Teoría de la Computación
Ejercicios resueltos *Rosen. Matemáticas Discretas. 5ta edición*

Ingeniería en Informática FICH-UNL
www.cimec.org.ar/tcomp

1 Los fundamentos: lógica y demostración, conjuntos y funciones

1.1 Lógica

1.2 Equivalencias proposicionales

- **Ejercicio 9.** Demuestra, sin utilizar tablas de verdad, que cada una de las implicaciones del ejercicio 7 es una tautología (por brevedad, sólo se resolverán las implicaciones a) y d) de dicho ejercicio).

  Respuesta: Cuando se mencione "por equivalencia de implicación 1", o abreviadamente (EI1), se está haciendo referencia a la primer equivalencia lógica $p \longrightarrow q \equiv \neg p \vee q$ presentada en la tabla 6 del Rosen.

  – El ejercicio 7a) propone la siguiente implicación: $(p \wedge q) \longrightarrow p$

$$
\begin{array}{rl}
 & (p \wedge q) \longrightarrow p \\
\text{(por EI1)} & \equiv \neg(p \wedge q) \vee p \\
\text{(por ley de De Morgan)} & \equiv (\neg p \vee \neg q) \vee p \\
\text{(por ley conmutativa)} & \equiv (\neg q \vee \neg p) \vee p \\
\text{(por ley asociativa)} & \equiv \neg q \vee (\neg p \vee p) \\
\text{(por ley de negación)} & \equiv \neg q \vee \mathbf{V} \\
\text{(por ley de dominación)} & \equiv \mathbf{V}
\end{array}
$$

  – El ejercicio 7d) propone la siguiente implicación: $(p \wedge q) \longrightarrow (p \longrightarrow q)$

$$
\begin{array}{rl}
 & (p \wedge q) \longrightarrow (p \longrightarrow q) \\
\text{(por EI1)} & \equiv (p \wedge q) \longrightarrow (\neg p \vee q) \\
\text{(por EI1)} & \equiv \neg(p \wedge q) \vee (\neg p \vee q) \\
\text{(por ley de De Morgan en el primer paréntesis)} & \equiv (\neg p \vee \neg q) \vee (\neg p \vee q) \\
\text{(por leyes conmutativa y asociativa)} & \equiv (\neg p \vee \neg p) \vee (\neg q \vee q) \\
\text{(por ley idempotente en el primer paréntesis)} & \equiv \neg p \vee (\neg q \vee q) \\
\text{(por ley de negación en el segundo paréntesis)} & \equiv \neg p \vee \mathbf{V} \\
\text{(por ley de dominación)} & \equiv \mathbf{V}
\end{array}
$$

- **Ejercicio 13.** Determina si $(\neg q \land (p \longrightarrow q)) \longrightarrow \neg p$ es o no una tautología.

  Respuesta:

  Para resolver este ejercicio utilizaremos las equivalencias lógicas de las tablas 5 y 6 del libro. Debemos utilizar las leyes allí listadas de manera de determinar si el valor de verdad de la fórmula proposicional es siempre **V** para cualquier combinación de valores de verdad de p y q, es decir, si es una tautología o no.

$$
\begin{aligned}
& & (\neg q \land (p \longrightarrow q)) \longrightarrow \neg p & \\
& \text{(por EI1)} & \equiv \neg(\neg q \land (p \longrightarrow q)) \lor \neg p & \\
& \text{(por EI1)} & \equiv \neg(\neg q \land (\neg p \lor q)) \lor \neg p & \\
& \text{(por ley distributiva)} & \equiv \neg((\neg q \land \neg p) \lor (\neg q \land q)) \lor \neg p & \\
& \text{(por ley de negación)} & \equiv \neg((\neg q \land \neg p) \lor \mathbf{F}) \lor \neg p & \\
& \text{(por ley de identidad)} & \equiv \neg(\neg q \land \neg p) \lor \neg p & \\
& \text{(por ley de De Morgan)} & \equiv q \lor p \lor \neg p & \\
& \text{(por ley de negación)} & \equiv q \lor \mathbf{V} & \\
& \text{(por ley de dominación)} & \equiv \mathbf{V} &
\end{aligned}
$$

  por lo que queda demostrado que es una tautología.

- **Ejercicio 22.** Demuestra que $(p \longrightarrow q) \lor (p \longrightarrow r)$ y $p \longrightarrow (q \lor r)$ son lógicamente equivalentes.

  Respuesta:

  Partiremos de la primer proposición compuesta y llegaremos a la segunda. Lo importande de ver es que las leyes que figuran en las tablas se leen de izquierda a derecha y de derecha a izquerda.

$$
\begin{aligned}
& & (p \longrightarrow q) \lor (p \longrightarrow r) & \\
& \text{(por EI1 en ambos paréntesis)} & \equiv (\neg p \lor q) \lor (\neg p \lor r) & \\
& \text{(por ley conmutativa)} & \equiv (q \lor \neg p) \lor (\neg p \lor r) & \\
& \text{(por ley asociativa)} & \equiv q \lor (\neg p \lor \neg p) \lor r & \\
& \text{(por ley idempotente)} & \equiv q \lor \neg p \lor r & \\
& \text{(por ley conmutativa)} & \equiv \neg p \lor q \lor r & \\
& \text{(por ley asociativa)} & \equiv \neg p \lor (q \lor r) & \\
& \text{(por EI1)} & \equiv p \longrightarrow (q \lor r) &
\end{aligned}
$$

  por lo que queda demostrada la equivalencia.

1.3 Predicados y cuantificadores

- **Ejercicio 9.** Sea $P(x)$ la sentencia «x habla ruso» y $Q(x)$ «x conoce el lenguaje de programación C++». Exprese cada una de las siguientes sentencias en términos de $P(x)$ y $Q(X)$, cuantificadores y conectivos lógicos. El dominio para los cuantificadores consiste en todos los estudiantes de la facultad.

  a) Hay un estudiante en tu facultad que habla ruso y conoce C++.

  b) Hay un estudiante en tu facultad que habla ruso pero que no conoce C++.

  c) Todos los estudiantes de tu facultad hablan ruso o conocen C++.

  d) Ningún estudiante de tu facultad habla ruso o conoce C++.

  Respuesta: Dados los predicados $P(x)$ y $Q(x)$ y siendo el dominio de x todos los alumnos de la facultad, se aplican cuantificadores y conectores lógicos.

  a) $\exists x[P(x) \wedge Q(x)]$

  b) $\exists x[P(x) \wedge \neg Q(x)]$

  c) $\forall x[P(x) \vee Q(x)]$

  d) $\neg\exists x[P(x) \vee Q(x)]$

- **Ejercicio 23.**

  Traduce cada una de estas frases a expresiones lógicas usando predicados, cuantificadores y conectivos lógicos.

  a) Nadie es perfecto.

  b) No todo el mundo es perfecto.

  c) Todos tus amigos son perfectos.

  d) Todo el mundo es tu amigo y es perfecto.

  e) No todo el mundo es tu amigo o alguien no es perfecto.

  Respuesta:

  Utilizaremos los predicados $P(x)$: « x es perfecto» y $A(x)$: « x es tu amigo», siendo el dominio de x son todas las personas.

  a) $\neg\exists x P(x) \qquad (\equiv \forall x \neg P(x))$

  b) $\neg\forall x P(x) \qquad (\equiv \exists x \neg P(x))$

  c) $\forall x\ [A(x) \longrightarrow P(x)]$

  d) $\forall x\ [A(x) \wedge P(x)]$

  e) $\neg\forall x A(x) \vee \exists x \neg P(x)$

- **Ejercicio 33.** Halla un contraejemplo, si es posible, a estas sentencias universalmente cuantificadas, donde el dominio para todas las variables consiste en todos los enteros.

a) $\forall x\ (x^2 \geq x)$

b) $\forall x\ (x > 0 \vee x < 0)$

c) $\forall x\ (x = 1)$

Respuesta: Aplicando simple razonamiento matemático, se concluye lo siguiente:

a) No existe un contraejemplo, la sentencia es siempre verdadera para el dominio de los enteros.

b) El único valor entero que no es mayor que 0 ni menor que 0, es el propio valor 0 ($x = 0$).

c) Cualquier número entero distinto de 1 es un contraejemplo válido. Por ejemplo, ($x = 3$).

- **Ejercicio 43.** Muestra que $\exists x(P(x) \vee Q(x))$ y $\exists x P(x) \vee \exists x Q(x)$ tienen el mismo valor de verdad.

  Respuesta: Suponiendo que $P(x)$ es verdadera para algún valor de x, entonces $\exists x P(x) \vee \exists x Q(x)$ es verdadera más allá del valor de $Q(x)$. De la misma manera, si $Q(x)$ es verdadera para algún valor de x entonces $\exists x P(x) \vee \exists x Q(x)$ es verdadera independientemente del valor de $P(x)$.

  Por lo tanto, $\exists x(P(x) \vee Q(x))$ es una expresión equivalente de $\exists x P(x) \vee \exists x Q(x)$.

1.4 Cuantificadores anidados

- **Ejercicio 3.** Sea $Q(x, y)$ la sentencia "x ha enviado un e-mail a y", donde el dominio tanto para x como para y consiste en todos los estudiantes de tu clase. Expresa cada una de las siguientes cuantificaciones en lenguaje natural.

  Respuesta:

  a) $\exists x \exists y Q(x, y)$: Hay un estudiante de tu clase que le ha enviado un e-mail a alguno (podría ser a él mismo?).

  b) $\exists x \forall y Q(x, y)$: Hay un estudiante de tu clase que le ha enviado un e-mail a todos.

  c) $\forall x \exists y Q(x, y)$: Todos los estudiantes de tu clase le han enviado un e-mail a al menos uno.

  d) $\exists y \forall x Q(x, y)$: Hay un estudiante de tu clase que ha recibido un e-mail de todos.

  e) $\forall y \exists x Q(x, y)$: Todos los estudiantes de tu clase han recibido un e-mail de alguno.

  f) $\forall x \forall y Q(x, y)$: Todos los estudiantes de tu clase le han enviado e-mails a todos.

- **Ejercicio 10.** Sea $F(x, y)$ la sentencia x puede engañar a y, donde el dominio para x como para y consiste en todas las personas del mundo. Utiliza cuantificadores para expresar cada una de las siguientes sentencias.

  a) Todo el mundo puede engañar a Fred.

  b) Evelyn puede engañar a todo el mundo.

  c) Todo el mundo puede engañar a alguien.

  d) No hay nadie que pueda engañar a todo el mundo.

  e) Todo el mundo puede ser engañado por alguien.

f) Nadie puede engañar a Fred y a Jerry (a los dos).

g) Nadie puede engañar exactamente a dos personas.

h) Hay exactamente una persona a quien todo el mundo puede engañar.

i) Nadie puede engañarse a sí mismo.

j) Hay alguien que puede engañar a exactamente una persona.

Respuesta:

a) $\forall x\ F(x, \text{Fred})$

b) $\forall x\ F(\text{Evelyn}, x)$

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

d) $\neg\exists x\ \forall y\ F(x, y) \qquad (\equiv \forall x \exists y\ \neg F(x, y))$

e) $\forall x\ \exists y\ F(y, x)$

f) $\neg\exists x\ [F(x, \text{Fred}) \wedge F(x, \text{Jerry})]$

g) $\neg\exists x\ \forall y\ \forall z\ [F(x, y) \wedge F(x, z) \wedge \forall w\ ((w \neq y) \wedge (w \neq z) \longrightarrow \neg F(x, w))]$

h) $\exists x\ \forall y\ [F(y, x) \wedge \forall z\ (F(y, z) \longrightarrow x = z)]$

i) $\neg\exists x\ F(x, x)$

j) $\exists x\ \exists y\ [F(x, y) \wedge \forall z\ (F(x, z) \longrightarrow z = y)]$

- **Ejercicio 28.** Determina el valor de verdad de cada una de estas sentencias si el dominio de todas las variables es el conjunto de los números reales.

  a) $\forall x\ \exists y\ (x^2 = y)$

  b) $\forall x\ \exists y\ (x = y^2)$

  c) $\exists x\ \forall y\ (xy = 0)$

  d) $\exists x\ \exists y\ (x + y \neq y + x)$

  e) $\forall x\ (x \neq 0 \longrightarrow\ \exists y\ (xy = 1))$

  f) $\exists x \forall y\ (y \neq 0 \longrightarrow\ xy = 1)$

  g) $\forall x \exists y\ (x + y = 1)$

  h) $\exists x \exists y\ (x + 2y = 2 \wedge 2x + 4y = 5)$

  i) $\forall x \exists y\ (x + y = 2 \wedge 2x - y = 1)$

  j) $\forall x \forall y \exists z\ (z = (x + y)/2)$

  Respuesta:

  a) **V**. El cuadrado de un número real es otro número real.

  b) **F**. El cuadrado de un número real es no negativo, por lo que cualquier $x < 0$ no es el cuadrado de ningún número real.

c) **V**. Tomando $x = 0$.

d) **F**. Si fuese verdadero estaríamos violando la propiedad conmutativa de la suma, por lo que se concluye que es falso.

e) **V**. Ya que todo número real no nulo tiene su inverso multiplicativo.

f) **F**. No existe número x que sea inverso multiplicativo de todos los números reales no nulos.

g) **V**. Seleccionando $y = 1 - x$ la propiedad se cumple para todo x.

h) **F**. El sistema de ecuaciones es incompatible, por lo que no tiene solución.

i) **F**. El sistema de ecuaciones solo tiene solución con $x = 1$ e $y = 1$. Para cualquier otro valor de x las igualdades no se cumplen para ninguna y.

j) **V**. Debido a que z es el promedio entre x e y.

- **Ejercicio 37.** Encuentra un contraejemplo, si es posible, de estas sentencias universalmente cuantificadas, donde el dominio de todas las variables consiste en todos los enteros.

  a) $\forall x \forall y (x^2 = y^2 \rightarrow x = y)$

  b) $\forall x \exists y (y^2 = x)$

  c) $\forall x \forall y (xy \geq x)$

  Respuesta: Lo primero que tengo que realizar es determinar el valor de verdad de cada proposición. Si es falsa, tengo que encontrar el contraejemplo. En cambio, si es verdadera, no existe el contraejemplo.

  a) La sentencia nos dice que si dos enteros cumplen que sus cuadrados son iguales, entonces son el mismo entero. Esto no es cierto, porque estamos trabajando con los enteros (positivos, nulo y negativos). Para hallar el contraejemplo me tengo que preguntar: ¿Hay un par de enteros, distintos entre si, cuyos cuadrados son iguales? Es decir, un par de enteros que hagan falsa la implicación en cuestión. Claramente hay muchos (infinitos). Tomamos un entero cualquiera, por ejemplo, el $x = -7$ y vemos que con el $y = 7$ cumplen que $x^2 = 49 = y^2$. Pero claramente $x \neq y$.

  b) Esta sentencia afirma que, dado un entero, puedo hallar otro tal que su cuadrado es el entero dado. Dicho de otra forma, todo entero es el cuadrado de algún otro. Así, por ejemplo, para el 1 puedo hallar el -1, para el 0, puedo hallar el mismo 0, para el 25 puedo hallar el 5. Claramente estoy haciendo trampa, porque estoy tomando cuadrados exactos. Entonces, vemos que la sentencia no es cierta, porque, por ejemplo para el -8 no puedo hallar ningún entero cuyo cuadrado sea -8 (en realidad para ningún negativo, ni para ningún entero positivo que no sea cuadrado perfecto).

  c) En este caso, nos dice que el producto de dos enteros cualesquiera es mayor o igual que ellos. Por ejemplo, si tomamos $x = 2$ y $y = 1$, el producto $xy = 2$ es mayor o igual a x (y a y). ¿Ésto se cumple siempre? Claramente no; basta con tomar un entero x positivo y un entero y negativo para que esto se cumpla. También es válido como contraejemplo, tomar un x positivo y $y = 0$.

1.5 Métodos de demostración

- **Ejercicio 3.** Construye un argumento utilizando reglas de inferencia para mostrar que las hipótesis *"Randy trabaja duro"*, *"Si Randy trabaja duro, será un chico soso"*, *"Si Randy es un chico soso, no conseguirá el trabajo"* implican la conclusión *"Randy no conseguirá el trabajo"*.

  Respuesta: En primer lugar, se deben identificar las hipótesis y la conclusión del argumento deductivo que debemos construir. Estas son:

  - H_1 : "Randy trabaja duro".
  - H_2 : "Si Randy trabaja duro, será un chico soso".
  - H_3 : "Si Randy es un chico soso, no conseguirá el trabajo".
  - C : "Randy no conseguirá el trabajo".

  Luego, el argumento deductivo lo vamos a construir de la siguiente manera:

  1. De H_1 y H_2, aplicando el *Modus Ponens*, puedo concluir C_1: "Randy será un chico soso". $(H_1 \wedge H_2 \longrightarrow C_1)$
  2. A partir de C_1 y H_3, aplicando nuevamente el *Modus Ponens*, puedo concluir C: "Randy no conseguirá el trabajo", que era lo que lo que deseábamos concluir. $(C_1 \wedge H_3 \longrightarrow C)$

- **Ejercicio 13.** Determina si es correcto cada uno de los siguientes argumentos. Si el argumento es correcto, cuál es la regla de inferencia utilizada? Si no lo es, qué error lógico ocurre?

  a) Si n es un número real tal que $n > 1$, entonces $n^2 > 1$. Supongamos que $n^2 > 1$, entonces $n > 1$.

  b) El número $\log_2(3)$ es irracional si no es la razón de dos enteros. Por lo tanto, como $\log_2(3)$ no se puede escribir en la forma a/b donde a y b son enteros, es irracional.

  c) Si n es un número real y $n > 3$, entonces $n^2 > 9$. Supongamos que $n^2 \leq 9$, entonces $n \leq 3$.

  d) Si n es un número real y $n > 2$, entonces $n^2 > 4$. Supongamos que $n \leq 2$, entonces $n^2 \leq 4$.

  Respuesta:

  a) El argumento es incorrecto, ya que se comete la falacia de afirmar la conclusión. Esto es así ya que podemos identificar en el argumento que la primera sentencia se puede escribir como $p \longrightarrow q$, teniendo en cuenta que $p : n > 1$, $q : n^2 > 1$. Luego, asume que se cumple q, con lo cual concluye p, es decir, el argumento se puede expresar como: $[(p \longrightarrow q) \wedge q] \longrightarrow p$, que es la falacia de afirmar la conclusión.

  b) El argumento se puede reescribir de la siguiente manera: Si $\log_2(3)$ no es la razón de dos enteros, entonces es irracional. Luego, como $\log_2(3)$ no se puede escribir como la razón de dos enteros a y b, puedo concluir que es irracional. Identificando a p: "$\log_2(3)$ no es la razón de dos enteros" y q: "$\log_2(3)$ es irracional", el argumento anterior se puede expresar como: $[(p \longrightarrow q) \wedge p] \longrightarrow q$, que es el *Modus Ponens*. Es decir que el argumento es correcto.

  c) En este caso, el argumento es correcto ya que se puede expresar en la forma $[(p \longrightarrow q) \wedge \neg q] \longrightarrow \neg p$, que es el *Modus Tollens*.

  d) Este argumento o razonamiento lo podemos escribir en la forma $[(p \longrightarrow q) \wedge \neg p] \longrightarrow \neg q$. El mismo es incorrecto, ya que es la falacia de negar la hipótesis.

- **Ejercicio 17.** Demuestra la proposición $P(0)$, donde $P(n)$ es la proposición: *si n es un entero positivo mayor que* 1, *entonces* $n^2 > n$. ¿Qué tipo de demostración has empleado?

  Respuesta: En este ejercicio debemos demostrar que la proposición $P(n)$ es verdadera para el caso $n = 0$. Realizando dicho reemplazo nos queda:

  $P(0)$: *si* 0 *es un entero positivo mayor que* 1, *entonces* $0^2 > 0$.

  La implicación resultante tiene valor de verdad **T**, dado que la hipótesis es falsa ($\mathbf{F} \longrightarrow q \equiv \mathbf{T}$), quedando demostrado $P(0)$. La demostración utilizada es una *demostración vacua*.

- **Ejercicio 20.** Demuestra que el cuadrado de un número par es un número par utilizando:

  a) una demostración directa

  b) una demostración indirecta

  c) una reducción al absurdo

  Respuesta: En primer lugar debemos definir la proposición $p \longrightarrow q$ a demostrar. En el ejercicio puede verse que p: n es un número par, q: el cuadrado de n es par. Acto seguido, podemos escribir en lenguaje matemático estricto la sentencia, esto es:

  $$(n = 2k_1) \longrightarrow (n^2 = 2k_2)$$

  donde n, k_1 y k_2 son números enteros.

  a) Para la demostración directa, comenzamos desde la hipótesis y a partir de operaciones algebraicas que preserven la igualdad, intentamos arribar a la conclusión.

  $$\begin{aligned} & n = 2k_1 \\ \text{multiplicando a ambos lados por } n \quad & n^2 = 2k_1 n \\ \text{considerando } k_2 = k_1 n \quad & n^2 = 2k_2 \\ & q.e.d \end{aligned}$$

  b) Para la demostración indirecta utilizamos la contrarrecíproca de la implicación que expresa a nuestro enunciado. Es decir, suponemos que el cuadrado de n es un número impar y debemos arribar a que n es impar.

  $$\begin{aligned} \text{hipótesis} \quad & n^2 = 2k_2 - 1 \\ \text{sumo } 2n + 1 \text{ a ambos lados} \quad & n^2 + 2n + 1 = 2k_2 + 2n \\ \text{simplificando} \quad & (n+1)^2 = 2(k_2 + n) \\ \text{tomando } k_3 = k_2 + n \quad & (n+1)^2 = 2k_3 \qquad \text{(a)} \end{aligned}$$

  En este punto sabemos que $(n+1)^2$ es un número par, algo que no nos alcanza para determinar la paridad de n. Por lo tanto, vamos a utilizar una demostración auxiliar para desenredar el camino.

Demostración auxiliar. Quiero demostrar ahora que si un número m cumple que si m^2 es par, entonces m es par (notesé que es la implicación recíproca de la que se pretende demostrar en el ejercicio). Utilizando una demostración indirecta:

$$\begin{aligned} &\text{hipótesis con } m, c \text{ enteros} && m = 2c + 1 \\ &\text{elevo al cuadrado a ambos lados} && m^2 = (2c_1 + 1)^2 \\ &\text{manipulando} && m^2 = 2(2c_1^2 + 2c_1) + 1 \\ &\text{tomando } c_2 = 2c_1^2 + 2c_1 && m^2 = 2c_2 + 1 \\ & && q.e.d \end{aligned} \tag{b}$$

Regresando a (a), (tomando a $n + 1$ como el m de la demostración auxiliar), y utilizando el resultado recién hallado (b), podemos asegurar ahora que $n + 1$ es un número par y con una simple manipulación algebraica, encontrar que n es impar, completando la demostración.

$$\begin{aligned} &\text{por (a) y (b)} && n + 1 = 2k_1 \\ &\text{despejo } n && n = 2k_1 - 1 \\ & && q.e.d \end{aligned}$$

c) Para la demostración por reducción al absurdo suponemos que p y $\neg q$ son verdaderas, esto es n es un número par y n^2 es un número impar, en símbolos: $(p \wedge \neg q)$. Ahora bien, siguiendo los pasos de la demostración indirecta, vimos que $\neg q \longrightarrow \neg p$, por lo que $\neg p$ debe ser verdadera también. Esto conduce a la contradicción $p \wedge \neg p$ (n es un número par e impar a la vez) lo que es un absurdo ($p \wedge \neg p \equiv \mathbf{F}$). q.e.d.

NOTA: La reducción al absurdo utilizada aquí puede definirse simbólicamente como:

$$[(p \wedge \neg q) \longrightarrow \mathbf{F}] \longrightarrow [p \longrightarrow q]$$

- **Ejercicio 25.** Demuestra que la suma de un número irracional y un número racional es un número irracional utilizando una demostración por reducción al absurdo.

  Respuesta: Se aplica demostración por reducción al absurdo. Supongamos que r es un número racional e i un número irracional, y que la suma $s = r + i$ también es racional.

  Por definición, un número real es racional si existen dos enteros a y b, con $b \neq 0$, tales que $r = a/b$. Por lo tanto, la suma entre dos números racionales r y $s = c/d$, con c y d enteros y $d \neq 0$, también puede expresarse como la razón de números enteros:

$$r + s = \frac{a}{b} + \frac{c}{d} = \frac{ad + bc}{bd}$$

  Despejando i de la suma, obtenemos que $s + (-r) = i$ es racional, lo cual es un absurdo.

- **Ejercicio 29.** Demuestra que si x es irracional, entonces $1/x$ también lo es.

  Respuesta: Resulta conveniente aplicar una demostración indirecta, es decir, mostraremos que si $1/x$ es racional, entonces x también es racional. Partimos entonces de suponer que $1/x$ es racional. Luego, por definición de número racional $1/x = a/b$, con a y b enteros y $b \neq 0$.

  Pero $1/x$ no puede ser 0 ya que si multiplicamos por x ambos lados de la ecuación, estaríamos ante el absurdo $1 = 0 \cdot x$. Por lo tanto, $a \neq 0$.

  Aplicando álgebra, tenemos que:

$$x = 1/(1/x) = 1/(a/b) = b/a$$

  que es el cociente entre dos números enteros no nulos. Por lo tanto, x es racional.

- **Ejercicio 43.** Demuestra que estas tres sentencias son equivalentes. *(i)* $3x + 2$ es un entero par; *(ii)* $x + 5$ es un entero impar, y *(iii)* x^2 es un entero par.

  Respuesta: Para este tipo de ejercicios, se deben demostrar, en principio, 3 dobles implicaciones (6 implicaciones), a saber, $(i) \leftrightarrow (ii)$, $(ii) \leftrightarrow (iii)$ y $(iii) \leftrightarrow (i)$. Pero teniendo en cuenta dos de ellas, alcanza (4 implicaciones). Estas últimas, se pueden reducir a 3 siempre que podamos, por lo que demostraremos sólo las siguientes implicaciones: $(i) \longrightarrow (ii) \longrightarrow (iii) \longrightarrow (i)$.

  - $(i) \longrightarrow (ii)$ (por demostración indirecta)

    Supongamos que $x + 5$ es par (debemos demostrar que $3x + 2$ es impar). Luego, existe $k \in \mathbb{Z}$ tal que $x + 5 = 2k$. Ahora trabajemos con esta igualdad:

$$\begin{aligned} x + 5 &= 2k \\ x &= 2k - 5 \\ 3x &= 3(2k - 5) \\ 3x + 2 &= 3(2k - 5) + 2 \\ &= 6k - 15 + 2 \\ &= 6k - 13 \\ &= 6k - 14 + 1 \\ &= 2(3k - 7) + 1 \\ &= 2l + 1 \end{aligned}$$

    donde $l = 3k - 7$ es entero por ser producto y diferencia de enteros. Luego, hemos demostrado que $3x + 2$ es impar.

  - $(ii) \longrightarrow (iii)$ (por demostración directa)

Supongamos que $x + 5$ es impar. Luego existe $k \in \mathbb{Z}$ tal que $x + 5 = 2k + 1$. Entonces:

$$\begin{aligned} x + 5 &= 2k + 1 \\ x &= 2k - 4 = 2(k - 2) \\ x^2 &= 4(k - 2)^2 = 2(2(k - 2)^2) = 2m \end{aligned}$$

donde $m \in \mathbb{Z}$ por ser producto de enteros. Luego x^2 es par.

- $(iii) \longrightarrow (i)$ (por demostración indirecta)

  Supongamos que $3x+2$ es impar (debo probar que x^2 es impar). Luego, existe $k_1 \in \mathbb{Z}$ tal que $3x+2 = 2k_1+1$. Entonces,

$$\begin{aligned} 3x + 2 &= 2k_1 + 1 \\ 3x &= 2(k_1 - 1) + 1 \end{aligned}$$

  Es decir, $3x$ es impar, lo que implica que x también lo es (de lo contrario, $3x$ sería par).

  Si x es impar, existe $k_2 \in \mathbb{Z}$ tal que $x = 2k_2 + 1$, luego

$$\begin{aligned} x^2 &= (2k_2 + 1)^2 \\ &= 2(2k_2^2 + 2k_2) + 1 \\ &= 2k + 1 \end{aligned}$$

  donde $k \in \mathbb{Z}$ por ser producto y sumas de enteros. Finalmente, x^2 es impar.

1.6 Conjuntos

- **Ejercicio 7.** Determina si cada una de estas sentencias es verdadera o falsa.

  a) $0 \in \emptyset$

  b) $\emptyset \in \{0\}$

  c) $\{0\} \subset \emptyset$

  d) $\emptyset \subset \{0\}$

  e) $\{0\} \in \{0\}$

  f) $\{0\} \subset \{0\}$

  g) $\{\emptyset\} \subseteq \{\emptyset\}$

  Respuesta:

  a) $0 \in \emptyset$: **F**. El conjunto vacío no contiene elementos.

  b) $\emptyset \in \{0\}$: **F**. El conjunto de la derecha tiene un único elemento, el cero (0). El vacío no es elemento de ese conjunto.

  c) $\{0\} \subset \emptyset$: **F**. El conjunto vacío (el de la derecha) no contiene subconjuntos propios.

d) $\emptyset \subset \{0\}$: **V**. El conjunto vacío es subconjunto propio de cualquier conjunto no vacío (en particular el de la derecha, que posee un elemento: el cero).

e) $\{0\} \in \{0\}$: **F**. El único elemento que posee el conjunto de la derecha es el cero. Por lo tanto, el conjunto $\{0\}$ no es elemento del conjunto de la derecha.

f) $\{0\} \subset \{0\}$: **F**. Para que un conjunto sea subconjunto propio de otro, no pueden ser iguales.

g) $\{\emptyset\} \subseteq \{\emptyset\}$: **V**. Todo conjunto es subconjunto de si mismo.

- **Ejercicio 8.** Determina si cada una de estas sentencias es verdadera o falsa.

  a) $\emptyset \in \{\emptyset\}$

  b) $\emptyset \in \{\emptyset, \{\emptyset\}\}$

  c) $\{\emptyset\} \in \{\emptyset\}$

  d) $\{\emptyset\} \in \{\{\emptyset\}\}$

  e) $\{\emptyset\} \subset \{\emptyset, \{\emptyset\}\}$

  f) $\{\{\emptyset\}\} \subset \{\emptyset, \{\emptyset\}\}$

  g) $\{\{\emptyset\}\} \subset \{\{\emptyset\}, \{\emptyset\}\}$

  Respuesta:

  a) $\emptyset \in \{\emptyset\}$: **V** ya que $\emptyset$ es el único elemento perteneciente o que está en el conjunto $\{\emptyset\}$.

  b) $\emptyset \in \{\emptyset, \{\emptyset\}\}$: **V** ya que el $\emptyset$ es uno de los elementos que están en el conjunto $\{\emptyset, \{\emptyset\}\}$.

  c) $\{\emptyset\} \in \{\emptyset\}$: **F** ya que $\{\emptyset\}$ no es un elemento de $\{\emptyset\}$.

  d) $\{\emptyset\} \in \{\{\emptyset\}\}$: **V** ya que en éste caso $\{\emptyset\}$ sí es elemento de $\{\{\emptyset\}\}$.

  e) $\{\emptyset\} \subset \{\emptyset, \{\emptyset\}\}$: **V** ya que $\{\emptyset\}$ es subconjunto de $\{\emptyset, \{\emptyset\}\}$ porque todo elemento de $\{\emptyset\}$ está en $\{\emptyset, \{\emptyset\}\}$.

  f) $\{\{\emptyset\}\} \subset \{\emptyset, \{\emptyset\}\}$: **V** (ídem anterior)

  g) $\{\{\emptyset\}\} \subset \{\{\emptyset\}, \{\emptyset\}\}$: **F** ya que si bien todo elemento de $\{\{\emptyset\}\}$ está en $\{\{\emptyset\}, \{\emptyset\}\}$, ambos conjuntos son iguales y el símbolo $\subset$ está indicando que no pueden ser iguales los conjuntos. Si hubiese sido $\{\{\emptyset\}\} \subseteq \{\{\emptyset\}, \{\emptyset\}\}$ entonces sería **V**.

- **Ejercicio 18.** Determina si alguno de estos conjuntos es el conjunto de partes de algún conjunto

  a) $\emptyset$

  b) $\{\emptyset, \{a\}\}$

  c) $\{\emptyset, \{a\}, \{\emptyset, a\}\}$

  d) $\{\emptyset, \{a\}, \{b\}, \{a, b\}\}$

  Respuesta:

  a) $\emptyset$: no es el conjunto de partes de ningún conjunto, ya que el conjunto de partes es aquél conjunto cuyos elementos son *todos* los subconjuntos de un conjunto dado. Es decir, que al menos el conjunto de partes

debería poseer un elemento que sería el conjunto vacío, en cuyo caso lo denotaríamos como $P(\emptyset) = \{\emptyset\}$.

b) $\{\emptyset, \{a\}\}$: sí, es el conjunto de partes del conjunto $S = \{a\}$.

c) $\{\emptyset, \{a\}, \{\emptyset, a\}\}$: no es conjunto de partes de ningún conjunto (notar que el cardinal del conjunto dado es igual a 3, lo cual no sería posible si el conjunto dado fuese el conjunto de partes de otro conjunto, ya que su cardinal sería $2^{|S|}$).

d) $\{\emptyset, \{a\}, \{b\}, \{a, b\}\}$: sí, es el conjunto de partes del conjunto $S = \{a, b\}$.

- **Ejercicio 22.** Supongamos que $A \times B = \emptyset$, donde A y B son conjuntos. ¿Qué se puede concluir?

  Respuesta: Podemos concluir que $A = \emptyset$ o $B = \emptyset$. Si no fuera así, tanto A como B tendrían al menos un elemento cada uno, es decir, que existen $a \in A$ y $b \in B$. Entonces, hay al menos un par ordenado (a, b) en el producto cartesiano $A \times B$, por lo tanto no sería vacío. Esta contradicción nos asegura que A o B (o ambos) es vacío.

1.7 Operaciones con Conjuntos

- **Ejercicio 6.** Sea A un conjunto. Demuestra que

  a) $A \cup \emptyset = A$

  b) $A \cap \emptyset = \emptyset$

  c) $A \cup A = A$

  d) $A \cap A = A$

  e) $A - \emptyset = A$

  f) $A \cup U = U$

  Respuesta: En este ejercicio vamos a realizar varias demostraciones (algunas de ellas son identidades listadas en la Tabla 1 de la sección), para lo cual vamos a utilizar la notación constructiva de conjuntos y los operadores lógicos ya estudiados en secciones anteriores.

  a) $A \cup \emptyset = A$: Ley de identidad.

$$
\begin{aligned}
A \cup \emptyset = & \\
\text{notación constructiva} \quad & = \{x | x \in A\} \cup \{x | x \in \emptyset\} \\
\text{def. de unión} \quad & = \{x | (x \in A \vee x \in \emptyset)\} \\
& = \{x | (x \in A \vee \mathbf{F})\} \\
\text{por ley de identidad (lógica)} \quad & = \{x | x \in A\} \\
\text{por def. de conjunto} \quad & = A
\end{aligned}
$$

b) $A \cap \emptyset = \emptyset$: Ley de dominación.

$$
\begin{aligned}
A \cap \emptyset = & \\
\text{notación constructiva} \quad & = \{x | x \in A\} \cap \{x | x \in \emptyset\} \\
\text{def. de intersección} \quad & = \{x | (x \in A \wedge x \in \emptyset)\} \\
& = \{x | (x \in A \wedge \mathbf{F})\} \\
\text{por ley de dominación (lógica)} \quad & = \{x | \mathbf{F}\} \\
\text{por def. de conjunto vacío} \quad & = \emptyset
\end{aligned}
$$

c) $A \cup A = A$: Ley idempotentes.

$$
\begin{aligned}
A \cap \emptyset = & \\
\text{notación constructiva} \quad & = \{x | x \in A\} \cup \{x | x \in A\} \\
\text{def. de unión} \quad & = \{x | (x \in A \vee x \in A)\} \\
\text{por ley idempotente (lógica)} \quad & = \{x | x \in A\} \\
\text{por def. de conjunto} \quad & = A
\end{aligned}
$$

d) $A \cap A = A$: Ley idempotentes.

$$
\begin{aligned}
A \cap \emptyset = & \\
\text{notación constructiva} \quad & = \{x | x \in A\} \cap \{x | x \in A\} \\
\text{def. de intersección} \quad & = \{x | (x \in A \wedge x \in A)\} \\
\text{por ley idempotente (lógica)} \quad & = \{x | x \in A\} \\
\text{por def. de conjunto} \quad & = A
\end{aligned}
$$

e) $A - \emptyset = A$.

$$
\begin{aligned}
A - \emptyset = & \\
\text{notación constructiva} \quad & = \{x | x \in A\} - \{x | x \in \emptyset\} \\
\text{def. de diferencia} \quad & = \{x | (x \in A \wedge x \notin \emptyset)\} \\
& = \{x | x \in A \wedge \mathbf{T}\} \\
\text{identidad lógica} \quad & = \{x | x \in A\} \\
\text{por def. de conjunto} \quad & = A
\end{aligned}
$$

f) $A \cup U = U$.

$$
\begin{aligned}
A \cup U = & \\
\text{notación constructiva} \quad & = \{x | x \in A\} \cup \{x | x \in U\} \\
\text{def. de unión} \quad & = \{x | (x \in A \vee x \in U)\} \\
\text{todo elemento está en el universal} \quad & = \{x | x \in A \wedge \mathbf{T}\} \\
\text{identidad lógica} \quad & = \{x | x \in A\} \\
\text{por def. de conjunto} \quad & = A
\end{aligned}
$$

- **Ejercicio 12.** Sean A y B conjuntos, demuestra que:

  a) $(A \cap B) \subseteq A$

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

  c) $A - B \subseteq A$

  d) $A \cap (B - A) = \emptyset$

  e) $A \cup (B - A) = A \cup B$

  Respuesta:

  a) $(A \cap B) \subseteq A$. Debemos demostrar, por definición de subconjunto, que $\forall x\ (x \in (A \cap B) \longrightarrow x \in A)$. Tomando un elemento arbitrario x, por definición de intersección de conjuntos, si $x \in (A \cap B)$, entonces $(x \in A) \wedge (x \in B)$. De esta manera, se concluye que $x \in A$ es verdadero.

  b) $A \subseteq (A \cup B)$. Debemos demostrar, por definición de subconjunto, que $\forall x\ (x \in A \longrightarrow x \in (A \cup B))$. Tomando un elemento arbitrario x, por definición de unión de conjuntos y leyes de De Morgan, si $x \notin (A \cup B)$, entonces $(x \notin A) \wedge (x \notin B)$. De esta manera, se concluye que $x \notin A$ es verdadero, concluyendo la demostración indirecta.

  c) $A - B \subseteq A$. Debemos demostrar, por definición de subconjunto, que $\forall x\ (x \in (A - B) \longrightarrow x \in A)$. Tomando un elemento arbitrario x, por definición de diferencia de conjuntos, si $x \in (A - B)$, entonces $(x \in A) \wedge (x \notin B)$. De esta manera, se concluye que $x \in A$ es verdadero, concluyendo la demostración directa.

  d) $A \cap (B - A) = \emptyset$

$$
\begin{aligned}
A \cap (B - A) = & \\
\text{notación constructiva} \quad & = \{x | x \in A\} \cap \{x | x \in (B - A)\} \\
\text{def. de intersección y diferencia} \quad & = \{x | (x \in A \wedge x \in B \wedge x \notin A)\} \\
\text{ley conmutativa y de negación (lógica)} \quad & = \{x | x \in B \wedge \mathbf{F}\} \\
\text{dominación (lógica)} \quad & = \{x | \mathbf{F}\} \\
\text{por def. de conjunto} \quad & = \emptyset
\end{aligned}
$$

  e) $A \cup (B - A) = A \cup B$

$$
\begin{aligned}
A \cup (B - A) = & \\
\text{notación constructiva} \quad & = \{x | x \in A\} \cup \{x | x \in (B - A)\} \\
\text{def. de unión y diferencia} \quad & = \{x | (x \in A \vee (x \in B \wedge x \notin A))\} \\
\text{ley distributiva (lógica)} \quad & = \{x | (x \in A \vee x \in B) \wedge (x \in A \vee x \in A)\} \\
\text{idempotente y absorción (lógica)} \quad & = \{x | (x \in A \vee x \in B)\} \\
\text{por def. de conjunto y de unión} \quad & = A \cup B
\end{aligned}
$$

- **Ejercicio 15.** Demuestra que si A y B son conjuntos, entonces $A - B = A \cap \overline{B}$.

Respuesta: Por definición de diferencia de conjuntos, tenemos que:

$$A - B = \{x | x \in A \wedge x \notin B\}$$

Dada la definición de intersección de dos conjuntos $A \cap B$, se expresa como:

$$A \cap B = \{x | x \in A \wedge x \in B\}$$

A partir de la definición de complemento de un conjunto, B en este caso, se expresa como:

$$\overline{B} = U - B = \{x | x \notin B\}$$

Reescribiendo el segundo miembro de la igualdad $A \cap \overline{B}$ según la definición de complemento y de intersección de conjuntos, tenemos que:

$$A \cap \overline{B} = \{x | x \in A \wedge x \notin B\}$$

Por lo tanto, queda demostrado que $A - B = A \cap \overline{B}$ son iguales.

- **Ejercicio 29.** Demuestra que si A es un subconjunto del conjunto universal U, entonces
  a) $A \oplus A = \emptyset$
  b) $A \oplus \emptyset = A$
  c) $A \oplus U = \overline{A}$
  d) $A \oplus \overline{A} = U$

Respuesta: Según la definición de diferencia simétrica, denotada por $A \oplus B$, ésta da como resultado un conjunto que contiene los elementos que bien están en A o bien están en B, pero no en ambos. Esta definición puede expresarse como:

$$A \oplus B = (A \cup B) - (A \cap B) = (A - B) \cup (B - A)$$

Aplicando esta equivalencia con los conjuntos A y U, tenemos:

a) $A \oplus A = \emptyset$ (nilpotencia)

$$\begin{aligned} A \oplus A &= (A - A) \cup (A - A) \\ &= \emptyset \cup \emptyset \\ &= \emptyset \end{aligned}$$

b) $A \oplus \emptyset = A$ (elemento neutro)

$$\begin{aligned} A \oplus \emptyset &= (A - \emptyset) \cup (\emptyset - A) \\ &= A \cup \emptyset \\ &= A \end{aligned}$$

c) $A \oplus U = \overline{A}$

$$\begin{aligned} A \oplus U &= (A - U) \cup (U - A) \\ &= \emptyset \cup \overline{A} \\ &= \overline{A} \end{aligned}$$

d) $A \oplus \overline{A} = U$

$$\begin{aligned} A \oplus \overline{A} &= (A - \overline{A}) \cup (\overline{A} - A) \\ &= A \cup \overline{A} \\ &= U \end{aligned}$$

1.8 Funciones

- **Ejercicios 12 y 13.** Determina si estas funciones de los $\mathbb{Z}$ en $\mathbb{Z}$ son inyectivas y sobreyectivas.

  a) $f(n) = n - 1$

  b) $f(n) = n^2 + 1$

  c) $f(n) = n^3$

  d) $f(n) = \lceil n/2 \rceil$

  Respuesta: en todos los casos en los cuales consideremos o intuyamos que la función es inyectiva o sobreyectiva, debemos demostrarlo de manera general haciendo uso de las definiciones de función inyectiva o sobreyectiva. En caso contrario, si consideramos que no cumple con alguna de esas propiedades, entonces podemos demostrarlo haciendo uso de contraejemplos.

  a) $f(n) = n - 1$

  Primero demostraremos la inyectividad. Para ello, asumamos que $z_1, z_2 \in \mathbb{Z}$ son dos elementos cualesquiera del dominio de la función, con $z_1 \neq z_2$. Luego, si restamos 1 en ambos lados de la anterior nos queda $z_1 - 1 \neq z_2 - 1$. Es decir que si $z_1 \neq z_2$, entonces $f(z_1) \neq f(z_2)$. De esta manera mostramos que la función es inyectiva.

  Para demostrar la sobreyectividad de la función, consideremos un elemento z cualquiera del codominio de la función (es decir, $z \in \mathbb{Z}$). Luego, si consideramos que la función es sobre, tenemos que mostrar que z se puede escribir como la imagen por f de algún elemento del dominio (en este caso, como imagen de algún entero). Entonces, nos preguntamos si podemos escribir $z = n - 1$ con $n \in \mathbb{Z}$. Puesto que de la ecuación anterior puedo despejar $n = z + 1$ y que el n así despejado es entero, hemos mostrado que la función es sobreyectiva.

b) $f(n) = n^2 + 1$

Demostración de inyectividad: se mostrará con un contraejemplo (C.E.) que la función no es inyectiva (la presencia del n^2 así lo hace sospechar!). Asumamos $z_1 = -1$ y $z_2 = 1$. Luego, aplicando la función a estos se tiene: $f(z_1) = 2$ y $f(z_2) = 2$. Vemos entonces que para elementos distintos del dominio, sus respectivas imágenes por la función son iguales. Luego, concluímos que f no es inyectiva.

Demostración de sobreyectividad: en este caso, se mostrará con un C.E. que la función no es sobre. Para ello, consideremos el elemento del codominio $z = 4$. Si la función fuera sobreyectiva, entonces podría escribir que $4 = n^2 + 1$ con $n \in \mathbb{Z}$. Pero despejando n de la anterior veo que $n = \sqrt{(}3)$. Pero aquí vemos que $n \notin \mathbb{Z}$. Luego la función no es sobre.

c) $f(n) = n^3$

Inyectividad: sean z_1 y z_2 dos enteros cualesquiera (elementos del dominio de la función), con $z_1 \neq z_2$. Luego podemos ver que $z_1^3 \neq z_2^3$, con lo cual se muestra que la función es inyectiva (nota: si el módulo de ambos enteros es distinto entonces es claro que el cubo de ambos será distinto. Si el módulo de ambos enteros es el mismo, para que sean distintos necesariamente deben tener distinto signo. Como la función cubo preserva el signo de su argumento, entonces las imágenes de ambos números serán distintas).

Sobreyectividad: mostraremos con un C.E. que la función no es sobreyectiva. Consideremos el elemento del codominio $z = 7$. Es posible escribir $7 = n^3$ con $n \in \mathbb{Z}$? Despejando n de la anterior tenemos que $n = \sqrt[3]{7}$ con lo cual, claramente $n \notin \mathbb{Z}$. Luego, no hemos podido encontrar ningún elemento del dominio de la función tal que su imagen por f sea igual a 7. Es decir, la función no es sobre.

d) $f(n) = \lceil n/2 \rceil$: para el entretiempo.

- **Ejercicio 17.** Da una fórmula explícita para una función del conjunto de los enteros al conjunto enteros positivos que sea

  a) inyectiva, pero no sobre,

  b) sobre, pero no inyectiva,

  c) inyectiva y sobre,

  d) ni inyectiva ni sobre.

  Respuesta:

  a) $f(n) = 2n + 1$ para $n \geq 0$ y $f(n) = -2n + 2$ para $n < 0$.

  b) $f(n) = |n| + 1$.

  c) $f(n) = 2n + 1$ para $n \geq 0$ y $f(n) = -2n$ para $n < 0$.

  d) $f(n) = n^2 + 2$.

- **Ejercicio 19.** Determina si estas funciones son biyecciones de $\mathbb{R}$ en $\mathbb{R}$:

  a) $f(x) = 2x + 1$

  b) $f(x) = x^2 + 1$

c) $f(x) = x^3$

d) $f(x) = (x^2 + 1)/(x^2 + 2)$

Respuesta:

a) Demostración de inyectividad. Supongamos que $x_1, x_2 \in \mathbb{R}$ son dos elementos del dominio de la función. Si $f(x_1) = f(x_2)$, entonces para que la función f sea inyectiva debe cumplirse que $x_1 = x_2$.

$$\begin{aligned} \text{hipótesis} \qquad & f(x_1) = f(x_2) \\ & 2x_1 + 1 = 2x_2 + 1 \\ \text{resto 1 a ambos lados} \qquad & 2x_1 = 2x_2 \\ \text{divido por 2 a ambos lados} \qquad & x_1 = x_2 \end{aligned}$$

Como $x_1 = x_2$, queda demostrado que la función es inyectiva.

Demostración de sobreyectividad. Consideremos un elemento r cualquiera del codominio de la función (es decir, $r \in \mathbb{R}$). Luego, si consideramos que la función es sobre, tenemos que mostrar que r se puede escribir como la imagen por f de algún elemento del dominio (en este caso, como imagen de algún real). Entonces, nos preguntamos si podemos escribir $r = 2x + 1$ con $r \in \mathbb{R}$. De la ecuación anterior puedo despejar $x = (r - 1)/2$ y ver que el x así despejado es real, con lo cual hemos mostrado que la función es sobreyectiva.

Como la función es inyectiva y sobreyectiva, concluímos que también es biyectiva.

b) No. La función no es inyectiva dado que $f(2) = f(-2) = 5$, pero $2 \neq -2$.

c) Sí. Demostración similar a item **a**.

d) No es inyectiva, con $x_1 = 1$ y $x_2 = -1$, $f(x_1) = f(x_2)$. Entonces tampoco es biyectiva.

- **Ejercicio 25.** Supongamos que g es una función de A en B y f es una función de B en C.

a) Demuestra que si tanto f como g son funciones inyectivas, entonces $f \circ g$ también lo es.

b) Demuestra que si tanto f como g son funciones sobreyectivas, entonces $f \circ g$ también lo es.

Respuesta:

a) Para resolver este ejercicio utilizaremos las hipótesis (tanto f como g son inyectivas) para arribar a la conclusión.

Como f es inyectiva entonces se cumple que si $f(b_1) = f(b_2) \longrightarrow b_1 = b_2$, con b_1 y b_2 en B y $f(b_1)$ y $f(b_2)$ en C (i). Del mismo modo, si g es inyectiva entonces se cumple que si $g(a_1) = g(a_2) \longrightarrow a_1 = a_2$, con a_1 y a_2 en A y $g(a_1)$ y $g(a_2)$ en B (ii).

Tomando dos elementos $a_1, a_2 \in A$, y utilizando un ligero cambio de nomenclatura tal que $(f \circ g)(a_i) = f(g(a_i))$ podemos asegurar que

$$f(g(a_1)) = f(g(a_2)) \underbrace{\longrightarrow}_{\text{por (i)}} g(a_1) = g(a_2) \underbrace{\longrightarrow}_{\text{por (ii)}} a_1 = a_2$$

lo que demuestra la inyectividad de la composición.

b) En este caso las hipótesis son que $\forall c \exists b\ (f(b) = c)$ (i) y del mismo modo $\forall b \exists a\ (g(a) = b)$ (ii), con $a \in A$, $b \in B$ y $c \in C$.

Tomando un $c \in C$ arbitrario, por (i) sé que $\exists b \in B\ (f(b) = c)$. Luego, por (ii) sé que para dicho b $\exists\ a \in A\ (g(a) = b)$. De esta manera, puedo reemplazar en la primera expresión y determinar que $\exists a\ f(g(a)) = c$, quedando demostrada la sobreyectividad de la composición.

---

3 Inducción y recursividad

3.3 Inducción Matemática

- **Ejercicio 3.** Usar inducción matemática para probar que $3 + 3 \cdot 5 + 3 \cdot 5^2 + \cdots + 3 \cdot 5^n = 3(5^{n+1} - 1)/4$ para todo $n \in \mathbb{Z}_0^+$.

  Respuesta: Podemos escribir el enunciado del ejercicio en la forma $\forall n \in \mathbb{Z}_0^+ P(n)$, donde

$$P(n)\ :\ 3 + 3 \cdot 5 + 3 \cdot 5^2 + \ldots 3 \cdot 5^n = 3(5^{n+1} - 1)/4 \tag{1}$$

  A su vez, utilizando la notación de sumatoria, se puede escribir

$$P(n)\ :\ \sum_{j=0}^{n} 3 \cdot 5^j = 3(5^{n+1} - 1)/4 \tag{2}$$

  El paso base (P.B) de la demostración corresponde a $n = 0$. En este caso, consideremos primero el lado izquierdo de $P(n)$

$$\sum_{j=0}^{0} 3 \cdot 5^j = 3 \cdot 5^0 = 3 \tag{3}$$

  Si ahora consideramos el lado derecho de $P(n)$ para $n = 0$, se observa que $3(5^{0+1} - 1)/4 = 3(5 - 1)/4 = 3$. Como el lado izquierdo y el lado derecho son iguales, se concluye que se cumple el P.B.

  Para demostrar el paso inductivo, primero debemos explicitar la hipótesis inductiva (H.I) de nuestra demostración. Asumamos entonces que se cumple $P(k)$,

$$P(k)\ :\ \sum_{j=0}^{k} 3 \cdot 5^j = 3(5^{k+1} - 1)/4 \tag{4}$$

  Queremos demostrar que entonces se cumple $P(k + 1)$

$$P(k+1)\ :\ \sum_{j=0}^{k+1} 3 \cdot 5^j = 3(5^{k+2} - 1)/4 \tag{5}$$

Luego comenzaremos la demostración partiendo del lado izquierdo de $P(k+1)$,

$$\begin{aligned}
\sum_{j=0}^{k+1} 3 \cdot 5^j &= \\
\text{(Explicitando último término de la sumatoria)} &= \sum_{j=0}^{k} 3 \cdot 5^j + 3 \cdot 5^{k+1} \\
\text{(Por H.I.)} &= 3(5^{k+1} - 1)/4 + 3 \cdot 5^{k+1} \\
\text{(Aplicando distributiva y sumando los dos términos)} &= \frac{3 \cdot 5^{k+1} - 3 + 4 \cdot 3 \cdot 5^{k+1}}{4} \\
\text{(Sumando los términos en } 3 \cdot 5^{k+1}\text{)} &= \frac{5 \cdot 3 \cdot 5^{k+1} - 3}{4} \\
\text{(Aplicando producto de potencias de igual base y sacando factor común 3)} &= \frac{3(\cdot 5^{k+2} - 1)}{4}
\end{aligned}$$

que es el lado derecho de $P(k+1)$. Luego, el principio de inducción matemático nos permite afirmar que, como se cumple el paso base y el paso inductivo, entonces se cumple el enunciado del ejercicio, es decir, se cumple $\forall n \in \mathbb{Z}_0^+, P(n)$.

- **Ejercicio 7.** Demuestra que $1^2 + 2^2 + \cdots + n^2 = n(n+1)(2n+1)/6$ para todo entero n positivo.

  Respuesta: Sea $P(n) : 1^2 + 2^2 + \cdots + n^2 = n(n+1)(2n+1)/6$ con $n \geq 1$.

  PASO BASE: Reemplazando con $n = 1$ en el lado izquierdo de la igualdad tenemos $1^2 = 1$. El mismo reemplazo del lado derecho nos queda $1(1+1)(2+1)/6 = 1$. Quedando demostrado el paso base.

  PASO INDUCTIVO: Tomando un k arbitrario pero fijo debemos demostrar que $P(k) \longrightarrow P(k+1)$. Lo vamos a hacer a través de una demostración directa.

$P(k)$	$1^2 + 2^2 + \cdots + k^2$	$= k(k+1)(2k+1)/6$
sumo $(k+1)^2$ a ambos lados	$1^2 + 2^2 + \cdots + k^2 + (k+1)^2$	$= k(k+1)(2k+1)/6 + (k+1)^2$
factor común $k+1$ en el lado derecho	$1^2 + 2^2 + \cdots + k^2 + (k+1)^2$	$= (k+1)(k(2k+1)/6 + (k+1))$
factor común $(k+1)/6$ en el lado derecho	$1^2 + 2^2 + \cdots + k^2 + (k+1)^2$	$= \frac{(k+1)}{6}(k(2k+1) + 6(k+1))$
desarrollando	$1^2 + 2^2 + \cdots + k^2 + (k+1)^2$	$= \frac{(k+1)}{6}(2k^2 + 7k + 6)$
factorizando el polinomio de orden 2	$1^2 + 2^2 + \cdots + k^2 + (k+1)^2$	$= \frac{(k+1)}{6}2(k+2)(k+3/2)$
reacomodando	$1^2 + 2^2 + \cdots + k^2 + (k+1)^2$	$= \frac{(k+1)}{6}(k+2)(2k+3)$
reacomodando	$1^2 + 2^2 + \cdots + k^2 + (k+1)^2$	$= \frac{(k+1)}{6}(k+2)(2(k+1)+1)$
llegamos a $P(k+1)$	$q.e.d$	

Luego, el principio de inducción matemática nos permite afirmar que, como se cumple el paso base y el paso inductivo, entonces se cumple el enunciado del ejercicio, es decir, se cumple $\forall n \in \mathbb{Z}^+, P(n)$.

- **Ejercicio 13.** Demuestra que $2^n > n^2$ para todo n entero mayor que 4.

  Respuesta: Sea $P(n)$ la proposición que afirma que $2^n > n^2$ para todo n entero mayor que 4.

  PASO BASE: Si tomamos el primer entero mayor que 4, tenemos que $P(5)$ es verdadera, dado que $2^5 = 32 > 5^2 = 25$.

  PASO INDUCTIVO: Suponemos que $P(k)$ es verdadera, es decir $2^k > k^2$. Entonces debemos demostrar que $P(k) \longrightarrow P(k+1)$. Para ello, planteamos

	$2^k > k^2$
multiplicamos ambos miembros por 2	$2 \cdot 2^k > 2 \cdot k^2$
reescribimos el primer miembro	$2^{k+1} > 2 \cdot k^2$
desarrollamos el segundo miembro	$2^{k+1} > k^2 + k^2$

Sabemos que $k^2 > 2k + 1$ para $k > 4$. Reemplazando uno de los k^2 del segundo miembro, tenemos

$$
\begin{aligned}
& & 2^{k+1} &> k^2 + k^2 \\
& & 2^{k+1} &> k^2 + 2k + 1 \\
\text{cuadrado del binomio del segundo miembro} & & 2^{k+1} &> (k+1)^2 \\
\text{llegamos a } P(k+1) & & q.e.d &
\end{aligned}
$$

Luego, el principio de inducción matemática nos permite afirmar que, como se cumple el paso base y el paso inductivo, entonces se cumple el enunciado del ejercicio, es decir, se cumple $\forall n \in \mathbb{Z}$, con $n > 4, P(n)$.

- **Ejercicio 20.** Demuestra utilizando el principio de inducción que 3 divide a $n^3 + 2n$ si n es un entero no negativo.

  Respuesta: Sea $P(n)$ la proposición que afirma que $n^3 + 2n$ es divisible por 3 para todo n entero no negativo.

  PASO BASE: Si tomamos el primer entero no negativo, tenemos que $P(0)$ es verdadera, dado que $0^3 + 2 \cdot 0 = 0$, que es divisible por 3.

  PASO INDUCTIVO: Suponemos que $P(k)$ es verdadera, es decir $k^3 + 2k$ es divisible por 3. Entonces debemos demostrar que $P(k) \longrightarrow P(k+1)$. Para ello, planteamos

$$
\begin{aligned}
(k+1)^3 + 2(k+1) &= (k+1)(k+1)^2 + 2k + 2 \\
&= (k+1)(k^2 + 2k + 1) + 2k + 2 \\
&= k^2(k+1) + 2k(k+1) + (k+1) + 2k + 2 \\
&= k^3 + k^2 + 2k^2 + 2k + k + 1 + 2k + 2 \\
&= (k^3 + 2k) + 3k^2 + 3k + 3 \\
&= (k^3 + 2k) + 3(k^2 + k + 1)
\end{aligned}
$$

  que también es divisible por 3, puesto que ambos términos de la suma lo son.

  Luego, el principio de inducción matemática nos permite afirmar que, como se cumple el paso base y el paso inductivo, entonces se cumple el enunciado del ejercicio, es decir, se cumple $\forall n \in \mathbb{Z}^{\geq}, P(n)$.

- **Ejercicio 42.** Supongamos que

$$
A = \begin{bmatrix} a & 0 \\ 0 & b \end{bmatrix}
$$

  donde a y b son números reales, demuestra que

$$
A^n = \begin{bmatrix} a^n & 0 \\ 0 & b^n \end{bmatrix}
$$

para todo entero n positivo.

Respuesta: Sea

$$P(n) \,:\, A^n = \begin{bmatrix} a^n & 0 \\ 0 & b^n \end{bmatrix}$$

PASO BASE: Reemplazando con $n = 1$ en el lado izquierdo de la igualdad tenemos A. El mismo reemplazo del lado derecho nos queda $\begin{bmatrix} a & 0 \\ 0 & b \end{bmatrix}$. Debido a la propia definición de la matriz A queda demostrado el paso base.

PASO INDUCTIVO: Tomando un k arbitrario pero fijo debemos demostrar que $P(k) \longrightarrow P(k+1)$. Lo vamos a hacer a través de una demostración directa.

$$\begin{aligned}
P(k) \qquad & A^k = \begin{bmatrix} a^k & 0 \\ 0 & b^k \end{bmatrix} \\
\text{post-multiplicamos por } A \text{ a ambos lados} \qquad & A^k A = \begin{bmatrix} a^k & 0 \\ 0 & b^k \end{bmatrix} A \\
\text{manipulando} \qquad & A^{k+1} = \begin{bmatrix} a^k & 0 \\ 0 & b^k \end{bmatrix} \begin{bmatrix} a & 0 \\ 0 & b \end{bmatrix} \\
\text{realizando el producto matricial} \qquad & A^{k+1} = \begin{bmatrix} a^k a & 0 \\ 0 & b^k b \end{bmatrix} \\
\text{manipulando} \qquad & A^{k+1} = \begin{bmatrix} a^{k+1} & 0 \\ 0 & b^{k+1} \end{bmatrix} \\
\text{llegamos a } P(k+1) \qquad & q.e.d
\end{aligned}$$

Luego, el principio de inducción matemática nos permite afirmar que, como se cumple el paso base y el paso inductivo, entonces se cumple el enunciado del ejercicio, es decir, se cumple $\forall n \in \mathbb{Z}^+, P(n)$.

- **Ejercicio 47.** Use inducción matemática para probar que si $A_1, A_2, \ldots, A_n$ son subconjuntos del conjunto universal U, entonces

$$P(n) \,:\, \overline{\bigcup_{j=1}^{n} A_j} = \bigcap_{j=1}^{n} \overline{A_j} \tag{6}$$

Respuesta: Podemos escribir el enunciado del ejercicio en la forma $\forall n \in \mathbb{Z}^+ P(n)$. Iniciamos la demostración por inducción analizando el P.B., que se corresponde al caso $n = 2$. Comenzamos analizando el lado izquierdo de $P(n = 2)$

$$\overline{\bigcup_{j=1}^{2} A_j} = \overline{A_1 \cup A_2} \tag{7}$$

Por otro lado, el lado derecho de $P(n = 2)$ se puede escribir de la siguiente manera,

$$\bigcap_{j=1}^{2} \overline{A_j} = \overline{A_1} \cap \overline{A_2} \tag{8}$$

Luego por la ley de De Morgan para conjuntos, ambos lados son iguales, con lo cual podemos concluir que se cumple el P.B.

Para mostrar el paso inductivo, identificamos primero nuestra H.I., en éste caso

$$P(k) : \overline{\bigcup_{j=1}^{k} A_j} = \bigcap_{j=1}^{k} \overline{A_j} \tag{9}$$

Luego queremos mostrar que si se cumple $P(k)$ entonces $P(k+1)$, la cual viene expresada por

$$P(k+1) : \overline{\bigcup_{j=1}^{k+1} A_j} = \bigcap_{j=1}^{k+1} \overline{A_j} \tag{10}$$

Partiendo del lado izquierdo de la anterior se tiene

$$\begin{aligned}
\overline{\bigcup_{j=1}^{k+1} A_j} = & \\
\text{(Explicitando la unión con el } A_{k+1}) \quad &= \overline{(\bigcup_{j=1}^{k} A_j) \cup A_{k+1}} \\
\text{(Aplicando ley de De Morgan para conjuntos)} \quad &= \overline{(\bigcup_{j=1}^{k} A_j)} \cap \overline{A_{k+1}} \\
\text{(Aplicando la H.I.)} \quad &= \bigcap_{j=1}^{k} \overline{A_j} \cap \overline{A_{k+1}} \\
\text{(Asociando el último conjunto con los demás)} \quad &= \bigcap_{j=1}^{k+1} \overline{A_j}
\end{aligned}$$

con lo cual llegamos al lado derecho de $P(k+1)$. Luego, por el principio de inducción matemático podemos afirmar que, como se cumple el paso base y el paso inductivo, entonces se cumple el enunciado del ejercicio, es decir, se cumple $\forall n \in \mathbb{Z}^+, P(n)$.

3.4 Definiciones recursivas e inducción estructural

- **Ejercicio 8.** Da una definición recursiva para la sucesión a_n, $n = 1, 2, 3 \ldots$, si
  a) $a_n = 4n - 2$
  b) $a_n = 1 + (-1)^n$

c) $a_n = n(n+1)$

d) $a_n = n^2$

Respuesta: Para encontrar una expresión recursiva de cada sucesión debemos determinar como se relaciona el término n-ésimo con los predecesores.

a) Una estrategia es listar los primeros elementos de la sucesión para tratar de encontrar algún patrón. Reemplazando con n=1,2, etc, tenemos, $a_1 = 2$, $a_2 = 6$, $a_3 = 10$, $a_4 = 14$, con lo que ya podemos predecir que el término actual de la sucesión es el anterior más cuatro, lo que es lo mismo que $a_n = a_{n-1} + 4$, con el paso base $a_1 = 2$.

b) Listando los primeros elementos $a_1 = 0$, $a_2 = 2$, $a_3 = 0$, $a_4 = 2$, de lo cual podemos deducir que $a_n = a_{n-2}$ y necesitaremos los pasos base $a_1 = 0$ y $a_2 = 2$.

c) Listando los primeros elementos $a_1 = 2$, $a_2 = 6$, $a_3 = 12$, $a_4 = 20$, $a_5 = 30$, pero el patrón no es tan evidente. Una estrategia más robusta es analizar la diferencia (o razón, según el caso) entre dos términos sucesivos. Para ello planteamos

$$a_n - a_{n-1} = n(n+1) - (n-1)n = n(n+1-(n-1)) = 2n$$

de donde podemos despejar $a_n = 2n + a_{n-1}$, con el paso base $a_1 = 2$.

d) Con el mismo planteo que el incíso anterior se puede arribar a $a_n = a_{n-1} + 2n - 1$, con el paso base $a_1 = 1$.

- **Ejercicio 13.** Demuestra que $f_1 + f_3 + \cdots + f_{2n-1} = f_{2n}$ para todo entero positivo n.

  Respuesta: Utilizaremos el PIM para la demostración. Además es importante recordar la definición de la sucesión de Fibonacci:

$$f_n = \begin{cases} 0, & n = 0 \\ 1, & n = 1 \\ f_{n-1} + f_{n-2}, & n \geq 2 \end{cases}$$

  PASO BASE: Reemplazando con $n = 1$ en el lado izquierdo de la igualdad tenemos f_1, que por definición de Fibonacci es $f_1 = 1$. El mismo reemplazo del lado derecho nos queda f_2, donde $f_2 = 1$ también por definición de Fibonacci. La igualdad demuestra el paso base.

  PASO INDUCTIVO: Tomando un k arbitrario pero fijo debemos demostrar que $P(k) \longrightarrow P(k+1)$. Lo vamos a hacer a través de una demostración directa.

$P(k)$	$f_1 + f_3 + \cdots + f_{2k-1}$	$= f_{2k}$
sumamos a ambos lados el siguiente término necesario	$f_1 + f_3 + \cdots + f_{2k-1} + f_{2(k+1)-1}$	$= f_{2k} + f_{2(k+1)-1}$
manipulando índices en el lado derecho	$f_1 + f_3 + \cdots + f_{2k-1} + f_{2(k+1)-1}$	$= f_{2k} + f_{2k+1}$
utilizando la definición de Fibonacci	$f_1 + f_3 + \cdots + f_{2k-1} + f_{2(k+1)-1}$	$= f_{2k+2}$
manipulando índices	$f_1 + f_3 + \cdots + f_{2k-1} + f_{2(k+1)-1}$	$= f_{2(k+1)}$
llegamos a $P(k+1)$	$q.e.d$	

Luego, por el principio de inducción matemática podemos afirmar que, como se cumple el paso base y el paso inductivo, entonces se cumple el enunciado del ejercicio, es decir, se cumple $\forall n \in \mathbb{Z}^+, P(n)$.

- **Ejercicio 17.** Determinar el número de divisiones realizadas por el algoritmo de Euclides para encontrar el máximo común divisor de los números de Fibonacci f_n y f_{n+1}, donde n es un entero no negativo. Verifique su respuesta utilizando inducción matemática.

---

2 Enteros y sucesiones

2.4 Enteros y división

- **Ejercicio 9.** ¿Cuál es el cociente y el resto cuando

  a) 19 se divide entre 7?

  b) -111 se divide entre 11?

  c) 789 se divide entre 23?

  d) 1.001 se divide entre 13?

  e) 0 se divide entre 19?

  f) 3 se divide entre 5?

  g) -1 se divide entre 3?

  h) 4 se divide entre 1?

  Respuesta: Aplicando el algoritmo de la división, podemos expresar el dividendo a como una suma entre el divisor d multiplicado por el cociente q y el resto r, es decir $a = dq + r$.

  Para obtener el cociente q de una división, hay que aplicar el operador **div**, el cual se define como $q = \lfloor a/d \rfloor$.

  Para obtener el resto r de una división, podemos despejar r del algoritmo de la división: $r = a - dq$, o bien utilizando una de las definiciones del operador módulo: $r = a - (d \cdot \ \mathbf{int}(a/d))$, siendo **int** la parte entera de la división.

  a) Si $a = 19$ y $d = 7$, entonces $q = a \ \mathbf{div} \ d = 19 \ \mathbf{div} \ 7 = 2$ y $r = a \ \mathbf{mod} \ d = 19 \ \mathbf{mod} \ 7 = 5$. Por lo tanto, $19 = 2 \cdot 7 + 5$.

  b)

  c)

  d)

  e)

  f)

  g) Si $a = -1$ y $d = 3$, entonces $q = -1 \ \mathbf{div} \ 3 = -1$ y $r = -1 \ \mathbf{mod} \ 3 = 2$. Por lo tanto, $-1 = (-1) \cdot 3 + 2$.

h)

- **Ejercicio 11.** Obtén la descomposición en factores primos de cada uno de estos enteros

  a) 88

  b) 126

  c) 729

  d) 1.001

  e) 1.111

  f) 909.090

  Respuesta: Para calcular la descomposición de un entero en producto de primos, primero se divide dicho entero por los primeros primos sucesivos, comenzando por el 2.

  a) 88/2 = 44, 44/2 = 22, 22/2 = 11. Como 11 es un número primo, el procedimiento se ha completado. Entonces $88 = 2 \cdot 2 \cdot 2 \cdot 11 = 2^3 \cdot 11$.

  b) 126/2 = 63, 63/3 = 21, 21/3 = 7. Como 7 es un número primo, el procedimiento se ha completado. Entonces $126 = 2 \cdot 3 \cdot 3 \cdot 7 = 2 \cdot 3^2 \cdot 7$.

  c)

  d)

  e)

  f)

- **Ejercicios 29 y 31.** Cuáles son los mcm y mcd de los siguientes pares de enteros?

  a) $3^7 \cdot 5^3 \cdot 7^3$, $2^{11} \cdot 3^5 \cdot 5^9$

  b) $11 \cdot 13 \cdot 17$, $2^9 \cdot 3^7 \cdot 5^5 \cdot 7^3$

  Respuesta: dada la descomposición en factores primos de dos enteros a y b de la siguiente manera

$$a = p_1^{a_1} \cdot p_2^{a_2} \cdot \cdots \cdot p_n^{a_n} \tag{11}$$
$$b = p_1^{b_1} \cdot p_2^{b_2} \cdot \cdots \cdot p_n^{b_n} \tag{12}$$

  los $\text{mcm}(a, b)$ y el $\text{mcd}(a, b)$ se pueden calcular como

$$\text{mcm}(a, b) = p_1^{\max(a_1, b_1)} \cdot p_2^{\max(a_2, b_2)} \cdot \cdots \cdot p_n^{\max(a_n, b_n)} \tag{13}$$
$$\text{mcd}(a, b) = p_1^{\min(a_1, b_1)} \cdot p_2^{\min(a_2, b_2)} \cdot \cdots \cdot p_n^{\min(a_n, b_n)} \tag{14}$$

  Aplicando las ecuaciones anterior a los pares de enteros dados, calculamos primero los mcm:

  a) $\text{mcm}(3^7 \cdot 5^3 \cdot 7^3, 2^{11} \cdot 3^5 \cdot 5^9) = 2^{11} \cdot 3^7 \cdot 5^9 \cdot 7^3$

  b) $\text{mcm}(11 \cdot 13 \cdot 17, 2^9 \cdot 3^7 \cdot 5^5 \cdot 7^3) = 2^9 \cdot 3^7 \cdot 5^5 \cdot 7^3 \cdot 11 \cdot 13 \cdot 17$

y a continuación los mcd:

a) $\text{mcd}(3^7 \cdot 5^3 \cdot 7^3, 2^{11} \cdot 3^5 \cdot 5^9) = 3^5 \cdot 5^3$

b) $\text{mcd}(11 \cdot 13 \cdot 17, 2^9 \cdot 3^7 \cdot 5^5 \cdot 7^3) = 1$

- **Ejercicio 50.** ¿Qué sucesión de números pseudoaleatorios se genera utilizando el generador de congruencia lineal $x_{n+1} = (5x_n + 3) \bmod 7$, con la semilla $x_0 = 3$ (enunciado modificado).

  Respuesta: Partiendo de la semilla dada, reemplazamos en la expresión y obtenemos:

  $$x_1 = (5.3 + 3) \bmod 7 = 4$$

  Realizando el mismo reemplazo con el último resultado obtenido, se logra la secuencia: $x = 3, 4, 2, 6, 5, 0, 3, 4, 2, 6, 5, \ldots$. Notar que se generan seis números en forma aleatoria y luego el ciclo se repite (el 1 nunca aparece).

- **Ejercicio 53.** Cifra el mensaje 'NO PASAR' traduciendo las letras a números, aplicando la función de cifrado dada y pasando los números obtenidos a letras (utilizar alfabeto español de 27 letras).

  Extra: Determina cuales son funciones de cifrado que admiten descifrado y cuales no.

  a) $f(p) = (p + 3) \bmod 27$

  b) $f(p) = (p + 13) \bmod 27$

  c) $f(p) = (3p + 7) \bmod 27$

  Respuesta: En primer lugar convertimos letras a números, por lo que el mensaje 'NO PASAR' queda como 1315 1600190018. Notar para que no haya ambigüedades, cada letra se representa por dos dígitos, completando con ceros (zero-padding) cuando sea necesario. De a pares de dígitos evaluamos la función de cifrado obteniendo el mensaje a enviar.

  a) 1618 1903220321 $\longrightarrow$ PR SDVDU. Admite descifrado utilizando la función inversa $f^{-1}(p) = (p - 3) \bmod 27$

  b) 2601 0213051304 $\longrightarrow$ ZB CNFNE. Admite descifrado utilizando la función inversa $f^{-1}(p) = (p - 13) \bmod 27$

  c) 1925 0107100707 $\longrightarrow$ SY BHKHH. No admite descrifrado ya que f no es inyectiva. Ej: $f(\text{A}) = f(\text{R})$ con A≠R, por lo que no admite inversa.

2.5 Enteros y algoritmos

- **Ejercicio 21.** Utilice el algoritmo de Euclides para encontrar

  a) $\text{mcd}(12, 18)$

  b) $\text{mcd}(111, 201)$

  c) $\text{mcd}(1001, 1331)$

  d) $\text{mcd}(12345, 54321)$

  Respuesta: el algoritmo de Euclides se basa en el lema 1 de la pág.178 del libro de Rosen, 5ta Ed., el cual enuncia: sea $a = bq + r$, donde a, b, q y r son enteros. Luego, el $\text{mcd}(a, b) = \text{mcd}(b, r)$. Se debe tener en cuenta

que el mcd(a, b) *es el último resto no nulo* calculado por la aplicación reiterada de la igualdad mencionada por este lema.

Aplicando entonces el algoritmo de Euclides se tiene,

a) $\text{mcd}(12, 18) = \text{mcd}(18, 12) = \text{mcd}(12, 6) = 6$.

   Expandiendo cada uno de los pasos a partir del algoritmo de la división se tiene:

$$12 = 18.0 + 12$$
$$18 = 12.1 + 6$$
$$12 = 6.2 + 0$$

b) $\text{mcd}(111, 201) = \text{mcd}(111, 90) = \text{mcd}(90, 21) = \text{mcd}(21, 6) = \text{mcd}(6, 3) = 3$.

   Expandiendo cada uno de los pasos a partir del algoritmo de la división se tiene:

$$111 = 201.0 + 111$$
$$201 = 111.1 + 90$$
$$111 = 90.1 + 21$$
$$90 = 21.4 + 6$$
$$21 = 6.3 + 3$$
$$6 = 3.2 + 0$$

c) $\text{mcd}(1001, 1331)$

d) $\text{mcd}(12345, 54321)$
