Capítulo 7

Teoría de Conjuntos

7.1. Introducción

Intuitivamente, un *conjunto* es una colección bien definida de objetos a los que llamaremos *elementos*. Es habitual denotar a los conjuntos con letras mayúsculas (A, B, X,...) reservando las letras minúsculas para los elementos. Para indicar que a es un elemento de A se escribe $a \in A$ y se dice que *a pertenece a A*. Si *a no pertenece a A* se escribe $a \notin A$.

En esta asignatura estamos interesados especialmente en conjuntos de números. Algunos de ellos reciben nombres propios y para ellos se usan símbolos especiales:

1. Los *números naturales*: $\mathbb{N} = \{1, 2, 3, 4, 5, \dots\}$ ó $\mathbb{N} = \{0, 1, 2, 3, 4, 5, \dots\}$.
2. Los *números enteros*: $\mathbb{Z} = \{\dots, -3, -2, -1, 0, 1, 2, 3, \dots\}$.
3. Los *números racionales*, $\mathbb{Q}$: cociente de dos números enteros con denominador distinto de cero.
4. Los *números reales*, $\mathbb{R}$. De una manera intuitiva, podemos identificar los números reales con los puntos de una recta sin principio ni final.

En el capítulo 1, dedicado a la Aritmética se estudian las principales propiedades de los números enteros, la base de la *Matemática discreta*.

Si los elementos pertenecen a un conjunto fijo U, se dice que U es un *universo* o *conjunto universal*. Hay diversas formas de definir conjuntos:

1. Por *extensión*, escribiendo todos y cada uno de sus elementos separados por comas y encerrados entre llaves: $A = \{1, 3, 5, 7\}$, $B = \{0, -1, 24, 333, 7/4, \pi\}$.
2. Por *compresión*, especificando el universo al que pertenecen sus elementos y las propiedades que los caracterizan:
$$C = \{x \in \mathbb{Z} \mid 0 \leq x \leq 9, x \text{ es par}\}, \quad D = \{n \in \mathbb{Z}; n^2 = -1\}.$$

Ejemplo 7.1.- *Piensa en cómo están definidos los siguientes conjuntos y analiza las posibles pegas que puedan surgir.*

- *A es el conjunto de los 20 mejores jugadores de la liga de fútbol española.*
- $B = \{x \mid 1 \leq x \leq 5\}$.

Definición 7.1.- *Dados dos conjuntos A y B, decimos que A* es un subconjunto *de B, y lo denotamos $A \subseteq B$ si todos y cada uno de los elementos de A pertenecen a B, es decir*

$$a \in A \Rightarrow a \in B.$$

Si $A \subseteq B$ y $B \subseteq A$, entonces A y B son iguales *y se denota $A = B$ ($A \neq B$ en caso contrario). Si $A \subseteq B$ pero $A \neq B$, entonces A se dice un* subconjunto propio *de B y se denota $A \subset B$.*

De forma inmediata se puede formular el siguiente resultado:

Teorema 7.1 *Dados tres conjuntos A, B y C que cumplen $A \subseteq B$ y $B \subseteq C$, entonces $A \subseteq C$.*

Como ejercicio, enuncia los resultados que se obtendrían si se cambia $\subseteq$ por $\subset$ en alguna (o las dos) inclusiones del teorema anterior.

Otros conjuntos importantes, con nombres y símbolos especiales, son:

Definición 7.2.- *El* conjunto vacío, $\emptyset$, *es el único conjunto que no contiene elementos. Se tiene que $\emptyset \subseteq A$, para todo conjunto A en un universo U.*

Definición 7.3.- *Dado $A \in U$ se define el conjunto de las* partes de A, $\mathcal{P}(A)$, *como el conjunto de todos los subconjuntos de A:*

$$\mathcal{P}(A) = \{B \subseteq U \mid B \subseteq A\}.$$

Por ejemplo, si $A = \{1, 2, 3\}$,

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

En general, el número de subconjuntos (contando el conjunto vacío) de un conjunto de n elementos es 2^n (véase el ejemplo 2.8).

7.2. Operaciones con conjuntos

Supongamos fijado un universo U y sean $A, B \subseteq U$. Se definen las siguientes operaciones

1. Unión: $A \cup B = \{x \in U \mid x \in A \text{ o } x \in B\}$.
2. Intersección: $A \cap B = \{x \in U \mid x \in A \text{ y } x \in B\}$.
3. Diferencia simétrica: $A \triangle B = \{x \in U \mid x \in A \cup B \text{ y } x \notin A \cap B\}$.
4. Complemento de B relativo a A: $A - B = \{x \in U \mid x \in A \text{ y } x \notin B\}$.
5. Complementario de A: $\overline{A} = A^c = \{x \in U \mid x \notin A\}$.

Damos un listado de algunas propiedades de las operaciones con conjuntos. Sean $A, B, C \subseteq U$:

(i) Ley del doble complementario: $\overline{\overline{A}} = A$.

(ii) Leyes de Morgan: $\overline{A \cup B} = \overline{A} \cap \overline{B}$, $\overline{A \cap B} = \overline{A} \cup \overline{B}$.

(iii) Propiedad conmutativa: $A \cup B = B \cup A$, $A \cap B = B \cap A$.

(iv) Propiedades asociativas: $A \cup (B \cup C) = (A \cup B) \cup C$, $A \cap (B \cap C) = (A \cap B) \cap C$.

(v) Propiedades distributivas: $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$, $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$.

(vi) Prop. idempotente: $A \cup A = A$, $A \cap A = A$.

(vii) Elementos neutros: $A \cup \emptyset = A$, $A \cap U = A$.

(viii) Inversos: $A \cup \overline{A} = U$, $A \cap \overline{A} = \emptyset$.

(ix) Dominación: $A \cup U = U$, $A \cap \emptyset = \emptyset$.

(x) Absorción: $A \cup (A \cap B) = A$, $A \cap (A \cup B) = A$.

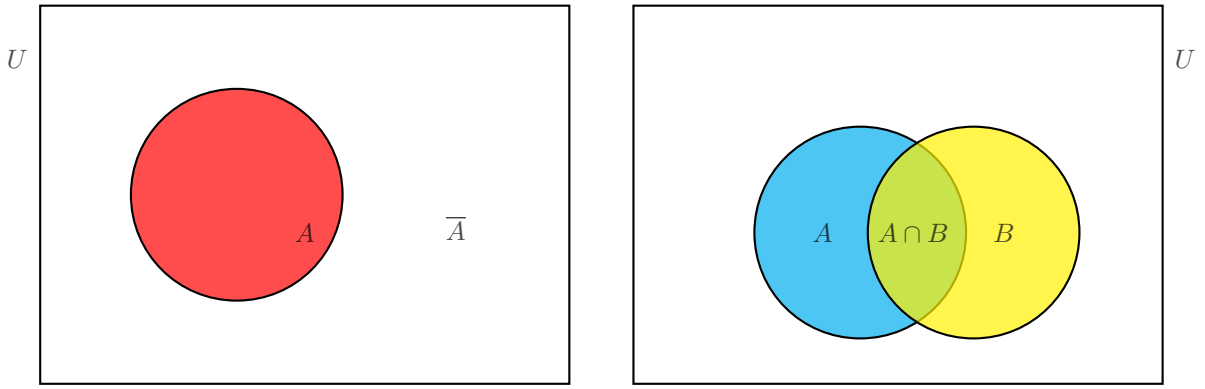


Figura 7.1: En la figura de la izquierda, la región coloreada representa al conjunto A y el resto del rectángulo es su complementario $\overline{A}$. En la figura de la izquierda se representa al conjunto A (de azul), al conjunto B (de amarillo) y su intersección (de verde). Nótese que el conjunto $A \cup B$ es toda la zona coloreada.

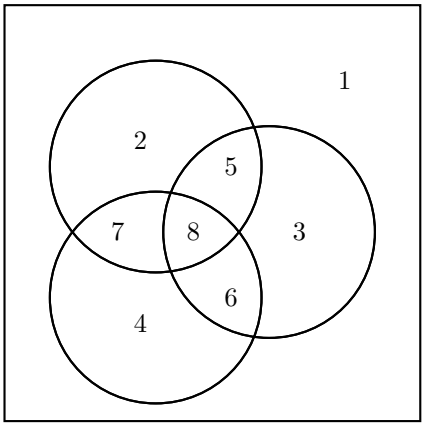


Figura 7.2: Diagrama de Venn con las regiones numeradas.

Una forma muy habitual de estudiar las relaciones entre conjuntos son los *diagramas de Venn*. Consisten en una representación gráfica donde el espacio universal U se muestra como el interior de un rectángulo, mientras que los subconjuntos de U se muestran como interiores de curvas u otras curvas cerradas (véase la figura 7.1).

Otro enfoque que se utiliza en los diagramas de Venn es el de numerar las regiones, como se hace en la figura 7.2. En el mismo vemos 8 regiones cuya unión nos da el conjunto universal U. Las regiones 2, 5, 7 y 8 forman el conjunto A, las regiones 3, 5, 6 y 8 forman el conjunto B y las regiones 4, 6, 7 y 8 forman el conjunto C. La región 1 es $\overline{A \cup B \cup C}$, la región 2 es $A \cap \overline{B} \cap \overline{C}$ y la región 7 es $A \cap \overline{B} \cap C$. Cada región es de la forma $R_1 \cap R_2 \cap R_3$ donde R_1 puede ser A o $\overline{A}$, R_2 B o $\overline{B}$ y R_3 C o $\overline{C}$. Como ejercicio, puedes intentar determinar el resto de regiones, así como caracterizar las regiones $\overline{A}$, $A \cap B$, $A \cup B$, $(\overline{A} \cap \overline{B}) \cup \overline{C}$ o $(\overline{A} \cup \overline{B}) \cap C$.

Los diagramas de Venn son muy útiles como apoyo en problemas de conteo. Nótese que al contar el número de elementos contenidos en un esquema como el de las figuras 7.1 o 7.2 hay que tener en cuanta el principio de inclusión-exclusión visto en la sección 2.3.

Definición 7.4 *Sean I un conjunto no vacío y U un universo. Si a cada $i \in I$ se la asocia un conjunto $A_i \in U$, entonces se dice que I es* un conjunto de índices *y cada $i \in I$ se dice* índice. *Se define*

$$\cup_{i \in I} A_i = \{x \in U \mid x \in A_i \text{ para al menos un } i \in I\}$$

$$\cap_{i \in I} A_i = \{x \in U \mid x \in A_i \text{ para todo } i \in I\}.$$

Por ejemplo, si $I = \{2, 3, 4, 5\}$, $U = \mathbb{N}$, y $A_i = \{1, 2, \ldots, i\}$, se tiene que $\cup_{i \in I} A_i = A_5 = \{1, 2, 3, 4, 5\}$ y $\cap_{i \in I} A_i = A_2 = \{1, 2\}$.

Con notación de índices, podemos enunciar las leyes de Morgan generalizadas como sigue:

$$\overline{\cup_{i \in I} A_i} = \cap_{i \in I} \overline{A_i}, \qquad \overline{\cap_{i \in I} A_i} = \cup_{i \in I} \overline{A_i}.$$

Definición 7.5 *Sean A y B dos conjuntos. Se define el* producto cartesiano *de A y B, y se denota $A \times B$, como el conjunto de pares ordenados*

$$\{(a, b)); a \in A,\, b \in B\}.$$

Algunas consideraciones relacionadas con esta definición:

- a es la primera componente del par ordenado.
- b es la segunda componente del par ordenado.
- $(a, b) = (a', b')$ si $a = a'$, $b = b'$.
- Se puede generalizar a $A_1 \times \cdots \times A_n$.

7.3. Relaciones

Definición 7.6 *Sean A y B dos conjuntos. Una* relación binaria *entre dos conjuntos A y B es cualquier subconjunto $R \subseteq A \times B$. Si $(a, b) \in R$ se dice que a* está relacionado con *b y se denota aRb. Si $A = B$ se habla de una relación binaria en A.*

Para representar gráficamente una relación binaria R en un conjunto finito $A = \{a_1, \ldots, a_n\}$ se pueden usar *digrafos* (véase el capítulo 5) con los siguientes criterios:

1. Se dibuja un vértice por cada elemento $a_i \in A$.
2. Se dibuja una arista dirigida de a_i a a_j si $a_i R a_j$.

Ejemplo 7.2.- *Dibuja el digrafo asociado a la relación $R = \{(1,1), (1,3), (1,5), (2,2), (2,3), (3,1), (3,4), (4,1), (4,2), (5,3), (5,$ en el conjunto $A = \{1, 2, 3, 4, 5\}$.*

Definición 7.7 *Sea $R \subseteq A \times A$. Se dice que:*

- *R es reflexiva si aRa $\forall a \in A$.*

- *R es simétrica si aRb implica que bRa.*
- *R es antisimétrica si aRa y bRa implica que $a = b$.*
- *R es transitiva si aRb y bRc, entonces que aRc.*

Definición 7.8 *Correspondencia, función o aplicación Sean A y B dos conjuntos. Se define una* correspondencia *o* función *o* aplicación *de A en B, y se denota $f : A \to B$, como el conjunto de pares*

$$\{(a, f(a)); a \in A,\ f(a) \in B\},$$

definido de forma que a cada elemento $a \in A$ se le asocia un elemento, y solo uno, del conjunto B. A este último elemento se le denota por $f(a)$ y se le llama valor *o* imagen *de a por la aplicación f. Recíprocamente, si dado un elemento $b \in B$, existe un elemento $a \in A$ tal que $f(a) = b$, entonces a se dice una* preimagen *de b.*

Al conjunto A se le llama conjunto inicial *de la aplicación f, mientras que al conjunto B se le llama* conjunto final *de f*

Sea $f : A \to B$ una aplicación entre dos conjuntos A y B.

- Se dice que f es *inyectiva* si para cada par de elementos $x, y \in A$ tales que $f(x) = f(y)$ se tiene que $x = y$. Es decir, no puede haber dos elementos distintos en A que tengan la misma imagen.
- Se dice que f es *suprayectiva* si para todo $b \in B$ existe un elemento $a \in A$ tal que $f(a) = b$. Es decir, todo elemento en el conjunto B tiene una preimagen.
- Se dice que f es *biyectiva* si es inyectiva y suprayectiva a la vez. En muchos textos, a las aplicaciones biyectivas también se les llama aplicaciones 1–1 (es decir, uno a uno).

Para ilustrar la idea de biyección podemos usar palabras del escritor y matemático Antonio J. Durán en «Vida de los números», T Ediciones, Madrid 2006. En una parte del libro, el autor habla de la evolución de las técnicas artísticas, de la escritura y de los rudimentos numéricos:

> *... caiga el lector en la cuenta de que en un principio los números no fueros manejados como hacemos hoy, esto es, no contaban el rebaño y dejaban apuntado el número de animales que lo formaban. No podían proceder así porque le pastoreo fue anterior a la invención de la escritura, y apuntar, aunque sea números , es ya escribir. Según leí una vez en algún sitio, en principio los pastores procedieron de forma algo más* rudimentaria*: dejaban en la aldea una vejiga de uro que tenía en su interior una cuenta de arcilla por cada animal del rebaño, de manera que a la vuelta pudiera comprobarse que en el pellejo había tantas cuentas como cabras regresaban...*

Este texto nos lleva a pensar que contar los elementos de un conjunto A es establecer una biyección de A con el conjunto $\mathbb{N}_n = \{1, 2, \ldots, n\}$, para algún $n \in \mathbb{N}$. Como se indica en la sección 2.2, si tal biyección existe, se dice que el conjunto A es *finito* y que su número de elementos, o *cardinal*, es n. Este número lo denotamos por $\text{card}(A)$ o por $|A|$. Recordemos que el cardinal de un conjunto es único.

Diremos que un conjunto no vacío A es *infinito* si no existe ninguna aplicación biyectiva de $\mathbb{N}_n$ en A, cualquiera que sea $n \in \mathbb{N}$. Un conjunto es infinito si existe una biyección entre él y un subconjunto propio del mismo.

A la hora de calcular el cardinal de la unión de dos o más conjuntos es fundamental usar el *principio de inclusión-exclusión*, que se explica con más detalle en la sección **??**. Recordamos que dicho principio establece que dados dos conjuntos finitos A y B, entonces

$$|A \cup B| = |A| + |B| - |A \cap B|.$$

De forma análoga, para tres conjuntos finitos A, B y C,

$$|A \cup B \cup C| = |A| + |B| + |C| - |A \cap B| - |A \cap C| - |B \cap C| + |A \cap B \cap C|.$$

Nos centramos ahora en dos tipos de relaciones binarias entre los elementos de un conjunto A que tienen particular interés por sus aplicaciones en otros campos de la informática o de las matemáticas: las relaciones dorden y las relaciones de equivalencia.

7.3.1. Relaciones de orden

Definición 7.9 *Una relación binaria R en un conjunto A se dice* relación de orden parcial *si cumple las propiedades reflexiva, antisimétrica y transitiva. En este caso A se dice* un conjunto parcialmente ordenado. *Para las relaciones de orden se usa la notación $a \leq b$ en lugar de aRb y $a < b$ si aRb y $a \neq b$.*

Definición 7.10 *Dos elementos de A se dicen comparables si $a \leq b$ o $b \leq a$. Si todos los elementos de A son comparables entre sí, la relación se dice* relación de orden total *y el conjunto A se dice* totalmente ordenado. *Un elemento $a \in A$ se dice* minimal *si no existe otro elemento $b \in A$ tal que $b < a$. Se dice que b cubre a a si $a < b$ y no existe $c \in A$ tal que $a < c < b$.*

Como ejemplos de relaciones de orden, podemos citar:

- Los números reales con su ordenación habitual es un conjunto totalmente ordenado.
- El orden léxico gráfico en el conjunto de todas las palabras es un orden total.
- Los números naturales con la relación mRn si m divide a n es un orden parcial.
- El *orden de Sarkovskii* de los números naturales es:

$$3 \succ 5 \succ 7 \succ \cdots \succ 2 \cdot 3 \succ 2 \cdot 5 \succ 2 \cdot 7 \succ \cdots \succ 2^2 \cdot 3 \succ 2^2 \cdot 5 \succ 2^2 \cdot 7 \succ \cdots$$

$$\cdots \succ 2^n \cdot 3 \succ 2^n \cdot 5 \succ 2^n \cdot 7 \succ \cdots \succ 2^3 \succ 2^2 \succ 2 \succ 1,$$

  donde $n \succ m$ significa que n precede a m en el orden. Se trata de una relación de orden total.

Sa R una relación de orden parcial en un conjunto A. Se llama *diagrama de Hasse* asociado al par (A, R) al digrafo obtenido asociando un vértice a cada elemento de A y una arista dirigida ascendente de a a b si b cubre a a.

Ejemplo 7.3.- *Sea $A = \{1, 2, 3\}$ y $\mathcal{P}(A)$ el conjunto de las partes de A ordenado con la relación de inclusión. Comprueba que es una relación de orden parcial y dibuja su diagrama de Hasse.*

El algoritmo de ordenación topológica

En ocasiones, resulta conveniente incluir un orden parcial R en un orden total T, es decir $R \subseteq T$. Por ejemplo, si hay restricciones a la hora de efectuar unas tareas, ¿cómo podemos establecer un listado de tareas que respete dichas restricciones? Veamos esto con un ejemplo:

Ejemplo 7.4.- *Pensemos en las fases necesarias para desarrollar un programa:*

a) *Desarrollar los módulos.*

b) *Escribir la documentación de los usuarios.*

c) *Comprobación interna y posibles cambios.*

d) *Preparar un entorno de prueba.*

e) *Integrar los módulos.*

f) *Determinar las necesidades del usuario.*

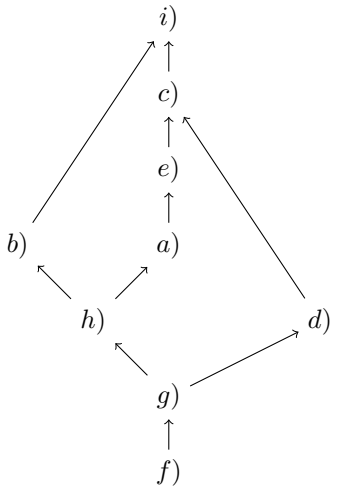
g) *Especificar los requisitos de hardware y software.*

h) *Especificar los módulos y las relaciones.*

i) *Comprobación externa y posibles cambios.*

Se define el siguiente orden parcial en el conjunto de tareas: xRy si la tarea x debe terminarse antes de comenzar la tarea y. Dibuja el diagrama de Hasse asociado a dicha ordenación y da un listado de tareas que puedan hacerse respetando el orden parcial establecido.

El diagrama de Hasse asociado al conjunto de tareas es:



Una posible lista de tareas que garantiza las restricciones es, por tanto:

$$f) \leq g) \leq h) \leq d) \leq a) \leq b) \leq e) \leq c) \leq i).$$

Notemos que no es la única lista posible que cumple las restricciones. Otra podría ser:

$$f) \leq g) \leq d) \leq h) \leq b) \leq a) \leq e) \leq c) \leq i).$$

■

Dado un conjunto finito A, el *algoritmo de ordenación topológica* permite insertar un orden parcial R dentro de un orden total T. Para ello, se toman los elementos minimales $a_1, \ldots, a_i$ de A (nivel 0), después los minimales $a_{i+1}, \ldots, a_f$ de $A - \{a_1, \ldots, a_i\}$ (nivel 1) y así sucesivamente. La relación de orden total que se busca se obtiene ordenando los elementos en orden creciente de nivel. Los elementos dentro de un mismo nivel pueden ordenarse indistintamente, por eso, en muchas ocasiones lel orden total obtenido no es único.

En el ejemplo anterior tenemos: nivel 0: $\{f)\}$; nivel 1: $\{g)\}$; nivel 2: $\{d), h)\}$; nivel 3: $\{a), b)\}$; nivel 4: $\{e)\}$; nivel 5: $\{c)\}$; nivel 6: $\{i)\}$. Cualquier ordenación total posible deberá empezar por $f) \leq g)$ y acabar por $e) \leq c) \leq i)$. Podremos elegir a la hora de ordenar los elementos de los niveles 2 y 3. En consecuencia, en este caso, se obtienen 4 ordenaciones totales posibles que son, ademas de las dos indicadas en el ejemplo anterior, las siguientes:

$$f) \leq g) \leq h) \leq d) \leq b) \leq a) \leq e) \leq c) \leq i),$$
$$f) \leq g) \leq d) \leq h) \leq a) \leq b) \leq e) \leq c) \leq i).$$

Otros algoritmos de ordenación

Un problema sencillo de describir, pero con interesantes y no triviales aplicaciones en informática es el de tener que ordenar una lista de números que inicialmente puede estar desordenada. Existen varios algoritmos para este fin que usan estrategias diferentes y con distinta complejidad.

Por ejemplo, dad una lista de números $\{a_1, \ldots, a_n\}$, el *algoritmo de la burbuja* consiste en ir intercambiando dos elementos sucesivos si están en orden incorrecto. Si empezamos comparando a_1 con a_2 y así sucesivamente, al final de la primera pasada, el número mayor estará situado en el orden correcto. Se realiza una segunda pasada para asegurar que el segundo número más grande esté en su sitio correcto. Notemos que en esta segunda pasada sólo es necesario comparar los $n-1$ primeros números de la lista. En el peor de los casos, repitiendo el proceso un $n-1$ veces, conseguimos ordenar la lista inicial. De forma totalmente análoga, se puede aplicar el algoritmo haciendo las ordenaciones de forma descendente, comparando a_n con a_{n-1} y así sucesivamente. El nombre del algoritmo viene asociado al símil de que los números mayores (o menores) se van desplazando hacia los extremos de la lista como si fuesen burbujas que ascienden a la superficie de un líquido.

Ejemplo 7.5.- *Usando el algoritmo de la burbuja (descendente) ordena la siguiente lista:* $\{4,2,5,3,1\}$.

Vamos indicando las comparaciones sucesivas con una caja. Cuando después de comparar dos elementos, hay que intercambiar su posición, lo indicamos con $\rightsquigarrow$. Si no hay que hacer intercambio, ponemos $\rightarrow$. Con estos criterios, en la primera pasada se obtiene:

$$\{4,2,5,\boxed{3,1}\} \rightsquigarrow \{4,2,\boxed{5,1},3\} \rightsquigarrow \{4,\boxed{2,1},5,3\} \rightsquigarrow \{\boxed{4,1},2,5,3\} \rightsquigarrow \{1,4,2,5,3\}.$$

Como vemos, la burbuja formada por el menor número, el 1, se ha desplazado hacia la izquierda. En la segunda iteración se obtiene

$$\{1,4,2,\boxed{5,3}\} \rightsquigarrow \{1,4,\boxed{2,3},5\} \rightarrow \{1,\boxed{4,2},3,5\} \rightsquigarrow \{1,2,4,3,5\}.$$

Notemos que en el último paso no es necesario comparar $\boxed{1,2}$, pues tras la primera iteración ya estamos seguros de que el 1 ocupa su posición correcta. La tercera y cuarta iteración son las siguientes:

$$\{1,2,4,\boxed{3,5}\} \rightarrow \{1,2,\boxed{4,3},5\} \rightsquigarrow \{1,2,3,4,5\}.$$

$$\{1,2,3,\boxed{4,5}\} \rightarrow \{1,2,3,4,5\}.$$

Aunque en este ejemplo particular la lista ha quedado totalmente ordenada con sólo tres iteraciones, en general hay que realizar todas las iteraciones. ■

En el ejemplo anterior, hemos tenido que hacer 10 comparaciones y realizar intercambios en 7 de ellas. Para estimar la complejidad del algoritmo en el caso general, se cuentan las comparaciones que se deberían hacer. El número resultante nos da también la cota superior para el número de posibles intercambios. Dicho número es

$$\sum_{i=1}^{n-1}\sum_{j=i+1}^{n} 1 = \sum_{i=1}^{n-1}(n-i) = \sum_{i=1}^{n-1} n - \sum_{i=1}^{n-1} i = n(n-1) - (1+2+\cdots+(n-1)) = n(n-1) - \frac{n(n-1)}{2} = \frac{n(n-1)}{2}.$$

En definitiva, la complejidad del algoritmo de la burbuja es $O(n^2)$.

Otro algoritmo clásico de ordenación es el conocido como *ordenación por mezcla* o *mergesort*. Es un ejemplo de la técnica algorítmica conocida como *divide y vencerás*. La idea del algoritmo mergesort consiste en dividir una lista de n elementos en dos mitades (de k elementos cada una si $n = 2k$ o de k y $k+1$ elementos si $n = 2k+1$) y ordenar cada mitad recursivamente aplicando el ordenamiento por mezcla. Al final se combinan las dos listas manteniendo el orden creciente.

Ejemplo 7.6.- *Usa el algoritmo mergesort para ordenar la siguiente lista:* $\{7,4,8,2,5,3,1,6\}$.

Dividimos en dos listas, $\{7,4,8,2\}$ y $\{5,3,1,6\}$, que a su vez volvemos a subdividir en $\{7,4\}$, $\{8,2\}$, $\{5,3\}$, $\{1,6\}$. La ordenación de estas listas es $\{4,7\}$, $\{2,8\}$, $\{3,5\}$, $\{1,6\}$. Mezclamos las dos primeras listas y las dos últimas para obtener $\{2,4,7,8\}$, $\{1,3,5,6\}$. Finalmente, obtenemos la lista total ordenada. Mostramos con detalle en este último paso cómo se aplica el algoritmo de mezcla para combinar dos listas ordenadas. El símbolo $\bowtie$ indica que comparamos los elementos minimales de las dos listas.

$$\{\boxed{2},4,7,8\} \bowtie \{\boxed{1},3,5,6\} \rightarrow \{1\}$$

$$\{\boxed{2},4,7,8\} \bowtie \{\boxed{3},5,6\} \rightarrow \{1,2\}$$

$$\{\boxed{4},7,8\} \bowtie \{\boxed{3},5,6\} \rightarrow \{1,2,3\}$$

$$\{\boxed{4},7,8\} \bowtie \{\boxed{5},6\} \rightarrow \{1,2,3,4\}$$

$$\{\boxed{7},8\} \bowtie \{\boxed{5},6\} \rightarrow \{1,2,3,4,5\}$$

$$\{\boxed{7},8\} \bowtie \{\boxed{6}\} \rightarrow \{1,2,3,4,5,6\}$$

$$\{\boxed{7},8\} \bowtie \{\} \rightarrow \{1,2,3,4,5,6,7\}$$

$$\{\boxed{8}\} \bowtie \{\} \rightarrow \{1,2,3,4,5,6,7,8\}.$$ ■

Para hacernos una idea de la complejidad del algoritmo mergesort, tenemos en cuenta que para mezclar dos listas de n elementos en total hay que hacer $n-1$ comparaciones. Si denotamos $M(n)$ al número de operaciones necesarias para ordenar una lista de n elementos, se tiene que

$$M(n) = M\left(\lceil n/2 \rceil\right) + M\left(\lfloor n/2 \rfloor\right) + n - 1$$

Para facilitar los cálculos, supongamos que $n = 2^j$. Además cambiaremos $n-1$ por n, por lo que realmente obtendremos una cota superior para el número de operaciones. Si denotamos $m(j) = M(2^j)$, se tiene que

$$m(j) = 2m(j-1) + 2^j.$$

Además, $m(0) = M(1) = 0$ pues para ordenar una lista de un único elemento no hay que hacer ninguna operación. Aplicando recursivamente la igualdad anterior, se obtiene que

$$\begin{aligned} m(j) &= 2m(j-1) + 2^j = 2(2m(j-2) + 2^{j-1}) + 2^j = 2^2 m(j-2) + 2 \cdot 2^j \\ &= 2^2(2m(j-3) + 2^{j-2}) + 2 \cdot 2^j = 2^3 m(j-3) + 3 \cdot 2^j \\ &= \cdots = 2^j m(0) + j \cdot 2^j = j2^j. \end{aligned}$$

Por lo tanto, tenemos que una cota superior para el número de ordenaciones de una lista de n elementos es $n \log_2 n$. Esta misma conclusión se puede obtener aunque n no sea una potencia de 2. En consecuencia, se tiene que la complejidad del algoritmo mergesort es $O(n \log n)$.

Para hacernos una idea de la importancia de la complejidad a la hora de diseñar algoritmos, tengamos en cuenta el siguiente ejemplo. Para ordenar una lista de un millón de números ($n = 10^6$), se tiene que

$$\frac{n^2}{n \log n} \approx 72382$$

por lo que el algoritmo de la burbuja necesitaría realizar 72382 veces más operaciones que el mergesort.

Otros algoritmos de ordenación muy empleados son el de *ordenamiento rápido* o *quicksort*, también basado en la técnica de *divide y vencerás* y el de *ordenación por montones* o *heapsort*. Ambos permiten ordenar un conjunto de n elementos en un tiempo proporcional a $n \log n$, es decir, su complejidad es $O(n \log n)$. A pesar de tener la misma complejidad, todos estos algoritmos tienen peculiaridades que los diferencian desde el punto de vista computacional (espacio de memoria empleado, estabilidad, capacidad de paralelización, etc.).

7.3.2. Relaciones de equivalencia

Otro tipo de relación importante, que conduce a la identificación de objetos que satisfacen una propiedad común, es la *relación de equivalencia*.

Definición 7.11 *Una relación binaria R en un conjunto A se dice* relación de equivalencia *si cumple las propiedades reflexiva, simétrica y transitiva. Dos elementos relacionados se dicen* equivalentes.

Definición 7.12 *Dada una relación de equivalencia R en un conjunto A y un elemento $a \in A$ se define la* clase de equivalencia de a*:*

$$[a] = \{b \in A \mid aRb\}.$$

Definición 7.13 *El* conjunto cociente de A *es el conjunto formado por sus clases de equivalencia:*

$$A/R = \{[a] \mid a \in A\} \subseteq \mathcal{P}(A).$$

Un elemento de una clase de equivalencia se dice un representante *de ella.*

A continuación listamos una serie de propiedades relacionadas con las relaciones de equivalencia.

1. Cualquier representante genera su clase de equivalencia.
2. Dos elementos $a, b \in A$ originan la misma clase de equivalencia si y solo si aRb.
3. O bien $[a] = [b]$ o $[a] \cap [b] = \emptyset$.

4. $A = \cup_{[a]\in A/R}[a]$.

5. Sea $\{A_i \mid i \in I\}$ una partición de un conjunto A. Existe una relación de equivalencia en A de modo que sus clases de equivalencia son los conjuntos de A.

Como ejemplos de relaciones de recurrencia en el conjunto $\mathbb{Z}$ de los números enteros, tenemos las *congruencias*. Por ejemplo, consideramos la siguiente relación en $\mathbb{Z}$: xRy si $x - y$ es par. Notemos que en este caso tenemos que números distintos como 4 y 6 comparten una propiedad común: la de ser pares. Lo mismo ocurre con el 2 y el 250 o con el -1 y el 3. Si embargo, esto no ocurre con el 2 y el 3. Con este ejemplo se pon de manifiesto que más que el número en sí, lo que interesa es una propiedad: *ser par o impar*. Notemos además, que esta relación de equivalencia divide a $\mathbb{Z}$ en dos subconjuntos disjuntos:

$$\mathbb{Z} = \{\ldots, -3, -1, 1, 3, \ldots\} \cup \{\ldots, -4, -2, 0, 2, 4, \ldots\}.$$

En general, la *relación de congruencia módulo n* en $\mathbb{Z}$ se define por xRy si $x - y$ es múltiplo de n y divide a $\mathbb{Z}$ en n subconjuntos disjuntos.

Asociado a una relación de equivalencia aparece el concepto de *partición*.

Definición 7.14 *Una familia $\{A_i \mid i \in I\}$ de subconjuntos de A se cice una* partición de A *si*

1. $A_i \neq \emptyset$ *para todo* $i \in I$.

2. $A_i \cap A_j = \emptyset$ *si* $i \neq j$.

3. $A = \cup_{i\in I} A_i$.

El vínculo entre relaciones de equivalencia y particiones viene dado por los siguientes resultados.

Teorema 7.2 *Sea R una relación de equivalencia en un conjunto A. Entonces la colección de clases de equivalencia $\{[a] \mid a \in A\}$ es una partición de A.*

Recíprocamente, también se tiene:

Teorema 7.3 *Sea $\{A_i \mid i \in I\}$ una partición en un conjunto A. Entonces existe una relación de equivalencia en A de modo que sus clases de equivalencia son los conjuntos A_i.*

Por ejemplo, para la relación de congruencia módulo n en $\mathbb{Z}$ las distintas clases de equivalencia son:

$$[0] = \{kn \mid k \in \mathbb{Z}\}, \quad [1] = \{kn + 1 \mid k \in \mathbb{Z}\}, \quad \ldots, \quad [n-1] = \{kn + n - 1 \mid k \in \mathbb{Z}\}.$$

El conjunto cociente de dicha relación de equivalencia da lugar a un conjunto de especial interés (criptografía, estructuras algebraicas, etc.) conocido como el *conjunto de los enteros módulo n*:

$$\mathbb{Z}_n = \{[0], [1], \ldots, [n-1]\}.$$

7.4. Problemas resueltos

1. Simplifica la siguiente expresión, haciendo uso de las operaciones con conjuntos:

$$(A \cap B) \cup \left(B \cap \left((C \cap D) \cup \left(C \cap \overline{D}\right)\right)\right).$$

Solución. Por la propiedad distributiva:

$$(A \cap B) \cup \left(B \cap \left(C \cup \left(D \cap \overline{D}\right)\right)\right),$$

que es igual a

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

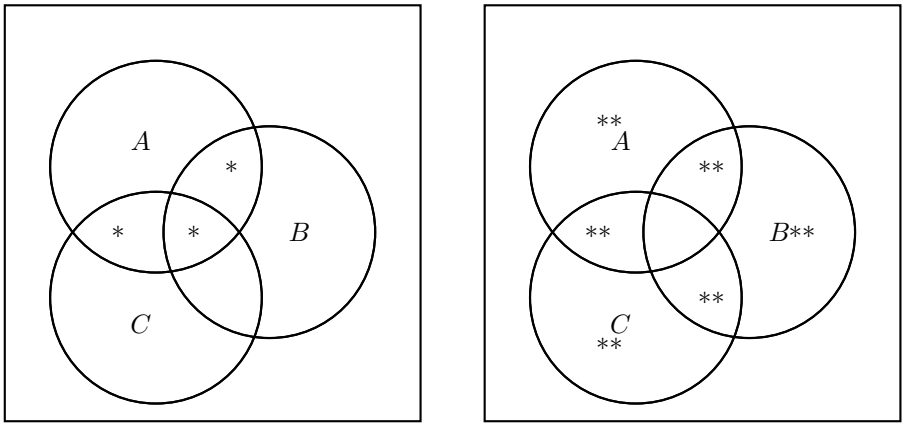
Aplicando la propiedad conmutativa y luego la distributiva llegamos a

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

■

2. Demuestra si la siguiente igualdad es cierta o no: $A \triangle (B \cup C) = (A \triangle B) \cup (A \triangle C)$.

   Solución. Usando diagramas de Venn, tenemos que el conjunto $A \triangle (B \cup C)$ está formado por la unión de las regiones marcadas con $*$ en la figura de la izquierda, mientras que el conjunto $(A \triangle B) \cup (A \triangle C)$ está formado por la unión de las regiones marcadas con $**$ en la figura de la derecha.



   Pero sin duda, una forma mucho más contundente para demostrar que una afirmación es falsa es buscar un contraejemplo. En nuestro caso, supongamos que $A = \{2, 4, 6, 8\}$, $B = \{1, 2, 3, 4, 5\}$ y $C = \{0, 1, 2\}$. Entonces $B \cup C = \{0, 1, 2, 3, 4, 5\}$ y $A \triangle (B \cup C) = \{0, 1, 3, 5, 6, 8\}$. Por otra parte, $A \triangle B = \{1, 3, 5, 6, 8\}$, $A \triangle C = \{0, 1, 4, 6, 8\}$ y $(A \triangle B) \cup (A \triangle C) = \{0, 1, 3, 4, 5, 6, 8\}$. Evidentemente, $A \triangle (B \cup C) \neq (A \triangle B) \cup (A \triangle C)$, pues hay un elemento (el 4) que no está en el primer conjunto, pero sí en el segundo. ■

3. Justifica si las siguiente son relacionen de orden en los conjuntos indicados:

   a) En $\mathbb{R}^2$: $(x, y) \leq (u, v)$ si $x \leq u$ e $y \leq v$.

   b) En $\mathbb{C}$: $z_1 \leq z_2$ si $|z_1|^2 \leq |z_2|^2$. Recordemos que si $z = x + iy$, entones su módulo es $|z| = \sqrt{x^2 + y^2}$.

   Solución. La relación indicada en a) es de orden pues es:

   - Reflexiva: $(x, y) \leq (x, y)$ para todo $(x, y) \in \mathbb{R}^2$ ya que $x = x$ e $y = y$;
   - Antisimétrica: si $(x, y) \leq (u, v)$ y $(u, v) \leq (x, y)$, entonces $x \leq u$, $y \leq v$, $u \leq x$ y $v \leq y$. Por lo tanto $x = u$, $y = v$ y $(x, y) = (u, v)$.
   - Transitiva: si $(x, y) \leq (u, v)$ y $(u, v) \leq (s, t)$, entonces $x \leq u$, $y \leq v$, $u \leq s$ y $v \leq t$. Por lo tanto $x \leq s$, $y \leq t$ y $(x, y) \leq (s, t)$.

   Notemos que se trata de una ordenación de orden parcial pues hay elementos en $\mathbb{R}^2$ que no están relacionados. Por ejemplo, $(1, 2)$ y $(2, 1)$.

   La relación indicada en b) no es de orden ya que no cumple la propiedad antisimétrica. En efecto, $\sqrt{2} \leq 1 + i$, $1 + i \leq \sqrt{2}$ (ya que $|\sqrt{2}|^2 = |1 + i|^2 = 2$) pero, sin embargo, $\sqrt{2} \neq 1 + i$. ■

4. Justifica si las siguiente son relaciones de equivalencia en los conjuntos indicados. En caso afirmativo, encuentra sus clases de equivalencia.

   a) En $\mathbb{Z}$: $m \mathcal{R} n$ si $mn \geq 0$.

   b) La relación $m \mathcal{R} n$ si $n - m$ es un múltiplo de 3 es una relación de equivalencia en el conjunto $A = \{1, 2, 3, 4, 5, 6, 7\}$.

   Solución. La relación indicada en a) no es de equivalencia puesto que no cumple la propiedad transitiva: $1 \mathcal{R} 0$, $0 \mathcal{R} - 1$, pero 1 no está relacionado con -1. La relación indicada en b) sí es de equivalencia ya que es

   - Reflexiva: cualquier elemento $m \in A$ está relacionado consigo mismo ya que $m - m = 0$, que es múltiplo de 3.

- Simétrica: si $m\mathcal{R}n$ entonces $n-m$ es un múltiplo de 3, digamos que $n-m=3k$ para algún $k\in\mathbb{Z}$. Entones $m-n=-3k=3(-k)$ y, por tanto $m-n$ también es múltiplo de 3. Por lo tanto $n\mathcal{R}m$.
- Transitiva: si $m\mathcal{R}n$ entonces $n-m$ es un múltiplo de 3, digamos que $n-m=3k$ para algún $k\in\mathbb{Z}$. Si $n\mathcal{R}p$ entonces $p-n$ es un múltiplo de 3, digamos que $p-n=3j$ para algún $j\in\mathbb{Z}$. Entonces

$$p-m=p-n+n-m=3j-3k=3(j-k),$$

por lo que $p-m$ es múltiplo de 3 y $m\mathcal{R}p$.

Las clases de equivalencia son: $[1]=\{1,4,7\}$, $[2]=\{2,5\}$, $[3]=\{3,6\}$. ■

5. Clasifica las siguientes funciones según sean inyectivas, suprayectivas o biyectivas:

$a)f:\mathbb{N}\to\mathbb{N}$, $f(n)=n^2$ $\quad b)f:\mathbb{R}\to\mathbb{R}$, $f(x)=x^4$ $\quad c)f:[0,\infty)\to[0,\infty)$, $f(x)=x^2$

$d)f:[0,\infty)\to\mathbb{R}$, $f(x)=x^2$ $\quad e)f:\mathbb{C}\to\mathbb{C}$, $f(z)=z^2$ $\quad f)f:\mathbb{R}\to\mathbb{R}$, $f(x)=x^2-2x+1$.

Solución. La relación definida en a) es inyectiva (si $n^2=m^2$ y $n>0$, $m>0$, entonces $n=m$) pero no es suprayectiva (hay elementos en $\mathbb{N}$ sin antiimagen, cualquiera que no sea un cuadrado perfecto como el 2, 3, 5 o 6).

La relación definida en b) no es inyectiva ($f(1)=f(-1)$ pero $1\neq-1$) ni suprayectiva (los reales negativos no tienen antiimagen).

La relación definida en c) es inyectiva, por el mismo razonamiento que en a), y suprayectiva ya que la antiimagen de un número real positivo y es $\sqrt{y}\in[0,\infty)$ (en este caso no tenemos en cuenta $-\sqrt{y}$.

La relación definida en d) es inyectiva, de nuevo, por el mismo razonamiento que en a), pero no suprayectiva ya que los reales negativos no tienen antiimagen.

La relación definida en e) no es inyectiva ($f(1)=f(-1)$ pero $1\neq-1$) pero sí suprayectiva ya que podemos calcular la raíz cuadrada de cualquier número complejo.

La relación definida en f) no es inyectiva ($f(0)=f(2)$ pero $0\neq2$) ni suprayectiva ya que los reales negativos no tienen antiimagen. En este caso, puede ser de utilidad darse cuenta que $f(x)=(x-1)^2$ y dibujar la gráfica de la función $f(x)$. ■

6. Calcula cuántos números naturales menores o iguales que 10000 son primos con 30. Nota: dos números son primos entre sí si no tienen divisores comunes.

Solución. Como $30=2\cdot3\cdot5$, se trata de calcular cuántos números menores o iguales que 10000 no son divisibles ni por 2 ni por 3 ni por 5. Para ello, definimos los conjuntos

$$A=\{n\in\mathbb{Z}\mid 1\leq n\leq 10000, n \text{ no es divisible por } 2\},$$

$$B=\{n\in\mathbb{Z}\mid 1\leq n\leq 10000, n \text{ no es divisible por } 3\},$$

$$C=\{n\in\mathbb{Z}\mid 1\leq n\leq 10000, n \text{ no es divisible por } 5\},$$

y calculamos $x=|A\cup B\cup C|$. La cantidad x nos dice cuántos números menores o iguales que 10000 son múltiplos de 2, 3 o 5, por lo que el resultado final será $10000-x$.

Para el cálculo de x nos apoyamos en el principio de inclusión-exclusión, que dice

$$|A\cup B\cup C|=|A|+|B|+|C|-|A\cap B|-|A\cap C|-|B\cap C|+|A\cap B\cap C|.$$

Como uno de cada dos números es múltiplo de 2, tenemos que

$$|A|=\frac{10000}{2}=5000.$$

Análogamente, como uno de cada tres números es múltiplo de 3, tenemos que

$$|B|=\left\lfloor\frac{10000}{3}\right\rfloor=3333.$$

donde $\lfloor a \rfloor$ es la parte entera de a, que denota al entero m más próximo a a tal que $m < a$.
De forma parecida

$$|C| = \left\lfloor \frac{10000}{5} \right\rfloor = 2000.$$

El conjunto $A \cap B$ está formado por los múltiplos de 2 y de 3, es decir, por los múltiplos de 6. En consecuencia:

$$|A \cap B| = \left\lfloor \frac{10000}{6} \right\rfloor = 1666.$$

Con razonamientos similares a los anteriores, llegamos a que

$$|A \cap C| = \left\lfloor \frac{10000}{10} \right\rfloor = 1000,$$

$$|B \cap C| = \left\lfloor \frac{10000}{15} \right\rfloor = 666,$$

$$|A \cap B \cap C| = \left\lfloor \frac{10000}{15} \right\rfloor = 333.$$

Por lo tanto,

$$x = |A \cup B \cup C| = 5000 + 3333 + 2000 - 1666 - 1000 - 666 + 333 = 7334$$

y la solución es $10000 - 7334 = 2666$.

7. Calcula cuántos números enteros positivos menores o iguales que 100000 hay que no sean múltiplos de 2 ni de 5. Calcula cuánto vale la suma de dichos números (ten en cuenta cuánto vale la suma de $1 + 2 + 3 + \cdots + n$).

$a) f : \mathbb{N} \to \mathbb{N}\ f(n) = n^2$ $\quad b) f : \mathbb{R} \to \mathbb{R}\ f(x) = x^4$ $\quad c) f : [0, \infty) \to [0, \infty)\ f(x) = x^2$

$d) f : [0, \infty) \to \mathbb{R}\ f(x) = x^2$ $\quad e) f : \mathbb{C} \to \mathbb{C}\ f(z) = z^2$ $\quad f) f : \mathbb{R} \to \mathbb{R}\ f(x) = x^2 - 2x + 1.$

Solución. Definimos los conjuntos

$$A = \{n \in \mathbb{Z} \mid 1 \leq n \leq 100000, n \text{ es divisible por } 2\},$$

$$B = \{n \in \mathbb{Z} \mid 1 \leq n \leq 100000, n \text{ es divisible por } 5\},$$

$$A \cap B = \{n \in \mathbb{Z} \mid 1 \leq n \leq 100000, n \text{ es divisible por } 10\},$$

y calculamos $x = |A \cup B|$. La cantidad x nos dice cuántos números menores o iguales que 100000 son múltiplos de 2 o 5, por lo que el resultado final será $100000 - x$.
Para el cálculo de x nos apoyamos en el principio de inclusión-exclusión, que dice

$$|A \cup B| = |A| + |B| - |A \cap B| = 50000 + 20000 - 10000 = 60000.$$

Por lo tanto, la solución es que hay $100000 - 60000 = 40000$ números enteros positivos menores o iguales que 100000 hay que no son múltiplos de 2 ni de 5.
Para calcular su suma, hallamos en primer lugar la suma de los números de 1 a 100000:

$$S = 1 + 2 + 3 + \cdots + 100000 = \frac{100000 \times 100001}{2}.$$

A continuación, la suma de los elementos de A:

$$s_1 = 2 + 4 + 6 + \cdots + 100000 = 2(1 + 2 + 3 + \cdots + 50000) = 2\frac{50000 \times 50001}{2},$$

la suma de los elementos de B:

$$s_2 = 5 + 10 + 15 + \cdots + 100000 = 5(1 + 2 + 3 + \cdots + 20000) = 5\frac{20000 \times 20001}{2},$$

y la suma de los elementos de $A \cap B$:

$$s_3 = 10 + 20 + 30 + \cdots + 100000 = 10(1 + 2 + 3 + \cdots + 10000) = 10\frac{10000 \times 10001}{2}.$$

La suma total es $S - (s_2 + s_2 - s_3) = 2000000000$. ■

7.5. Problemas propuestos

1. Halla la cardinalidad de los siguientes conjuntos: $\{a\}$, $\{\{a\}\}$, $\{a, \{a\}\}$, $\{a, \{a\}, \{a, \{a\}\}\}$.

2. Señala los conjuntos de los cuales 2 es un elemento:

   a) $\{x \in \mathbb{R} \mid x \text{ es un entero mayor que uno}\}$
   b) $\{x \in \mathbb{R} \mid x \text{ es el cuadrado de un entero}\}$
   c) $\{x, \{2\}\}$
   d) $\{\{2\}, \{\{2\}\}\}$
   e) $\{\{2\}, \{2, \{2\}\}\}$
   e) $\{\{\{2\}\}\}$.

3. Halla la cardinalidad de los siguientes conjuntos: $\emptyset$, $\{\emptyset\}$, $\{\emptyset, \{\emptyset\}\}$, $\{\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\}\}$.

4. **(Paradoja de Russell)** Se define S como el conjunto cuyos elementos son conjuntos A tales que $A \notin A$. Prueba que

   a) Si $S \in S$ se origina una contradicción.
   b) Si $S \notin S$ también se origina una contradicción.

   Concluye que hay algún problema en la definición de S y encuentra el origen de este problema.

5. Encuentra los conjuntos A y B si $A - B = \{1, 5, 7, 8\}$, $B - A = \{2, 10\}$ y $A \cap B = \{3, b, 9\}$.

6. Sean $A = \{0, 2, 4, 6, 8, 10\}$, $B = \{0, 1, 2, 3, 4, 5, 6\}$ y $C = \{4, 5, 6, 7, 8, 9, 10\}$. Calcula $A \cap B \cap C$, $A \cup B \cup C$, $(A \cup B) \cap C$ y $(A \cap B) \cup C$.

7. Dibuja los diagramas de Venn de las siguientes combinaciones de los con- juntos A, B y C: $A \cap (B \cup C)$, $\overline{A} \cap \overline{B} \cap \overline{C}$, $(A - B) \cup (A - C) \cup (B - C)$.

8. ¿Qué puedes concluir acerca de los conjuntos A y B si una de las siguientes firmaciones es cierta?

   - $A \cup B = A$,
   - $A - B = A$,
   - $A - B = B - A$,
   - $A \cap B = A$,
   - $A \cap B = B \cap A$.

9. ¿Es cierto que $(A \triangle B) \triangle (C \triangle D) = (A \triangle C) \triangle (B \triangle D)$?

10. Halla mediante el principio de inclusión-exclusión el número de divisores positivos de 60.

11. Halla el número de maneras de ordenar las letras A, E, M, O, U, Y en una sucesi´on de forma que no aparezcan las palabras ME y YOU.

12. El profesor McBrain ha decretado que, por necesidadades administrativas, cada estudiante ha de hacer exactamente cuatro asignaturas de entre siete posibles. Los profesores informan que el número de asistentes a las asignaturas es 52, 30, 30, 20, 25, 12, 18. ¿Qué puede deducirse?

13. En la clase de Análisis de la doctora Cynthia Angst, 32 de los estudiantes son chicos. Cada chico conoce a cinco de las chicas de la clase, y cada chica conoce a ocho de los chicos. ¿Cuántas chicas hay en la clase?

14. Sea la relación $R = \{(1,1),(2,1),(3,2),(4,3)\}$. Encuentra $R \circ R$, $R \circ R \circ R$, ... Interpreta el significado de estas relaciones.

15. Considera en el conjunto $A = \{1,2,3,4,5,6\}$ la relación $R = \{(a,b) \in A \times A \mid a \text{ divide a } b\}$. ¿Es una relación de orden? ¿Es de orden total? Dibuja el digrafo correspondiente a esta relación.

16. Decide si las siguientes relaciones en el conjunto $\{1,2,3,4\}$ son re?exivas, simétricas, antisimétricas o transitivas:

    a) $\{(2,2),(2,3),(2,4),(3,2),(3,3),(3,4)\}$,
    b) $\{(1,1),(1,2),(2,1),(2,2),(3,3),(4,4)\}$,
    c) $\{(2,4),(4,2)\}$,
    d) $\{(1,2),(2,3),(3,4)\}$,
    e) $\{(1,3),(1,4),(2,3),(2,4),(3,1),(3,4)\}$.

17. Da un ejemplo de una relación en $\mathbb{N}$ que sea:

    a) Simétrica y antisimétrica.
    b) Ni simétrica ni antisimétrica

18. Encuentra el error en la demostración que se presenta de la siguiente afirmación (falsa): Sea R una relación simétrica y transitiva en un conjunto A. Se tiene que R es reflexiva.

    Demostración. Sea a un elemento de A. Elegimos $b \in A$ tal que $(a,b) \in R$. Puesto que R es simétrica entonces $(b,a) \in R$, y como R es transitiva entonces $(a,a) \in R$. Por lo tanto R es reflexiva. ∎

19. Sean R y S dos relaciones de equivalencia en un conjunto A. Prueba que $R \cap S$ es también una relación de equivalencia. Si R es la relación aRb si $b - a$ es divisible por 2 y S es la relación aSb si $b - a$ es divisible por 3, describe la relación $R \cap S$.

20. Considera la relación de equivalencia $R = \{(x,y) \in \mathbb{Q} \times \mathbb{Q} \mid y - x \in \mathbb{Z}\}$. Describe la clase de equivalencia del elemento 1 y la clase de equivalencia del elemento $1/2$.

21. Considera el conjunto de los divisores de 1296 con la relación de orden parcial aRb si a divide a b. Dibuja el diagrama de Hasse correspondiente.

22. Se consideran los siguientes pasos para construir una casa: cimientos, estructura, techo, revestimiento exterior, pintar exterior, fontanería, cableado, paredes interiores, recubrimiento de suelos, recubrimiento de paredes interiores, retoques interiores, retoques exteriores, entrega de llaves. Define una relación de orden parcial, dibuja el correspondiente diagrama de Hasse y encuentra un orden total que extienda dicho orden parcial.

23. Ordena las siguientes listas utilizando los algoritmos de la burbuja y mergesort: $A = \{1,3,5,7,2,4,6,8\}$, $B = \{8,7,6,5,4,3,2,1\}$.

24. Prueba que la composición de aplicaciones inyectivas es inyectiva.

25. Prueba que la composición de aplicaciones suprayectivas es suprayectiva.

26. Prueba que la inversa de una aplicación, si existe es única.

27. Comprueba que que $(f \circ g) \circ h = f \circ (g \circ h)$ en los siguientes casos

a) $f, g, h : \mathbb{N} \to \mathbb{N}$ definidas por

$$f(x) = x - 1, \quad g(x) = 3x, h(x) = \begin{cases} 0 & \text{si } x \text{ es par} \\ 1 & \text{si } x \text{ es impar.} \end{cases}$$

b) $f, g, h : \mathbb{R} \to \mathbb{R}$ definidas por $f(x) = x^2$, $g(x) = x + 5$ y $h(x) = \sqrt{x^2 + 2}$.

c) $f, g, h : \mathbb{Z} \to \mathbb{Z}$ definidas por $f(n) = n^2$, $g(n) = n + 1$ y $h(n) = n - 1$.

28. Para cada una de las siguientes aplicaciones $f : \mathbb{R} \to \mathbb{R}$ determina si es inyectiva, suprayectiva o biyectiva (en tal caso encuentra su inversa):

a) $f(x) = -x + 5$.

b) $f(x) = x^3$.

c) $f(x) = x^2$.

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

29. Sean $A = \{1, 2, 3\}$ y $B = \{x, y\}$. ¿Cuántas aplicaciones $f : A \to B$ hay? ¿Cuántas son inyectivas? ¿Cuántas son suprayectivas?

Capítulo 8

Aritmética modular

8.1. Congruencias

Recordemos la siguiente relación de equivalencia en $\mathbb{Z}$:

Definición 8.1 *Dados $a, b \in \mathbb{Z}$, decimos que a es* congruente *con b módulo n si $a - b$ es divisible por n. En este caso, denotamos*

$$a \equiv b \ (n) \quad \text{o} \quad a \equiv b \pmod{n}.$$

Algunas observaciones acerca de esta definición:

1. Existe un entero $k \in \mathbb{Z}$ tal que $a = kn + b$.
2. Podemos identificar una relación de congruencia módulo n como un reloj redondo de n posiciones. Por ejemplo, si $n = 5$, $a = 3$ y $b = 8$ coinciden en la misma posición.
3. Con las hora seguimos una aritmética modular ($n = 12$ o $n = 24$).

Las clases de equivalencia de un elemento $j \in \mathbb{Z}$ se denotan indistintamente $[j]$ o $\overline{j}$. Dichas clases son:

$$\begin{array}{rcl} \overline{0} & = & \{0, n, -n, 2n, -2n, \dots\} \\ \overline{1} & = & \{1, n+1, -n+1, 2n+1, -2n+1, \dots\} \\ \vdots & \vdots & \vdots \\ \overline{n-1} & = & \{n-1, 2n-1, -1, 3n-1, -n-1, \dots\} \end{array}$$

Definición 8.2 *El* conjunto de los enteros módulo n *es el conjunto cociente de esta relación de equivalencia. Se denota $\mathbb{Z}_n$ ($\mathbb{Z}$ módulo n) y está formado por todas las clases de equivalencia:*

$$\mathbb{Z}_n = \{\overline{0}, \overline{1}, \dots, \overline{n-1}\}.$$

Se usa el nombre de *aritmética modular* para referirse a las operaciones que se pueden hacer con los elementos del conjunto $\mathbb{Z}_n$. Su estudio sistemático se atribuye al matemático alemán Carl Friedrich Gauss, quien publicó en 1801 su obra *Disquisitiones Arithmeticae* en la que las congruencias juegan un papel fundamental. En dicha obra Gauss recopila resultados de matemáticos de la talla de Fermat, Euler, Lagrange y Legendre, y, además, incluye nuevos resultados descubiertos por él mismo. La aritmética modular tiene importantes aplicaciones en campos de las matemáticas tales como la teoría de números, las estructuras algebraicas o la criptografía, así como en otras disciplinas como las artes visuales y musicales.

Una observación importante es darse cuenta de que si $a = cn + r$ con $0 \leq c < n$ entonces $[a] = [r]$. De hecho, cualquier elemento de $[a]$ genera esta clase. Por lo tanto

$$[a] = [b] \iff a \equiv b \pmod{n} \iff n \mid (b - a).$$

Por ejemplo, si trabajamos módulo 10, tenemos que $13 \equiv 23 \equiv 33 \equiv 4563$. A esta lista podríamos añadir cualquier número terminado en 3, ya que todos ellos dejan el mismo resto al dividir por 10 (el 3) o, equivalentemente, su diferencia es un múltiplo de 10.

De la propia definición de congruencia se siguen de forma inmediata una serie de propiedades:

1. Si $a_1 \equiv a_2 \pmod{n}$ y $b_1 \equiv b_2 \pmod{n}$, $a_1 + b_1 \equiv a_2 + b_2 \pmod{n}$.
2. Si $a_1 \equiv a_2 \pmod{n}$ y $b_1 \equiv b_2 \pmod{n}$, $a_1 b_1 \equiv a_2 b_2 \pmod{n}$.
3. $a \equiv b \pmod{n}$ si y solo si $a^k \equiv b^k \pmod{n}$, para cualquier $k \in \mathbb{N}$.
4. $ac \equiv bc \pmod{cn}$ si y solo si $a \equiv b \pmod{n}$.
5. Si m.c.d.$(c, n) = 1$, $ac \equiv bc \pmod{n}$ si y solo si $a \equiv b \pmod{n}$.
6. Si $a \equiv b \pmod{n_1}$, $a \equiv b \pmod{n_2}$, $\ldots$, $a \equiv b \pmod{n_k}$, entonces $a \equiv b \pmod{\text{m.c.d.}(n_1, n_2, \ldots, n_k)}$.
7. Si $a \equiv b \pmod{n}$ y d es un divisor de n entonces $a \equiv b \pmod{d}$.

8.2. Ecuaciones en congruencias

Nos centramos ahora en el problema de encontrar la solución de una congruencia lineal $ax \equiv b\,(n)$ donde a, b y n son enteros desconocidos y x es un entero desconocido. Este problema puede resolverse de dos formas:

- Como una ecuación diofántica.
- Usando aritmética modular.

Como la primera técnica ya se analiza en la sección 1.5, desarrollamos a continuación la segunda. Para ello necesitamos introducir unos conceptos y resultados nuevos.

Definición 8.3 *Un elemento $\overline{a} \in \mathbb{Z}_n$ se dice* invertible *si existe otro $\overline{x} \in \mathbb{Z}_n$ tal que $\overline{ax} = \overline{1}$, es decir, $ax \equiv 1 \pmod{n}$. En este caso decimos que x es el* inverso de a módulo n.

El conjunto de elementos invertibles se denota por $\mathbb{Z}_n^*$.

Teorema 8.1 *El inverso modular, si existe, es único.*

Demostración. En efecto, sea $\overline{x} \in \mathbb{Z}_n$ tal que $\overline{ax} = \overline{1}$. Si $\overline{y} \in \mathbb{Z}_n$ es otro inverso modular de $\overline{x}$, entonces, por una parte,

$$\overline{xay} = (\overline{xa})\overline{y} = \overline{1}\overline{y} = \overline{y}.$$

Por otra parte

$$\overline{xay} = \overline{x}(\overline{ay}) = \overline{x}\overline{1} = \overline{x}.$$

Por lo tanto, $\overline{x} = \overline{y}$. ∎

Teorema 8.2 *$\overline{a} \in \mathbb{Z}_n^*$ si y solo si m.c.d.$(a, n) = 1$.*

Demostración. Demostramos en primer lugar $\overline{a} \in \mathbb{Z}_n^* \Leftarrow$ m.c.d.$(a, n) = 1$. Para ello aplicamos la identidad de Bézout (véase el teorema 1.5) para deducir que existen $x, y \in \mathbb{Z}$ tales que $ax + ny = 1$. Operando con aritmética modular y teniendo en cuenta que $\overline{n} = \overline{0}$, llegamos a

$$\overline{ax + ny} = \overline{1} \Rightarrow \overline{ax} + \overline{ny} = \overline{1} \Rightarrow \overline{ax} = \overline{1} \Rightarrow \overline{a} \in \mathbb{Z}_n^*.$$

Probamos ahora la otra implicación, $\overline{a} \in \mathbb{Z}_n^* \Rightarrow$ m.c.d.$(a, n) = 1$. Si $\overline{a} \in \mathbb{Z}_n^*$ entonces existe $x \in \mathbb{Z}$ tal que $\overline{ax} = \overline{1}$ o, equivalentemente, $\overline{1 - ax} = \overline{0}$. Por lo tanto, existe $y \in \mathbb{Z}$ tal que $1 - ax = ny$. Reordenando esta igualdad, tenemos $ax + ny = 1$, por lo que se tiene que m.c.d.$(a, n) = 1$, como queríamos demostrar. ∎

Las funciones aritméticas son funciones que se definen sobre los enteros positivos. Entre ellas, una de las más conocidas y empleadas es la *función de Euler*

Definición 8.4 *Dado $n \geq 2$, se define la* función de Euler *de n como el número de enteros positivos menores o iguales que n y coprimos con n, es decir,*

$$\phi(n) = \text{card}\left(\{a \mid 1 \leq a < n,\ \text{m.c.d.}(a, n) = 1\}\right) = |\mathbb{Z}_n^*|.$$

Los siguientes resultados pueden sernos de utilidad en el cálculo de $\phi(n)$.

a) Si $n = p_1^{e_1} p_2^{e_2} \cdots p_r^{e_r}$ con $e_1, \ldots, e_r \geq 1$ entonces:

$$\phi(n) = p_1^{e_1-1}(p_1 - 1) \cdots p_r^{e_r-1}(p_r - 1).$$

b) Si m.c.d.$(m, n) = 1$, $\phi(mn) = \phi(m)\phi(n)$.

c) **Teorema de Euler-Fermat.** Si m.c.d.$(a, n) = 1$, con $a \geq 2$, entonces $a^{\phi(n)} \equiv 1 \pmod{n}$.

d) **Pequeño teorema de Fermat.** Si p es un primo que no divide a a entonces $a^{p-1} \equiv 1 \pmod{p}$.

Veamos algunos ejemplos de cálculo:

1. $\phi(42) = \phi(2 \cdot 3 \cdot 7) = \phi(2)\phi(3)\phi(7) = 1 \cdot 2 \cdot 6 = 12$.
2. $\phi(72) = \phi(2^3 \cdot 3^2) = 2^2 \cdot 1 \cdot 3 \cdot 2 = 24$.

Ejemplo 8.1.- *¿En qué cifra termina 7^{339}?*

Para responder a esta pregunta, basta con calcular el resto de dividir 7^{339} entre 10, es decir calcular $7^{339} \pmod{10}$. Como m.c.d.$(7, 10) = 1$ y $\phi(10) = \phi(2)\phi(5) = 1 \cdot 4 = 4$, se tiene, por el pequeño teorema de Fermat, que $7^4 \equiv 1 \pmod{10}$.

Por otra parte, al dividir 339 entre 4, se tiene $339 = 4 \cdot 84 + 3$. Entonces, operando módulo 10:

$$7^{339} = (7^4)^{84}7^3 \equiv 1^{84}7^3 = 49 \cdot 7 \equiv 9 \cdot 7 = 63 \equiv 3 \pmod{10}.$$

Por lo tanto, 7^{339} acaba en 3. ■

Ejemplo 8.2.- (Regla del 9) *Demuestra que un número natural n es divisible por 9 si la suma de sus cifras lo es.*

Escribimos n de la siguiente forma: $n = d_r 10^r + \cdots + d_1 10 + d_0$. Como $10 \equiv 1 \pmod{9}$, entonces $10^j \equiv 1 \pmod{9}$ para cualquier $j \in \mathbb{N}$. Entonces $n \equiv d_r + \cdots + d_1 + d_0 \pmod{9}$. Por lo tanto, si 9 divide a n, se tiene que $[n] = [0]$, es decir $[d_r + \cdots + d_1 + d_0] = [0]$ y, en consecuencia, 9 divide a la suma de las cifras $d_r + \cdots + d_1 + d_0$. ■

El siguiente ejemplo nos muestra otra técnica para calcular potencias modulares sin usr la función ϕ de Euler.

Ejemplo 8.3.- *Calcula 5^{300} en $\mathbb{Z}_{123}$.*

La técnica consiste en expresar la potencia en binario, en este caso, $300 = (100101100)_2$ o lo que es igual $300 = 2^8 + 2^5 + 2^3 + 2^2$. Entonces

$$5^{300} = 5^{2^8+2^5+2^3+2^2} = 5^{2^8}5^{2^5}5^{2^3}5^{2^2} \pmod{123}.$$

Ahora bien,

$$\begin{aligned}
5^{2} &= 25 \pmod{123} \\
5^{2^2} &= 5^2 5^2 = 125 \cdot 5 \equiv 2 \cdot 5 = 10 \pmod{123} \\
5^{2^3} &= 5^{2^2}5^{2^2} \equiv 10^2 = 100 \pmod{123} \\
5^{2^4} &= 5^{2^3}5^{2^3} \equiv 100^2 \equiv 37 \pmod{123} \\
5^{2^5} &= 5^{2^4}5^{2^4} \equiv 37^2 = 1369 \equiv 16 \pmod{123} \\
5^{2^6} &= 5^{2^5}5^{2^5} \equiv 16^2 = 256 \equiv 10 \pmod{123}.
\end{aligned}$$

Notemos que, en este caso, $5^{2^6} \equiv 10 \equiv 5^{2^2} \pmod{123}$, luego a partir de aquí se van repitiendo las potencias: $5^{2^7} \equiv 5^{2^3} \equiv 100 \pmod{123}$ y $5^{2^8} \equiv 5^{2^4} \equiv 37 \pmod{123}$. Por lo tanto

$$5^{300} = 5^{2^8+2^5+2^3+2^2} = 5^{2^8}5^{2^5}5^{2^3}5^{2^2} \equiv 37 \cdot 16 \cdot 100 \cdot 10 = 370 \cdot 1600 \equiv 1 \cdot 1 = 1 \pmod{123}.$$

■

8.3. Aplicaciones de la aritmética modular

La aritmética modular tiene aplicaciones interesantes en diversos ámbitos de las matemáticas y de la informática, y también en otras disciplinas. Presentamos a continuación algunas de ellas.

Generación de números pseudoaleatorios

Se trata de generar números de una forma que parezca aleatoria, aunque realmente no es así. Es una técnica que se usa para hacer simulaciones.

Para ello, se toma un *módulo* n, un *incremento* c, un *multiplicador* a y una *semilla* x_0. A continuación se genera una sucesión de números $x_1, x_2, \dots$ de forma que x_{i+1} es el resto de dividir $ax_i + c$ entre n.

Por ejemplo, para $a = 9$, $c = 2$, $n = 17$ y $x_0 = 12$ se obtienen los números $12, 8, 6, 5, 13, 0, 2, 3, 12, \dots$, repitiéndose a partir de aquí.

Para $a = 9$, $c = 2$, $n = 101$ y $x_0 = 12$ se obtienen los números 12, 9, 83, 42, 77, 89, 96, 58, 19, 72, 44, 95, 49, 39, 50, 48, 30, 70, 26, 34, 5, 47, 21, 90, 4, 38, 41, 68, 8, 74, 62, 55, 93, 31, 79, 6, 56, 1, 11, 0, 2, 20, 81, 24, 16, 45, 3, 29, 61, 46, 12.... En este caso, hace falta calcular 50 iteraciones para que la lista se vuelva a repetir.

Para $a = 7^5$, $c = 0$, $n = 2^{31} - 1$ y x_0 cualquiera se obtiene una lista que proporciona 2147483647 números pseudoaleatorios antes de repetirse.

Criterio de primalidad de Fermat

Determinar si un número es primo o no es un problema complicado, incluso computacionalmente hablando (refiriéndonos a números del tamaño de 2^{1024}. El *criterio de primalidad de Fermat* establece que si p es un primo que no divide a b entonces $b^{p-1} \equiv 1 \pmod{p}$. Tomamos distintas bases b si para alguna de ellas se tiene que b^{p-1} no es congruente con 1 $\pmod{p}$, entonces p no es primo. La importancia de este método es que a veces se puede concluir que un número no es primo sin tener que factorizarlo.

Por ejemplo, usando este criterio ¿es 35 primo? Tomamos $b = 2$ y calculamos $2^{34} \pmod{35}$:

$$2^{34} = (2^5)^6 2^4 = (32)^6 2^4 \equiv (-3)^6 2^4 = 6^4 3^2 = (6^2)^2 3^2 \equiv 1^2 3^2 = 9 \pmod{35}.$$

No se cumple el criterio de primalidad de Fermat y, por tanto, 35 no es primo.

Teorema chino de los restos

El *teorema chino de los restos* es una herramienta crucial en criptografía, en especial para reducir operaciones con grandes números mediante el paso a congruencias, como por ejemplo en el algoritmo RSA.

En su fromulación más sencilla, el teorema chino de los restos permite encontrar un número entero n que al dividirlo por unos divisores dados, nos proporciona unos restos también determinados previamente. Por ejemplo, nos permite encontrar el menos entero n que al dividirse por 3 da de resto 2, cuando se divide por 5 da de resto 3 y al dividirse por 7 de de resto 2. Por supuesto, la solución es $n = 23$.

Su enunciado es el siguiente:

Teorema 8.3 *Sean $n_1, \dots, n_r \geq 2$ primos entre sí. Sean $a_1, \dots, a_r \in \mathbb{Z}$. Existen soluciones $x \in \mathbb{Z}$ del sistema*

$$\begin{cases} x & \equiv & a_1 \,(n_1) \\ \vdots & \vdots & \vdots \\ x & \equiv & a_r \,(n_r). \end{cases}$$

Además si x_0 es una solución particular, el conjunto de soluciones es

$$\{x_0 + kn_1 \cdots n_r \mid k \in \mathbb{Z}\}.$$

La demostración del teorema nos da una técnica constructiva para calcular la solución particular x_0 que permite definir el conjunto de soluciones.

El teorema chino de los restos también sirve para simplificar expresiones en congruencias.

Ejemplo 8.4.- *Calcula* $23^{40} \pmod{105}$.

Como $105 = 3 \cdot 5 \cdot 7$, calculamos 23^{40} módulo 3, 5 y 7:

$$\begin{aligned} 23^{40} &\equiv 2^{40} \equiv (-1)^{40} = 1 \pmod 3 \\ 23^{40} &\equiv 3^{40} \equiv (9)^{20} = 1 \pmod 5 \\ 23^{40} &\equiv 2^{40} \equiv (2^6)^6 2^4 = (64)^6 2^4 \equiv 16 \equiv 2 \pmod 7. \end{aligned}$$

Buscamos ahora x tal que $x \equiv 1 \pmod 3$, $x \equiv 1 \pmod 5$ y $x \equiv 2 \pmod 7$. Aplicando el teorema chino de los restos tenemos

$$x_0 = 1 \cdot (-35) + 1 \cdot (21) + 2 \cdot (15) = 16.$$

Como 16 es la única solución entre 0 y 105, tenemos que $23^{40} \equiv 16 \pmod{105}$. ■

8.4. Problemas resueltos

1. Encuentra las dos últimas cifras de 2011^{2011} y de 2011^{2012}.

   Solución. Para encontrar las dos últimas cifras de un número, nos interesa trabajar módulo 100. Como $2011^{2011} \pmod{100} \equiv 11^{2011} \pmod{100}$, $11^{\phi(100)} \equiv 1 \pmod{100}$ y $2011 = 50 \times 40 + 11$, se tiene que

   $$11^{2011} \pmod{100} \equiv 11^{11} \pmod{100} = 11^{2^3} 11^2 11 \pmod{100}$$

   $$\equiv 81 \cdot 21 \cdot 11 \pmod{100} \equiv 11 \pmod{100},$$

   las dos últimas cifras de 2011^{2011} son 11.
   Análogamente, las dos últimas cifras de 2011^{2012} son 21 pues

   $$2011^{2012} \pmod{100} \equiv 11^{12} \pmod{100} = 11^{2^3} 11^{2^2} \pmod{100}$$

   $$\equiv 81 \cdot 41 \pmod{100} \equiv 21 \pmod{100}.$$

   ■

2. Encuentra la última cifras de 2012^{2012}.

   Solución. Para encontrar la última cifra de un número, nos interesa trabajar módulo 10. Por lo tanto, $2012^{2012} \pmod{10} \equiv 2^{2012} \pmod{10}$.
   Como m.c.d.$(2, 10) = 2 \neq 1$, no podemos usar el Teorema de Euler-Fermat. De hecho, $2^{\phi(10)} = 2^4 = 16 \equiv 6 \pmod{10}$ y no es cierto $2^{\phi(10)} \equiv 1 \pmod{10}$. Ahora bien, analizando en qué terminan las potencias de 2,

   $$2^1 \equiv 2 \pmod{10}, \quad 2^2 \equiv 4 \pmod{10}, \quad 2^3 \equiv 8 \pmod{10}, \quad 2^4 \equiv 6 \pmod{10},$$

   observamos que, en general, para $k \geq 1$:

   $$2^{4k} \equiv 6 \pmod{10}, \quad 2^{4k+1} \equiv 2 \pmod{10}, \quad 2^{4k+2} \equiv 4 \pmod{10}, \quad 2^{4k+3} \equiv 8 \pmod{10}.$$

   Por lo tanto, como $2012 = 4 \times 503$, tenemos que $2^{2012} \equiv 6 \pmod{10}$.

   ■

3. Prueba por el principio de inducción que $2^{2^n} \equiv 6 \pmod{10}$ para $n \geq 2$.

   Solución. Para probar por el principio de inducción que $2^{2^n} \equiv 6 \pmod{10}$ para $n \geq 2$, se siguen dos pasos:

   a) $n = 2$: $2^4 = 16 \equiv 6 \pmod{10}$.

b) Si es cierto para $n = k$: $2^{2^k} \equiv 6 \pmod{10}$, entonces

$$2^{2^{k+1}} = (2^{2^k})^2 \equiv 6^2 \equiv 6 \pmod{10}.$$

■

4. Prueba por el principio de inducción que $2^{2^n} \equiv 1 \pmod{5}$ para $n \geq 2$.

Solución. Análogamente al ejercicio anterior, para probar por el principio de inducción que $2^{2^n} \equiv 1 \pmod{5}$ para $n \geq 2$, se siguen dos pasos:

a) $n = 2$: $2^4 = 16 \equiv 1 \pmod{5}$.

b) Si es cierto para $n = k$: $2^{2^k} \equiv 1 \pmod{5}$, entonces

$$2^{2^{k+1}} = (2^{2^k})^2 \equiv 1^2 \equiv 1 \pmod{5}.$$

■

5. Sea p un número primo distinto de 2 y 5. Usando aritmética modular, encuentra la última cifra de p^{2012}.

Solución. Como $\text{mcd}(p, 10) = 1$, por el el teorema de Euler-Fermat tenemos que $p^{\phi(10)} \equiv 1 \pmod{10}$, es decir $p^4 \equiv 1 \pmod{10}$, donde ϕ es la función de Euler. Por lo tanto $p^{2012} \equiv (p^4)^{503} \equiv 1 \pmod{10}$. En consecuencia, la última cifra es 1. ■

6. Demuestra que $n^2 + 1$ no es múltiplo de 19 para ningún $n \in \mathbb{N}$.

Solución. Razonamos por reducción al absurdo, suponiendo que 19 divide a $n^2 + 1$ para algún $n \in \mathbb{N}$. Entonces

$$n^2 + 1 \equiv 0 \pmod{19} \Rightarrow n^2 \equiv -1 \pmod{19} \Rightarrow n^2 \equiv 18 \pmod{19}.$$

Calculamos los posibles cuadrados en $\mathbb{Z}_{19}$: $1^2 \equiv 1 \pmod{19}$; $2^2 \equiv 4 \pmod{19}$; $3^2 \equiv 9 \pmod{19}$; $4^2 \equiv 16 \pmod{19}$; $5^2 \equiv 6 \pmod{19}$; $6^2 \equiv 17 \pmod{19}$; $7^2 \equiv 11 \pmod{19}$; $8^2 \equiv 7 \pmod{19}$; $9^2 \equiv 5 \pmod{19}$; $10^2 \equiv 5 \pmod{19}$; $11^2 \equiv 7 \pmod{19}$; $12^2 \equiv 11 \pmod{19}$; $13^2 \equiv 17 \pmod{19}$; $14^2 \equiv 6 \pmod{19}$; $1^2 \equiv 16 \pmod{19}$; $16^2 \equiv 9 \pmod{19}$; $17^2 \equiv 4 \pmod{19}$; $18^2 \equiv 1 \pmod{19}$.

Por lo tanto, ninguno de ellos cumple que $n^2 \equiv 18 \pmod{19}$ y, en consecuencia, $n^2 + 1$ no puede ser múltiplo de 19 para ningún $n \in \mathbb{N}$. ■

8.5. Problemas propuestos

1. Encuentra cinco elementos en cada una de las siguientes clases de equivalencia: $[2] \in \mathbb{Z}_8$, $[3] \in \mathbb{Z}_9$, $[5] \in \mathbb{Z}_{11}$

2. Haz la tabla de sumar y multiplicar en $\mathbb{Z}_6$ y $\mathbb{Z}_7$. Comprueba, en los dos casos, si tienen divisores de cero y elementos inversibles.

3. Resuelve, cuando sea posible, las siguientes ecuaciones:

$$\begin{array}{lll} a)\ 3x \equiv 5 \pmod{13} & b)\ 5x \equiv 1 \pmod{11} & c)\ 4x \equiv 3 \pmod{7} \\ d)\ 3x \equiv 9 \pmod{15} & e)\ 8x \equiv 2 \pmod{10} & f)\ 91x \equiv 84 \pmod{147}. \end{array}$$

4. Sabiendo que $1234567 \equiv 7 \pmod{10}$, $90123 \equiv 3 \pmod{10}$, $2468 \equiv 18 \pmod{25}$ y $13579 \equiv 4 \pmod{25}$, halla el menor entero z no negativo que cumple

   a) $1234567 \times 90123 \equiv z \pmod{10}$

   b) $2468 \times 13579 \equiv z \pmod{25}$.

5. Prueba que si p es primo y $1234567 \equiv 1 \pmod 3$, entonces $p \equiv 1 \pmod 6$.

6. Halla los elementos inversibles en $\mathbb{Z}_5$, $\mathbb{Z}_8$ y $\mathbb{Z}_9$.

7. Encuentra los inversos de $\overline{6} \in \mathbb{Z}_5$, $\overline{6} \in \mathbb{Z}_{17}$, $\overline{3} \in \mathbb{Z}_{10}$ y $\overline{5} \in \mathbb{Z}_{12}$.

8. Halla los restos potenciales de $5 \pmod{12}$, de $12 \pmod 7$ y de $10 \pmod{112}$.

9. Prueba que un número entero es divisible por 11 si la suma de sus cifras que ocupan lugar impar (empezando a contar por la derecha) menos la suma de sus cifras en posición par es un número múltiplo de 11.

10. Halla los restos de dividir 3^{15} entre 17, de 15^{90} entre 13, de 125^{4577} entre 13, 2^{56} entre 10, 2^{56} entre 11 y de 2^{4k} entre 5, para $k \geq 1$.

11. Halla la última cifra 7^{139} y de 9^{1989}.

12. Resuelve la ecuación en congruencias $3x \equiv 3 \pmod{12}$ y expresa las distintas clases de soluciones congruentes en $\mathbb{Z}_{12}$.

13. Encuentra todas las soluciones enteras de la ecuación $261x \equiv 3 \pmod{69}$ y describe las soluciones que no sean congruentes entre sí.

14. Resuelve el sistema de ecuaciones en congruencias

$$\begin{cases} x \equiv 3 & (\text{mód } 19) \\ x \equiv 7 & (\text{mód } 13). \end{cases}$$