \big(2^2 \cdot 3^2 + 2^1 \cdot 3^3\big) - \big(2^2 + 2^1\big)\Big) + 2^0 \cdot 3^4 - 2^0 \\ &= \big(2^4\big) + \big(2^2 \cdot 3^2 + 2^1 \cdot 3^3 + 2^0 \cdot 3^4\big) - \big(2^2 + 2^1 + 2^0\big) \end{aligned}$$

$$\vdots$$

$$\begin{aligned} P(n) &= \big(2^n\big) + \big(2^{n-2} \cdot 3^2 + 2^{n-3} \cdot 3^3 + \ldots + 2^0 \cdot 3^n\big) - \big(2^{n-2} + 2^{n-3} + \ldots + 2^0\big) \\ &= \big(2^n\big) + 3^2\big(2^{n-2} \cdot 3^0 + 2^{n-3} \cdot 3^1 + \ldots + 2^0 \cdot 3^{n-2}\big) - \big(2^0 + 2^1 + \ldots + 2^{n-2}\big) \end{aligned}$$

$$\begin{aligned} P(n) = {} & \underbrace{\big(2^n\big)}_{\substack{\textit{término generado por el caso base de la relación de recurrencia}}} \\ & + 3^2\big(\underbrace{2^{n-2} \cdot 3^0 + 2^{n-3} \cdot 3^1 + \ldots + 2^0 \cdot 3^{n-2}}_{\textit{Sumatoria A}}\big) \\ & - \big(\underbrace{2^0 + 2^1 + \ldots + 2^{n-2}}_{\textit{Sumatoria B}}\big) \end{aligned}$$

Sumatoria A:

La sumatoria A es una serie geométrica con primer término $a = 2^{n-2}$, razón constante $r = \frac{3}{2}$ y potencia más grande igual a $n-2$, reemplazando en la formula se tiene:

$$\frac{a \cdot r^{(\textit{potencia más grande})+1} - a}{r - 1} = \frac{2^{n-2} \cdot \left(\frac{3}{2}\right)^{(n-2)+1} - 2^{n-2}}{\frac{3}{2} - 1}$$

$$
\begin{aligned}
&= \frac{2^{n-2} \cdot \left(\frac{3}{2}\right)^{n-1} - 2^{n-2}}{\frac{3}{2} - \frac{2}{2}} \\
&= \frac{2^{n-2} \cdot \frac{3^{n-1}}{2^{n-1}} - 2^{n-2}}{\frac{3-2}{2}} \\
&= \frac{2^{n-2} \cdot \frac{3^{n-1}}{2 \cdot 2^{n-2}} - 2^{n-2}}{\frac{1}{2}} \\
&= \frac{\frac{3^{n-1}}{2} - \frac{2}{2} \cdot 2^{n-2}}{\frac{1}{2}} \\
&= \frac{\frac{3^{n-1} - 2^{n-1}}{2}}{\frac{1}{2}} \\
&= 3^{n-1} - 2^{n-1}
\end{aligned}
$$

Sumatoria B:

La sumatoria B es una serie geométrica con primer término $a = 2^0 = 1$, razón constante $r = 2$ y potencia más grande igual a $n - 2$, reemplazando en la formula se tiene:

$$
\begin{aligned}
\frac{a \cdot r^{(\textit{potencia más grande})+1} - a}{r - 1} &= \frac{1 \cdot 2^{(n-2)+1} - 1}{2 - 1} \\
&= \frac{1 \cdot 2^{n-1} - 1}{1} \\
&= 2^{n-1} - 1
\end{aligned}
$$

Solución Relación de recurrencia:

$$
\begin{aligned}
P(n) = &\ (\textit{término generado por el caso base de la relación de recurrencia}) \\
&+ 3^2 \cdot (\textit{Solución Sumatoria A}) - (\textit{Solución Sumatoria B}) \\
P(n) &= \left(2^n\right) + 3^2\left(3^{n-1} - 2^{n-1}\right) - \left(2^{n-1} - 1\right) \\
&= 2 \cdot 2^{n-1} + 3^2 \cdot 3^{n-1} - 3^2 \cdot 2^{n-1} - 2^{n-1} + 1 \\
&= 3^{n-1+2} + 2 \cdot 2^{n-1} - 9 \cdot 2^{n-1} - 2^{n-1} + 1
\end{aligned}
$$

$$= 3^{n+1} + \big(2 - 9 - 1\big) \cdot 2^{n-1} + 1$$
$$= 3^{n+1} - 8 \cdot 2^{n-1} + 1$$
$$= 3^{n+1} - 2^3 \cdot 2^{n-1} + 1$$
$$= 3^{n+1} - 2^{n-1+3} + 1$$
$$= 3^{n+1} - 2^{n+2} + 1$$

Ejemplo 6:

Resolver la siguiente relación de recurrencia:

$P(1) = 1$
$P(n) = 2P(\frac{n}{2}) + n$, para $n = 2^m$, $m \in \mathbb{Z}^+$.

El objetivo principal de este ejemplo es poner en evidencia que el llamado recursivo de la relación de recurrencia no siempre tiene que ser en términos de $n - 1$. Perfectamente el valor de n puede decrecer al dividir éste de forma constante por un mismo valor, en este ejemplo dicho valor es 2.

Para poder utilizar el método de iteración sobre esta relación de recurrencia es necesario primero hacer un cambio de variables.

Cambio de variables:

Como $n = 2^m$, entonces la relación de recurrencia original puede ser reescrita como:

$P(2^0) = 2^0$
$P(2^m) = 2P(\frac{2^m}{2}) + 2^m$, $m \geq 1$
$P(2^m) = 2P(2^m \cdot 2^{-1}) + 2^m$, $m \geq 1$
$P(2^m) = 2P(2^{m-1}) + 2^m$, $m \geq 1$

Método iterativo

$P(2^0) = 2^0$
$P(2^1) = 2P(2^0) + 2^1 = 2^1 \cdot 2^0 + 2^1 = 2^1 + 2^1$
$P(2^2) = 2P(2^1) + 2^2 = 2[2^1 + 2^1] + 2^2 = 2^2 + 2^2 + 2^2$
$P(2^3) = 2P(2^2) + 2^3 = 2[2^2 + 2^2 + 2^2] + 2^3 = 2^3 + 2^3 + 2^3 + 2^3$
$\vdots$

$$P(2^m) = \underbrace{2^m \ + \ 2^m \ + \ 2^m \ + \ldots + \ 2^m}_{m+1 \ veces} = (m+1)2^m$$

De esta forma se halla la solución a la relación de recurrencia.

Ahora, después de obtener la solución de la relación de recurrencia es necesario utilizar algún mecanismo para ratificar o refutar la validez de la solución, por este motivo es normal que se utilice la técnica de demostración por inducción matemática para éste fin.

Prueba por inducción matemática:

Caso base $m = 0$:

$$\begin{aligned} P(2^0) &= 1 = (0+1)2^0 \\ &= (1)1 \\ &= 1 \end{aligned}$$

Como se cumple la igualdad entre el caso base de la relación de recurrencia y la solución de la relación de recurrencia evaluada en $m = 0$, entonces la demostración continua en el caso inductivo.

Caso inductivo $m = k$:

Se asume como cierto que: $P(2^k) = (k+1)2^k$

Caso post-inductivo $m = k + 1$:

Recordar el caso recursivo de la relación de recurrencia:

$P(2^m) = 2P(2^{m-1}) \ + \ 2^m$

Al reemplazar m por $k + 1$ se tiene:

$P(2^{k+1}) = 2P(2^k) \ + \ 2^{k+1}$

Se reemplaza a $P(2^{k+1})$ y $P(2^k)$ por su equivalente en el caso inductivo.

$$\underbrace{((k+1)+1)2^{k+1}}_{P(2^{k+1})} = 2\underbrace{\left[(k+1)2^k\right]}_{P(2^k)} \ + \ 2^{k+1}$$

$$\begin{aligned} (k+2)2^{k+1} &= (k+1)2^{k+1} \ + \ 2^{k+1} \\ &= ((k+1)+1)2^{k+1} \\ &= (k+2)2^{k+1} \end{aligned}$$

Se cumple la igualdad por lo tanto es correcta la solución de la relación de recurrencia.

Con respecto al cambio de variables se resolvió la relación de recurrencia y se demostró por inducción matemática que dicha solución es correcta, ahora lo que se va a hacer es presentar la solución de la relación de recurrencia con respecto a la variable original, para esto se debe recordar que $n = 2^m$, entonces $\lg_2 n = \lg_2 2^m$, $\lg_2 n = m$, $m = \lg_2 n$, reemplazando n y m en la solución de la relación de recurrencia $P(2^m) = (m+1)2^m$, se tiene $P(n) = ((\lg_2 n) + 1)n$, $P(n) = n(1 + \lg_2 n)$, $P(n) = n + n \lg_2 n$.

Ejemplo 7:

Resolver la siguiente relación de recurrencia:

$P(1) = 1$
$P(n) = 3P(\frac{n}{5}) + n$, para $n = 5^m$, $m \in \mathbb{Z}^+$.

En este ejemplo es necesario hacer primero el cambio de variables y reescribir la relación de recurrencia.

Cambio de variables:

Como $n = 5^m$, entonces la relación de recurrencia original puede ser reescrita de la siguiente forma:

$$P(5^0) = 5^0$$
$$P(5^m) = 3P(\tfrac{5^m}{5}) + 5^m,\ m \geq 1$$
$$P(5^m) = 3P(5^m \cdot 5^{-1}) \ + \ 5^m,\ m \geq 1$$
$$P(5^m) = 3P(5^{m-1}) \ + \ 5^m,\ m \geq 1$$

Método iterativo

$$P(5^0) = 5^0$$
$$P(5^1) = 3P(5^0) \ + \ 5^1 = 3^1 \cdot 5^0 \ + \ 3^0 \cdot 5^1$$
$$P(5^2) = 3P(5^1) \ + \ 5^2 = 3[3^1 \cdot 5^0 \ + \ 3^0 \cdot 5^1] \ + \ 5^2$$
$$= 3^2 \cdot 5^0 \ + \ 3^1 \cdot 5^1 \ + \ 3^0 \cdot 5^2$$
$$P(5^3) = 3P(5^2) \ + \ 5^3 = 3[3^2 \cdot 5^0 \ + \ 3^1 \cdot 5^1 \ + \ 3^0 \cdot 5^2] \ + \ 5^3$$
$$= 3^3 \cdot 5^0 \ + \ 3^2 \cdot 5^1 \ + \ 3^1 \cdot 5^2 \ + \ 3^0 \cdot 5^3$$
$$P(5^4) = 3P(5^3) \ + \ 5^4 = 3[3^3 \cdot 5^0 \ + \ 3^2 \cdot 5^1 \ + \ 3^1 \cdot 5^2 \ + \ 3^0 \cdot 5^3] \ + \ 5^4$$
$$= 3^4 \cdot 5^0 \ + \ 3^3 \cdot 5^1 \ + \ 3^2 \cdot 5^2 \ + \ 3^1 \cdot 5^3 \ + \ 3^0 \cdot 5^4$$

$$\vdots$$

$$P(5^m) = 3^m \cdot 5^0 \ + \ 3^{m-1} \cdot 5^1 \ + \ 3^{m-2} \cdot 5^2 \ + \ldots + \ 3^1 \cdot 5^{m-1} \ + \ 3^0 \cdot 5^m$$

$$= \sum_{i=0}^{m} 3^m \cdot \left(\tfrac{5}{3}\right)^i$$

La Sumatoria que describe a $P(5^m)$ es una serie geométrica con primer término $a = 3^m$, razón constante $r = \frac{5}{3}$ y potencia más grande igual a m, reemplazando en la fórmula de la serie geométrica se tiene:

$$P(5^m) = \left[\frac{3^m \cdot \left(\frac{5}{3}\right)^{m+1} \ - \ 3^m}{\frac{5}{3} \ - \ 1}\right]$$

$$= 3^m \cdot \left[\frac{\frac{5^{m+1}}{3^{m+1}} \ - \ 1}{\frac{2}{3}}\right] = 3^m \cdot \left[\frac{\frac{5^{m+1} \ - \ 3^{m+1}}{3^{m+1}}}{\frac{2}{3}}\right]$$

$$= 3^{m+1} \cdot \left[\frac{5^{m+1} \ - \ 3^{m+1}}{2 \cdot 3^{m+1}}\right]$$

$$= \frac{5^{m+1} \ - \ 3^{m+1}}{2}$$

De esta forma se halla la solución a la relación de recurrencia.

Para ratificar que es correcta la solución de la relación de recurrencia, entonces a continuación se utilizará la técnica de demostración por inducción matemática para éste fin.

Prueba por inducción matemática:

Caso base $m = 0$:

$$P(5^0) = 1 = \frac{5^{0+1} \ - \ 3^{0+1}}{2}$$

$$= \frac{5^1 \ - \ 3^1}{2}$$

$$= \frac{5 \ - \ 3}{2} = \frac{2}{2} = 1$$

Como se cumple la igualdad entre el caso base de la relación de recurrencia y la solución de la relación de recurrencia evaluada en $m = 0$, entonces la demostración continua en el caso inductivo.

Caso inductivo $m = k$:

Se asume como cierto que: $P(5^k) = \dfrac{5^{k+1} \ - \ 3^{k+1}}{2}$

Caso post-inductivo $m = k + 1$:

Recordar el caso recursivo de la relación de recurrencia:

$P(5^m) = 3P(5^{m-1}) \ + \ 5^m$

Al reemplazar m por $k + 1$ se tiene:

$P(5^{k+1}) = 3P(5^k) \ + \ 5^{k+1}$

Se reemplaza a $P(5^{k+1})$ y $P(5^k)$ por su equivalente en el caso inductivo.

$$\underbrace{\frac{5^{k+2} \ - \ 3^{k+2}}{2}}_{P(5^{k+1})} = 3 \underbrace{\left[\frac{5^{k+1} \ - \ 3^{k+1}}{2}\right]}_{P(5^k)} \ + \ 5^{k+1}$$

$$= \frac{3 \ \cdot \ 5^{k+1} \ - \ 3 \ \cdot \ 3^{k+1}}{2} \ + \ \frac{2}{2} \cdot 5^{k+1}$$

$$= \frac{3 \ \cdot \ 5^{k+1} \ - \ 3^{k+2} \ + \ 2 \ \cdot \ 5^{k+1}}{2}$$

$$= \frac{3 \ \cdot \ 5^{k+1} \ + \ 2 \ \cdot \ 5^{k+1} \ - \ 3^{k+2}}{2}$$

$$= \frac{5^{k+1}(3 \ + \ 2) \ - \ 3^{k+2}}{2}$$

$$= \frac{5^{k+1}(5) \ - \ 3^{k+2}}{2}$$

$$= \frac{5^{k+2} \ - \ 3^{k+2}}{2}$$

Se cumple la igualdad por lo tanto es correcta la solución de la relación de recurrencia.

Ejemplo 8:

Sea la siguiente relación de recurrencia:

$P(1) = 4$
$P(n) = 4P(\frac{n}{4}) + n^2 + 2$, para $n = 4^m$, $m \in \mathbb{Z}^+$.

El aporte fundamental de este ejemplo es que el caso base de la relación de recurrencia no siempre tiene que comenzar en uno, en este ejemplo comienza en cuatro (pudiéndose utilizar cualquier otro valor), y no se afecta en nada la utilización del método de iteración.

Ahora, primero se debe hacer el cambio de variables y reescribir la relación de recurrencia.

Cambio de variables:

Como $n = 4^m$, entonces la relación de recurrencia original puede ser reescrita de la siguiente forma:

$$P(4^0) = 4$$
$$P(4^m) = 4P(\tfrac{4^m}{4}) \ + \ (4^m)^2 \ + \ 2,\ m \geq 1$$
$$P(4^m) = 4P(4^m \cdot 4^{-1}) \ + \ (4^2)^m \ + \ 2,\ m \geq 1$$
$$P(4^m) = 4P(4^{m-1}) \ + \ 16^m \ + \ 2,\ m \geq 1$$

La cantidad de términos independientes en el caso recursivo de la relación de recurrencia indica cuantas sumatorias diferentes se presentan para solucionar la relación de recurrencia, en este ejemplo se generarán dos sumatorias, una en términos de 16^m y la otra en términos de 2, adicionalmente es normal que el término que se genera gracias al caso base de la relación de recurrencia no encaje en ninguna de las sumatorias, por este motivo se deja por aparte como si fuera una nueva sumatoria, pero de un solo término.

Método iterativo:

$$\begin{aligned}
&P(4^0) = 4\\
&P(4^1) = 4P(4^0) \ + \ 16^1 \ + \ 2\\
&\qquad = 4(4) \ + \ 16^1 \ + \ 2\\
&\qquad = 4^2 \ + \ 16^1 \ + \ 2\\
&P(4^2) = 4P(4^1) \ + \ 16^2 \ + \ 2\\
&\qquad = 4(4^2 \ + \ 16^1 \ + \ 2) \ + \ 16^2 \ + \ 2\\
&\qquad = 4^3 + 4^1 \cdot 16^1 \ + \ 4 \cdot 2 \ + \ 16^2 \ + \ 2\\
&\qquad = 4^3 + 4^1 \cdot 16^1 \ + \ 4 \cdot 2 \ + \ 16^2 \ + \ 2\\
&P(4^3) = 4P(4^2) \ + \ 16^3 \ + \ 2 = 4(4^3 + 4^1 \cdot 16^1 \ + \ 4 \cdot 2 \ + \ 16^2 \ + \ 2) \ + \ 16^3 \ + \ 2\\
&\qquad = 4^4 \ + \ 4^2 \cdot 16^1 \ + \ 2 \cdot 4^2 \ + \ 4 \cdot 16^2 \ + \ 2 \cdot 4 \ + \ 16^3 \ + \ 2\\
&\qquad = 4^4 \ + \ 4^2 \cdot 16^1 \ + \ 4 \cdot 16^2 \ + \ 16^3 \ + \ 2 \cdot 4^2 \ + \ 2 \cdot 4 \ + \ 2\\
&\qquad = 4^4 \ + \ (4^2 \cdot 16^1 \ + \ 4 \cdot 16^2 \ + \ 16^3) \ + \ 2(4^2 \ + \ 4^1 \ + \ 4^0)\\
&P(4^4) = 4P(4^3) \ + \ 16^4 \ + \ 2\\
&\qquad = 4[4^4 \ + \ (4^2 \cdot 16^1 \ + \ 4^1 \cdot 16^2 \ + \ 16^3) \ + \ 2(4^2 \ + \ 4^1 \ + \ 4^0)] \ + \ 16^4 \ + \ 2\\
&\qquad = 4^5 \ + \ (4^3 \cdot 16^1 \ + \ 4^2 \cdot 16^2 \ + \ 4^1 \cdot 16^3) \ + \ 2(4^3 \ + \ 4^2 \ + \ 4^1) \ + \ 4^0 \cdot 16^4 \ + \ 2 \cdot 4^0\\
&\qquad = 4^5 \ + \ (4^3 \cdot 16^1 \ + \ 4^2 \cdot 16^2 \ + \ 4^1 \cdot 16^3 \ + \ 4^0 \cdot 16^4) \ + \ 2(4^3 \ + \ 4^2 \ + \ 4^1 \ + \ 4^0)\\
&\qquad = 4^5 \ + \ 16(4^3 \cdot 16^0 \ + \ 4^2 \cdot 16^1 \ + \ 4 \cdot 16^2 \ + \ 4^0 \cdot 16^3) \ + \ 2(4^0 \ + \ 4^1 \ + \ 4^2 \ + \ 4^3)\\
&\ \ \vdots
\end{aligned}$$

$$P(4^m) = \overbrace{4^{m+1}}^{término\ generado\ por\ el\ caso\ base\ de\ la\ relación\ de\ recurrencia} + 16\overbrace{(4^{m-1}\cdot 16^0 \ + \ 4^{m-2}\cdot 16^1 \ + \ldots + \ 4^1\cdot 16^{m-2} \ + \ 4^0\cdot 16^{m-1})}^{Sumatoria\ A} + 2\underbrace{(4^0 \ + \ 4^1 \ + \ \ldots \ + \ 4^{m-1})}_{Sumatoria\ B}$$

Sumatoria A:

La Sumatoria A es una serie geométrica con primer término $a = 4^{m-1}$, razón constante $r = \frac{16}{4} = 4$ y potencia más grande igual a $m-1$, reemplazando en la formula se tiene:

$$\frac{a \ \cdot \ r^{(potencia\ más\ grande)+1} \ - \ a}{r \ - \ 1} = \frac{4^{m-1}(4^{(m-1)+1}) \ - \ 4^{m-1}}{4 \ - \ 1}$$

$$= \frac{4^{m-1}(4^m) \ - \ 4^{m-1}}{3}$$

$$= 4^{m-1}\left(\frac{4^m \ - \ 1}{3}\right)$$

Sumatoria B:

La Sumatoria B es una serie geométrica con primer término $a = 4^0 = 1$, razón constante $r = 4$ y potencia más grande igual a $m-1$, reemplazando en la formula se tiene:

$$\frac{a \ \cdot \ r^{(potencia\ más\ grande)+1} \ - \ a}{r \ - \ 1} = \frac{1 \ \cdot \ (4^{(m-1)+1}) \ - \ 1}{4 \ - \ 1}$$

$$= \frac{4^m \ - \ 1}{3}$$

Solución Relación de recurrencia:

$$P(4^m) = (término\ generado\ por\ el\ caso\ base\ de\ la\ relación\ de\ recurrencia) + \ 16 \cdot (Sumatoria\ A) \ + \ 2 \cdot (Sumatoria\ B)$$

$$P(4^m) = 4^{m+1} \ + \ 16\left[4^{m-1}\left(\frac{4^m \ - \ 1}{3}\right)\right] \ + \ 2\left[\frac{4^m \ - \ 1}{3}\right]$$

$$= 4^{m+1} \ + \ 4^2 \cdot 4^{m-1}\left(\frac{4^m \ - \ 1}{3}\right) \ + \ 2\left(\frac{4^m \ - \ 1}{3}\right)$$

$$= 4^{m+1} \ + \ 4^{m+1}\left(\frac{4^m \ - \ 1}{3}\right) \ + \ 2\left(\frac{4^m \ - \ 1}{3}\right)$$

$$= 4^{m+1} \ + \ \left(4^{m+1} \ + \ 2\right)\left(\frac{4^m \ - \ 1}{3}\right)$$

Se puede utilizar la técnica de demostración por inducción matemática para ratificar o refutar la validez de la solución de la relación de recurrencia.

Ejercicios

1. Resolver las siguientes relaciones de recurrencia utilizando el *Método de Iteración*:

   a) $P(1) = \frac{1}{4}$
   $P(n) = P(n-1) + n^3 - \frac{3}{4}n^2$, para $n \in \mathbb{Z}^+$ y $n \geq 2$.

   b) $P(1) = \frac{1}{2}$
   $P(n) = P(n-1) + n^2 - \frac{1}{2}n$, para $n \in \mathbb{Z}^+$ y $n \geq 2$.

   c) $P(1) = \frac{1}{5}$
   $P(n) = P(n-1) + n^3 - \frac{4}{5}n$, para $n \in \mathbb{Z}^+$ y $n \geq 2$.

   d) $P(1) = \frac{3}{2}$
   $P(n) = P(n-1) + 2n - \frac{n}{2^n}$, para $n \in \mathbb{Z}^+$ y $n \geq 2$.

   e) $P(1) = 1$
   $P(n) = 3P(\frac{n}{2}) + n$, para $n = 2^m$, $m \in \mathbb{Z}^+$.

   f) $P(1) = 1$
   $P(n) = 3P(\frac{n}{4}) + n$, para $n = 4^m$, $m \in \mathbb{Z}^+$.

g) $P(1) = 1$
$P(n) = 2P(\frac{n}{3}) + n$, para $n = 3^m$, $m \in \mathbb{Z}^+$.

h) $P(1) = 1$
$P(n) = 4P(\frac{n}{3}) + n$, para $n = 3^m$, $m \in \mathbb{Z}^+$.

i) $P(1) = 1$
$P(n) = 9P(\frac{n}{3}) + n$, para $n = 3^m$, $m \in \mathbb{Z}^+$.

2. Demostrar o refutar por inducción matemática que las relaciones de recurrencia siguientes tienen la solución que se plantea para cada una de ellas :

a) $P(1) = 1$
$P(n) = P(n-1) + 4n - 3$, para $n \geq 2$, $n \in \mathbb{Z}^+$.
Solución:
$P(n) = 2n^2 - n$, para $n \geq 1$

b) $P(1) = 2$
$P(n) = P(n-1) + n^2 + n$, para $n \geq 2$, $n \in \mathbb{Z}^+$.
Solución:
$P(n) = \frac{n(n+1)(n+2)}{3}$, para $n \geq 1$

c) $P(1) = \frac{2}{3}$
$P(n) = P(n-1) + n^2 - \frac{1}{3}n$, para $n \geq 2$, $n \in \mathbb{Z}^+$.
Solución:
$P(n) = \frac{n^2(n+1)}{3}$, para $n \geq 1$

d) $P(1) = 0$
$P(n) = P(n-1) + n^2 - 1$, para $n \geq 2$, $n \in \mathbb{Z}^+$.
Solución:
$P(n) = \frac{n(2n+5)(n-1)}{6}$, para $n \geq 1$

e) $P(1) = 1$
$P(n) = 3P(n-1) + 2^n - 1$, para $n \geq 2$, $n \in \mathbb{Z}^+$.
Solución:
$P(n) = \frac{3^{n+1}+1}{2} - 2^{n+1}$, para $n \geq 1$

Capítulo 5

Conjuntos

Definición:

Un conjunto es una colección de objetos en la que no importa el orden en que estos aparecen.

Hay varias formas para describir un conjunto. Una forma es describir todos los elementos del conjunto, cuando esto es posible, entre llaves separados por comas.

Ejemplo 1:

- El conjunto de todas las vocales del alfabeto es: $V = \{a,\ e,\ i,\ o,\ u\}$.
- el conjunto de todos los enteros impares positivos menores que 10 es $I = \{1,\ 3,\ 5,\ 7,\ 9\}$.

Otra forma para describir un conjunto sin listar todos los elementos del conjunto es, listar algunos elementos del conjunto y colocar puntos suspensivos cuando el patrón general de los elementos es obvio.

Ejemplo 2:

El conjunto de los enteros positivos estrictamente menores que 100 es
$E = \{1,\ 2,\ 3,\ ...,\ 99\}$

Algunos de los conjuntos más importantes en matemáticas discretas son:

- $\mathbb{N} = \{0,\ 1,\ 2,\ 3, ...\ \}$ El conjunto de los números naturales
- $\mathbb{Z} = \{\ ...,\ -3,\ -2,\ -1,\ 0,\ 1,\ 2,\ 3, ...\ \}$ El conjunto de los números enteros
- $\mathbb{Z}^+ = \{1,\ 2,\ 3,\ 4, ...\ \}$ El conjunto de los números enteros positivos
- $\mathbb{Q} = \{\ \frac{p}{q} \mid p \in \mathbb{Z},\ q \in \mathbb{Z}^+,\ q \neq 0\ \}$ El conjunto de los números racionales
- $\mathbb{R}$; es el conjunto de los números reales.

Definición:

Dos conjuntos son iguales si y únicamente si tienen los mismos elementos.

Ejemplo 3:

Los conjuntos $A = \{1,\ 3,\ 5\}$ y $B = \{3,\ 5,\ 1\}$ son iguales porque contienen los mismos elementos.

Se debe tener en cuenta que el orden en que son presentados los elementos de un conjunto no tiene importancia, tampoco tiene importancia listar varias veces el mismo elemento de un conjunto, de todas maneras sigue siendo el mismo conjunto, por ejemplo el conjuntos $A = \{3,\ 3,\ 5,\ 3,\ 1,\ 3,\ 5\}$ es igual al conjunto $B = \{1,\ 3,\ 5\}$.

Otra forma para construir conjuntos es usando una "notación para construir conjuntos". Todos los elementos del conjunto se caracterizan porque cumplen la propiedad de pertenencia al conjunto.

Ejemplo 4:

$I = \{x \mid x$ es un número entero positivo impar menor que $100\}$

Los conjuntos pueden ser representados gráficamente utilizando diagramas de Venn. En los diagramas de Venn el conjunto universal U , el cual contiene todos los objetos bajo consideración, es representado por un rectángulo. Internamente en el rectángulo, los círculos u otra figura geométrica son utilizados para representar conjuntos.

Ejemplo 5:

Dibujar un diagrama de Venn para representar el conjunto de las vocales del alfabeto español.

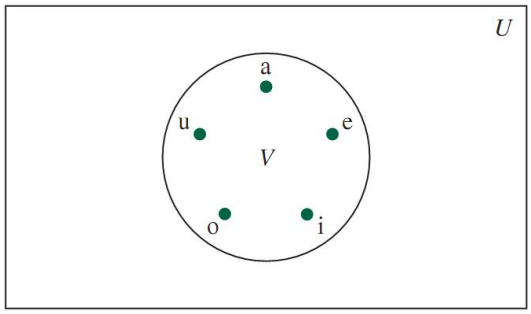


Diagrama de Venn para el conjunto de las vocales.

La pertenencia de un elemento a un conjunto se representa por $a \in A$. La notación $a \notin A$ indica que el elemento a no pertenece al conjunto A.

Tener en cuenta que las letras mayúsculas se utilizan para representar conjuntos y que las letras minúsculas se utilizan para representar elementos.

El conjunto vacío o nulo es aquel que no tiene elementos y se representa por $A = \{\ \}$ o $A = \emptyset$.

Definición:

El conjunto A es subconjunto de B si y únicamente si cada elemento de A es también un elemento de B. La notación $A \subseteq B$ indica que A es un subconjunto del conjunto B.

Se puede decir que $A \subseteq B$ si y únicamente si $\forall_x(x \in A \ \rightarrow \ x \in B)$.

Ejemplo 6:

Sean los conjuntos: $B = \{1,\ 2,\ 3,\ 4,\ 5,\ 6,\ 7,\ 8,\ 9,\ 10\}$ $A = \{1,\ 2,\ 5,\ 7\}$, entonces $A \subseteq B$.

Teorema:

Para cualquier conjunto S, $\emptyset \subseteq S$ y $S \subseteq S$.

Cuando el conjunto A es un subconjunto de B pero $A \neq B$, entonces se escribe $A \subset B$ y se dice que A es un subconjunto propio de B.

Gráficamente un subconjunto propio se representa de la siguiente manera:

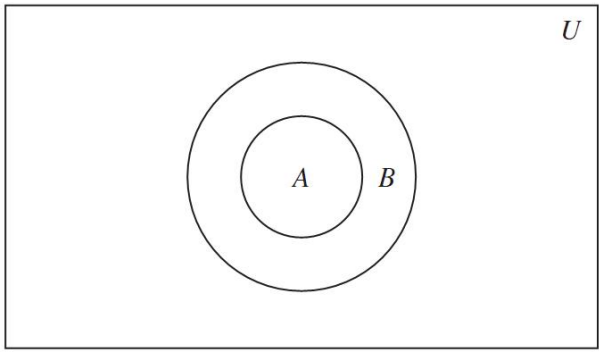


Diagrama de Venn para mostrar que A es un subconjunto propio de B.

Definición:

Sea S un conjunto. Si hay exactamente n elementos distintos en S donde n es un entero positivo, se dice que S es un conjunto finito y que n es la cardinalidad de S. La cardinalidad de S es denotada por $|S|$.

Ejemplo 7:

Sea el conjunto $A = \{1,\ 3,\ 5,\ 7,\ 3,\ 5,\ 1,\ 7\}$ $|A| = 4$.

Ejemplo 8:

$|\emptyset| = 0$, porque el conjunto vacío no tiene elementos.

5.1. El conjunto potencia

Definición:

Dado un conjunto S, el conjunto potencia de S es el conjunto de todos los subconjuntos de S. El conjunto potencia de S es denotado por $\mathcal{P}(S)$.

Ejemplo 9:

¿Cuál es el conjunto potencia del conjunto $A = \{\ 0,\ 1,\ 2\}$?

$$\mathcal{P}(A) = \{\{\ \},\ \{0\},\ \{1\},\ \{2\},\ \{0,\ 1\},\ \{0,\ 2\},\ \{1,\ 2\},\ \{0,\ 1,\ 2\}\}$$

Si un conjunto A tiene cardinalidad n ($|A| = n$), entonces el conjunto potencia de A tiene 2^n elementos.

Ejemplo 10:

¿Cuántos elementos tiene $\mathcal{P}(A)$ si $|A| = 3$?

$$|\mathcal{P}(A)| = 2^{|A|} = 2^3 = 8$$

5.2. Producto cartesiano

Definición:

La n-tupla ordenada $(a_1,\ a_2,\ a_3,\ \ldots,\ a_n)$ es la colección ordenada que tiene a_1 como el primer elemento, a_2 como el segundo elemento, ..., y a_n como el n-ésimo elemento.

Dos n-tuplas son iguales si y únicamente si cada par de sus elementos es igual. En otras palabras, $(a_1,\ a_2,\ a_3,\ \ldots,\ a_n) = (b_1,\ b_2,\ b_3,\ \ldots,\ b_n)$ si y únicamente si $a_i = b_i$, para $i = 1,\ 2,\ \ldots,\ n$. En particular, una 2-tupla es llamada *par ordenado*.

Los pares ordenados $(a,\ b)$ y $(c,\ d)$ son iguales si y únicamente si $a = c$ y $b = d$. $(a,\ b)$ y $(b,\ a)$ no son iguales, a no ser que $a = b$.

Definición:

Sea A y B conjuntos. El producto cartesiano de A y B, denotado por $A \times B$, es el conjunto de todos los pares ordenados $(a,\ b)$ donde $a \in A$ y $b \in B$. Donde $A \times B = \{(a,\ b) \mid a \in A\ \wedge\ b \in B\}$.

Ejemplo 11:

Sean los conjuntos $A = \{1,\ 2,\ 3,\ 4\}$ y $B = \{a,\ b,\ c\}$

- ¿Cuál es el conjunto $A \times B$?
- ¿Cuál es el conjunto $B \times A$?
- ¿Cuál es el conjunto $B \times B$?

$$A \times B = \{(1,\ a),\ (1,\ b),\ (1,\ c),\ (2,\ a),\ (2,\ b),\ (2,\ c),\ (3,\ a),\ (3,\ b),\ (3,\ c),\ (4,\ a),\ (4,\ b),\ (4,\ c)\}$$

$$B \times A = \{(a,\ 1),\ (a,\ 2),\ (a,\ 3),\ (a,\ 4),\ (b,\ 1),\ (b,\ 2),\ (b,\ 3),\ (b,\ 4),\ (c,\ 1),\ (c,\ 2),\ (c,\ 3),\ (c,\ 4)\}$$

$$B \times B = \{(a,\ a),\ (a,\ b),\ (a,\ c),\ (b,\ a),\ (b,\ b),\ (b,\ c),\ (c,\ a),\ (c,\ b),\ (c,\ c)\}$$

Un subconjunto R del producto cartesiano $A \times B$ es llamado una relación del conjunto A al conjunto B. Los elementos de R son pares ordenados donde el primer elemento pertenece a A y el segundo pertenece a B.

Ejemplo 12:

Sea $A = \{1,\ 2,\ 3,\ 4\}$ y $B = \{1,\ 4,\ 9,\ 16\}$

$$A \times B = \{(1,\ 1),\ (1,\ 4),\ (1,\ 9),\ (1,\ 16),\ (2,\ 1),\ (2,\ 4),\ (2,\ 9),\ (2,\ 16),\ (3,\ 1),\ (3,\ 4),\ (3,\ 9),\ (3,\ 16),\ (4,\ 1),\ (4,\ 4),\ (4,\ 9),\ (4,\ 16)\}$$

y sea $R = \{(1,\ 1),\ (2,\ 4),\ (3,\ 9),\ (4,\ 16)\}$ donde la segunda componente de cada pareja es el cuadrado de la primera.

Definición:

El producto cartesiano de los conjuntos $A_1,\ A_2,\ \ldots,\ A_n$ denotado por $A_1 \times A_2 \times \cdots \times A_n$, es el conjunto ordenado de n-tuplas $(a_1,\ a_2,\ \ldots,\ a_n)$ donde $a_i \in A_i$ para $i = 1,\ 2,\ \ldots,\ n$.

En otras palabras, $A_1 \times A_2 \times \cdots \times A_n = \{(a_1,\ a_2,\ \ldots,\ a_n) \mid a_i \in A_i \textit{ para } i = 1,\ 2,\ \ldots,\ n\}$.

Ejemplo 13:

Sea $A = \{1,\ 2\}$, $B = \{a,\ e\}$ y $C = \{x,\ y\}$, ¿cuál es el resultado de $A \times B \times C$?

$$A \times B \times C = \{(1,\ a,\ x),\ (1,\ a,\ y),\ (1,\ e,\ x),\ (1,\ e,\ y),\ (2,\ a,\ x),\ (2,\ a,\ y),\ (2,\ e,\ x),\ (2,\ e,\ y)\}$$

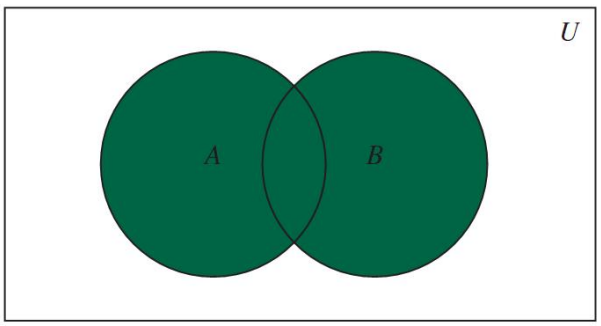
5.3. Operaciones de conjuntos

Definición de la operación de unión:

Sean A y B conjuntos. La unión de los conjuntos A y B denotada por $A \cup B$ es el conjunto que contiene elementos que son de A o B, o de ambos.

Un elemento x pertenece a la unión de A y B si y únicamente si x pertenece a A o x pertenece a B. Formalmente se tiene: $A \cup B = \{x \mid x \in A \quad \vee \quad x \in B\}$.

Gráficamente se tiene:



La parte sombreada es $A \cup B$.

Ejemplo 14:

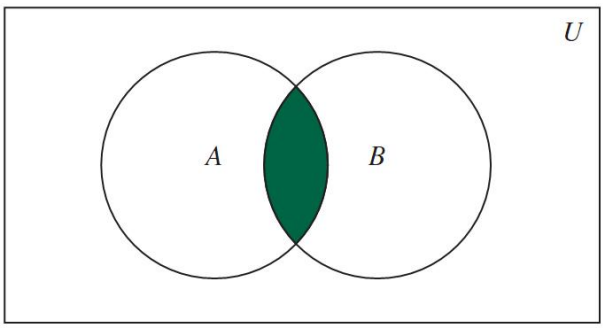
La unión de los conjuntos $A = \{1,\ 3,\ 5\}$ y $B = \{1,\ 2,\ 3\}$ es $A \cup B = \{1,\ 2,\ 3,\ 5\}$.

Definición de la operación de intersección:

Sean A y B conjuntos. La intersección de los conjuntos A y B denotada por $A \cap B$ es el conjunto que contiene los elementos que están al mismo tiempo en A y B.

Un elemento x pertenece a la intersección de los conjuntos A y B si y únicamente si x pertenece a A y x pertenece a B. Formalmente se tiene: $A \cap B = \{x \mid x \in A \ \wedge \ x \in B\}$.

Gráficamente se tiene:



La parte sombreada es $A \cap B$.

Ejemplo 15:

La intersección de los conjuntos $A = \{1,\ 3,\ 5\}$ y $B = \{1,\ 2,\ 3\}$ es $A \cap B = \{1,\ 3\}$.

Definición de conjuntos disyuntos:

Dos conjuntos A y B son disyuntos si su intersección $(A \cap B)$ es vacía.

Ejemplo 16:

Sea $A = \{1,\ 3,\ 5,\ 7,\ 9\}$ y $B = \{2,\ 4,\ 6,\ 8,\ 10\}$. $A \cap B = \{\ \}$, por lo tanto A y B son disyuntos.

La cardinalidad de la unión de los conjuntos A y B es:
$|A \cup B| = |A| + |B| - |A \cap B|$.

La generalización de la cardinalidad para la unión de un número arbitrario de conjuntos es llamado el principio de inclusión-exclusión.

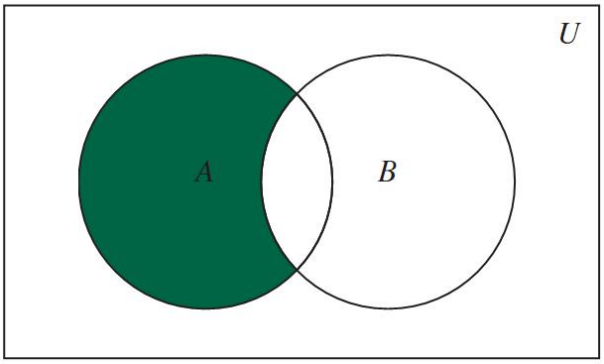
Definición de la operación de diferencia:

Sean A y B conjuntos. La diferencia de los conjuntos A y B denotada por $A - B$, es el conjunto que contiene los elementos que están en A pero no en B. La diferencia de A

y B es también llamada el complemento de B con respecto a A.

Un elemento x pertenece a la diferencia de A y B si y únicamente si $x \in A$ y $x \notin B$. Formalmente se tiene: $A - B = \{x \mid x \in A \ \wedge \ x \notin B\}$.

Gráficamente se tiene:



La parte sombreada es $A - B$.

Ejemplo 17:

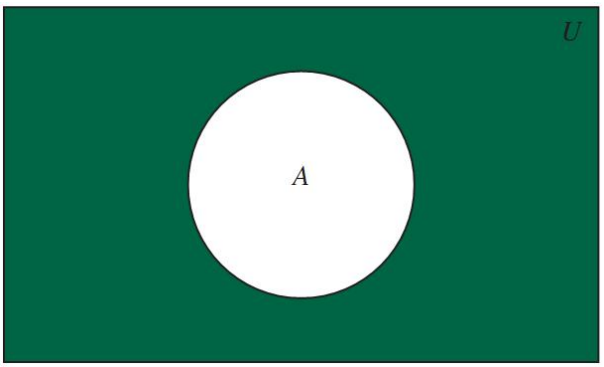
La diferencia de los conjuntos $A = \{1, \ 3, \ 5\}$ y $B = \{1, \ 2, \ 3\}$ es $A - B = \{5\}$, $B - A = \{2\}$.

Definición de la operación de complemento:

Sea $\mathcal{U}$ el conjunto universo, el complemento del conjunto A, denotado por $\overline{A}$, es el complemento del conjunto A con respecto a $\mathcal{U}$. En otras palabras, el complemento del conjunto A es $\mathcal{U} - A$.

Un elemento x pertenece a $\overline{A}$ si y únicamente si $x \notin A$. Formalmente se tiene: $\overline{A} = \{x \mid x \notin A\}$.

Gráficamente se tiene:



La parte sombreada es $\overline{A}$.

Ejemplo 18:

Sea $A = \{a,\ e,\ i,\ o,\ u\}$ y el universo son todas las letras del alfabeto español. Entonces $\overline{A} = \{b,\ c,\ d,\ f,\ g,\ h,\ j,\ k,\ l,\ m,\ n,\ \widetilde{n},\ p,\ q,\ r,\ s,\ t,\ v,\ w,\ x,\ y,\ z\}$.

5.4. Identidades en conjuntos

En la siguiente tabla las letras mayúsculas A, B y C representan conjuntos, el conjunto universal es representado con el símbolo $\mathcal{U}$ y el conjunto vacío es representado con el símbolo $\emptyset$.

Identidad	**Nombre**
$A \cup \emptyset = A$	Ley de Identidad
$A \cap \mathcal{U} = A$	Ley de Identidad
$A \cup \mathcal{U} = \mathcal{U}$	Ley de Dominación
$A \cap \emptyset = \emptyset$	Ley de Dominación
$A \cup A = A$	Ley de Idempotencia
$A \cap A = A$	Ley de Idempotencia
$\overline{\overline{A}} = A$	Ley de Doble Complemento
$A \cup B = B \cup A$	Ley Conmutativa
$A \cap B = B \cap A$	Ley Conmutativa
$A \cup (B \cup C) = (A \cup B) \cup C$	Ley Asociativa
$A \cap (B \cap C) = (A \cap B) \cap C$	Ley Asociativa
$A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$	Ley Distributiva
$A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$	Ley Distributiva
$\overline{A \cup B} = \overline{A} \cap \overline{B}$	Ley de De Morgan
$\overline{A \cap B} = \overline{A} \cup \overline{B}$	Ley de De Morgan
$A \cup (A \cap B) = A$	Ley de Absorción
$A \cap (A \cup B) = A$	Ley de Absorción
$A \cup \overline{A} = \mathcal{U}$	Ley de Complemento
$A \cap \overline{A} = \emptyset$	Ley de Complemento

Ejemplo 19:

Probar que $\overline{A \cap B} = \overline{A} \cup \overline{B}$.

Estrategia: Se debe probar que los dos conjuntos son iguales al mostrar que cada uno es subconjunto del otro.

- $\overline{A \cap B} \subseteq \overline{A} \cup \overline{B}$?.

  $x \in \overline{A \cap B}$, $x \notin (A \cap B)$, $\neg(x \in A \ \wedge \ x \in B)$, por la ley de Morgan $\neg(x \in A) \ \vee \ \neg(x \in B)$, $x \notin A \ \vee \ x \notin B$, $x \in \overline{A} \ \vee \ x \in \overline{B}$ por la definición de complemento, $x \in (\overline{A} \cup \overline{B})$ por la definición de la unión, por lo tanto $\overline{A \cap B} \subseteq \overline{A} \cup \overline{B}$.

- $\overline{A} \cup \overline{B} \subseteq \overline{A \cap B}$?.

  $x \in (\overline{A} \cup \overline{B})$,
  $x \in \overline{A} \ \vee \ x \in \overline{B}$ definición de la unión,
  $x \notin A \ \vee \ x \notin B$ definición de complemento,
  $\neg(x \in A) \ \vee \ \neg(x \in B)$ equivalencia lógica,
  $\neg((x \in A) \ \wedge \ (x \in B))$ ley de Morgan,
  $\neg(x \in (A \cap B))$ definición de la intersección,
  $x \notin (A \cap B)$, $x \in \overline{(A \cap B)}$ definición de complemento,
  por lo tanto $\overline{A} \cup \overline{B} \subseteq \overline{A \cap B}$.

  Como cada lado es subconjunto del otro entonces queda demostrado que $\overline{A \cap B} = \overline{A} \cup \overline{B}$.

Ejemplo 20:

Usar notación y equivalencia lógica para probar que $\overline{A \cap B} = \overline{A} \cup \overline{B}$.

Estrategia: Utilizar una cadena de equivalencias para proveer una demostración de esta identidad.

$$\begin{aligned}
\overline{A \cap B} &= \{x \mid x \notin (A \cap B)\} \\
&= \{x \mid \neg(x \in (A \cap B))\} \\
&= \{x \mid \neg(x \in A \ \wedge \ x \in B)\} \\
&= \{x \mid \neg(x \in A) \ \vee \ \neg(x \in B)\} \\
&= \{x \mid x \notin A \ \vee \ x \notin B\} \\
&= \{x \mid x \in \overline{A} \ \vee \ x \in \overline{B}\} \\
&= \{x \mid x \in (\overline{A} \cup \overline{B})\} \\
&= \overline{A} \cup \overline{B}
\end{aligned}$$

5.5. Uniones e intersecciones generalizadas

Definición de unión generalizada:

La unión de una colección de conjuntos es el conjunto que contiene todos los elementos que son miembros de al menos un conjunto de la colección. Se usa la notación:

$$A_1 \cup A_2 \cup A_3 \cup \ ... \ \cup A_n = \bigcup_{i=1}^{n} A_i$$

Definición de intersección generalizada:

La intersección de una colección de conjuntos es el conjunto que contiene los elementos que son miembros de todos los conjuntos de la colección. Se usa la notación:

$$A_1 \cap A_2 \cap A_3 \cap \ ... \ \cap A_n = \bigcap_{i=1}^{n} A_i$$

Ejemplo 21:

Sea $A_i = \{i,\ i+1,\ i+2,\ ...\ \}$ donde

$$\bigcup_{i=1}^{n} A_i = \bigcup_{i=1}^{n} \{i,\ i+1,\ i+2,\ ...\ \} = \{1,\ 2,\ 3,\ ...\ \}$$

y

$$\bigcap_{i=1}^{n} A_i = \bigcap_{i=1}^{n} \{i,\ i+1,\ i+2,\ ...\ \} = \{n,\ n+1,\ n+2,\ ...\ \}$$

5.6. Ejercicios

1. Suponer que A es el conjunto de estudiantes de segundo semestre de Ingeniería de Sistemas de Jornada Especial de la Universidad Tecnológica y B el conjunto de estudiantes de Ingeniería de Sistemas de Jornada Especial que tienen matriculado el curso de Matemáticas II. Expresar estos conjuntos en términos de A y B.

   a) El conjunto de estudiantes de segundo semestre de Ingeniería de Sistemas de Jornada Especial de la Universidad Tecnológica que tienen matriculado el curso de Matemáticas II.

   b) El conjunto de estudiantes de segundo semestre de Ingeniería de Sistemas de Jornada Especial de la Universidad Tecnológica que no tienen matriculado el curso de Matemáticas II.

   c) El conjunto de estudiantes o bien que son segundo semestre de Ingeniería de Sistemas de Jornada Especial de la Universidad Tecnológica o bien que están matriculados en el curso de Matemáticas II.

d) El conjunto de estudiantes o bien que no son de segundo semestre de Ingeniería de Sistemas de Jornada Especial de la Universidad Tecnológica o bien que no están matriculados en el curso de Matemáticas II.

2. Un profesor tiene 24 libros de texto introductorios de *Ciencias de la Computación*, y le interesa saber en qué medida tratan los temas: (A) análisis de algoritmos, (B) estructuras de datos y (C) compiladores. Los siguientes datos presentan el número de libros que contienen material sobre estos temas:

   - $|A| = 8$
   - $|B| = 13$
   - $|C| = 13$
   - $|A \cap B| = 5$
   - $|A \cap C| = 3$
   - $|B \cap C| = 6$
   - $|A \cap B \cap C| = 2$

   a) ¿Cuántos textos incluyen material de exactamente uno de los temas?

   b) ¿Cuántos textos incluyen material de exactamente dos de los temas?

   c) ¿Cuántos textos tratan al menos alguno de los temas?

   d) ¿Cuántos textos no tratan ninguno de los temas?

   e) ¿Cuántos textos no tratan el tema de compiladores?

   f) ¿Cuántos textos no tratan ni el tema de compiladores ni el tema de estructuras de datos?

3. Sean A y B conjuntos. Mostrar gráficamente utilizando diagramas de Venn que se cumplen cada una de las siguientes igualdades:

   a) $(A \cap B) \cup (A \cap \overline{B}) = A$.

   b) $A - B = A \cap \overline{B}$.

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

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

4. Sean A y B conjuntos. Representar gráficamente utilizando diagramas de Venn el conjunto resultado de $((\overline{A} \cap B) \cup (A \cap \overline{B})) \cap \overline{B}$.

5. Sean A y B conjuntos. Utilizando las identidades de conjuntos demostrar las igualdades de cada uno de los siguientes puntos:

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

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

c) $A - B = A \cap \overline{B}$.

d) $(A \cap B) \cup (A \cap \overline{B}) = A$.

6. Sean A y B conjuntos. Simplificar las siguientes expresiones en la teoría de conjuntos $((\overline{A} \cap B) \cup (A \cap \overline{B})) \cap B$, en cada paso indicar la ley utilizada.

7. Sean A y B conjuntos. Simplificar las siguientes expresiones en la teoría de conjuntos, en cada paso indicar la ley utilizada. Validar el resultado obtenido utilizando diagramas de Venn. ¿El gráfico de la simplificación es igual al gráfico de la expresión original?.

   a) $\overline{A} \cup (A \cap B) \cup \overline{B}$.

   b) $\overline{A} \cap (A \cup B) \cap \overline{B}$.

   c) $((\overline{A} \cap B) \cup (A \cap \overline{B})) \cap A$.

   d) $((\overline{A} \cap B) \cup (A \cap \overline{B})) \cap \overline{A}$.

8. Sean los conjuntos $A = \{1,\ 2,\ 3,\ 4\}$, $B = \{a,\ b,\ c\}$ y $C = \{a,\ 1,\ b,\ 2,\ c,\ 4\}$. ¿Cuál es el resultado de $(C \times C) - (B \times A)$?

9. Sean los conjuntos $A = \{1,\ 2,\ 3\}$, $B = \{a,\ b,\ c\}$ y $C = \{a,\ 1,\ b,\ 2\}$. ¿Cuál es el resultado de $(C \times C) - (B \times A)$?

10. Sean los conjuntos $A = \{1,\ 2,\ 3\}$, $B = \{a,\ b,\ c\}$ y $C = \{a,\ 1,\ b,\ 2\}$. ¿Cuál es el resultado de $(C \times C) - (A \times B)$?

11. Sean los conjuntos $A = \{1,\ 2,\ 3\}$, $B = \{a,\ b,\ c\}$ y $C = \{a,\ 1,\ b,\ 2,\ c\}$. ¿Cuál es el resultado de $(C \times C) - (B \times A)$?

12. Sean los conjuntos $A = \{1,\ 2,\ 3\}$, $B = \{a,\ b,\ c\}$ y $C = \{a,\ 1,\ b,\ 2,\ c\}$. ¿Cuál es el resultado de $(A \times B) - (C \times C)$?

13. Sea $A_i = \{i^i,\ i^{2i},\ i^{3i},\ \ldots,\ i^{i*i}\}$. ¿Cuántos elementos tiene el conjunto resultado de $\cup_{i=1}^{n}(A_i)$?

14. Sea $A_i = \{2^i,\ 2^{i+1},\ 2^{i+2},\ \ldots,\ 2^{2i}\}$. ¿Cuál es el conjunto resultado de $\cup_{i=0}^{n} A_i$?

15. Sea $A_i = \{2^i,\ 2^{i+1},\ 2^{i+2},\ \ldots,\ 2^{2i}\}$. ¿Cuál es el conjunto resultado de $\cap_{i=2}^{n} A_i$?

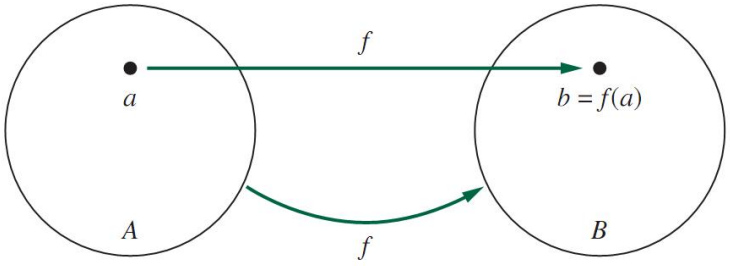
Capítulo 6

Funciones

6.1. Conceptos fundamentales

Definición de función:

Sean A y B conjuntos. Una función f de A a B es una asignación de exactamente un elemento de B a cada elemento de A. Se escribe $f(a) = b$ si b es el único elemento de B asignado por la función f al elemento a de A. Si f es una función de A a B, se escribe $f : A \to B$.



La función f mapea A en B.

Definición de dominio de una función:

Si f es una función de A a B, se dice que A es el dominio de f y B es el codominio de f. Si $f(a) = b$, se dice que b es la imagen de a y a es la pre-imagen de b. El rango de f es el conjunto de todas las imágenes de A. Así mismo, si f es una función de A a B, se dice que f mapea A en B.

Ejemplo 1:

Sea el conjunto A todas las cadenas de bits de longitud 2 y sea B el conjunto de los números 0, 1 y 2. La función f cuenta la cantidad de ceros que hay en la cadena de bits de longitud 2.

El dominio de la función f es $Dom_f = \{00,\ 01,\ 10,\ 11\}$, $Codom_f = \{0,\ 1,\ 2\}$, $f(00) = 2$, 2 es la imagen de 00 y 00 es la pre-imagen de 2.

Ejemplo 2:

Sea $f : \mathbb{Z} \to \mathbb{N}$ la función que calcula el cuadrado de un número entero. Donde:
$f(x) = x^2$
$Dom_f = \mathbb{Z}$
$Codom_f = \mathbb{N}$
$Rango_f = \{0,\ 1,\ 4,\ 9,\ 16,\ 25,\ ...,\ n^2\}$

Ejemplo 3:

Cuando se programan funciones en lenguaje C o JAVA se definen el dominio y codominio de la función. Por ejemplo al programar la función piso:

```
int piso(float numero)
  {
   -
   -
   -
  }
```

El dominio de la función son los reales de precisión sencilla (float) y codominio son los números enteros (int).

Definición de suma y multiplicación de funciones:

Sean f_1 y f_2 funciones de A a $\mathbb{R}$. Entonces $f_1 + f_2$ y $f_1 \cdot f_2$ son también funciones de A a $\mathbb{R}$ definidas por:
$(f_1 + f_2)(x) = f_1(x) + f_2(x)$
$(f_1 \cdot f_2)(x) = f_1(x) \cdot f_2(x)$

Ejemplo 4:

f_1 y f_2 son funciones de $\mathbb{R}$ a $\mathbb{R}$ tales que $f_1(x) = x^2$ y $f_2(x) = x - x^2$.
¿Cuáles son las funciones $f_1 + f_2$ y $f_1 \cdot f_2$?
$(f_1 + f_2)(x) = f_1(x) + f_2(x) = x^2 + x - x^2 = x$
$(f_1 \cdot f_2)(x) = f_1(x) \cdot f_2(x) = x^2 \cdot (x - x^2) = x^3 - x^4$.

Definición:

Sea f una función del conjunto A al conjunto B y sea S un subconjunto de A. La imagen de S es un subconjunto de B que consiste de las imágenes de los elementos de S. Se define la imagen de S por $f(S)$, tal que $f(S) = \{f(s) \mid s \in S\}$.

Ejemplo 5:

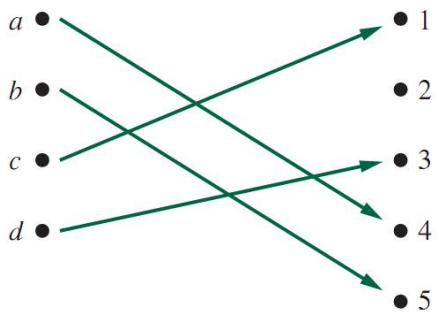
Sea $A = \{a,\ b,\ c,\ d,\ e\}$ y $B = \{1,\ 2,\ 3,\ 4\}$ con $f(a) = 2$, $f(b) = 1$, $f(c) = 4$, $f(d) = 1$ y $f(e) = 1$.
La imagen del subconjunto $S = \{b,\ c,\ d\}$ es el conjunto $f(S) = \{1,\ 4\}$.

6.2. Funciones inyectivas (o funciones uno a uno)

Una función es inyectiva o uno a uno si y únicamente si $f(x) = f(y)$ implica que $x = y$ para toda x y y en el dominio de f.

Ejemplo 6:

Determinar si la función f de $\{a,\ b,\ c,\ d\}$ a $\{1,\ 2,\ 3,\ 4,\ 5\}$ con $f(a) = 4$, $f(b) = 5$, $f(c) = 1$ y $f(d) = 3$ es inyectiva (uno a uno).



Función inyectiva.

La función f si es inyectiva (uno a uno).

Ejemplo 7:

Determinar si la función $f : \mathbb{Z} \to \mathbb{Z}$, $f(x) = x^2$ es uno a uno (inyectiva).

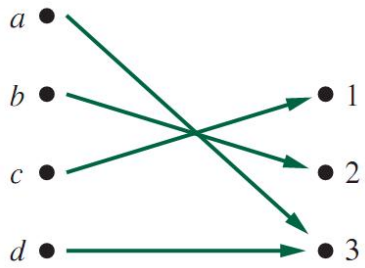
La función f no es uno a uno porque $f(-1) = f(1) = 1$, donde $-1 \neq 1$. Pero, si la función es $f : \mathbb{Z}^+ \to \mathbb{Z}^+$ entonces sí es uno a uno.

6.3. Funciones sobreyectivas

Una función f de A a B es llamada sobreyectiva si y únicamente si para cada elemento $b \in B$ hay como mínimo un elemento $a \in A$ con $f(a) = b$.

Ejemplo 8:

Sea f la función de $\{a,\ b,\ c,\ d\}$ a $\{1,\ 2,\ 3\}$ definida por $f(a) = 3$, $f(b) = 2$, $f(c) = 1$ y $f(d) = 3$. ¿Es f una función sobreyectiva?.



Función sobreyectiva.

La función f si es sobreyectiva.

Ejemplo 9:

¿Es la función $f : \mathbb{Z} \to \mathbb{Z}$, $f(x) = x^2$ sobreyectiva?

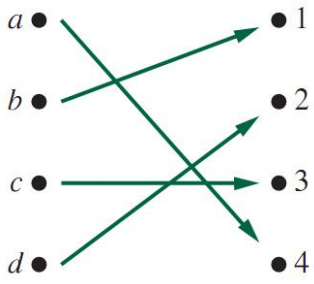
No, porque -1 no es un resultado de f y éste pertenece al conjunto de posibles respuestas ($-1 \in \mathbb{Z}$).

6.4. Funciones biyectivas

La función f tiene la propiedad de biyectividad (o también llamada correspondencia uno a uno) si ésta tiene al mismo tiempo las propiedades de inyectividad y sobreyectividad.

Ejemplo 10:

f es una función biyectiva de $\{a,\ b,\ c,\ d\}$ a $\{1,\ 2,\ 3,\ 4\}$ con $f(a) = 4$, $f(b) = 1$, $f(c) = 3$ y $f(d) = 2$.



Función biyectiva.

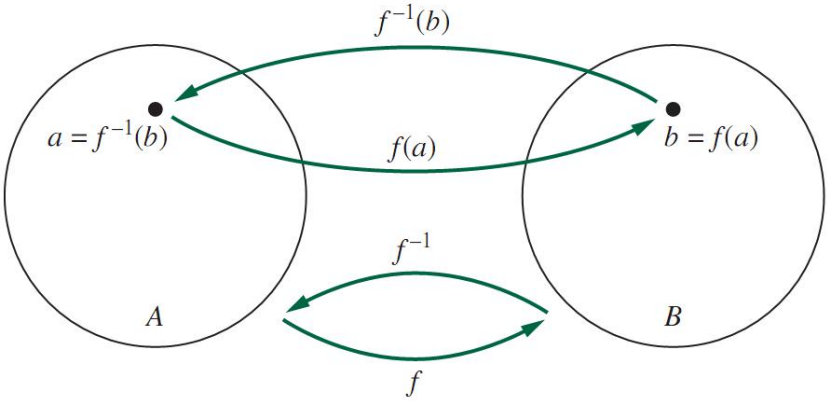
6.5. Funciones inversas y composición de funciones

Definición de función inversa:

Sea f una función biyectiva del conjunto A al conjunto B. La función inversa de f es la función que asigna a un elemento b que pertenece al conjunto B el único elemento a

en el conjunto A tal que $f(a) = b$. La función inversa de f es denotada por f^{-1}, donde, $f^{-1}(b) = a$ si y solo si $f(a) = b$.

Gráficamente:



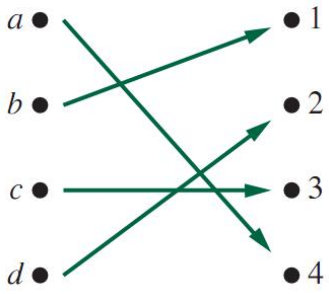
La función f^{-1} es la inversa de la función f.

Si una función f no es biyectiva, entonces no se puede definir una función inversa de f.

Una función biyectiva es también llamada función invertible.

Ejemplo 11:

Sea f la función de $\{a,\ b,\ c,\ d\}$ a $\{1,\ 2,\ 3,\ 4\}$ tal que $f(a) = 4$, $f(b) = 1$, $f(c) = 3$ y $f(d) = 2$. ¿Es f una función invertible, y si es así, cuál es su inversa?



Función invertible.

Al analizar el gráfico se evidencia que f es una función que tiene las propiedades de inyectividad y de sobre-inyectividad, por lo tanto f es una función con la propiedad de biyectividad. Como f es una función biyectiva entonces se obtiene la siguiente función inversa: $f^{-1}(1) = b$, $f^{-1}(2) = d$, $f^{-1}(3) = c$ y $f^{-1}(4) = a$.

Ejemplo 12:

Sea la función $f : \mathbb{Z} \to \mathbb{Z}$, donde $f(x) = x + 1$. ¿Es f una función invertible?, si es así, ¿cuál es la función inversa?

f es una función inyectiva y sobreyectiva, por lo tanto es una función biyectiva y es en consecuencia, una función que tiene inversa.

Tenemos que $f(x) = x + 1$, $y = x + 1$, $x = y - 1$. Entonces la función inversa de f es $f^{-1}(y) = y - 1$.

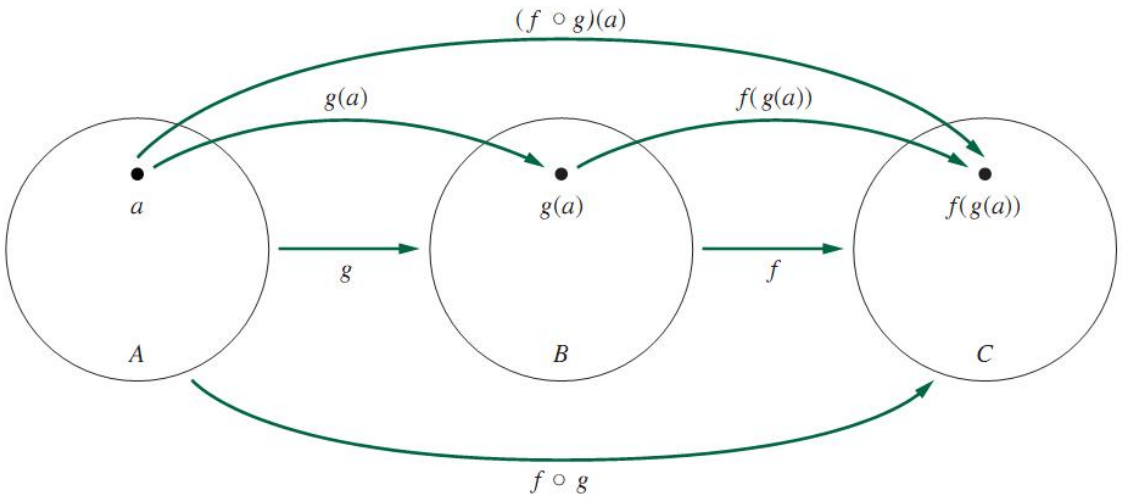
Ejemplo 13:

Sea la función $f : \mathbb{Z} \to \mathbb{Z}$, donde $f(x) = x^2$. ¿Es f una función invertible?, si es así, ¿cuál es la función inversa?

Se tiene que $f(-1) = (-1)^2 = 1$ y que $f(1) = (1)^2 = 1$, como dos valores diferentes del dominio son mapeados por la función f al mismo valor del codominio, entonces la función f no es una función inyectiva, por lo tanto la función f no es biyectiva y al no ser f una función biyectiva, entonces la función f no tiene inversa.

Definición de composición de funciones:

Sea g una función del conjunto A al conjunto B y sea f una función del conjunto B al conjunto C. La composición de las funciones f y g denotado por $f \circ g$, es la función definida por $(f \circ g)(a) = f(g(a))$, para cada $a \in A$.



Composición de las funciones f y g.

Ejemplo 14:

Sea g la función del conjunto $\{a,\ b,\ c\}$ a sí mismo tal que $g(a) = b$, $g(b) = c$ y $g(c) = a$.

Sea f la función del conjunto $\{a,\ b,\ c\}$ al conjunto $\{1,\ 2,\ 3\}$ tal que $f(a) = 3$, $f(b) = 2$ y $f(c) = 1$. ¿Cuál es la composición de f y g?, ¿Cuál es la composición de g y f?

Se da respuesta a la primer pregunta, f compuesto g:
$(f \circ g)(a) = f(g(a)) = f(b) = 2$.
$(f \circ g)(b) = f(g(b)) = f(c) = 1$.
$(f \circ g)(c) = f(g(c)) = f(a) = 3$.

Para la segunda pregunta, g compuesto f no esta definido porque el codominio de la función f no es un subconjunto del dominio de la función g, es decir, $\{1,\ 2,\ 3\} \not\subseteq \{a,\ b,\ c\}$

Ejemplo 15:

Sean f y g la funciones del conjunto de los números enteros al conjunto de los números enteros definidas por $f(x) = 2x + 3$ y $g(x) = 3x + 2$. ¿Cuál es la composición de f y g?, ¿cuál es la composición de g y f?

Primero se da respuesta a la pregunta de f compuesto g,
$(f \circ g)(x) = f(g(x)) = f(3x + 2) = 2(3x + 2) + 3 = 6x + 4 + 3 = 6x + 7$.

Ahora se da respuesta a la segunda pregunta con respecto a g compuesto f,
$(g \circ f)(x) = g(f(x)) = g(2x + 3) = 3(2x + 3) + 2 = 6x + 9 + 2 = 6x + 11$.

Con respecto a los resultados anteriores se tiene que $(f \circ g)(x) \neq (g \circ f)(x)$, por lo tanto se evidencia que la propiedad conmutativa no se presenta en la composición de funciones.

Cuando se hace la composición de una función y su inversa, en algún orden, una identidad de la función es obtenida. Primero se debe suponer que f es una función biyectiva del conjunto A al conjunto B. Entonces la función inversa f^{-1} existe y es una función biyectiva del conjunto B al conjunto A. La inversa de la función inversa es la función original, tal que $f^{-1}(b) = a$ donde $f(a) = b$ y $f(a) = b$ donde $f^{-1}(b) = a$. Por lo tanto, $(f^{-1} \circ f)(a) = f^{-1}(f(a)) = f^{-1}(b) = a$, $(f \circ f^{-1})(b) = f(f^{-1}(b)) = f(a) = b$ y $(f^{-1})^{-1} = f$.

6.6. Gráfica de una función

El gráfico de una función ayuda a que ésta sea más fácilmente comprendida, discutiendo si esta es inyectiva, sobreyectiva o biyectiva.

Ejemplo 16:

La siguiente es la gráfica de la función $f(n) = 2n + 1$, donde $f : \mathbb{Z} \to \mathbb{Z}$, es decir, la función f va del conjunto de los números enteros al conjunto de los números enteros

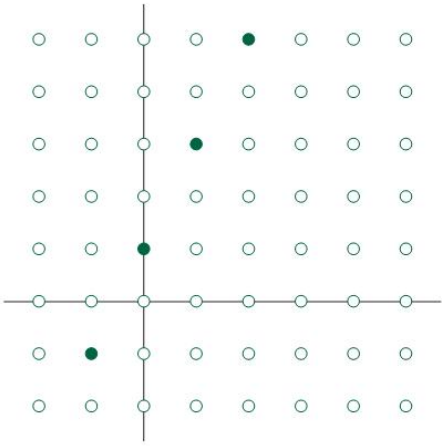


Gráfico de la función $f(n) = 2n + 1$ de $f : \mathbb{Z} \to \mathbb{Z}$.

En la gráfica fácilmente se puede observar que la función f es inyectiva porque cada número entero en el dominio referencia a un número entero en el codominio que no es referenciado por ningún otro número entero en el dominio. En la gráfica también se puede apreciar que la función f no es sobreyectiva porque hay números enteros del codominio que no son la imagen de algún número entero, tal es el caso de cualquier número entero par el cual no es referenciado por ningún número entero. Por lo tanto la función f no es biyectiva.

6.7. Ejercicios

1. Sean los conjuntos $A = \{2,\ 3,\ 4,\ 5\}$ y $B = \{6,\ 7,\ 8,\ 9,\ 10\}$, con $|A| = 4$ y $|B| = 5$, determinar

   a) ¿Cuántas funciones hay de A a B?

   b) ¿Cuántas funciones $f : A \to B$ cumplen $f(2) = 6$?

   c) ¿Cuántas funciones hay de B a A?

   d) ¿Cuántas funciones $g : B \to A$ cumplen $g(10) = 5$ y $g(8) = 3$?

   e) ¿se obtiene el mismo valor en las dos preguntas anteriores?

   f) ¿Cuántas funciones inyectivas hay de A a B?

   g) ¿Cuántas funciones sobreyectivas hay de A a B?

   h) ¿Cuántas funciones biyectivas hay de A a B?

   i) ¿Cuántas funciones inyectivas hay de B a A?

j) ¿Cuántas funciones sobreyectivas hay de B a A[1]?

k) ¿Cuántas funciones biyectivas hay de B a A?

2. Si hay 2187 funciones $f : A \to B$ y $|B| = 3$, ¿cuál es el valor de $|A|$?

3. Si $A = \{1,\ 2,\ 3,\ 4,\ 5\}$ y hay 6720 funciones inyectivas $f : A \to B$, ¿cuál es el valor de $|B|$?

4. Encontrar el rango y el dominio de la función que asigna a cada entero positivo su último dígito.

5. Encontrar el rango y el dominio de la función que asigna a cada entero positivo la multiplicación de sus dígitos.

6. Encontrar el rango y el dominio de la función f que asigna a cada entero positivo la suma de sus dígitos. Por ejemplo $f(1) = 1$, $f(11) = 1 + 1 = 2$ y $f(532) = 5 + 3 + 2 = 10$.

7. Encontrar el rango y el dominio de la función que asigna a cada entero positivo el entero que le sigue (es decir, su sucesor.)

8. Encontrar el rango y el dominio de la función que asigna a una cadena de bits la cantidad de unos que esta contiene.

9. Sean las siguientes funciones $F_i\ :\ \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$

$$F_1(m,\ n) = |4m| - |2n|$$
$$F_2(m,\ n) = m^3 - n^3$$
$$F_3(m,\ n) = 3m - n$$
$$F_4(m,\ n) = m^2 - n$$
$$F_5(m,\ n) = 2m - n$$
$$F_6(m,\ n) = m^2 - n^2$$
$$F_7(m,\ n) = |m| - |n|$$

¿Cuáles de las funciones anteriores son uno a uno?, ¿cuáles son sobreyectivas? y ¿cuáles son biyectivas?

10. Sea la función $F(m,\ n) = |m| \cdot |n|$ donde $F\ :\ \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$, ¿La función es uno a uno?, ¿la función es sobreyectiva?, y ¿la función es biyectiva?

11. Sea la función $F(m,\ n) = 3m - |n|$ donde $F\ :\ \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$, ¿La función es uno a uno?, ¿la función es sobreyectiva?, y ¿la función es biyectiva?

12. Sea la función $F(m,\ n) = n$ donde $F\ :\ \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$, ¿La función es uno a uno?, ¿la función es sobreyectiva?, y ¿la función es biyectiva?

[1] **Ayuda:** Leer la sección: "*Funciones Suprayectivas: Números de Stirling de Segundo Tipo*" del libro: "*Matemáticas Discreta y Combinatoria*" de Ralph P. Grimaldi, en donde se presenta una buena explicación del conteo de funciones sobreyectivas (o suprainyectivas.)

13. Sea la función $F(m,\ n) = m \cdot n$ donde $F\ :\ \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$, ¿La función es uno a uno?, ¿la función es sobreyectiva?, y ¿la función es biyectiva?

14. ¿Cuántas funciones biyectivas hay del conjunto A al conjunto B si $|A| = |B|$?

15. Sea la función $f : \mathbb{N} \to \mathbb{N} \times \mathbb{N}$,

    $f(0) = (x_0,\ y_0) = (0,\ 0)$

    $$f(n+1) = (x_{n+1},\ y_{n+1}) = \begin{cases} (x_n - 1,\ y_n + 1) & si \quad x_n \geq 1 \\ (y_n + 1,\ 0) & si \quad x_n = 0 \end{cases}$$

    Determinar:

    a) ¿Qué es $f(8)$?

    b) ¿Es f una función inyectiva?

    c) ¿Es f una función sobreyectiva?

    d) ¿Es f una función biyectiva?, si esto es así, ¿entonces el conjunto $\mathbb{N}$ tiene la misma cardinalidad que el conjunto $\mathbb{N} \times \mathbb{N}$?

    e) ¿Es f una función invertible?, si es así, ¿cuál es la inversa de f?

16. Sea $C = \{0,\ 1,\ 00,\ 01,\ 10,\ 11,\ 000,\ 001,\ 010,\ 011,\ 100,\ 101,\ 110,\ 111,\ ...\}$, donde C es el conjunto de todas las cadenas que se pueden formar con ceros y unos. Sea la función $f : C \times C \to C$ donde $f(s,\ r) = s00r$, lo que hace la función f es concatenar dos cadenas s y r colocando en medio de ellas la cadena 00.

    Determinar:

    a) ¿Qué es $f(001,\ 110)$?

    b) ¿Es f una función inyectiva?

    c) ¿Es f una función sobreyectiva?

    d) ¿Es f una función biyectiva?

    e) ¿Es f una función invertible?, si es así, ¿cuál es la inversa de f?

Capítulo 7

Relaciones

7.1. Relación binaria

Sean A y B conjuntos. Una relación binaria de A a B es un subconjunto de $A \times B$. En otras palabras, una relación binaria de A a B es un conjunto R de pares ordenados donde el primer elemento de cada par ordenado pertenece a A y el segundo pertenece a B. Se utiliza la notación aRb para denotar que $(a,\ b) \in R$ y $a\ \not Rb$ para denotar que $(a,\ b) \notin R$.

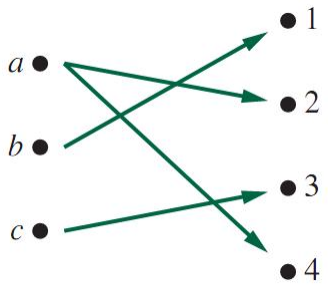
Ejemplo 1:

Sea A el conjunto de estudiantes de Ingeniería de Sistemas de la Institución, y sea B el conjunto de materias de Ingeniería de Sistemas de la institución. Sea R la relación que consiste de todos los pares ordenados $(a,\ b)$ donde a es un estudiante que tiene matriculada la materia b. Si los estudiantes "Jaime" y "Claudia" están matriculados en la materia "Matemáticas Discretas" entonces los pares ordenados $(Jaime,\ Matemáticas\ Discretas)$ y $(Claudia,\ Matemáticas\ Discretas)$ pertenecen a la relación R, adicionalmente "Claudia" también tiene matriculado el curso de "Bases de Datos", lo cual se representa con el par ordenado $(Claudia,\ Bases\ de\ Datos)$, que también pertenece a la relación R.

Ejemplo 2:

Sea $A = \{a,\ b,\ c\}$ y $B = \{1,\ 2,\ 3,\ 4\}$. Entonces $\{(a,\ 2),\ (a,\ 4),\ (b,\ 1),\ (c,\ 3)\}$ es una relación de A a B, la cual también se puede representar como ${}_aR_2$, ${}_aR_4$, ${}_bR_1$ y ${}_cR_3$. Esta relación puede ser fácilmente representada de forma gráfica y tabular de la siguiente forma:

Gráficamente:



Tabularmente:

R	1	2	3	4
a		X		X
b	X			
c			X	

7.2. Funciones como relaciones

Si R es una relación del conjunto A al conjunto B tal que cada elemento de A es la primera componente de exactamente un par ordenado de R, entonces una función puede ser definida con la relación R. De esta forma se evidencia que las relaciones son una generalización de las funciones y sirven para representar una clase más amplia de relaciones entre conjuntos.

7.3. Relaciones en un conjunto

Las relaciones de un conjunto A consigo mismo son de gran interés.

Definición de relación:

Una relación en el conjunto A es una relación del conjunto A al conjunto A, es decir, una relación en un conjunto A es un subconjunto de $A \times A$.

Ejemplo 3:

Sea $A = \{1,\ 2,\ 3,\ 4\}$ y la relación $R = \{(a,\ b) \mid a \text{ divide } b\}$ definida sobre el conjunto A. ¿Cuáles pares ordenados pertenecen a la relación R?.

El producto cruz del conjunto A es el siguiente:

$$A \times A = \{(1,\ 1),\ (1,\ 2),\ (1,\ 3),\ (1,\ 4),\\ (2,\ 1),\ (2,\ 2),\ (2,\ 3),\ (2,\ 4),\\ (3,\ 1),\ (3,\ 2),\ (3,\ 3),\ (3,\ 4),\\ (4,\ 1),\ (4,\ 2),\ (4,\ 3),\ (4,\ 4)\}$$

y los pares ordenados de este producto cruz donde la primera componente divide a la segunda son: $(1,\ 1)$, $(1,\ 2)$, $(1,\ 3)$, $(1,\ 4)$, $(2,\ 2)$, $(2,\ 4)$, $(3,\ 3)$, y $(4,\ 4)$, los cuales conforman la relación R

$$R = \{(1,\ 1),\ (1,\ 2),\ (1,\ 3),\ (1,\ 4),\ (2,\ 2),\ (2,\ 4),\ (3,\ 3),\ (4,\ 4)\}.$$

Observe que $R \subseteq A \times A$.

Ejemplo 4:

Considerar las siguientes relaciones definidas en el conjunto de los números enteros:

$$R_1 = \{(a,\ b) \mid a \leq b\}$$
$$R_2 = \{(a,\ b) \mid a > b\}$$
$$R_3 = \{(a,\ b) \mid a = b \ \vee \ a = -b\}$$
$$R_4 = \{(a,\ b) \mid a = b\}$$
$$R_5 = \{(a,\ b) \mid a = b + 1\}$$
$$R_6 = \{(a,\ b) \mid a + b \leq 3\}$$

¿Cada uno de los siguientes pares ordenados $(1,\ 1)$, $(1,\ 2)$, $(2,\ 1)$, $(1,\ -1)$ y $(2,\ 2)$ pertenecen a cuáles relaciones?

El par ordenado $(1,\ 1)$ se encuentra presente en las relaciones R_1, R_3, R_4 y R_6, el par ordenado $(1,\ 2)$ se encuentra presente en las relaciones R_1 y R_6, el par ordenado $(2,\ 1)$ se encuentra presente en las relaciones R_2, R_5 y R_6, el par ordenado $(1,\ -1)$ se encuentra presente en las relaciones R_2, R_3 y R_6 y el par ordenado $(2,\ 2)$ se encuentra presente en las relaciones R_1, R_3 y R_4.

Ejemplo 5:

¿Cuántas relaciones hay en un conjunto de n elementos?

Una relación en un conjunto A es un subconjunto de $A \times A$, donde $A \times A$ tiene n^2 pares ordenados cuando $|A| = n$. Recordar que un conjunto con m elementos tiene 2^m subconjuntos, entonces $2^{|A \times A|} = 2^{n^2}$ es el número total de relaciones del conjunto A al conjunto A.
Por ejemplo si $A = \{a,\ b,\ c\}$ entonces hay $2^{|A|^2} = 2^{3^2} = 2^9 = 512$ relaciones en el conjunto A.

Ejemplo 6:

¿Cuántas y cuáles relaciones hay en el conjunto $A = \{1,\ 2\}$?

Primero se debe calcular el producto cruz del conjunto A con el mismo:

$A \times A = \{(1,\ 1),\ (1,\ 2),\ (2,\ 1),\ (2,\ 2)\}$

Luego, como una relación es cualquier subconjunto que se puede sacar del producto cruz del conjunto que se esta trabajando, entonces se debe comenzar con los subconjuntos de tamaño cero, tamaño uno, tamaño dos y así sucesivamente hasta el subconjunto que tiene la misma cardinalidad de $A \times A$.

$R_1 = \{\}$
$R_2 = \{(1,\ 1)\}$
$R_3 = \{(1,\ 2)\}$
$R_4 = \{(2,\ 1)\}$
$R_5 = \{(2,\ 2)\}$
$R_6 = \{(1,\ 1),\ (1,\ 2)\}$
$R_7 = \{(1,\ 1),\ (2,\ 1)\}$
$R_8 = \{(1,\ 1),\ (2,\ 2)\}$
$R_9 = \{(1,\ 2),\ (2,\ 1)\}$
$R_{10} = \{(1,\ 2),\ (2,\ 2)\}$
$R_{11} = \{(2,\ 1),\ (2,\ 2)\}$
$R_{12} = \{(1,\ 1),\ (1,\ 2),\ (2,\ 1)\}$
$R_{13} = \{(1,\ 1),\ (1,\ 2),\ (2,\ 2)\}$
$R_{14} = \{(1,\ 1),\ (2,\ 1),\ (2,\ 2)\}$
$R_{15} = \{(1,\ 2),\ (2,\ 1),\ (2,\ 2)\}$
$R_{16} = \{(1,\ 1),\ (1,\ 2),\ (2,\ 1),\ (2,\ 2)\}$

Son 16 relaciones las cuales coinciden con el resultado que se obtiene al utilizar la fórmula que se trabajo en el ejemplo anterior, $2^{|A|^2} = 2^{2^2} = 2^4 = 16$.

7.4. Propiedades de las relaciones

7.4.1. Propiedad de reflexividad

Una relación R en un conjunto A tiene la propiedad de reflexividad si $(a,\ a) \in R$ para cada elemento $a \in A$.

Ejemplo 7:

Considerar las siguientes relaciones en el conjunto $A = \{1,\ 2,\ 3,\ 4\}$

$R_1 = \{(1,\ 1),\ (1,\ 2),\ (2,\ 1),\ (2,\ 2),\ (3,\ 4),\ (4,\ 1),\ (4,\ 4)\}$
$R_2 = \{(1,\ 1),\ (1,\ 2),\ (2,\ 1)\}$
$R_3 = \{(1,\ 1),\ (1,\ 2),\ (1,\ 4),\ (2,\ 1),\ (2,\ 2),\ (2,\ 4),\ (3,\ 3),\ (4,\ 1),\ (4,\ 2),\ (4,\ 4)\}$
$R_4 = \{(2,\ 1),\ (3,\ 1),\ (3,\ 2),\ (4,\ 1),\ (4,\ 2),\ (4,\ 3)\}$
$R_5 = \{(1,\ 1),\ (1,\ 2),\ (1,\ 3),\ (1,\ 4),\ (2,\ 2),\ (2,\ 3),\ (2,\ 4),\ (3,\ 3),\ (3,\ 4),\ (4,\ 4)\}$
$R_6 = \{(3,\ 4)\}$

¿Cuáles de estas relaciones tienen la propiedad de reflexividad?

Se tiene que entrar a analizar que se encuentren presentes todos los siguientes pares ordenados: (1, 1), (2, 2), (3, 3), (4, 4). Estos pares ordenados se encuentran todos presentes únicamente en las relaciones R_3 y R_5, las cuales son relaciones que tienen la propiedad de reflexividad.

7.4.2. Propiedad de simetría

Una relación R en un conjunto A tiene la propiedad de simetría si cuando $(a,\ b) \in R$ entonces también $(b,\ a) \in R$, para $a,\ b \in A$.

Ejemplo 8:

¿Cuáles de las relaciones del ejemplo 7 anterior tienen la propiedad de simetría?

Las únicas relaciones que tienen la propiedad de simetría son R_2 y R_3.

7.4.3. Propiedad de antisimetría

Una relación R en un conjunto A tiene la propiedad de antisimetría si $(a,\ b) \in R$ y $a \neq b$ entonces $(b,\ a) \notin R$, para $a,\ b \in A$.

Ejemplo 9:

¿Cuáles de las relaciones del ejemplo 7 tienen la propiedad de antisimetría?

Las únicas relaciones que tienen la propiedad de antisimetría son R_4, R_5 y R_6.

7.4.4. Propiedad de transitividad

Una relación R en un conjunto A tiene la propiedad de transitividad si cuando se presentan $(a,\ b) \in R$ y $(b,\ c) \in R$ también se presenta $(a,\ c) \in R$, para $a,\ b,\ c \in A$.

Ejemplo 10:

¿Cuáles de las relaciones del ejemplo 7 tienen la propiedad de transitividad?

Las únicas relaciones que tienen la propiedad de transitividad son R_3, R_4, R_5 y R_6.

Ejemplo 11:

Considerar la siguiente relación definida en el conjunto de los números enteros:

$$R = \{(a,\ b) \mid a \geq b\}$$

¿La relación R cumple la propiedad de reflexividad?, ¿cumple la propiedad de simetría?, ¿cumple la propiedad de antisimetría?, y, ¿cumple la propiedad de transitividad?

R cumple la propiedad de reflexividad porque cualquier número entero es mayor o igual a el mismo. R no cumple la propiedad de simetría porque hay pares ordenamos que pertenecen a la relación para los cuales el par ordenado simétrico no pertenece a la relación, tal es el caso del par ordenado $(2,\ 1) \in R$ porque $2 \geq 1$ pero $(1,\ 2) \notin R$ porque $1 \ngeq 2$. La relación R cumple la propiedad de antisimetría porque la única posibilidad de que $a \geq b$ y $b \geq a$ es que $a = b$, de esta forma $(a,\ b) \in R$ y $(b,\ a) \in R$ si y solo si $a = b$. La relación R también cumple la propiedad de transitividad ya que para cualquier conjunto de tres números enteros a, b y c, si $a \geq b$ y $b \geq c$ entonces se cumple que $a \geq c$, con lo cual se tiene que si $(a,\ b) \in R$ y $(b,\ c) \in R$ entonces $(a,\ c) \in R$.

Ejemplo 12:

Considerar la siguiente relación definida en el conjunto de los números enteros:

$$R = \{(a,\ b) \mid a = b\}$$

¿La relación R cumple la propiedad de reflexividad?, ¿cumple la propiedad de simetría?, ¿cumple la propiedad de antisimetría?, ¿cumple la propiedad de transitividad?, y, ¿es posible que al mismo tiempo una relación tenga las propiedades de simetría y antisimetría?

La relación R cumple la propiedad de reflexividad porque cualquier número entero es igual a el mismo. R cumple la propiedad de simetría porque todos los pares ordenados que pertenecen a la relación R son de la forma $(a,\ a)$ para $a \in \mathbb{Z}$ con lo cual todo par ordenado es simétrico con el mismo. R cumple la propiedad de antisimetría porque todos los pares ordenados que pertenecen a la relación R son de la forma $(a,\ a)$ para $a \in \mathbb{Z}$ con lo cual se garantiza la definición de antisimetría donde $a = a$. La relación R también cumple la propiedad de transitividad ya que para cualquier conjunto de tres números enteros a, b y c, si $(a,\ b) \in R$ y $(b,\ c) \in R$ es porque $a = b$ y $b = c$, de donde se obtiene que $a = c$ y que por lo tanto $(a,\ c) \in R$, con lo cual se cumple la definición de la propiedad de transitividad.
Con respecto a la última pregunta, ¿es posible que al mismo tiempo una relación tenga las propiedades de simetría y antisimetría?, la respuesta es que si y este ejemplo es uno de esos casos, es de vital importancia recalcar que dichas propiedades no son excluyentes en una relación, donde las dos pueden estar presentes o las dos pueden estar ausentes

al mismo tiempo.

7.5. Combinación de relaciones

Como las relaciones de A a B son subconjuntos del conjunto de pares ordenados $A \times B$, entonces dos relaciones de A a B pueden ser combinadas (u operadas) de la forma en que se combinan dos conjuntos.

Ejemplo 13:

Sean los conjuntos $A = \{1,\ 2,\ 3\}$ y $B = \{1,\ 2,\ 3,\ 4\}$. Las siguientes relaciones R_1 y R_2 están definidas del conjunto A al conjunto B, donde $R_1 = \{(1,\ 1),\ (2,\ 2),\ (3,\ 3)\}$ y $R_2 = \{(1,\ 1),\ (1,\ 2),\ (1,\ 3),\ (1,\ 4)\}$, estas relaciones pueden ser combinadas obteniendo:

$R_1 \cup R_2 = \{(1,\ 1),\ (1,\ 2),\ (1,\ 3),\ (1,\ 4),\ (2,\ 2),\ (3,\ 3)\}$
$R_1 \cap R_2 = \{(1,\ 1)\}$
$R_1 - R_2 = \{(2,\ 2),\ (3,\ 3)\}$
$R_2 - R_1 = \{(1,\ 2),\ (1,\ 3),\ (1,\ 4)\}$

Ejemplo 14:

Sean las siguientes relaciones R_1 y R_2 que están definidas en el conjunto de los números enteros, donde $R_1 = \{(x,\ y) \mid x < y\}$ y $R_2 = \{(x,\ y) \mid x > y\}$.

¿Qué es $R_1 \cup R_2$, $R_1 \cap R_2$, $R_1 - R_2$ y $R_2 - R_1$?

$R_1 \cup R_2 = \{(x,\ y) \mid x \neq y\}$
$R_1 \cap R_2 = \{\}$
$R_1 - R_2 = R_1$
$R_2 - R_1 = R_2$

7.6. Composición y potencia de relaciones

Definición de composición de relaciones:

Sea R una relación del conjunto A al conjunto B y sea S una relación del conjunto B al conjunto C. La composición de las relaciones R y S es la relación consistente de los pares ordenados $(a,\ c)$, donde $a \in A$ y $c \in C$ y para los cuales existe un elemento $b \in B$ tales que $(a,\ b) \in R$ y $(b,\ c) \in S$. Se denota la composición de R y S por $S \circ R$.

Ejemplo 15:

Sean los conjuntos $A = \{1,\ 2,\ 3\}$, $B = \{1,\ 2,\ 3,\ 4\}$, $C = \{0,\ 1,\ 2\}$ y las relaciones $R = \{(1,\ 1),\ (1,\ 4),\ (2,\ 3),\ (3,\ 1),\ (3,\ 4)\}$ del conjunto A al conjunto B y $S = \{(1,\ 0),\ (2,\ 0),\ (3,\ 1),\ (3,\ 2),\ (4,\ 1)\}$ del conjunto B al conjunto C. ¿Qué es $S \circ R$?

$$S \circ R = \{(1,\ 0),\ (1,\ 1),\ (2,\ 1),\ (2,\ 2),\ (3,\ 0),\ (3,\ 1)\}$$

Ejemplo 16:

Sea R la relación en el conjuntos de las personas del mundo tal que $(a,\ b) \in R$ si a es el padre de b. ¿Qué da como resultado $R \circ R$?

$R \circ R$ da como resultado una relación que es el conjunto de pares ordenados de personas donde la primer componente es el abuelo paterno de la segunda componente.

Definición de potencia de una relación:

Sea R una relación en el conjunto A. La *potencia* R^n, donde $n \in \mathbb{Z}^+$, es definida recursivamente por

$$R^n = \begin{cases} R & si \quad n = 1 \\ R^{n-1} \circ R & si \quad n > 1 \end{cases}$$

Ejemplo 17:

Sea la relación $R = \{(1,\ 1),\ (2,\ 1),\ (3,\ 2),\ (4,\ 3)\}$. ¿Cuál es la potencia R^n para $n \geq 1$?

$$\begin{aligned}
R^1 &= R = \{(1,\ 1),\ (2,\ 1),\ (3,\ 2),\ (4,\ 3)\} \\
R^2 &= R^1 \circ R = \{(1,\ 1),\ (2,\ 1),\ (3,\ 2),\ (4,\ 3)\} \circ \{(1,\ 1),\ (2,\ 1),\ (3,\ 2),\ (4,\ 3)\} \\
&= \{(1,\ 1),\ (2,\ 1),\ (3,\ 1),\ (4,\ 2)\} \\
R^3 &= R^2 \circ R = \{(1,\ 1),\ (2,\ 1),\ (3,\ 1),\ (4,\ 2)\} \circ \{(1,\ 1),\ (2,\ 1),\ (3,\ 2),\ (4,\ 3)\} \\
&= \{(1,\ 1),\ (2,\ 1),\ (3,\ 1),\ (4,\ 1)\} \\
R^4 &= R^3 \circ R = \{(1,\ 1),\ (2,\ 1),\ (3,\ 1),\ (4,\ 1)\} \circ \{(1,\ 1),\ (2,\ 1),\ (3,\ 2),\ (4,\ 3)\} \\
&= \{(1,\ 1),\ (2,\ 1),\ (3,\ 1),\ (4,\ 1)\}
\end{aligned}$$

Como $R^4 = R^3$ entonces $R^n = R^3$ para $n > 3$.

7.7. Representación de relaciones

7.7.1. Representación de relaciones utilizando matrices

Una relación entre conjuntos finitos puede ser representada usando matrices de ceros y unos. Suponer que R es una relación del conjunto $A = \{a_1,\ a_2,\ a_3,\ \ldots,\ a_m\}$ al con-

junto $B = \{b_1,\ b_2,\ b_3,\ \ldots,\ b_n\}$. La relación R puede ser representada por la matriz $M_R = [m_{ij}]$, donde

$$m_{ij} = \begin{cases} 1 & si\ \ (a_i,\ b_j) \in R \\ 0 & si\ \ (a_i,\ b_j) \notin R \end{cases}$$

Ejemplo 18:

Sean los conjuntos $A = \{1,\ 2,\ 3\}$ y $B = \{1,\ 2\}$, sea la relación $R = \{(a,\ b) \mid a > b\}$ $= \{(2,\ 1),\ (3,\ 1),\ (3,\ 2)\}$ definida del conjunto A al conjunto B. La representación de la relación R por medio de matrices es la siguiente:

$$M_R = \begin{bmatrix} 0 & 0 \\ 1 & 0 \\ 1 & 1 \end{bmatrix}$$

Ejemplo 19:

Sea la relación R en el conjunto $A = \{1,\ 2,\ 3,\ 4\}$. ¿Cuáles pares ordenados están en la relación R representados por la matriz

$$M_R = \begin{bmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 \end{bmatrix} \quad ?$$

La relación contiene los siguientes pares ordenados:
$R = \{(1,\ 2),\ (2,\ 1),\ (2,\ 3),\ (2,\ 4),\ (3,\ 2),\ (3,\ 3),\ (4,\ 2),\ (4,\ 4)\}$.

Las matrices cuadradas son utilizadas para determinar si las relaciones tienen ciertas propiedades. Ellas son:

- La propiedad de reflexividad: si la diagonal principal esta compuesta de unos.

$$\begin{bmatrix} 1 & & & & \\ & 1 & & & \\ & & \ddots & & \\ & & & 1 & \\ & & & & 1 \end{bmatrix}$$

Recordar que R es reflexiva si únicamente si $(a_i,\ a_i) \in R$ para $i = 1,\ 2,\ 3,\ \ldots,\ n$

- La propiedad de Simetría.

$$\begin{bmatrix} & & 1 & & \\ & \nearrow & & & \\ 1 & & \ddots & & 0 \\ & & & \nearrow & \\ & & 0 & & \end{bmatrix}$$

Recordar que R es simétrica si y únicamente si $(a,\ b) \in R$ si $M_r = (M_r)^t$ entonces R es simétrica

- La propiedad de Antisimetría.

$$\begin{bmatrix} & & 1 & & \\ & \nearrow & & 0 & \\ 0 & & \nearrow & & 0 \\ & 0 & & \nearrow & \\ & & 1 & & \end{bmatrix}$$

Recordar que R es antisimétrica si y únicamente si $(a,\ b) \in R$ y $(b,\ a) \in R$ implica que $a = b$

Ejemplo 20:

Suponer que la relación R en un conjunto es representada por la matriz:

$$M_r = \begin{bmatrix} 1 & 1 & 0 \\ 1 & 1 & 1 \\ 0 & 1 & 1 \end{bmatrix}$$

La relación R es reflexiva.

La relación R es simétrica.

La relación R no es antisimétrica.

Las operaciones de unión e intersección de relaciones se pueden realizar con la representación en matrices
$M_{R_1 \cup R_2} = M_{R_1} \vee M_{R_2}$
$M_{R_1 \cap R_2} = M_{R_1} \wedge M_{R_2}$

Ejemplo 21:

Las relaciones R_1 y R_2 en un conjunto A son representados por las matrices

$$M_{R_1} = \begin{bmatrix} 1 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix} \qquad \text{y} \qquad M_{R_2} = \begin{bmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \\ 1 & 0 & 0 \end{bmatrix}$$

$$M_{R_1 \cup R_2} = M_{R_1} \vee M_{R_2} = \begin{bmatrix} 1 & 0 & 1 \\ 1 & 1 & 1 \\ 1 & 1 & 0 \end{bmatrix}$$

$$M_{R_1 \cap R_2} = M_{R_1} \wedge M_{R_2} = \begin{bmatrix} 1 & 0 & 1 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix}$$

La composición de relaciones que son representadas por medio de matrices es $M_{S \circ R} = M_r \odot M_s$, donde $\odot$ es la multiplicación de matrices binarias.

Ejemplo 22:

Encontrar la matriz que represente la relación $S \circ R$ donde las matrices que representa R y S son:

$$M_R = \begin{bmatrix} 1 & 0 & 1 \\ 1 & 1 & 0 \\ 0 & 0 & 0 \end{bmatrix} \qquad \text{y} \qquad M_S = \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 1 \end{bmatrix}$$

$$M_{S \circ R} = M_R \odot M_S = \begin{bmatrix} 1 & 1 & 1 \\ 0 & 1 & 1 \\ 0 & 0 & 0 \end{bmatrix}$$

La matriz que representa la composición de dos relaciones puede ser usada para encontrar la matriz de M_{R^n}. En particular $M_{R^n} = M_R^n$

Ejemplo 23:

Encontrar la matriz que representa la relación R^2, donde la matriz que representa la relación R es:

$$M_R = \begin{bmatrix} 0 & 1 & 0 \\ 0 & 1 & 1 \\ 1 & 0 & 0 \end{bmatrix}$$

El resultado es el siguiente:

$$M_{R^2} = M_R^2 = M_R \odot M_R = \begin{bmatrix} 0 & 1 & 1 \\ 1 & 1 & 1 \\ 0 & 1 & 0 \end{bmatrix}$$

7.8. Ejercicios

1. Sean los conjuntos $A = \{2,\ 3,\ 4,\ 5,\ 6\}$ y $B = \{15,\ 16,\ 17,\ 18,\ 19,\ 20\}$, listar los elementos de la relación $R \subseteq A \times B$ donde aRb si a divide (exactamente) a b.

2. Sea el conjunto $A = \{1,\ 2,\ 3,\ 4,\ 5,\ 6,\ 7\}$ sobre el cual está definida la relación $R = \{(a,\ b) \mid a - b \text{ es múltiplo de } 3\}$. Para la relación R contestar las siguientes preguntas

   a) ¿Cuáles son los pares ordenados de $|A \times A|$ que pertenecen a la relación R?

   b) ¿La relación R tiene la propiedad de reflexividad?

   c) ¿La relación R tiene la propiedad de simetría?

   d) ¿La relación R tiene la propiedad de antisimetría?

   e) ¿La relación R tiene la propiedad de transitividad?

3. Sean A y B conjuntos con $|B| = 3$. Si hay 4096 relaciones de A a B, ¿cuál es el valor de $|A|$?

4. Sean los conjuntos $A = \{1,\ 3,\ 5\}$ y $B = \{2,\ 4,\ 6,\ 8\}$, determinar

   a) $A \times B$

   b) $|A \times B|$

   c) El número de relaciones de A a B

   d) El número de relaciones binarias en A

   e) El número de relaciones de A a B que contenga $(1,\ 2)$ y $(3,\ 4)$

   f) El número de relaciones de A a B que contenga exactamente cuatro pares ordenados

   g) El número de relaciones binarias en A que contenga como mínimo cinco pares ordenados

5. Sean las siguientes relaciones definidas en el conjunto $A = \{1,\ 2\}$

$R_1 = \{\}$
$R_2 = \{(1,\ 1)\}$
$R_3 = \{(1,\ 2)\}$
$R_4 = \{(2,\ 1)\}$
$R_5 = \{(2,\ 2)\}$
$R_6 = \{(1,\ 1),\ (1,\ 2)\}$
$R_7 = \{(1,\ 1),\ (2,\ 1)\}$
$R_8 = \{(1,\ 1),\ (2,\ 2)\}$
$R_9 = \{(1,\ 2),\ (2,\ 1)\}$
$R_{10} = \{(1,\ 2),\ (2,\ 2)\}$
$R_{11} = \{(2,\ 1),\ (2,\ 2)\}$

$R_{12} = \{(1,\ 1),\ (1,\ 2),\ (2,\ 1)\}$
$R_{13} = \{(1,\ 1),\ (1,\ 2),\ (2,\ 2)\}$
$R_{14} = \{(1,\ 1),\ (2,\ 1),\ (2,\ 2)\}$
$R_{15} = \{(1,\ 2),\ (2,\ 1),\ (2,\ 2)\}$
$R_{16} = \{(1,\ 1),\ (1,\ 2),\ (2,\ 1),\ (2,\ 2)\}$

a) ¿Cuáles de las relaciones cumplen la propiedad de reflexividad?
b) ¿Cuáles de las relaciones cumplen la propiedad de simetría?
c) ¿Cuáles de las relaciones cumplen la propiedad de antisimetría?
d) ¿Cuáles de las relaciones cumplen la propiedad de transitividad?

6. Sea el conjunto $A = \{1,\ 2,\ 3\}$.

   a) ¿Cuántas relaciones hay en el conjunto A?
   b) ¿Cuántas relaciones hay en el conjunto A que sean reflexivas?
   c) ¿Cuántas relaciones hay en el conjunto A que sean simétricas?
   d) ¿Cuántas relaciones hay en el conjunto A que sean antisimétricas?
   e) ¿Cuántas relaciones hay en el conjunto A que sean transitivas?

7. Sea R una relación del conjunto A al conjunto B. La relación inversa de B a A, denotada por R^{-1}, es el conjunto de los pares ordenados $\{(b,\ a) \mid (a,\ b) \in R\}$. La relación complemento $\overline{R}$ es el conjunto de pares ordenados $\{(a,\ b) \mid (a,\ b)$ no pertenece a $R\}$. Calcular R^{-1} y $\overline{R}$ para:

   a) $R = \{(a,\ b) \mid a < b\}$ en el conjunto de los números enteros.
   b) $R = \{(a,\ b) \mid a$ divide a $b\}$ en el conjunto de los números enteros.
   c) R la relación en el conjunto de todos los departamentos de Colombia, la relación R consiste de todos los pares ordenados $(a,\ b)$ donde el departamento a limita con el departamento b.
   d) $R = \{(a,\ b) \mid a + b \leq 3\}$ en el conjunto de los números enteros.
   e) $R = \{(1,\ 2),\ (1,\ 3),\ (1,\ 4),\ (1,\ 5),\ (2,\ 3),\ (2,\ 4),\ (2,\ 5),\ (3,\ 4),\ (3,\ 5),\ (4,\ 5)\}$, en el conjunto $A = \{1,\ 2,\ 3,\ 4,\ 5\}$.
   f) $R = \{(1,\ 1),\ (1,\ 2),\ (2,\ 1),\ (2,\ 2),\ (3,\ 3),\ (4,\ 4),\ (4,\ 5),\ (5,\ 4),\ (5,\ 5),\ (6,\ 6)\}$, en el conjunto $A = \{1,\ 2,\ 3,\ 4,\ 5,\ 6\}$

8. Sea R la relación en el conjunto $\{1,\ 2,\ 3,\ 4,\ 5\}$ que contiene los pares ordenados $(1,\ 2)$, $(1,\ 3)$, $(2,\ 3)$, $(2,\ 4)$, $(3,\ 1)$, $(3,\ 4)$, $(3,\ 5)$, $(4,\ 2)$, $(4,\ 5)$, $(5,\ 1)$, $(5,\ 2)$ y $(5,\ 4)$. Calcular:

   a) R^2
   b) R^3
   c) R^4
   d) R^5

Capítulo 8

Relaciones de equivalencia

Definición (Relación de Equivalencia):

Una relación en un conjunto A es llamada una relación de equivalencia si ésta es reflexiva, simétrica y transitiva.

Dos elementos que son relacionados por una relación de equivalencia son llamados equivalentes.

Ejemplo 1:

Supóngase que R es una relación en el conjunto de las cadenas escritas con el alfabeto español tales que aRb si y únicamente si $l(a) = l(b)$ donde $l(x)$ es la longitud de la cadena x. ¿Es R una relación de equivalencia?.

Para que R sea una relación de equivalencia ésta tiene que ser reflexiva, simétrica y transitiva.

Reflexiva: $l(a) = l(a)$, de ésta forma aRa, por lo tanto R es reflexiva.

Simétrica: aRb lo que indica que $l(a) = l(b)$ como $l(b) = l(a)$ esto indica que bRa por lo tanto R es simétrica.

Transitiva: suponer que aRb y bRc, entonces $l(a) = l(b)$ y $l(b) = l(c)$, donde se obtiene que $l(a) = l(c)$, por lo tanto R es transitiva.

Como la relación R es reflexiva, simétrica y transitiva, entonces es una relación de equivalencia.

Ejemplo 2:

Sea R la relación en el conjunto de los números reales tales que aRb si y solo si, $a - b$ es un entero. ¿Es R una relación de equivalencia?

Para que R sea una relación de equivalencia ésta tiene que ser reflexiva, simétrica y transitiva.

Reflexiva: $a - a = 0$ que es un número entero para todos los números reales a. Así aRa. La relación R si es reflexiva.

Simétrica: Suponer que aRb, entonces $a - b$ es un número entero, también se tiene que $b - a$ es un número entero y se obtiene entonces bRa, de ésta forma se obtiene la propiedad de simetría en la relación R.

Transitiva : si aRb y bRc, entonces $a-b$ y $b-c$ son enteros, además $a-c = (a-b)+(b-c)$ que es también un entero, lo que conduce a tener aRc. Por lo tanto R es transitiva.

Como la relación R es reflexiva, simétrica y transitiva, entonces R es una relación de equivalencia.

Ejemplo 3: (Congruencia módulo m)

Sea m un entero positivo con $m > 1$, mostrar que la relación
$R = \{(a,\ b) \mid a \equiv b\ (mod\ m)\}$ es una relación de equivalencia en el conjunto de los números enteros.

Recordar que $a \equiv b\ (mod\ m)$ si y solo si m divide exactamente a $a - b$.

Reflexiva: $aRa,\ a \equiv a\ (mod\ m),\ a - a = 0$, cero es divisible exactamente por m por lo tanto la relación R es reflexiva.

Simétrica: Ahora suponer que $aRb,\ a \equiv b\ (mod\ m),\ a - b = k \cdot m$, de este modo $a - b$ es divisible por m. entonces $b - a = (-k) \cdot m$, por lo tanto bRa $(b \equiv a\ (mod\ m))$. De ésta forma la relación de congruencia módulo m es simétrica.

Transitividad: Si aRb y bRc es porque $a \equiv b\ (mod\ m)$ y $b \equiv c\ (mod\ m)$, por lo tanto el número entero m divide exactamente a $a - b$ y a $b - c$, de esta forma:
$a - b = k \cdot m$ y $b - c = l \cdot m$, donde $k,\ l \in \mathbb{Z}$

$$\begin{aligned} a - c &= a - c - b + b \\ &= (a - b) + (b - c) \\ &= k \cdot m \ + \ l \cdot m \\ &= (k + l) \cdot m \\ &= j \cdot m, \quad \text{donde } j = k + l,\ j \in \mathbb{Z}. \end{aligned}$$

como $a - c = j \cdot m$ entonces se cumple que $a \equiv c\ (mod\ m)$, de ésta forma se cumple que la relación R tiene la propiedad de transitividad.

Como la relación R es reflexiva, simétrica y transitiva entonces R es una relación de equivalencia.

8.1. Clases de equivalencia

Definición (Clase de equivalencia):

Sea R una relación de equivalencia en un conjunto A. El conjunto de todos los elementos que están relacionados con el elemento a (para $a \in A$) es llamada la clase de equivalencia de a. La clase de equivalencia de a con respecto a la relación de equivalencia R es denotada con $[a]_R$.

En otras palabras, si R es una relación de equivalencia en un conjunto A, la clase de equivalencia del elemento a es:

$$[a]_R = \{s \mid (a,\ s) \in R\}$$

Si $b \in [a]_R$, entonces b es llamado representante de ésta clase de equivalencia. Cualquier elemento de una clase de equivalencia puede representarla.

Ejemplo 4:

¿Cuál es la clase de equivalencia para el número 0 en la relación $a \equiv b\ (mod\ 4)$?

La clase de equivalencia del 0 contiene todos los números enteros a tales que $a \equiv 0\ (mod\ 4)$, es decir, contiene todos los números enteros a que son divisibles de forma exacta por 4.

$[0] = \{\ldots,\ -8,\ -4,\ 0,\ 4,\ 8,\ \ldots\}$

8.2. Clases de equivalencia y particiones

Teorema:

Sea R una relación de equivalencia en un conjunto A. Los siguientes tres ítems son equivalentes:

1. aRb
2. $[a]_R = [b]_R$
3. $[a]_R \cap [b]_R \neq \emptyset$

Sea R una relación de equivalencia en un conjunto A. La unión de todas las clases de equivalencia de R da como resultado el conjunto A

$$\bigcup_{a \in A} [a]_R = A$$

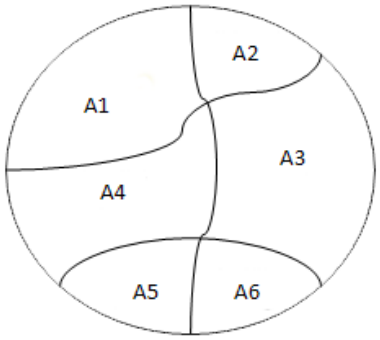
Si $[a]_R \cap [b]_R = \emptyset$ entonces $[a]_R \neq [b]_R$.

Las observaciones anteriores muestran que las clases de equivalencia forman una *partición* del conjunto A, donde ellas fraccionan al conjunto A en subconjuntos disyuntos. Más precisamente, una partición de un conjunto S es una colección de subconjuntos no vacíos disyuntos de S que tienen a S como su unión. En otras palabras, la colección de subconjuntos A_i, $i \in I$ (donde I es el conjunto de índices) forma una partición de conjunto S si y solo si $A_i \neq \emptyset$ para $i \in I$, $A_i \cap A_j = \emptyset$ cuando $i \neq j$, y $\bigcup_{i \in I} A_i = S$

Ejemplo 5:

Sea el conjunto $S = \{1,\ 2,\ 3,\ 4,\ 5,\ 6\}$. La colección de conjuntos $A_1 = \{1,\ 2,\ 3\}$, $A_2 = \{4,\ 5\}$ y $A_3 = \{6\}$ forman una partición del conjunto S, donde estos conjuntos son disyuntos y su unión es el conjunto S.

Los subconjuntos en una partición son clases de equivalencia.
Dos elementos son equivalentes con respecto a la relación si y únicamente si ellos están en el mismo subconjunto de la partición.



Teorema:

Sea R una relación de equivalencia en un conjunto S. Entonces las clases de equivalencia de R forman una partición de S. Así mismo, dada una partición $\{A_i \mid i \in I\}$ del conjunto S, hay una relación de equivalencia R que tiene el conjunto A_i, $i \in I$, como clase de equivalencia.

Ejemplo 6:

Listar los pares ordenados en la relación de equivalencia R producidos por la partición $A_1 = \{1,\ 2,\ 3\},\ A_2 = \{4,\ 5\}$ y $A_3 = \{6\}$ del conjunto $S = \{1,\ 2,\ 3,\ 4,\ 5,\ 6\}$

Los subconjuntos en la partición son clases de equivalencia de R, donde el par ordenado $(a,\ b) \in R$ si y solo si a y b están en el mismo subconjunto de la partición.

- Pares ordenados que aparecen en la relación de equivalencia R gracias a los elementos de la partición (o clase de equivalencia) A_1: $(1,\ 1)$, $(1,\ 2)$, $(1,\ 3)$, $(2,\ 1)$, $(2,\ 2)$, $(2,\ 3)$, $(3,\ 1)$, $(3,\ 2)$ y $(3,\ 3)$.

- Pares ordenados que aparecen en la relación de equivalencia R gracias a los elementos de la partición (o clase de equivalencia) A_2: $(4,\ 4)$, $(4,\ 5)$, $(5,\ 4)$ y $(5,\ 5)$

- Pares ordenados que aparecen en la relación de equivalencia R gracias a los elementos de la partición (o clase de equivalencia) A_3: $(6,\ 6)$

De esta forma la relación de equivalencia R contiene únicamente los siguientes pares ordenados:

$$R = \{(1,\ 1),\ (1,\ 2),\ (1,\ 3),\ (2,\ 1),\ (2,\ 2),\ (2,\ 3),\ (3,\ 1),\ (3,\ 2),\ (3,\ 3), (4,\ 4),\ (4,\ 5),\ (5,\ 4),\ (5,\ 5),\ (6,\ 6)\}$$

Hay m diferentes clases de congruencia módulo m, correspondientes a los m diferentes residuos posibles cuando un entero es dividido por m. Estas m clases de congruencia son denotadas por $[0]_m,\ [1]_m,\ \ldots,\ [m-1]_m$. Ellos forman una partición del conjunto de los enteros.

Ejemplo 7:

¿Cuales son los conjuntos en la partición de los números enteros para la relación $a \equiv b\ (mod\ 4)4$?

Hay cuatro clases de congruencia correspondientes a $[0]_{\equiv\ (mod\ 4)}$, $[1]_{\equiv\ (mod\ 4)}$, $[2]_{\equiv\ (mod\ 4)}$ y $[3]_{\equiv\ (mod\ 4)}$, ellas son los conjuntos:

$$[0]_{\equiv\ (mod\ 4)} = \{\ldots,\ -8,\ -4,\ 0,\ 4,\ 8,\ \ldots\}$$

$$[1]_{\equiv\ (mod\ 4)} = \{\ldots,\ -7,\ -3,\ 1,\ 5,\ 9,\ \ldots\}$$

$$[2]_{\equiv\ (mod\ 4)} = \{\ldots,\ -6,\ -2,\ 2,\ 6,\ 10,\ \ldots\}$$

$$[3]_{\equiv\ (mod\ 4)} = \{\ldots,\ -5,\ -1,\ 3,\ 7,\ 11,\ \ldots\}$$

Las clases de congruencia son disyuntas, y cada número entero está exactamente una sola de ellas.

8.3. Conjuntos parcialmente ordenados

Una relación $R \subseteq S \times S$ genera un ordenamiento parcial en el conjunto S si ésta cumple las propiedades de reflexividad, antisimetría y transitividad. Un conjunto S que es parcialmente ordenado con respecto a la relación R es denotado por $(S,\ R)$.

Ejemplo 8:

¿La relación "mayor o igual que" ($\geq$) genera un ordenamiento parcial en el conjunto de los números enteros?

Para dar respuesta a este interrogante primero se deben analizar las propiedades de reflexividad, antisimetría y transitividad de la relación, para esto se tiene:

Reflexiva: Sea $a \in \mathbb{Z}$, como cualquier número entero es mayor o igual a él mismo $(a \geq a)$ entonces aRa, de donde se concluye que la relación R tiene la propiedad de reflexividad.

Antisimétrica: Sea $a,\ b \in \mathbb{Z}$, si aRb es porque $(a \geq b)$ y si bRa es porque $(b \geq a)$, la única forma de que se presente al mismo tiempo aRb y bRa es cuando $a = b$, con lo cual se cumple la propiedad de antisimetría en la relación R.

Transitiva: Sea $a,\ b,\ c \in \mathbb{Z}$, si aRb y bRc es porque $(a \geq b)$ y $(b \geq c)$ de donde se obtiene que $(a \geq c)$ con lo cual se cumple que aRc, con lo cual se concluye que la relación R cumple la propiedad de transitividad.

Como la relación "mayor o igual que" cumple las propiedades reflexiva, antisimétrica y transitiva entonces la relación genera un ordenamiento parcial en el conjunto de los números enteros, o expresado de una forma equivalente $(\mathbb{Z}, \geq)$ es un conjunto parcialmente ordenado.

Ejemplo 9:

¿La relación divisibilidad ($\mid$) genera un ordenamiento parcial en el conjunto de los números enteros positivos?

Sea R la relación de divisibilidad, $R = \{(a,\ b) \mid a,\ b,\ m \in \mathbb{Z}^+ \wedge b = m \cdot a\}$, en palabras, aRb o $(a, b) \in R$ si a divide de forma exacta a b. La relación de divisibilidad R genera un ordenamiento parcial en el conjunto de los números enteros positivos si cumple las propiedades de reflexividad, antisimetría y transitividad. En el análisis de estas propiedades se tiene:

Reflexiva: Sea el número $a \in \mathbb{Z}^+$, a divide de forma exacta a a y se obtiene como resultado el número entero 1, sea cual sea el número entero positivo a, aRa, por lo tanto la relación de divisibilidad cumple la propiedad de reflexividad.

Antisimétrica: Sean los números $a,\ b \in \mathbb{Z}^+$, si aRb es porque a divide de forma exacta a b y si bRa es porque b divide de forma exacta a a, la única forma de que se presente al mismo tiempo aRb y bRa es cuando $a = b$, con lo cual se cumple la propiedad de antisimetría en la relación de divisibilidad.

Transitiva: Sean los números $a,\ b,\ c \in \mathbb{Z}^+$, si aRb es porque $b = m \cdot a$ para $m \in \mathbb{Z}^+$ y si bRc es porque $c = n \cdot b$ para $n \in \mathbb{Z}^+$, como $b = m \cdot a$ entonces $c = n \cdot (m \cdot a) = (n \cdot m) \cdot a = p \cdot a$ para $p = n \cdot m$ donde $p \in \mathbb{Z}^+$, como $c = p \cdot a$ entonces a divide de forma exacta a c, es decir aRc, de esta forma la relación de divisibilidad cumple la propiedad de transitividad.

Como la relación de "divisibilidad" cumple las propiedades reflexiva, antisimétrica y transitiva entonces la relación genera un ordenamiento parcial en el conjunto de los números enteros positivos, o expresado de una forma equivalente $(\mathbb{Z}^+,\ |\ )$ es un conjunto parcialmente ordenado.

Ejemplo 10:

Mostrar que la relación de inclusión $(\subseteq)$ genera un ordenamiento parcial en el conjunto potencia de un conjunto S.

Recordar que el conjunto potencia de un conjunto S, es el conjunto que contiene todos los subconjuntos que se encuentran presentes en el conjunto S, la notación que se utiliza para representar dicho conjunto es $\mathcal{P}(S)$.

Sea $R = \{(A,\ B) \mid A,\ B \in \mathcal{P}(S) \wedge A \subseteq B\}$ para S que es un conjunto, la relación R es de orden parcial si cumple las propiedades de reflexividad, antisimetría y transitividad. En el análisis de las propiedades se tiene:

Reflexiva: Sea el conjunto $A \in \mathcal{P}(S)$, $A \subseteq A$, el conjunto A esta contenido en el conjunto A, por lo tanto se cumple la propiedad de reflexividad donde $(A,\ A) \in R$.

Antisimétrica: Sean los conjuntos $A,\ B \in \mathcal{P}(S)$, si $(A,\ B) \in R$ es porque $A \subseteq B$ y si $(B,\ A) \in R$ es porque $B \subseteq A$, la única posibilidad de que se presente al mismo tiempo $(A,\ B) \in R$ y $(B,\ A) \in R$ es cuando $A = B$, con lo cual la relación R cumple la propiedad de antisimetría.

Transitiva: Sean los conjuntos $A,\ B,\ C \in \mathcal{P}(S)$, si $(A,\ B) \in R$ y $(B,\ C) \in R$ es porque $A \subseteq B$ y $B \subseteq C$ de donde se deduce que $A \subseteq C$ lo que garantiza que $(A,\ C) \in R$, con lo cual la relación R cumple la propiedad de transitividad.

Como la relación de inclusión cumple las propiedades de reflexividad, antisimetría y transitividad, entonces el conjunto potencia es un conjunto parcialmente ordenado con respecto a la relación de inclusión, o expresado de una forma equivalente $(\mathcal{P}(S),\ \subseteq)$ es un conjunto parcialmente ordenado.

Definición:

Sea una relación $R \subseteq S \times S$, si la relación R genera un orden parcial sobre el conjunto S, para $a,\ b \in S$ se dice que los elementos a y b son comparables si $(a,\ b) \in R$ o $(b,\ a) \in R$. Cuando $(a,\ b) \notin R$ y $(b,\ a) \notin R$ se dice que los elementos a y b son incomparables.

Ejemplo 11:

En un ejemplo anterior ya se demostró que la relación de divisibilidad genera un orden parcial sobre el conjunto de los números enteros positivos, lo que es representado como $(\mathbb{Z}^+, \mid)$. ¿Son los números 2 y 4 comparables en $(\mathbb{Z}^+, \mid)$?, ¿son los números 5 y 2 comparables en $(\mathbb{Z}^+, \mid)$?

Para dar respuesta a las preguntas se tiene:

- Se cumple que $2,\ 4 \in \mathbb{Z}^+$ y que $(2,\ 4) \in R$ porque el número 2 divide de forma exacta al número 4, por este motivo los números 2 y 4 son comparables sobre $(\mathbb{Z}^+, \mid)$.
- Se cumple que $5,\ 2 \in \mathbb{Z}^+$, pero, $(5,\ 2) \notin R$ porque el número 5 no divide de forma exacta al número 2 y $(2,\ 5) \notin R$ porque el número 2 no divide de forma exacta al número 5, como $(5,\ 2) \notin R$ y $(2,\ 5) \notin R$ entonces los números 2 y 5 son incomparables sobre $(\mathbb{Z}^+, \mid)$.

Definición:

Sea una relación $R \subseteq S \times S$. La relación R genera un orden total en un conjunto S cuando ésta cumple las propiedades de reflexividad, antisimetría y transitividad, y adicionalmente, para cualquier par de elementos $a,\ b \in S$, a y b tienen que ser comparables.

En esta definición se exige que para que una relación R genere un orden total sobre un conjunto S, primero, la relación tiene que generar un orden parcial sobre el conjunto S, y luego se tiene que cumplir que cualquier par de elementos a y b del conjunto S sean comparables.

Ejemplo 12:

¿La relación de divisibilidad genera un orden total en el conjunto de los números enteros positivos?

En un ejemplo anterior ya se demostró que la relación de divisibilidad genera un orden parcial sobre $\mathbb{Z}^+$, pero, no genera un orden total sobre $\mathbb{Z}^+$ porque existen pares ordenados de $\mathbb{Z}^+ \times \mathbb{Z}^+$ que son incomparables, por ejemplo los números 3 y 10 son incomparables.

Ejemplo 13:

¿La relación "mayor o igual que" genera un orden total en el conjunto de los números enteros?

En un ejemplo anterior ya se demostró que la relación "mayor o igual que" genera un orden parcial sobre $\mathbb{Z}$, ahora lo que hace falta es analizar si para cualquier par de números $a,\ b \in \mathbb{Z}$, a y b son comparables, para esto obligatoriamente se tiene que cumplir que $a \geq b$ o $b \geq a$, donde aRb o bRa con lo cual se cumple que cualquier par de números enteros a y b son comparables, por lo tanto la relación "mayor o igual que" genera un orden total sobre el conjunto de los números enteros.

8.4. Ejercicios

1. Demostrar o refutar que la relación $R = \{(a,\ b) \mid a - b \text{ es par}\}$ es una relación de equivalencia en el conjunto de los números enteros.

2. Demostrar o refutar que la relación $R = \{(a, b) \mid a \neq b\}$ es una relación de equivalencia en el conjunto de los números enteros.

3. Sea R una relación de equivalencia, ¿Qué se obtiene como resultado de $R \circ R$?.

4. Sea la siguiente relación en el conjunto de todas las personas del mundo, $R = \{(a,\ b) \mid\ a$ y b tienen el mismo año de nacimiento$\}$, ¿es R una relación de equivalencia?, si R es una relación de equivalencia, ¿Cuáles y cuántas son las clases de equivalencia?

5. Sea la siguiente relación en el conjunto de todas las personas del mundo, $R = \{(a,\ b) \mid\ a$ y b tienen la misma fecha de cumpleaños $\}$, ¿es R una relación de equivalencia?, si R es una relación de equivalencia, ¿Cuáles y cuántas son las clases de equivalencia?

   Nota: El hecho de que dos personas tengan la misma fecha de cumpleaños no indica que las dos personas tengan la misma fecha de nacimiento, por ejemplo Carlos y Manuel cumplen años el 22 de Julio, pero la fecha de nacimiento de Carlos es el 22 de Julio de 1968 mientras la fecha de nacimiento de Manuel es el 22 de Julio de 1975.

6. Sea la siguiente relación en el conjunto de todas las personas del mundo, $R = \{(a,\ b) \mid\ a$ y b tienen al menos un mismo padre en común$\}$, ¿es R una relación de equivalencia?, si R es una relación de equivalencia, ¿Cuáles y cuántas son las clases de equivalencia?

7. Sea la siguiente relación en el conjunto de todas las personas del mundo, $R = \{(a,\ b) \mid\ a$ y b hablan un lenguaje en común$\}$, ¿es R una relación de equivalencia?, si R es una relación de equivalencia, ¿Cuáles y cuántas son las clases de equivalencia?

8. Demostrar o refutar que la relación R en $\mathbb{Z}^+$ es un relación de equivalencia, donde R es definida por $a\ R\ b$ si y únicamente si $\tau(a) = \tau(b)$, donde $\tau(a)$ es igual al número de divisores positivos de a. Por ejemplo ${}_2R_3$ y ${}_4R_{25}$.

9. Demostrar o refutar que la relación R en $\mathbb{N}$ es un relación de equivalencia, donde R es definida por $a\ R\ b$ si y únicamente si $\tau(a) = \tau(b)$, donde $\tau(a)$ es igual al número de cifras del número a. Por ejemplo ${}_2R_3$ y ${}_{52}R_{25}$.

10. Demostrar o refutar que la relación R en $\mathbb{Z}^+$ es un relación de equivalencia, donde R es definida por $a\ R\ b$ si y únicamente si $\tau(a) = \tau(b)$, donde $\tau(a)$ es igual al número de dígitos diferentes que conforman al número a. Por ejemplo $\tau(100) = 2$, $\tau(123) = 3$, $\tau(1020) = 3$ y $\tau(10000) = 2$, por lo tanto ${}_{123}R_{1020}$ y ${}_{100}R_{10000}$.

11. Demostrar o refutar que la relación R en $\mathbb{N}$ es un relación de equivalencia, donde R es definida por $a\ R\ b$ si y únicamente si $\tau(a) = \tau(b)$, donde $\tau(a)$ devuelve el dígito menos significativo del número a. Por ejemplo $\tau(522) = 2$, $\tau(43) = 3$ y $\tau(7) = 7$, de esta forma, ${}_{52}R_{112}$ y ${}_{1000}R_{30}$.

12. Demostrar o refutar que la relación R en $\mathbb{N}$ es un relación de equivalencia, donde R es definida por $a\ R\ b$ si y únicamente si $\tau(a) = \tau(b)$, donde $\tau(a)$ devuelve la suma de las cifras que componen al número a. Por ejemplo $\tau(522) = 9$, $\tau(43) = 7$ y $\tau(7) = 7$, de esta forma, ${}_{52}R_{142}$ y ${}_{1000}R_{1}$.

13. Sea R la relación en el conjunto de pares ordenados de enteros positivos tales que $((a,\ b),\ (c,\ d)) \in R$ si y únicamente si $ad = bc$. ¿Es R una relación de equivalencia?, si es así, ¿cuál es la clase de equivalencia de $(1,\ 2)$?

14. Sea R la relación en el conjunto de pares ordenados de enteros positivos tales que $((a,\ b),\ (c,\ d)) \in R$ si y únicamente si $a + d = b + c$. ¿Es R una relación de equivalencia?, si es así, ¿cuál es la clase de equivalencia de $(1,\ 2)$?

15. Sea R la relación en el conjunto de pares ordenados de enteros positivos tales que $((a,\ b),\ (c,\ d)) \in R$ si y únicamente si $a - d = b - c$. ¿Es R una relación de equivalencia?, si es así, ¿cuál es la clase de equivalencia de $(1,\ 2)$?

16. Sea R la relación en el conjunto de pares ordenados de enteros positivos tales que $((a,\ b),\ (c,\ d)) \in R$ si y únicamente si $\frac{a}{d} = \frac{c}{b}$. ¿Es R una relación de equivalencia?, si es así, ¿cuál es la clase de equivalencia de $(2,\ 5)$?

17. Sea R la relación en el conjunto de pares ordenados de enteros positivos tales que $((a,\ b),\ (c,\ d)) \in R$ si y únicamente si $a = c$. ¿Es R una relación de equivalencia?, si es así, ¿cuál es la clase de equivalencia de $(1,\ 4)$?, y, ¿cómo se representada dicha clase de equivalencia en el plano cartesiano?

18. Demostrar o refutar que la relación $R = \{(a, b) \mid a > b\}$ genera un ordenamiento parcial en el conjunto de los números enteros.

19. Demostrar o refutar que la relación $R = \{(a, b) \mid a < b\}$ genera un ordenamiento parcial en el conjunto de los números enteros.

20. Demostrar o refutar que la relación $R = \{(a, b) \mid a \leq b\}$ genera un ordenamiento parcial en el conjunto de los números enteros.

Capítulo 9

Introducción a la teoría de números

9.1. Los números enteros y la división

9.1.1. Introducción

Las matemáticas discretas involucran a los números enteros y sus propiedades dentro de un campo que se llama Teoría de Números.

9.1.2. División entre números enteros

Cuando un número entero es dividido por un segundo número entero (diferente de cero), el resultado puede ser o no ser un entero. Por ejemplo $\frac{12}{3} = 4$ es un número entero, mientras que $\frac{11}{4} = 2{,}75$ no lo es. Esto conduce a la siguiente definición.

Definición: Si a y b son números enteros con $a \neq 0$, se dice que a divide a b si hay un número entero c tal que $b = ac$. Cuando a divide a b se dice que a es un factor de b y que b es un múltiplo de a. La notación $a|b$ denota que a divide b. Se escribe $a \nmid b$ cuando a no divide b.

Ejemplo 1:

Determinar si $4|9$ y si $4|20$.

Se tiene que $4 \nmid 9$ porque $\frac{9}{4} = 2{,}25$, y 2.25 no es un número entero.

Es cierto que $4|20$ porque existe el numero $c = 5$ el cual hace que $20 = 4 \cdot 5$.

Ejemplo 2:

Sean n y d enteros positivos. ¿Cuántos enteros positivos no exceden a n y son divisibles por d?

Los números enteros positivos divisibles por d son todos los enteros de la forma $d \cdot k$, donde k es un entero positivo. Por lo tanto, el número de enteros positivos divisibles por d que no exceden a n es igual al número de enteros k con $0 < d \cdot k \leq n$, o con $0 < k \leq \frac{n}{d}$, por lo tanto, hay un total de $\lfloor \frac{n}{d} \rfloor$ números enteros positivos que no exceden a n y que son divisibles por d.

Algunas de las propiedades básicas de divisibilidad de los números enteros son presentadas en el siguiente teorema.

Teorema:

Sean a, b y c números enteros. Entonces:

1. Si $a|\ b$ y $a|c$ entonces $a|(b+c)$
2. Si $a|\ b$ entonces $a|bc$ para todo entero c
3. Si $a|\ b$ y $b|c$ entonces $a|c$
4. Si $a|\ b$ y $a|c$ entonces $a|(mb+nc)$ donde m y n son enteros.

Para demostrar cada uno de los ítems del teorema se hará uso de la técnica de demostración directa y de la definición de división entre números enteros, donde se tiene:

1. Si $a|\ b$ y $a|c$ entonces $a|(b+c)$.

   Si $a|\ b$ es porque existe un número entero p tal que $b = a \cdot p$, si $a|c$ es porque existe un número q tal que $c = a \cdot q$, se tiene que $b + c = a \cdot p + a \cdot q$, $b + c = a \cdot (p + q)$, por lo tanto a partir de la definición de división entre números enteros se tiene que $a|(b + c)$ porque $b + c = a \cdot (p + q)$.

2. Si $a|\ b$ entonces $a|bc$ para todo entero c.

   Tenemos que si $a|\ b$ es porque existe un número entero p tal que $b = a \cdot p$, de este modo se tiene que $a|bc$ puede transformarse en $a|a \cdot p \cdot c$ con lo cual se obtiene que $b \cdot c$ es múltiplo de a por lo tanto $b \cdot c$ puede dividirse por a.

3. Si $a|\ b$ y $b|c$ entonces $a|c$.

   Si $b|\ c$ es porque existe un número entero p tal que $c = b \cdot p$, como se tiene que $a|b$ entonces existe un número entero q tal que $b = a \cdot q$, reemplazando el valor de b en $c = b \cdot p$ se tiene que $c = a \cdot q \cdot p$ donde c es un múltiplo de a, por lo tanto $a|c$.

4. Si $a|\ b$ y $a|c$ entonces $a|(mb+nc)$ donde m y n son enteros.

   Si $a|\ b$ es porque existe un número entero p tal que $b = a \cdot p$, si $a|c$ es porque existe un número q tal que $c = a \cdot q$, entonces $m \cdot b + n \cdot c = m \cdot a \cdot p + n \cdot a \cdot q = a \cdot (m \cdot p + n \cdot q)$ de donde se obtiene que $m \cdot b + n \cdot c$ es múltiplo de a por lo tanto $a|(mb + nc)$.

9.1.3. El algoritmo de la división entre números enteros

Cuando un número entero es dividido por un número entero positivo, hay un cociente y un residuo. En el Algoritmo de la División sea a un número entero y d un número entero positivo, entonces hay unos únicos enteros q y r, con $0 \leq r < d$, tal que $a = d \cdot q + r$. En la igualdad, d es llamado el divisor, a es llamado el dividendo, q es llamado el cociente y r es llamado el residuo.

La notación utilizada es:

- $q = a \; div \; d$, el operador *div* sirve para calcular la *parte entera* de la división entre números enteros.
- $r = a \; mod \; d$, el operador *mod* sirve para calcular el *residuo* de la división entre números enteros.

Ejemplo 3:

¿Cuál es el cociente y el residuo cuando 233 es dividido por 20?

El número 233 puede obtenerse de la siguiente forma con respecto al divisor 20,
$233 = 20 \cdot 11 + 13$

$233 \; div \; 20 = 11$, la cantidad de veces que se encuentra presente el 20 en el 233 es 11, el cual es el cociente, de donde se obtiene que $20 \cdot 11 = 220$.

$233 \; mod \; 20 = 13$, el residuo de la división entera es igual a 13, el cual también se obtiene de la siguiente manera $233 - 220 = 13$.

9.1.4. Los números primos

Cada número entero positivo mayor que 1 es divisible por al menos dos números enteros. Cuando un número entero mayor que 1 es divisible únicamente por uno (1) y por él mismo entonces este número es llamado número primo.

Definición (número primo): Un número entero positivo p más grande que uno es llamado número primo si únicamente los factores de p son 1 y p. Un número entero positivo que es más grande que 1 y no es un número primo es llamado número compuesto.

Nota: El número entero n es compuesto si y únicamente si existe un número entero a tal que $a|n$ y $1 < a < n$.

Ejemplo 4:

¿Los números 8 y 11 son números primos?

Los factores del 8 son 1, 2, 4 y 8, como se obtienen más de dos factores entonces el

número 8 no es un número primo, pero 8 si es un número compuesto.

Los únicos factores del 11 son el 1 y el 11, por lo tanto el 11 es un número primo.

9.1.5. Teorema fundamental de la aritmética

Cada número entero positivo mayor que 1 puede ser escrito únicamente con un número primo o con el producto de dos o más números primos donde los factores primos son escritos en orden creciente con respecto a su tamaño.

Ejemplos 5:

Utilizando el Teorema Fundamental de la Aritmética la representación prima de los números 100, 845, 999 y 1024 es la siguiente:

- $100 = 2 \cdot 2 \cdot 5 \cdot 5 = 2^2 \cdot 5^2$
- $845 = 5 \cdot 13 \cdot 13 = 5^1 \cdot 13^2$
- $999 = 3 \cdot 3 \cdot 3 \cdot 37 = 3^3 \cdot 37$
- $1024 = 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 = 2^{10}$

Teorema:

Si n es un número entero compuesto, entonces n tiene un divisor primo menor o igual a $\sqrt{n}$.

Se utilizará la técnica de demostración directa para demostrar la validez del teorema.

Si n es un número compuesto, éste tiene un factor a con $1 < a < n$, por lo tanto, $n = a \cdot b$, donde a y b son números enteros positivos más grandes que 1. Se tiene que $a \leq \sqrt{n}$ o $b \leq \sqrt{n}$, si no fuera así entonces $a \cdot b > \sqrt{n} \cdot \sqrt{n} = n$. Por lo tanto, n tiene un divisor positivo que no excede a $\sqrt{n}$. Este divisor o es un número primo, o, es un número compuesto, donde por el Teorema Fundamental de la Aritmética dicho divisor tiene un divisor primo. En cualquiera de los dos casos, n tiene un divisor primo que es menor o igual a $\sqrt{n}$.

Del teorema anterior se tiene que un número entero n es primo si este no es divisible por algún primo menor o igual a la raíz cuadrada de n.

Ejemplo 6:

¿El número entero 169 es un número primo?.

Utilizando el teorema anterior se tiene que si 169 es un número compuesto entonces tendrá un factor primo menor o igual a $\sqrt{169}$, como $\sqrt{169} = 13$ entonces dicho factor primo es el número 13, porque $13 * 13 = 13^2 = 169$. Por lo tanto el número 169 es un número compuesto lo que le impide ser un número primo.

Ejemplo 7:

¿El número entero 641 es un número primo?.

Utilizando de nuevo el teorema anterior se tiene que si 641 es un número compuesto entonces tendrá un factor primo menor o igual a $\sqrt{641} \cong 25{,}318$. Los únicos factores primos que son menores o iguales a 25.318 son: 2, 3, 5, 7, 11, 13, 17, 19 y 23, pero, el número 641 no es divisible por ninguno de estos factores primos, por lo tanto, el número 641 no es un número compuesto, pero, 641 si es un número primo.

El siguiente algoritmo está "inspirado " en el teorema anterior para determinar si un número es primo.

Booleano EsNumeroPrimo(n : *Entero Positivo*)
1. $d = 1$
2. $p = 3$
3. *Si* ($n = 2$ *o* $n = 3$) *Entonces*
4. *Retornar Cierto*
5. *Fin Si*
6. *Si* ($n > 3$) *Entonces*
7. *Si* ($n \ mod \ 2 = 0$) *Entonces*
8. $d = d + 1$
9. *Fin Si*
10. *Hacer Mientras* ($p \leq \lfloor \sqrt{n} \rfloor$ *y* $d = 1$)
11. *Si* ($n \ mod \ p = 0$) *Entonces*
12. $d = d + 1$
13. *Fin Si*
14. $p = p + 2$
15. *Fin Hacer Mientras*
16. *Si* ($d = 1$) *Entonces*
17. *Retornar Cierto*
18. *Fin Si*
19. *De Otro Modo*
20. *Retornar Falso*
21. *Fin Si*

Ejemplo 8:

Utilizar el algoritmo "EsNumeroPrimo" para determinar si el número entero 169 es un número primo?.

Al realizar el paso a paso del algoritmo se inicializan los valores de las variables d, p y n en:

$d = 1$

$p = 3$

$n = 169$

como 169 es mayor que 3 entonces el algoritmo sigue en la línea 7, donde el residuo de dividir 169 en 2 no es cero, por lo tanto el algoritmo sigue al ciclo de repetición "hacer mientras" de la línea 10, durante el cual siempre se tiene el siguiente valor:

$\lfloor \sqrt{n} \rfloor = \lfloor \sqrt{169} \rfloor = \lfloor 13 \rfloor = 13$

Iteración 1:

Se cumple la condición del ciclo de repetición hacer mientras porque el $3 \leq 13$ y $d = 1$.

El residuo de dividir 169 en 3 no es cero, por lo tanto no se incrementa el valor de la variable d.

$p = p + 2 = 3 + 2 = 5$

Iteración 2:

Se cumple la condición del ciclo de repetición hacer mientras porque el $5 \leq 13$ y $d = 1$.

El residuo de dividir 169 en 5 no es cero, por lo tanto no se incrementa el valor de la variable d.

$p = p + 2 = 5 + 2 = 7$

Iteración 3:

Se cumple la condición del ciclo de repetición hacer mientras porque el $7 \leq 13$ y $d = 1$.

El residuo de dividir 169 en 7 no es cero, por lo tanto no se incrementa el valor de la variable d.

$p = p + 2 = 7 + 2 = 9$

Iteración 4:

Se cumple la condición del ciclo de repetición hacer mientras porque el $9 \leq 13$ y $d = 1$.

El residuo de dividir 169 en 9 no es cero, por lo tanto no se incrementa el valor de la variable d.

$p = p + 2 = 9 + 2 = 11$

Iteración 5:

Se cumple la condición del ciclo de repetición hacer mientras porque el $11 \leq 13$ y $d = 1$.

El residuo de dividir 169 en 11 no es cero, por lo tanto no se incrementa el valor de la variable d.

$p = p + 2 = 11 + 2 = 13$

Iteración 6:

Se cumple la condición del ciclo de repetición hacer mientras porque el $13 \leq 13$ y $d = 1$.

El residuo de dividir 169 en 13 es cero, por lo tanto

$d = d + 1 = 1 + 1 = 2$

$p = p + 2 = 13 + 2 = 15$

Iteración 7:

No se cumple la condición del ciclo de repetición hacer mientras ya sea porque $15 \nleq 13$ o porque $d \neq 1$. El algoritmo continua en el condicional de la línea 16.

Por último:

Como $d \neq 1$ entonces no se cumple dicho condicional y la función termina retornando el "falso" de la línea 20, lo que indica que el número 169 no es un número primo.

Ejemplo 9:

¿El número entero 61 es un número primo?.

Al realizar el paso a paso del algoritmo se inicializan los valores de las variables d, p y n en:

$d = 1$

$p = 3$

$n = 61$

como 61 es mayor que 3 entonces el algoritmo sigue en la línea 7, donde el residuo de dividir 61 en 2 no es cero, por lo tanto el algoritmo sigue al ciclo de repetición "hacer mientras" de la línea 10, durante el cual siempre se tiene el siguiente valor:

$\lfloor \sqrt{n} \rfloor = \lfloor \sqrt{61} \rfloor = \lfloor 7{,}810249676 \rfloor = 7$

Iteración 1:

Se cumple la condición del ciclo de repetición hacer mientras porque el $3 \leq 7$ y $d = 1$.

El residuo de dividir 61 en 3 no es cero, por lo tanto no se incrementa el valor de la variable d.

$p = p + 2 = 3 + 2 = 5$

Iteración 2:

Se cumple la condición del ciclo de repetición hacer mientras porque el $5 \leq 7$ y $d = 1$.

El residuo de dividir 61 en 5 no es cero, por lo tanto no se incrementa el valor de la variable d.

$p = p + 2 = 5 + 2 = 7$

Iteración 3:

Se cumple la condición del ciclo de repetición hacer mientras porque el $7 \leq 7$ y $d = 1$.

El residuo de dividir 61 en 7 no es cero, por lo tanto no se incrementa el valor de la variable d.

$p = p + 2 = 7 + 2 = 9$

Iteración 4:

No se cumple la condición del ciclo de repetición hacer mientras porque $9 \nleq 7$. El algoritmo continua en el condicional de la línea 16.

Por último:

Como $d = 1$ entonces se cumple dicho condicional y la función termina retornando "cierto", lo que indica que el número 61 si es un número primo.

9.1.6. Procedimiento para generar la factorización prima de un número entero

Gracias al Teorema Fundamental de la Aritmética se garantiza que todo número entero n tiene una única factorización prima, dicha factorización prima se puede determinar con el siguiente algoritmo:

```
Procedimiento  FactorizacionPrima(n : Entero Positivo)
1.   i = 0
2.   p = 2
3.   Si (n > 1) Entonces
4.        Hacer Mientras (p ≤ ⌊√n⌋)
5.             Si  (n mod p = 0) Entonces
6.                  a_i = p
7.                  n = n div p
8.                  i = i + 1
9.             Fin Si
10.            De Otro Modo
11.                 p = GenerarSiguientePrimo(p)
12.       Fin Hacer Mientras
13.       a_i = n
14.  Fin Si
```

La factorización prima del número n es $a_0 \cdot a_1 \cdot a_2 \cdot \ldots \cdot a_k$, donde se obtienen k factores primos no necesariamente diferentes, donde $a_0 \leq a_1 \leq a_2 \leq \ldots \leq a_k$.

El procedimiento hace uso de la función "GenerarSiguientePrimo", la cual se define a continuación, dicha función lo que hace es generar el siguiente número que se obtiene a partir de un número primo p.

Entero Positivo GenerarSiguientePrimo(p : *Entero Positivo*)
1. *Si* ($p = 2$) *Entonces*
2. *Retornar* 3
3. *Fin Si*
4. *De Otro Modo Si* ($p > 2$) *Entonces*
5. $m = p + 2$
6. *Hacer Mientras* ($EsNumeroPrimo(m) \neq Cierto$)
7. $m = m + 2$
8. *Fin Hacer Mientras*
9. *Retornar* m
10. *Fin De Otro Modo*

Ejemplo 10:

Utilizar el algoritmo para generar la factorización prima del número entero 100.

Al realizar el paso a paso del algoritmo (o prueba de escritorio) se inicializan los valores de las variables i, p y n en:

$i = 0$

$p = 2$

$n = 100$

como 100 es mayor que 1 entonces el algoritmo sigue en el ciclo de repetición.

Iteración 1:

$\lfloor\sqrt{n}\rfloor = \lfloor\sqrt{100}\rfloor = \lfloor 10\rfloor = 10$

Se cumple la condición del ciclo de repetición hacer mientras porque el $2 \leq 10$.

El residuo de dividir 100 en 2 es cero, por lo tanto:

$a_i = a_0 = 2$

$n = \frac{100}{2} = 50$

$i = i + 1 = 0 + 1 = 1$

Iteración 2:

$\lfloor\sqrt{n}\rfloor = \lfloor\sqrt{50}\rfloor = \lfloor 7{,}071067812\rfloor = 7$

Se cumple la condición del ciclo de repetición hacer mientras porque el $2 \leq 7$.

El residuo de dividir 50 en 2 es cero, por lo tanto:

$a_i = a_1 = 2$

$n = \frac{50}{2} = 25$

$i = i + 1 = 1 + 1 = 2$

Iteración 3:

$\lfloor\sqrt{n}\rfloor = \lfloor\sqrt{25}\rfloor = \lfloor 5\rfloor = 5$

Se cumple la condición del ciclo de repetición hacer mientras porque el $2 \leq 5$.
El residuo de dividir 25 en 2 no es cero, por lo tanto:
$p = GenerarSiguientePrimo(2) = 3$

Iteración 4:
$\lfloor \sqrt{n} \rfloor = \lfloor \sqrt{25} \rfloor = \lfloor 5 \rfloor = 5$
Se cumple la condición del ciclo de repetición hacer mientras porque el $3 \leq 5$.
El residuo de dividir 25 en 3 no es cero, por lo tanto:
$p = GenerarSiguientePrimo(3) = 5$

Iteración 5:
$\lfloor \sqrt{n} \rfloor = \lfloor \sqrt{25} \rfloor = \lfloor 5 \rfloor = 5$
Se cumple la condición del ciclo de repetición hacer mientras porque el $5 \leq 5$.
El residuo de dividir 25 en 5 es cero, por lo tanto:
$a_i = a_2 = 5$
$n = \frac{25}{5} = 5$
$i = i + 1 = 2 + 1 = 3$

Iteración 6:
$\lfloor \sqrt{n} \rfloor = \lfloor \sqrt{5} \rfloor = \lfloor 2{,}236067978 \rfloor = 2$
No se cumple la condición del ciclo de repetición y se sale de él porque el $5 \nleq 2$.

Por último:
$a_i = a_3 = 5$

La factorización prima del número cien, es $100 = a_0 \cdot a_1 \cdot a_2 \cdot a_3 = 2 \cdot 2 \cdot 5 \cdot 5 = 2^2 \cdot 5^2$.

Ejemplo 11:

Utilizar el algoritmo para generar la factorización prima del número entero 641.

Al realizar el paso a paso del algoritmo se inicializan los valores de las variables i, p y n en:
$i = 0$
$p = 2$
$n = 641$
como 641 es mayor que 1 entonces el algoritmo sigue en el ciclo de repetición.

Iteración 1:
$\lfloor \sqrt{n} \rfloor = \lfloor \sqrt{641} \rfloor = \lfloor 25{,}3179778 \rfloor = 25$
Se cumple la condición del ciclo de repetición hacer mientras porque el $2 \leq 25$.
El residuo de dividir 641 en 2 no es cero, por lo tanto:

$p = GenerarSiguientePrimo(2) = 3$

Iteración 2:
$\lfloor\sqrt{n}\rfloor = \lfloor\sqrt{641}\rfloor = \lfloor 25{,}3179778\rfloor = 25$
Se cumple la condición del ciclo de repetición hacer mientras porque el $3 \leq 25$.
El residuo de dividir 641 en 3 no es cero, por lo tanto:
$p = GenerarSiguientePrimo(3) = 5$

Iteración 3:
$\lfloor\sqrt{n}\rfloor = \lfloor\sqrt{641}\rfloor = \lfloor 25{,}3179778\rfloor = 25$
Se cumple la condición del ciclo de repetición hacer mientras porque el $5 \leq 25$.
El residuo de dividir 641 en 5 no es cero, por lo tanto:
$p = GenerarSiguientePrimo(5) = 7$

Iteración 4:
$\lfloor\sqrt{n}\rfloor = \lfloor\sqrt{641}\rfloor = \lfloor 25{,}3179778\rfloor = 25$
Se cumple la condición del ciclo de repetición hacer mientras porque el $7 \leq 25$.
El residuo de dividir 641 en 7 no es cero, por lo tanto:
$p = GenerarSiguientePrimo(7) = 11$

Iteración 5:
$\lfloor\sqrt{n}\rfloor = \lfloor\sqrt{641}\rfloor = \lfloor 25{,}3179778\rfloor = 25$
Se cumple la condición del ciclo de repetición hacer mientras porque el $11 \leq 25$.
El residuo de dividir 641 en 11 no es cero, por lo tanto:
$p = GenerarSiguientePrimo(11) = 13$

Iteración 6:
$\lfloor\sqrt{n}\rfloor = \lfloor\sqrt{641}\rfloor = \lfloor 25{,}3179778\rfloor = 25$
Se cumple la condición del ciclo de repetición hacer mientras porque el $13 \leq 25$.
El residuo de dividir 641 en 13 no es cero, por lo tanto:
$p = GenerarSiguientePrimo(13) = 17$

Iteración 7:
$\lfloor\sqrt{n}\rfloor = \lfloor\sqrt{641}\rfloor = \lfloor 25{,}3179778\rfloor = 25$
Se cumple la condición del ciclo de repetición hacer mientras porque el $17 \leq 25$.
El residuo de dividir 641 en 17 no es cero, por lo tanto:
$p = GenerarSiguientePrimo(17) = 19$

Iteración 8:
$\lfloor\sqrt{n}\rfloor = \lfloor\sqrt{641}\rfloor = \lfloor 25{,}3179778\rfloor = 25$
Se cumple la condición del ciclo de repetición hacer mientras porque el $19 \leq 25$.

El residuo de dividir 641 en 19 no es cero, por lo tanto:
$p = GenerarSiguientePrimo(19) = 23$

Iteración 9:
$\lfloor\sqrt{n}\rfloor = \lfloor\sqrt{641}\rfloor = \lfloor 25{,}3179778\rfloor = 25$
Se cumple la condición del ciclo de repetición hacer mientras porque el $23 \leq 25$.
El residuo de dividir 641 en 23 no es cero, por lo tanto:
$p = GenerarSiguientePrimo(23) = 29$

Iteración 10:
$\lfloor\sqrt{n}\rfloor = \lfloor\sqrt{641}\rfloor = \lfloor 25{,}3179778\rfloor = 25$
No se cumple la condición del ciclo de repetición hacer mientras porque el $29 \nleq 25$.

Por último:
$a_i = a_0 = n = 641$

La factorización prima es $641 = a_0 = 641 = 641^1$.

Teorema:

Los números primos son infinitos.

Se probará este teorema utilizando la técnica de demostración por contradicción. Se asume que existe una cantidad finita de números primos, los cuales son: p_1, p_2, p_3, ..., p_n. Sea $Q = p_1 \cdot p_2 \cdot p_3 \cdot \ldots \cdot p_n + 1$. Por el Teorema Fundamental de la Aritmética, Q es un número primo o de otro modo puede ser escrito como el producto de dos o más números primos. Sin embargo, ninguno de los primos p_j divide a Q, por lo tanto Q es un número primo y se llega a una contradicción con respecto a que el conjunto de los números primos sea un conjunto finito. De esta forma queda demostrado que el conjunto de los números primos es infinito.

9.1.7. El máximo común divisor (MCD)

Sean a y b números enteros diferentes de cero. El entero más grande d tal que $d|a$ y $d|b$ es llamado el Máximo Común Divisor (MCD) de a y b. El máximo común divisor de a y b se denota por $MCD(a,\ b)$.

Ejemplo 12:

¿Cuál es el $MCD(24,\ 36)$?

Los divisores comunes de ambos números son: 1, 2, 3, 4, 6 y 12, donde

$$MCD(24,\ 36) = MAX(\{1,\ 2,\ 3,\ 4,\ 6,\ 12\}) = 12.$$

Ejemplo 13:

¿Cuál es el $MCD(17,\ 22)$?

$MCD(17,\ 22) = 1$.

Definición (primos relativos): Los números enteros a y b son primos relativos si el MCD es igual a 1.

Ejemplo 14:

17 y 22 son primos relativos porque $MCD(17,\ 22) = 1$.

Otra forma de encontrar el MCD de dos números enteros es usando la factorización prima de los dos números a y b, donde:

$$a = p_1^{a_1} p_2^{a_2} \ \dots \ p_n^{a_n}, \qquad\qquad b = p_1^{b_1} p_2^{b_2} \ \dots \ p_n^{b_n}$$

se debe tener en cuenta que los exponentes son números naturales.

El Máximo Común Divisor de los números enteros a y b se obtiene de la siguiente forma:

$$MCD(a,\ b) = p_1^{min(a_1,\ b_1)} p_2^{min(a_2,\ b_2)} \ \dots \ p_n^{min(a_n,\ b_n)}.$$

Ejemplo 15:

La factorización prima de 120 y 500 es: $120 = 2^3 \cdot 3^1 \cdot 5^1$, $500 = 2^2 \cdot 3^0 \cdot 5^3$

$$MCD(120,\ 500) = 2^{min(3,\ 2)} \cdot 3^{min(1,\ 0)} \cdot 5^{min(1,\ 3)} = 2^2 \cdot 3^0 \cdot 5^1 = 20$$

9.1.8. El mínimo común múltiplo(MCM)

El Mínimo Común Múltiplo de los números enteros positivos a y b es el número entero positivo más pequeño que es divisible por ambos números enteros a y b. El mínimo común múltiplo entre a y b es denotado por $MCM(a,\ b)$.

La forma más fácil de calcular el MCM entre dos números enteros es utilizando la factorización prima de dichos números, donde:

$$a = p_1^{a_1} p_2^{a_2} \ \dots \ p_n^{a_n}, \qquad\qquad b = p_1^{b_1} p_2^{b_2} \ \dots \ p_n^{b_n}$$

se debe tener en cuenta que los exponentes son números naturales.

El Mínimo Común Múltiplo de los números enteros a y b se obtiene de la siguiente forma:

$$MCM(a,\ b) = p_1^{max(a_1,\ b_1)} p_2^{max(a_2,\ b_2)} \ \dots \ p_n^{max(a_n,\ b_n)}.$$

Ejemplo 16:

¿Cuál es el $MCM(95256,\ 432)$?

La factorización prima de 95256 y 432 es: $95256 = 2^3 \cdot 3^5 \cdot 7^2$, $432 = 2^4 \cdot 3^3$

$MCM(95256,\ 432) = 2^{max(3,\ 4)} \cdot 3^{max(5,\ 3)} \cdot 7^{max(2,\ 0)} = 2^4 \cdot 3^5 \cdot 7^2 = 16 \cdot 243 \cdot 49 = 190512$

Ejemplo 17:

Sean los números enteros 50 y 25, $MCD(50,\ 25) = 25$ y $MCM(50,\ 25) = 50$, $50 \cdot 25 = MCD(50,\ 25) \cdot MCM(50,\ 25) = 25 \cdot 50$

9.1.9. El algoritmo de Euclides

La siguiente es una versión iterativa del algoritmo de Euclides para calcular el máximo común divisor de dos números enteros positivos:

Procedimiento $MCD(a,\ b :$ *Enteros Positivos*)
1. $x = a$
2. $y = b$
3. *Hacer Mientras* $(y \neq 0)$
4. $\quad r = x\ mod\ y$
5. $\quad x = y$
6. $\quad y = r$
7. *Fin Hacer Mientras*

en el algoritmo $x\ mod\ y$ es el residuo de la división entera de x por y.

Al finalizar el algoritmo el máximo común divisor de los números enteros x y y se encuentra almacenado en la variable x.

La siguiente es una versión recursiva del algoritmo de Euclides para calcular el máximo común divisor de dos números enteros positivos:

$$Euclides(x,\ y) = \begin{cases} y & si\ \ y \leq x \quad \text{y} \quad (x\ mod\ y) = 0 \\ Euclides(y,\ x) & si\ \ x < y \\ Euclides(y,\ (x\ mod\ y)) & de\ \ otro\ \ modo \end{cases}$$

Lema (en el que se apoya el algoritmo de Euclides): Sea $a = bq + r$, donde a, b, q y r son enteros. Entonces $MCD(a,\ b) = MCD(b,\ r)$.

Ejemplo 18:

Encontrar el $MCD(662,\ 414)$ usando el algoritmo de Euclides.

$$\begin{aligned} Euclides(662,\ 414) = Euclides(414,\ (662\ mod\ 414)) = Euclides(414,\ 248) = \\ Euclides(248,\ (414\ mod\ 248)) = Euclides(248,\ 166) = \\ Euclides(166,\ (248\ mod\ 166)) = Euclides(166,\ 82) = \\ Euclides(82,\ (166\ mod\ 82)) = Euclides(82,\ 2) = 2 \end{aligned}$$

9.2. Aritmética modular

En ocasiones lo único que interesa es el residuo de un número al ser dividido por otro. Por ejemplo, ¿qué hora será dentro de 50 horas a partir de este momento?, sabemos que dentro de 24 horas será exactamente la misma hora actual, lo mismo sucede dentro de 48 horas donde tendremos exactamente la misma hora actual, como simplemente faltan 2 horas para completar las 50 horas, entonces dentro de 50 horas tendremos exactamente la misma hora actual más dos horas.

Definición (congruencia): Si a y b son números enteros y m es un número entero positivo, entonces a es congruente a b modulo m si m divide a $(a - b)$. Se usa la notación $a \equiv b(mod\ m)$ para indicar que a es congruente a b modulo m. Si a y b no son congruentes modulo m, se escribe $a \not\equiv b(mod\ m)$.

Teorema (congruencia):
Sea a y b números enteros y m un entero positivo. Entonces $a \equiv b(mod\ m)$ si y únicamente si $a\ mod\ m = b\ mod\ m$.

Ejemplo 19:

Determinar si 17 es congruente a 5 modulo 6, es decir, ¿$17 \equiv 5(mod\ 6)$?

Utilizando la definición de congruencia se tiene que el 6 divide a $17 - 5 = 12$, es decir $6|(17 - 5) = 6|(12) = 6|(6 \cdot 2) = 2$, de donde se concluye que 17 es congruente a 5 modulo 6.

Utilizando el teorema de congruencia se tiene $17\ mod\ 6 = 5\ mod\ 6$, $5 = 5$, como se presenta la igualdad entonces es cierto que 17 es congruente a 5 modulo 6.

Ejemplo 20:

Determinar si 24 es congruente a 14 modulo 6, es decir, ¿$24 \equiv 14(mod\ 6)$?

Utilizando la definición de congruencia se tiene que el 6 no divide a $24 - 14 = 10$, es decir $6 \not| (24-14) = 6 \not| (10)$, de donde se concluye que 24 no es congruente a 14 modulo 6, $24 \not\equiv 14 (mod\ 6)$.

Utilizando el teorema de congruencia se tiene $24\ mod\ 6 \neq 14\ mod\ 6$, $0 \neq 2$, como no se presenta la igualdad entonces 24 no es congruente a 14 modulo 6.

Teorema:

Sea m un número entero positivo. Los números enteros a y b son congruentes modulo m si y únicamente si hay un entero k tal que $a = b + k \cdot m$.

Teorema:

Sea m un número entero positivo. Si $a \equiv b (mod\ m)$ y $c \equiv d (mod\ m)$ entonces $a + c \equiv b + d (mod\ m)$ y $a \cdot c \equiv b \cdot d (mod\ m)$

Ejemplo 21:

Se tiene que $7 \equiv 2 (mod\ 5)$ y que $11 \equiv 1 (mod\ 5)$ entonces con respecto al teorema anterior se tiene que $7 + 11 \equiv 2 + 1 (mod\ 5)$, $18 \equiv 3 (mod\ 5)$ que efectivamente es cierto y que $7 \cdot 11 \equiv 2 \cdot 1 (mod\ 5)$, $77 \equiv 2 (mod\ 5)$ lo cual también es cierto.

9.2.1. Aplicaciones de la aritmética modular

La Aritmética Modular tiene muchas aplicaciones en matemáticas discretas y ciencias de la computación. Algunas de la aplicaciones más importantes son las siguientes:

- Asignación de localizaciones de memoria en el computador.
- Generación de números pseudoaleatorios.
- Criptosistemas basados en aritmética modular.

9.2.2. Asignación de localizaciones de memoria en el computador

Para la asignación de localizaciones de memoria en el computador comúnmente son utilizadas las Funciones Hash (que al buscar en el español una traducción adecuada serían las "funciones resumen"). Las funciones hash son utilizadas cuando el dominio de los elementos que se van a almacenar en el computador es muy grande y la cantidad de elementos a guardar es muy poca o es muy pequeña con respecto al dominio de los elementos, tal es el caso de las nuevas cédulas de ciudadanía en Colombia que utilizan números mayores a mil millones y donde los colombianos no somos más que cuarenta millones de habitantes.

Sea $h(k)$ la función hash definida como $h(k) = k \ mod \ m$, donde k es la llave que representa al registro (en nuestro ejemplo k es el número de cédula de una persona y donde la cédula se considera como llave principal porque permite diferenciar de forma única a cualquier colombiano con respecto a todos los colombianos) y m es la cantidad de posiciones en memoria que se tienen para almacenar los registros, perfectamente en el contexto universitario un valor adecuado de m podría ser 100000, para considerar que se puede guardar como máximo la información de 100000 estudiantes.

Ejemplo 22:

¿En que posición de memoria debería de quedar almacenada la información del estudiante de cédula 1456452525 si se considera un valor de $m = 100000$?

La información deberá quedar almacenada en el registro ubicado en la posición 52.525, el cual es el resultado que se obtiene con la función hash

$$h(1456452525) = 1456452525 \ mod \ 100000 = 52525$$

La función h no es inyectiva porque dos llaves (cédulas) pueden hacer referencia al mismo registro para almacenar su información allí, tal es el caso de las cédulas 1456452525 y 4987152525 que hacen referencia al registro ubicado en la posición 52525, éste tipo de problemas es solucionado utilizando manejo de colisiones, las cuales están fuera del alcance de este libro.

9.2.3. Generación de números pseudoaleatorios

El procedimiento más comúnmente utilizado en los computadores para generar números pseudoaleatorios es el de Congruencia Lineal.
El procedimiento de Congruencia Lineal utiliza cuatro números enteros: el modulo m, el multiplicador a, el incremento c y la semilla x_0, con $2 \leq a < m$, $0 \leq c < m$ y $0 \leq x_0 < m$. Se genera una secuencia de números pseudoaleatorios $\{x_n\}$, con $0 \leq x_n < m$ para toda n, al usar sucesivamente la congruencia:

$$x_{n+1} = (a \cdot x_n + c) \ mod \ m$$

Ejemplo 23:

¿Cuál es la secuencia de números que se generan al elegir el modulo $m = 9$, el multiplicador $a = 7$, el incremento $c = 4$ y la semilla $x_0 = 3$?

$x_0 = 3$
$x_1 = (7 \cdot x_0 + 4) \ mod \ 9 = (7 \cdot 3 + 4) \ mod \ 9 = 25 \ mod \ 9 = 7$
$x_2 = (7 \cdot x_1 + 4) \ mod \ 9 = (7 \cdot 7 + 4) \ mod \ 9 = 53 \ mod \ 9 = 8$
$x_3 = (7 \cdot x_2 + 4) \ mod \ 9 = (7 \cdot 8 + 4) \ mod \ 9 = 60 \ mod \ 9 = 6$

$x_4 = (7 \cdot x_3 + 4)\ mod\ 9 = (7 \cdot 6 + 4)\ mod\ 9 = 46\ mod\ 9 = 1$
$x_5 = (7 \cdot x_4 + 4)\ mod\ 9 = (7 \cdot 1 + 4)\ mod\ 9 = 11\ mod\ 9 = 2$
$x_6 = (7 \cdot x_5 + 4)\ mod\ 9 = (7 \cdot 2 + 4)\ mod\ 9 = 18\ mod\ 9 = 0$
$x_7 = (7 \cdot x_6 + 4)\ mod\ 9 = (7 \cdot 0 + 4)\ mod\ 9 = 4\ mod\ 9 = 4$
$x_8 = (7 \cdot x_7 + 4)\ mod\ 9 = (7 \cdot 4 + 4)\ mod\ 9 = 32\ mod\ 9 = 5$
$x_9 = (7 \cdot x_8 + 4)\ mod\ 9 = (7 \cdot 5 + 4)\ mod\ 9 = 39\ mod\ 9 = 3$

Donde $x_9 = x_0 = 3$ y cada término en la secuencia depende únicamente del término previo, de esta forma la secuencia generada es: 3, 7, 8, 6, 1, 2, 0, 4, 5, 3, 7, 8, 6, 1, 2, 0, 4, 5, 3, ...

9.2.4. Criptosistemas basados en aritmética modular

Una de las aplicaciones más importantes de la aritmética modular es la criptografía. Para ilustrar este tema se presentará el método como se encriptaban los mensajes en la época del Emperador Julio Cesar.

El Método de Encriptación del Emperador Julio Cesar consiste en seleccionar un alfabeto sobre el cual se va a escribir un mensaje, cada letra que conforma el mensaje original es reemplazada por la letra que se encuentra m posiciones a la derecha en el alfabeto. Se considera que el alfabeto es cíclico, es decir que después de la última letra del alfabeto sigue la primer letra del alfabeto, de esta forma siempre se puede desplazar m posiciones a la derecha del alfabeto sin importar la posición que ocupa ésta sobre dicho alfabeto.

Ejemplo 24:

Considerar que se tiene el siguiente alfabeto: {a, b, c, d, e, f, g, h, i, j, k, l, m}, y que en el encriptamiento una letra se reemplaza por la que esté tres posiciones a la derecha de ésta, en los casos en que se necesita seguir contando letras y éstas se acaben entonces se sigue contando desde la primer letra del alfabeto, es decir se debe considerar que el alfabeto es cíclico. ¿Cómo se debe escribir la palabra *magia* encriptada de esta forma?

Según el alfabeto las letras de la palabra "magia" son reemplazadas por: $m \rightarrow c$, $a \rightarrow d$, $g \rightarrow j$, $i \rightarrow l$ y $a \rightarrow d$. *Encriptar*('magia')='cdjld'.

Formalmente el proceso consiste en:

- Si se están utilizando todas las letras del alfabeto español entonces reemplazar cada letra por un entero entre 0 y 26, donde $a \rightarrow 0$, $b \rightarrow 1$, ..., $z \rightarrow 26$.
- Para cada una de las posiciones de las letras calcular la nueva posición apoyado en la siguiente formula $f(p) = (p\ +\ desplazamiento)\ mod\ 27$
- Para cada una de las nuevas posiciones, reemplazar dichas posiciones por la letra que corresponde en el alfabeto para dicha ubicación.

Ejemplo 25:

¿Cuál es el mensaje secreto producido por la palabra "universidad" teniendo un desplazamiento de 8 en el método de Julio Cesar y considerando todo el alfabeto español?

Equivalencia de las letras a sus posiciones comenzando desde la posición cero:
$a \to 0$, $b \to 1$, $c \to 2$, $d \to 3$, $e \to 4$, $f \to 5$, $g \to 6$, $h \to 7$,
$i \to 8$, $j \to 9$, $k \to 10$, $l \to 11$, $m \to 12$, $n \to 13$, $\tilde{n} \to 14$, $o \to 15$,
$p \to 16$, $q \to 17$, $r \to 18$, $s \to 19$, $t \to 20$, $u \to 21$, $v \to 22$, $w \to 23$,
$x \to 24$, $y \to 25$, $z \to 26$.

$ReemplazarLetrasPosiciones('universidad') = '21\ \ 13\ \ 8\ \ 22\ \ 4\ \ 18\ \ 19\ \ 8\ \ 3\ \ 0\ \ 3'$

Los desplazamientos para cada una de las posiciones de las letras son:

$f(21) = (21\ +\ 8)\ mod\ 27 = 29\ mod\ 27 = 2$
$f(13) = (13\ +\ 8)\ mod\ 27 = 21\ mod\ 27 = 21$
$f(8) = (8\ +\ 8)\ mod\ 27 = 16\ mod\ 27 = 16$
$f(22) = (22\ +\ 8)\ mod\ 27 = 30\ mod\ 27 = 3$
$f(4) = (4\ +\ 8)\ mod\ 27 = 12\ mod\ 27 = 12$
$f(18) = (18\ +\ 8)\ mod\ 27 = 26\ mod\ 27 = 26$
$f(19) = (19\ +\ 8)\ mod\ 27 = 27\ mod\ 27 = 0$
$f(8) = (8\ +\ 8)\ mod\ 27 = 16\ mod\ 27 = 16$
$f(3) = (3\ +\ 8)\ mod\ 27 = 11\ mod\ 27 = 11$
$f(0) = (0\ +\ 8)\ mod\ 27 = 8\ mod\ 27 = 8$
$f(3) = (3\ +\ 8)\ mod\ 27 = 11\ mod\ 27 = 11$

$PosicionesDesplazadas('21\ \ 13\ \ 8\ \ 22\ \ 4\ \ 18\ \ 19\ \ 8\ \ 3\ \ 0\ \ 3') =$
$'2\ \ 21\ \ 16\ \ 3\ \ 12\ \ 26\ \ 0\ \ 16\ \ 11\ \ 8\ \ 11'$

$PosicionesPorLetras('2\ \ 21\ \ 16\ \ 3\ \ 12\ \ 26\ \ 0\ \ 16\ \ 11\ \ 8\ \ 11') = 'cupdmzaplil'$

De esta forma $Encriptar('universidad') = 'cupdmzaplil'$.

9.3. Representación de los enteros en el computador

La notación que típicamente utilizamos día a día es la de base 10, donde 913 es realmente $9 \times 10^2 + 1 \times 10^1 + 3 \times 10^0$. La notación que utilizan los computadores es base 2.

Teorema:

Sea b un entero positivo más grande que 1. Entonces si n es un número entero positivo

este puede ser representado de forma única como:

$$n = a_k b^k + a_{k-1} b^{k-1} + \cdots + a_1 b + a_0$$

donde k es un número entero no negativo, $a_0,\ a_1,\ \ldots,\ a_k$ son números enteros positivos menores que b y $a_k \neq 0$. La representación del número entero n en base b es $(a_k a_{k-1} a_{k-2} \cdots a_1 a_0)_b$.

Ejemplo 26:

¿Cuál es la representación decimal del número entero que tiene como representación binaria a $(10111100)_2$?

$$\begin{aligned}(10111100)_2 &= 1 \cdot 2^7 + 0 \cdot 2^6 + 1 \cdot 2^5 + 1 \cdot 2^4 + 1 \cdot 2^3 + 1 \cdot 2^2 + 0 \cdot 2^1 + 0 \cdot 2^0 \\ &= 2^7 + 2^5 + 2^4 + 2^3 + 2^2 \\ &= 128 + 32 + 16 + 8 + 4 \\ &= 188\end{aligned}$$

Ejemplo 27:

¿Cuál es la representación decimal del número entero que tiene como representación ternaria a $(210112)_3$?

$$\begin{aligned}(210112)_3 &= 2 \cdot 3^5 + 1 \cdot 3^4 + 0 \cdot 3^3 + 1 \cdot 3^2 + 1 \cdot 3^1 + 2 \cdot 3^0 \\ &= 2 \cdot 243 + 1 \cdot 81 + 1 \cdot 9 + 1 \cdot 3 + 2 \cdot 1 \\ &= 486 + 81 + 9 + 3 + 2 \\ &= 581\end{aligned}$$

Ejemplo 28:

¿Cuál es la representación decimal del número entero que tiene como representación en base 6 a $(310541)_6$?

$$\begin{aligned}(310541)_6 &= 3 \cdot 6^5 + 1 \cdot 6^4 + 0 \cdot 6^3 + 5 \cdot 6^2 + 4 \cdot 6^1 + 1 \cdot 6^0 \\ &= 3 \cdot 7776 + 1 \cdot 1296 + 5 \cdot 36 + 4 \cdot 6 + 1 \cdot 1 \\ &= 23328 + 1296 + 180 + 24 + 1 \\ &= 24829\end{aligned}$$

9.3.1. Representación de números enteros en base hexadecimal

La representación de números enteros en base hexadecimal o base 16 es utilizada comúnmente en ciencias de la computación. En esta base 16 símbolos son requeridos, éstos son: 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, A, B, C, D, E, F, donde las letras de la A a la E representan respectivamente los números decimales del 10 al 15.

Ejemplo 29:

¿Cuál es la representación decimal del número entero que tiene como representación en base hexadecimal a $(BC024)_{16}$?

$(BC024)_{16} = B \cdot 16^4 + C \cdot 16^3 + 0 \cdot 16^2 + 2 \cdot 16^1 + 4 \cdot 16^0$
$(BC024)_{16} = 11 \cdot 16^4 + 12 \cdot 16^3 + 0 \cdot 16^2 + 2 \cdot 16^1 + 4 \cdot 16^0$
$(BC024)_{16} = 11 \cdot 65536 + 12 \cdot 4096 + 2 \cdot 16 + 4 \cdot 1$
$(BC024)_{16} = 720896 + 49152 + 32 + 4 = (770084)_{10}$

9.3.2. Cambio de base de un número entero escrito en base 10

Ahora se describe un algoritmo para obtener la representación en base b de un número entero n escrito en base 10.

Utilizando el algoritmo de la división se tiene que: $n = b \cdot q_0 + a_0$, donde $0 \leq a_0 < b$, a_0 es el residuo de dividir n por b, q_0 es el cociente de dividir n por b, a_0 es el dígito situado más a la derecha en la representación del número entero n. Luego se repite de nuevo el proceso para q_0, de esta forma se tiene: $q_0 = b \cdot q_1 + a_1$, donde $0 \leq a_1 < b$, a_1 es el segundo dígito por la derecha de la representación del número entero n en base b. El proceso continúa dividiendo el cociente sucesivamente por b, obteniendo como residuos los dígitos de la representación en base b. El proceso termina cuando se obtiene un cociente igual a cero. La representación del número entero n en base b es $(a_k a_{k-1} a_{k-2} \cdots a_1 a_0)_b$.

Ejemplo 30:

¿Cuál es la representación binaria (o representación en base 2) del número entero 188 (el cual se sobre entiende que está en base 10 ó base decimal)?

$$
\begin{array}{lll}
188 = 2 \cdot 94 + 0, & q_0 = 94, & a_0 = 0 \\
94 = 2 \cdot 47 + 0, & q_1 = 47, & a_1 = 0 \\
47 = 2 \cdot 23 + 1, & q_2 = 23, & a_2 = 1 \\
23 = 2 \cdot 11 + 1, & q_3 = 11, & a_3 = 1 \\
11 = 2 \cdot 5 + 1, & q_4 = 5, & a_4 = 1 \\
5 = 2 \cdot 2 + 1, & q_5 = 2, & a_5 = 1 \\
2 = 2 \cdot 1 + 0, & q_6 = 1, & a_6 = 0 \\
1 = 2 \cdot 0 + 1, & q_7 = 0, & a_7 = 1
\end{array}
$$

como la presentación en la base b es $(a_7a_6\ldots a_1a_0)_b$ entonces el número entero 188 tiene la representación binaria $(10111100)_2$.

Ejemplo 31:

¿Cuál es la representación en base 3 (o base ternaria) del número entero 581?

$$\begin{array}{lll} 581 = 3\cdot 193 + 2, & q_0 = 193, & a_0 = 2 \\ 193 = 3\cdot 64 + 1, & q_1 = 64, & a_1 = 1 \\ 64 = 3\cdot 21 + 1, & q_2 = 21, & a_2 = 1 \\ 21 = 3\cdot 7 + 0, & q_3 = 7, & a_3 = 0 \\ 7 = 3\cdot 2 + 1, & q_4 = 2, & a_4 = 1 \\ 2 = 3\cdot 0 + 2, & q_5 = 0, & a_5 = 2 \end{array}$$

como la presentación en la base b es $(a_5a_4a_3a_2a_1a_0)_b$ entonces el número entero 581 tiene la siguiente representación en base 3: $(210112)_3$.

Ejemplo 32:

¿Cuál es la representación en base 6 del número entero 24829?

$$\begin{array}{lll} 24829 = 6\cdot 4138 + 1, & q_0 = 4138, & a_0 = 1 \\ 4138 \ = 6\cdot 689 + 4, & q_1 = 689\ , & a_1 = 4 \\ 689 \ = 6\cdot 114 + 5, & q_2 = 114\ , & a_2 = 5 \\ 114 \ = 6\cdot 19 + 0\ , & q_3 = 19\ \ , & a_3 = 0 \\ 19 \ = 6\cdot 3 + 1\ , & q_4 = 3\ \ , & a_4 = 1 \\ 3 \ = 6\cdot 0 + 3\ , & q_5 = 0\ \ , & a_5 = 3 \end{array}$$

como la presentación en la base b es $(a_5a_4a_3a_2a_1a_0)_b$ entonces el número entero 24829 tiene la siguiente representación en base 6: $(310541)_6$.

9.3.3. Algoritmo para construir la expansión de n en base b

Procedimiento $RepresentacionEnBaseB(n,\ b:$ *Enteros Positivos*$)$
1. *Si* $(b \geq 2)$ *Entonces*
2. $\quad q = n$
3. $\quad k = 0$
4. $\quad$ *Hacer Mientras* $(q \neq 0)$
5. $\quad\quad a_k = q\ mod\ b$
6. $\quad\quad q = q\ div\ b$
7. $\quad\quad k = k + 1$
8. $\quad$ *Fin Hacer Mientras*
9. *Fin Si*

La representación del número entero n en base b es $(a_{k-1}a_{k-2}a_{k-3}\cdots a_1a_0)_b$.

Ejemplo 33:

Utilizar el algoritmo "RepresentacionEnBaseB" para generar la representación en base 4 del número 531.

Al realizar el paso a paso del algoritmo se inicializan los valores de las variables n y b en:

$n = 531$

$b = 4$

como b es mayor o igual a 2 entonces el algoritmo sigue en la línea 2, donde se le asignan los siguientes valores a las variables q y k:

$q = n = 531$

$k = 0$

como la variable q tiene un valor diferente de cero, entonces el algoritmo entra al ciclo de repetición "hacer mientras" de la línea 4, las siguientes son las iteraciones que realiza el ciclo de repetición:

Iteración 1:

Se cumple la condición del ciclo de repetición hacer mientras porque $q = 531 \neq 0$, el trabajo que se realiza dentro del ciclo es el siguiente:

$a_k = q \ mod \ b,$	$a_0 = 531 \ mod \ 4,$	$a_0 = 3$
$q = q \ div \ b,$	$q = 531 \ div \ 4,$	$q = 132$
$k = k + 1,$	$k = 0 + 1,$	$k = 1$

Iteración 2:

Se cumple la condición del ciclo de repetición hacer mientras porque $q = 132 \neq 0$, el trabajo que se realiza dentro del ciclo es el siguiente:

$a_k = q \ mod \ b,$	$a_1 = 132 \ mod \ 4,$	$a_1 = 0$
$q = q \ div \ b,$	$q = 132 \ div \ 4,$	$q = 33$
$k = k + 1,$	$k = 1 + 1,$	$k = 2$

Iteración 3:

Se cumple la condición del ciclo de repetición hacer mientras porque $q = 33 \neq 0$, el trabajo que se realiza dentro del ciclo es el siguiente:

$a_k = q \ mod \ b,$	$a_2 = 33 \ mod \ 4,$	$a_2 = 1$
$q = q \ div \ b,$	$q = 33 \ div \ 4,$	$q = 8$
$k = k + 1,$	$k = 2 + 1,$	$k = 3$

Iteración 4:

Se cumple la condición del ciclo de repetición hacer mientras porque $q = 8 \neq 0$, el trabajo que se realiza dentro del ciclo es el siguiente:

$a_k = q \ mod \ b,$	$a_3 = 8 \ mod \ 4,$	$a_3 = 0$
$q = q \ div \ b,$	$q = 8 \ div \ 4,$	$q = 2$
$k = k + 1,$	$k = 3 + 1,$	$k = 4$

Iteración 5:

Se cumple la condición del ciclo de repetición hacer mientras porque $q = 2 \neq 0$, el trabajo que se realiza dentro del ciclo es el siguiente:

$a_k = q \ mod \ b,$	$a_4 = 2 \ mod \ 4,$	$a_4 = 2$
$q = q \ div \ b,$	$q = 2 \ div \ 4,$	$q = 0$
$k = k + 1,$	$k = 4 + 1,$	$k = 5$

Iteración 6:

Ya no se cumple la condición del ciclo de repetición porque la variable q es igual a cero, por lo tanto el algoritmo termina.

Por último:

Como la representación del número entero 531 en base 4 es $(a_4a_3a_2a_1a_0)_4$ entonces dicha representación es $(20103)_4$.

9.3.4. Algoritmos para operaciones de números enteros en base 2

Algoritmo para la suma de números enteros en base 2

Para el siguiente algoritmo las representaciones binarias de a y b son $(a_{n-1}a_{n-2}\ldots a_1a_0)_2$ y $(b_{n-1}b_{n-2}\ldots b_1b_0)_2$, respectivamente.

Procedimiento $SumaDeNumerosEnterosEnBaseBinaria(a, b : Enteros\ Positivos)$

1. $c = 0$
2. $n = MAX(CantidadBits(a),\ CantidadBits(b))$
3. $Para\ \ j = 0\ \ Hasta\ \ n - 1$
4. $\quad d = \lfloor (a_j + b_j + c)/2 \rfloor$
5. $\quad S_j = a_j + b_j + c - 2d$
6. $\quad c = d$
7. $Fin\ \ Para$
8. $S_n = c$

La representación binaria de la suma es $(S_nS_{n-1}\ldots S_1S_0)_2$

Ejemplo 34:

Utilizar el algoritmo "SumaDeNumerosEnterosEnBaseBinaria" para sumar los números enteros positivos a y b que tienen respectivamente las siguientes representaciones binarias $(1101010)_2$ y $(111100)_2$.

Al realizar el paso a paso del algoritmo se inicializan los valores de las variables c, j y n en:

$c = 0$

$n = 7$, donde n es la cantidad de bits del número más largo de los dos que se van a sumar, en el caso del número que tenga menos bits entonces éste se lleva a la misma longitud del otro número rellenando de tantos ceros como sean necesarios en la parte izquierda del número hasta alcanzar la longitud del número más largo, por este motivo el número b queda representado así: $(0111100)_2$.

El algoritmo entra al ciclo de repetición "Para" de la línea 3, las siguientes son las iteraciones que realiza el ciclo de repetición:

Iteración 1:

El ciclo de repetición para comienza incializando su contador de ciclo j en cero, el trabajo que se realiza dentro del ciclo es el siguiente:

$$d = \left\lfloor \frac{a_0 + b_0 + c}{2} \right\rfloor, \qquad d = \left\lfloor \frac{0 + 0 + 0}{2} \right\rfloor, \qquad d = 0$$
$$s_0 = a_0 + b_0 + c - 2d, \qquad s_0 = 0 + 0 + 0 - 2 \cdot 0, \qquad s_0 = 0$$
$$c = d, \qquad c = 0$$
$$j = 1$$

Iteración 2:

Se cumple la condición del ciclo de repetición para porque $j = 1 \leq 6$, el trabajo que se realiza dentro del ciclo es el siguiente:

$$d = \left\lfloor \frac{a_1 + b_1 + c}{2} \right\rfloor, \qquad d = \left\lfloor \frac{1 + 0 + 0}{2} \right\rfloor, \qquad d = 0$$
$$s_1 = a_1 + b_1 + c - 2d, \qquad s_1 = 1 + 0 + 0 - 2 \cdot 0, \qquad s_1 = 1$$
$$c = d, \qquad c = 0$$
$$j = 2$$

Iteración 3:

Se cumple la condición del ciclo de repetición para porque $j = 2 \leq 6$, el trabajo que se realiza dentro del ciclo es el siguiente:

$$d = \left\lfloor \frac{a_2 + b_2 + c}{2} \right\rfloor, \qquad d = \left\lfloor \frac{0 + 1 + 0}{2} \right\rfloor, \qquad d = 0$$
$$s_2 = a_2 + b_2 + c - 2d, \qquad s_2 = 0 + 1 + 0 - 2 \cdot 0, \qquad s_2 = 1$$
$$c = d, \qquad c = 0$$
$$j = 3$$

Iteración 4:

Se cumple la condición del ciclo de repetición para porque $j = 3 \leq 6$, el trabajo que se realiza dentro del ciclo es el siguiente:

$$d = \left\lfloor \frac{a_3 + b_3 + c}{2} \right\rfloor, \qquad d = \left\lfloor \frac{1 + 1 + 0}{2} \right\rfloor, \qquad d = 1$$
$$s_3 = a_3 + b_3 + c - 2d, \qquad s_3 = 1 + 1 + 0 - 2 \cdot 1, \qquad s_3 = 0$$
$$c = d, \qquad c = 1$$
$$j = 4$$

Iteración 5:

Se cumple la condición del ciclo de repetición para porque $j = 4 \leq 6$, el trabajo que se realiza dentro del ciclo es el siguiente:

$$\begin{array}{lll} d = \left\lfloor \frac{a_4 + b_4 + c}{2} \right\rfloor, & d = \left\lfloor \frac{0 + 1 + 1}{2} \right\rfloor, & d = 1 \\ s_4 = a_4 + b_4 + c - 2d, & s_4 = 0 + 1 + 1 - 2 \cdot 1, & s_4 = 0 \\ c = d, & c = 1 & \\ j = 5 & & \end{array}$$

Iteración 6:

Se cumple la condición del ciclo de repetición para porque $j = 5 \leq 6$, el trabajo que se realiza dentro del ciclo es el siguiente:

$$\begin{array}{lll} d = \left\lfloor \frac{a_5 + b_5 + c}{2} \right\rfloor, & d = \left\lfloor \frac{1 + 1 + 1}{2} \right\rfloor, & d = 1 \\ s_5 = a_5 + b_5 + c - 2d, & s_5 = 1 + 1 + 1 - 2 \cdot 1, & s_5 = 1 \\ c = d, & c = 1 & \\ j = 6 & & \end{array}$$

Iteración 7:

Se cumple la condición del ciclo de repetición para porque $j = 6 \leq 6$, el trabajo que se realiza dentro del ciclo es el siguiente:

$$\begin{array}{lll} d = \left\lfloor \frac{a_6 + b_6 + c}{2} \right\rfloor, & d = \left\lfloor \frac{1 + 0 + 1}{2} \right\rfloor, & d = 1 \\ s_6 = a_6 + b_6 + c - 2d, & s_6 = 1 + 0 + 1 - 2 \cdot 1, & s_6 = 0 \\ c = d, & c = 1 & \\ j = 7 & & \end{array}$$

Iteración 8:

Ya no se cumple la condición del ciclo de repetición para porque $j = 7 \nleq 6$, por lo tanto el ciclo de repetición termina y el algoritmo continua en la línea 8.

Por último:

$s_7 = 1$. El resultado de sumar los números a y b en representación binaria es $(s_7 s_6 s_5 s_4 s_3 s_2 s_1 s_0)_2$, con respecto a los valores obtenidos en el paso a paso del algoritmo el resultado es: $(10100110)_2$.

Las representaciones en base diez de los números a, b y el resultado s es:

$$\begin{aligned} a = (1101010)_2 &= 1 \cdot 2^6 + 1 \cdot 2^5 + 0 \cdot 2^4 + 1 \cdot 2^3 + 0 \cdot 2^2 + 1 \cdot 2^1 + 0 \cdot 2^0 \\ &= 1 \cdot 64 + 1 \cdot 32 + 1 \cdot 8 + 1 \cdot 2 \\ &= 64 + 32 + 8 + 2 \\ &= 106 \end{aligned}$$

$$\begin{aligned} b = (0111100)_2 &= 0 \cdot 2^6 + 1 \cdot 2^5 + 1 \cdot 2^4 + 1 \cdot 2^3 + 1 \cdot 2^2 + 0 \cdot 2^1 + 0 \cdot 2^0 \\ &= 1 \cdot 32 + 1 \cdot 16 + 1 \cdot 8 + 1 \cdot 4 \end{aligned}$$

$$= 32 + 16 + 8 + 4$$
$$= 60$$

$$s = (10100110)_2 = 1 \cdot 2^7 + 0 \cdot 2^6 + 1 \cdot 2^5 + 0 \cdot 2^4 + 0 \cdot 2^3 + 1 \cdot 2^2 + 1 \cdot 2^1 + 0 \cdot 2^0$$
$$= 1 \cdot 2^7 + 1 \cdot 2^5 + 1 \cdot 2^2 + 1 \cdot 2^1$$
$$= 1 \cdot 128 + 1 \cdot 32 + 1 \cdot 4 + 1 \cdot 2$$
$$= 128 + 32 + 4 + 2$$
$$= 166$$

y efectivamente $106 + 60 = 166$.

Algoritmo para la multiplicación de números enteros en base 2

Para el siguiente algoritmo las representaciones binarias de a y b son $(a_{n-1}a_{n-2}\ldots a_1a_0)_2$ y $(b_{n-1}b_{n-2}\ldots b_1b_0)_2$, respectivamente. Adicionalmente, c_0, c_1, …, c_{n-1} son los productos parciales.

Procedimiento MultiplicacionDeNumerosEnterosEnBaseBinaria(a, b : *Enteros Positivos*)

1. $n = CantidadBits(b)$
2. *Para* $j = 0$ *Hasta* $n - 1$
3. *Si* $(b_j = 1)$ *Entonces*
4. $c_j =$ (desplazar el número a j lugares a la izquierda)
5. *De Otro Modo*
6. $c_j = 0$
7. *Fin Para*
8. $p = 0$
9. *Para* $j = 0$ *to* $n - 1$
10. $p = p + c_j$
11. *Fin Para*

Al terminar el algoritmo en la variable p queda almacenado el resultado de multiplicar los números enteros a y b.

Ejemplo 35:

Utilizar el algoritmo "MultiplicacionDeNumerosEnterosEnBaseBinaria" para multiplicar los números enteros positivos a y b que tienen respectivamente las siguientes representaciones binarias $(1001)_2$ y $(1101)_2$.

Al realizar el paso a paso del algoritmo se inicia el valor de la variable n con el número entero positivo 4, porque el número b en su representación binaria tiene cuatro bits.

El algoritmo continúa en la línea 2 donde ingresa al ciclo de repetición "Para" donde se realizan las siguientes iteraciones:

Iteración 1, ciclo "para" que comienza en la línea 2:

El ciclo de repetición "para" comienza inicializando su contador de ciclo j en cero, el trabajo que se realiza dentro del ciclo es el siguiente:

como $b_0 = 1$ entonces a c_0 se le asigna el número a desplazado $j = 0$ posiciones a la izquierda, de esta forma se tiene que:

$c_0 = (1001)_2 = 1 \cdot 2^3 + 0 \cdot 2^2 + 0 \cdot 2^1 + 1 \cdot 2^0 = 8 + 1 = 9$

$j = j + 1 = 0 + 1 = 1$, se incrementa el contador del ciclo.

Iteración 2, ciclo "para" que comienza en la línea 2:

Se cumple la condición del ciclo de repetición "para" porque $j = 1 \leq 3$, el trabajo que se realiza dentro del ciclo es el siguiente:

como $b_1 = 0$ entonces a c_1 se le asigna el número 0 (línea 6 del algoritmo), de esta forma se tiene que $c_1 = 0$ y se incrementa el contador del ciclo, donde $j = j + 1 = 1 + 1 = 2$.

Iteración 3, ciclo "para" que comienza en la línea 2:

Se cumple la condición del ciclo de repetición "para" porque $j = 2 \leq 3$, el trabajo que se realiza dentro del ciclo es el siguiente:

como $b_2 = 1$ entonces a c_2 se le asigna el número a desplazado $j = 2$ posiciones a la izquierda, de esta forma se tiene que:

$c_2 = (100100)_2 = 1 \cdot 2^5 + 0 \cdot 2^4 + 0 \cdot 2^3 + 1 \cdot 2^2 + 0 \cdot 2^1 + 0 \cdot 2^0 = 32 + 4 = 36$

$j = j + 1 = 2 + 1 = 3$, se incrementa el contador del ciclo.

Iteración 4, ciclo "para" que comienza en la línea 2:

Se cumple la condición del ciclo de repetición "para" porque $j = 3 \leq 3$, el trabajo que se realiza dentro del ciclo es el siguiente:

como $b_3 = 1$ entonces a c_3 se le asigna el número a desplazado $j = 3$ posiciones a la izquierda, de esta forma se tiene que:

$c_3 = (1001000)_2 = 1 \cdot 2^6 + 0 \cdot 2^5 + 0 \cdot 2^4 + 1 \cdot 2^3 + 0 \cdot 2^2 + 0 \cdot 2^1 + 0 \cdot 2^0 = 64 + 8 = 72$

$j = j + 1 = 3 + 1 = 4$, se incrementa el contador del ciclo.

Iteración 5, ciclo "para" que comienza en la línea 2:

Ya no se cumple la condición del ciclo de repetición "para" porque $j = 4 \not\leq 3$, por lo tanto el ciclo de repetición termina y el algoritmo continua en la línea 8 donde se inicializa la variable p con el valor cero.

El algoritmo continúa en la línea 9 donde ingresa al ciclo de repetición "Para" donde se realizan las siguientes iteraciones:

Iteración 1, ciclo "para" que comienza en la línea 9:

El ciclo de repetición "para" comienza inicializando su contador de ciclo j en cero, el trabajo que se realiza dentro del ciclo es el siguiente:

$$\begin{array}{lll} p = p + c_0, & p = 0 + 9, & p = 9 \\ j = j + 1, & j = 0 + 1 = 1, & j = 1 \end{array}$$

Iteración 2, ciclo "para" que comienza en la línea 9:
Se cumple la condición del ciclo de repetición "para" porque $j = 1 \leq 3$, el trabajo que se realiza dentro del ciclo es el siguiente:

$$\begin{array}{lll} p = p + c_1, & p = 9 + 0, & p = 9 \\ j = j + 1, & j = 1 + 1 = 1, & j = 2 \end{array}$$

Iteración 3, ciclo "para" que comienza en la línea 9:
Se cumple la condición del ciclo de repetición "para" porque $j = 2 \leq 3$, el trabajo que se realiza dentro del ciclo es el siguiente:

$$\begin{array}{lll} p = p + c_2, & p = 9 + 36, & p = 45 \\ j = j + 1, & j = 2 + 1 = 1, & j = 3 \end{array}$$

Iteración 4, ciclo "para" que comienza en la línea 9:
Se cumple la condición del ciclo de repetición "para" porque $j = 3 \leq 3$, el trabajo que se realiza dentro del ciclo es el siguiente:

$$\begin{array}{lll} p = p + c_3, & p = 45 + 72, & p = 117 \\ j = j + 1, & j = 3 + 1 = 1, & j = 4 \end{array}$$

Iteración 5, ciclo "para" que comienza en la línea 9:
Ya no se cumple la condición del ciclo de repetición "para" porque $j = 4 \nleq 3$, por lo tanto el ciclo de repetición termina y el algoritmo también termina obteniéndose como resultado de la multiplicación el número almacenado en la variable p, cuyo valor es 117.

Las representaciones en base diez de los números a y b es:

$$\begin{aligned} a = (1001)_2 &= 1 \cdot 2^3 + 0 \cdot 2^2 + 0 \cdot 2^1 + 1 \cdot 2^0 \\ &= 1 \cdot 8 + 1 \cdot 1 \\ &= 8 + 1 \\ &= 9 \end{aligned}$$

$$\begin{aligned} b = (1101)_2 &= 1 \cdot 2^3 + 1 \cdot 2^2 + 0 \cdot 2^1 + 1 \cdot 2^0 \\ &= 1 \cdot 8 + 1 \cdot 4 + 1 \cdot 1 \\ &= 8 + 4 + 1 \\ &= 13 \end{aligned}$$

y efectivamente $9 + 13 = 117$.

9.4. Ejercicios

1. ¿El número entero positivo 1327 es un número primo?, demostrar o refutar utilizando las propiedades de los números primos.

2. ¿El número entero positivo 2371 es un número primo?, demostrar o refutar utilizando las propiedades de los números primos.

3. ¿El número entero positivo 3721 es un número primo?, demostrar o refutar utilizando las propiedades de los números primos.

4. ¿El número entero positivo 7231 es un número primo?, demostrar o refutar utilizando las propiedades de los números primos.

5. Escribir los siguientes números como un producto de factores primos, teniendo en cuenta que

$$p_1^{n_1} \cdot p_2^{n_2} \cdot \ldots \cdot p_k^{n_k}, \quad 0 < n_i, \quad 1 \leq i \leq k, \quad p_1 < p_2 < \ldots < p_k$$

   a) 407125

   b) 184600

   c) 842570

   d) 945677

6. ¿Cuántos divisores tiene el número 407125?

7. ¿Cuántos divisores tiene el número 184600?

8. ¿Cuántos divisores tiene el número 842570?

9. ¿Cuántos divisores tiene el número 945677?

10. Apoyados en el Teorema Fundamental de la Aritmética y utilizando la factorización prima de los números enteros, determinar el Máximo Común Divisor (MCD) y el Mínimo Común Múltiplo (MCM) de las siguientes parejas de números enteros:

    a) 225 y 350

    b) 254 y 896

    c) 425 y 789

    d) 486 y 964

    e) 487 y 765

    f) 504 y 540

    g) 1576, 8748 y 99500

    h) 1976, 4258 y 80275

    i) 6175, 8632 y 73853

    j) 9846, 5700 y 94567

11. Para cada $n \in \mathbb{Z}^+$, ¿cuál es el $MCD(n,\ n+1)$ y $MCM(n,\ n+1)$?

12. Para $a,\ b,\ d \in \mathbb{Z}^+$ y $d = MCD(a,\ b)$, demostrar que $MCD(\frac{a}{d},\ \frac{b}{d}) = 1$

13. Para $a,\ b,\ n \in \mathbb{Z}^+$, demostrar que $MCD(n \cdot a,\ n \cdot b) = n \cdot MCD(a,\ b)$

14. Sea la relación R en $\mathbb{Z}^+$, donde $(a,\ b) \in R$ si $MCD(a,\ b) = 1$. ¿Es la relación R reflexiva?, ¿es la relación R simétrica?, ¿es la relación R antisimétrica?, y ¿es la relación R transitiva?

15. Apoyados en el algoritmo de Euclides determinar el Máximo Común Divisor (MCD) de las siguientes parejas de números enteros:

    a) 225 y 350
    b) 254 y 896
    c) 425 y 789
    d) 486 y 964
    e) 487 y 765
    f) 504 y 540
    g) 576 y 748
    h) 1976 y 80275
    i) 6175 y 73853

16. Sea $m \in \{2,\ 3,\ 4,\ 5,\ 6,\ 7,\ 8,\ 9,\ 10,\ 11,\ 12\}$. Para los valores de m presentados anteriormente, ¿cuáles serían todos los valores que servirían para que 30 y 35 sean congruentes?

17. Sea $m \in \{2,\ 3,\ 4,\ 5,\ 6,\ 7,\ 8,\ 9,\ 10,\ 11,\ 12\}$. Para los valores de m presentados anteriormente, ¿cuáles serían todos los valores que servirían para que 40 y 52 sean congruentes?

18. Sea $m \in \{2,\ 3,\ 4,\ 5,\ 6,\ 7,\ 8,\ 9,\ 10,\ 11,\ 12\}$. Para los valores de m presentados anteriormente, ¿cuáles serían todos los valores que servirían para que 47 y 63 sean congruentes?

19. Sea $m \in \{2,\ 3,\ 4,\ 5,\ 6,\ 7,\ 8,\ 9,\ 10,\ 11,\ 12\}$. Para los valores de m presentados anteriormente, ¿cuáles serían todos los valores que servirían para que 58 y 70 sean congruentes?

20. Cuál es el mensaje original después de desencriptar "htwwjhyt" utilizando en el encriptamiento de Julio Cesar[1] un desplazamiento de cinco?

21. Cuál es el mensaje original después de desencriptar "htwwjhyt" utilizando en el encriptamiento de Julio Cesar[2] un desplazamiento de cinco?

[1] En este caso trabajar con el alfabeto inglés, el cual es: $\{A,\ B,\ C,\ D,\ E,\ F,\ G,\ H,\ I,\ J,\ K,\ L,\ M,\ N,\ O,\ P,\ Q,\ R,\ S,\ T,\ U,\ V,\ W,\ X,\ Y,\ Z\}$

[2] Utilizando el mismo alfabeto que en el ejercicio anterior.

22. ¿Cómo se representa el número $(3213310)_4$ en base 6?

23. ¿Cómo se representa el número $(3403414)_5$ en base 7?

24. ¿Cómo se representa el número $(3213310)_4$ en base 6?

25. ¿Cómo se representa el número $(14315234)_6$ en base 9?

26. ¿Cuál es el resultado de multiplicar los números en base dos 10101111 y 10011011?, justificar la respuesta al desarrollar la prueba de escritorio del algoritmo.

27. ¿Cuál es el resultado de multiplicar los números en base dos 11101011 y 10101010?, justificar la respuesta al desarrollar la prueba de escritorio del algoritmo.

28. ¿Cuál es el resultado de multiplicar los números en base dos 10011010 y 11101011?, justificar la respuesta al desarrollar la prueba de escritorio del algoritmo.

29. ¿Cuál es el resultado de multiplicar los números en base dos 10110010 y 11001101?, justificar la respuesta al desarrollar la prueba de escritorio del algoritmo.

Bibliografía

[B1988] Bustamente, Alfonso. 1988. "Elementos de Algebra en Ciencias de la Computación". Serie de textos universitarios, Universidad ICESI, Cali.

[C1989] Caicedo, Xavier. 1989. "Elementos de Lógica Matemática y Calculabilidad". Universidad de los Andes, Bogotá.

[dC2004] de Castro Korgi, Rodrigo. 2004. "Teoría de la Computación: lenguajes, autómatas, gramáticas", Universidad Nacional de Colombia, Facultad de Ciencias, Departamento de Matemáticas.

[G1997] Grimaldi, R.. 1997. "Matemáticas Discreta y Combinatoria". Addison-Wesley Iberoamericana.

[J1997] Johnsonbaugh, R.. 1997. "Matemáticas Discretas". Prentice Hall.

[J2009] Jiménez Murillo, José A.. 2009. "Matemáticas para la Computación". Alfaomega.

[KBR1997] Kolman, B., Busby, R. C. y Ross, S.. 1997. "Estructuras de Matemáticas Discretas para la Computación". Prentice Hall.

[MAI2004] Ministerio de Educación Nacional Republica de Colombia - Acofi - Icfes. 2004. "Exámenes de Calidad de la Educación Superior en Ingeniería de Sistemas: Guía de Orientación". ICFES, Bogotá D. C..

[MAI2005] Ministerio de Educación Nacional Republica de Colombia - Acofi - Icfes. 2005. "Exámenes de Calidad de la Educación Superior en Ingeniería de Sistemas: Guía de Orientación". ICFES, Bogotá D. C..

[MAI2006] Ministerio de Educación Nacional Republica de Colombia - Acofi - Icfes. 2006. "Exámenes de Calidad de la Educación Superior en Ingeniería de Sistemas: Guía de Orientación" [online]. ICFES, Bogotá D. C..

Disponible de internet:
http://200.14.205.63:8080/portalicfes/home_2/rec/arc_4928.pdf

[MI2010] Ministerio de Educación Nacional Republica de Colombia - Icfes. 2010. "Guía de Orientacion: Examen de Estado de Calidad de la Educación Superior en Ingeniería de Sistemas (ECAES)" [online]. ICFES, Bogotá D. C..

Disponible de internet:
http://web2.icfes.gov.co/index.php?option=com_docman&task=
doc_view&gid=2807

[MIA2003] Ministerio de Educación Nacional Republica de Colombia - Icfes - Acofi. 2003. "Exámenes de Calidad de la Educación Superior, Ingeniería de Sistemas: Cuadernillos de Preguntas Primera y Segunda Sesión". ICFES.

[MIA2004] Ministerio de Educación Nacional Republica de Colombia - Icfes - Acofi. 2004. "Exámenes de Calidad de la Educación Superior, Ingeniería de Sistemas: Cuadernillo de Preguntas y Respuestas Segunda Sesión" [online]. ICFES.

Disponible de internet:
http://200.14.205.63:8080/portalicfes/home_2/rec/arc_4181.pdf
http://200.14.205.63:8080/portalicfes/home_2/rec/arc_4237.xls

[R2004] Rosen, K. H.. 2004. "Matemática Discreta y sus Aplicaciones". Mc Graw Hill Interamericana de España.

[RW1990] Ross, K. A. y Wright, C. R. B.. 1990. "Matemáticas Discretas". Prentice Hall.