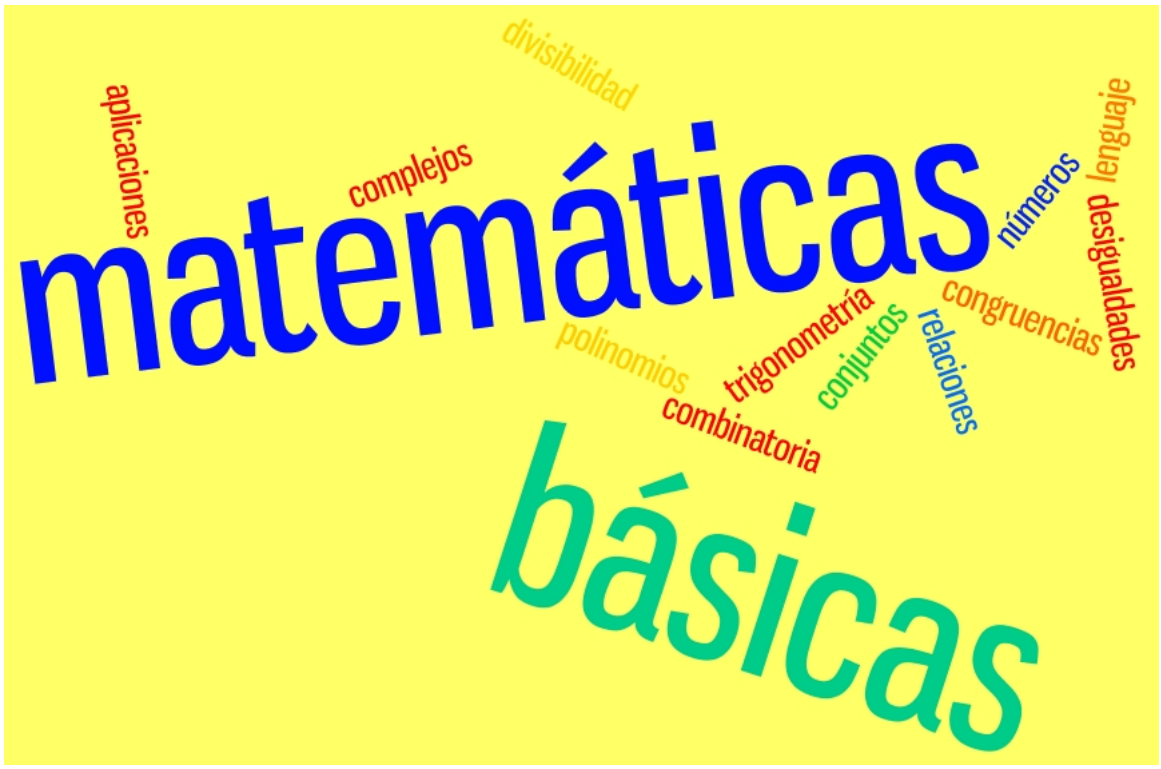
MATEMÁTICAS BÁSICAS

Curso 2010/2011



Prof. Marta Macho Stadler

Marta Macho Stadler
Departamento de Matemáticas
Facultad de Ciencia y Tecnología
Universidad del País Vasco–Euskal Herriko Unibertsitatea
Barrio Sarriena s/n, 48940 Leioa
e-mail: marta.macho@ehu.es
http://www.ehu.es/∼mtwmastm
Tlf: +34 946015352 Fax: +34 946012516

Portada: Contenidos del curso generados con **Wordle**, http://www.wordle.ne/

Índice general

Introducción

Como somos la delgada
disolución de un secreto,
a poco que cede el alma
desborda la fuente de un sueño.

Apenas
Alfonso Reyes (1889–1959)

El objetivo de este curso es aprender a manejar el lenguaje y el formalismo matemáticos a partir de contenidos básicos: teoría de conjuntos, funciones, relaciones binarias, combinatoria, aritmética, polinomios, desigualdades, números complejos, etc.

Esta asignatura se imparte al mismo tiempo que otras más específicas del primer curso del Grado de Matemáticas, y muchas de las técnicas que se van a aprender aquí se van a ir usando día a día en otras materias.

Se trata en nuestro caso de insistir en el método matemático, en los procedimientos de demostración, a través de problemas fundamentales y muy variados, con el objetivo de adquirir destrezas y "perder el miedo" a abordar problemas.

La gran variedad de temas tratados permitirá entender mejor los métodos propios de las matemáticas, y adquirir habilidades ante los problemas que se planteen.

Veremos, en particular, que la estrategia general para abordar la resolución de cualquier problema matemático es la siguiente:

1) analizar casos particulares, como manera de comenzar y entender que dice el problema,

2) buscar patrones, modelos, pautas,

3) simplificar el problema si es posible, para intentar entender cual es cuestión clave,

4) generalizar si puede ayudarnos a percibir mejor de que se trata,

5) dibujar siempre que se pueda: con este sistema no se realizan demostraciones, pero puede ayudarnos a captar la esencia del problema o darnos una clave para abordar su solución,

6) transformar el problema en otro que nos resulte más adecuado, etc.

Lo importante es ser cuidadosos, plantear las cuestiones con rigor e intentar abordar los problemas de diversas maneras... casi nunca se solucionan los ejercicios "a la primera", hay que aprender "a jugar" y esforzarse... os aseguro que vale la pena.

Leioa, septiembre de 2010

Capítulo 1

Lenguaje matemático

Son palabras que todos repetimos sintiendo
como nuestras, y vuelan. Son más que lo mentado.
Son lo más necesario: lo que no tiene nombre.
Son gritos en el cielo, y en la tierra son actos.

La poesía es un arma cargada de futuro
Gabriel Celaya (1911–1991)

1.1. Definiciones, notaciones, teoremas y demostraciones

Se da a continuación un breve repaso de algunos conceptos fundamentales relacionados con el razonamiento matemático.

1.1.1. Símbolos y conectores

En matemáticas, es fundamental la utilización de símbolos y conectores que sirven para modificar o combinar sentencias.

Definición 1.1. Los siguientes símbolos se llaman *cuantificadores*:

1) el *cuantificador universal*: $\forall$ (para todo);

2) el *cuantificador existencial*: $\exists$ (existe). Cuando la existencia es *única*, se suele denotar por $\exists_1$ o $\exists!$.

Definición 1.2. También es esencial el uso de los llamados *conectores*:

1) la *negación*: no;

2) la *conjunción*: $\wedge$ (y);

3) la *disyunción*: $\vee$ (o);

4) la *implicación*: $\Longrightarrow$ (si $-$, entonces);

5) la *doble implicación*: $\Longleftrightarrow$ (si y sólo si, es equivalente a).

Aunque en la práctica no se suelen manejar, una manera sencilla de entender como funcionan estos conectores es construir las denominadas *tablas de verdad*. Si $\mathfrak{P}$ y $\mathfrak{Q}$ son dos sentencias y se denota por **V** ó **F** respectivamente a su validez o falsedad, tenemos las siguientes tablas:

$\mathfrak{P}$	no-$\mathfrak{P}$
V	**F**
F	**V**

$\mathfrak{P}$	$\mathfrak{Q}$	$\mathfrak{P} \wedge \mathfrak{Q}$	$\mathfrak{P} \vee \mathfrak{Q}$	$\mathfrak{P} \Longrightarrow \mathfrak{Q}$	$\mathfrak{P} \Longleftrightarrow \mathfrak{Q}$
V	**V**	**V**	**V**	**V**	**V**
V	**F**	**F**	**V**	**F**	**F**
F	**V**	**F**	**V**	**V**	**F**
F	**F**	**F**	**F**	**V**	**V**

El manejo de los conectores es sencillo, pero es preciso tener cuidado al utilizarlos. Por ejemplo, si $\mathfrak{P}$ y $\mathfrak{Q}$ son propiedades relativas a los elementos de un conjunto X (definición 2.1), para expresar que x cumple $\mathfrak{P}$, se escribirá $\mathfrak{P}(x)$. Y entonces:

Proposición 1.1. *El enunciado $\mathfrak{P}(x) \vee \mathfrak{Q}(x)$, significa una de las tres posibilidades (mutuamente excluyentes) siguientes:*

(i) $\mathfrak{P}(x)$ y $\mathfrak{Q}(x)$;

(ii) $\mathfrak{P}(x)$ y no-$\mathfrak{Q}(x)$;

(iii) no-$\mathfrak{P}(x)$ y $\mathfrak{Q}(x)$.

Proposición 1.2. *Un enunciado se niega de la siguiente manera:*

1) no-$(\forall x \in X, \mathfrak{P}(x))$ es lo mismo que decir que $(\exists x \in X : \text{no-}\mathfrak{P}(x))$;

2) no-$(\exists x \in X : \mathfrak{P}(x))$ equivale a $(\forall x \in X, \text{no-}\mathfrak{P}(x))$;

3) no-$(\forall x \in X, \mathfrak{P}(x) \wedge \mathfrak{Q}(x))$ es lo mismo que $(\exists x \in X : \text{no-}\mathfrak{P}(x)$ o no-$\mathfrak{Q}(x))$;

4) no-$(\exists x \in X : \mathfrak{P}(x) \Longrightarrow \mathfrak{Q}(x))$ es equivalente a $(\forall x \in X, \mathfrak{P}(x) \not\Longrightarrow \mathfrak{Q}(x))$.

Proposición 1.3. *Cuando aparecen varios cuantificadores en un enunciado, es indiferente el orden en el que se escriben, siempre que los cuantificadores involucrados sean del mismo tipo. Si $\mathfrak{P}(x, y)$ es una propiedad relativa a los elementos x e y, entonces:*

1) $(\forall x, \forall y, \mathfrak{P}(x, y))$ *es lo mismo que decir que (*$\forall y$, $\forall x$, $\mathfrak{P}(x, y)$*);*

2) $(\exists x, \exists y : \mathfrak{P}(x, y))$ *es equivalente a* $(\exists y, \exists x : \mathfrak{P}(x, y))$ *.*

Contraejemplo 1.1. Hay que tener cuidado cuando se ven involucrados cuantificadores de distinto tipo. Por ejemplo, el enunciado $(\forall x, \exists y : \mathfrak{P}(x, y))$ no equivale a la expresión $(\exists y : \forall x, \mathfrak{P}(x, y))$. En efecto, si $X = \mathbb{N}$ y $\mathfrak{P}(x, y)$ es la propiedad "$x \leq y$", la primera expresión se lee como que todo número natural posee otro mayor (que es cierta) y la segunda significa que existe un número natural mayor que todos los demás (que es falsa).

Proposición 1.4. *El cuantificador existencial y el conector disyunción se pueden intercambiar en la escritura de un enunciado, así como el cuantificador universal y el conector conjunción:*

1) $(\forall x, \mathfrak{P}(x))$ *y* $(\forall y, \mathfrak{Q}(y))$ *es lo mismo que* $(\forall x, y, \mathfrak{P}(x) \wedge \mathfrak{Q}(y))$*;*

2) $(\exists x : \mathfrak{P}(x))$ *o* $(\exists y : \mathfrak{Q}(y))$ *es equivalente a* $(\exists x, y : \mathfrak{P}(x) \vee \mathfrak{Q}(y))$.

Contraejemplo 1.2. En general, no se pueden intercambiar cuantificadores y conectores en la escritura de un enunciado:

1) la expresión $(\forall x, \mathfrak{P}(x) \vee \mathfrak{Q}(x))$ no equivale a $(\forall x, \mathfrak{P}(x)) \vee (\forall x : \mathfrak{Q}(x))$. En efecto, si $X = \mathbb{N}$, $\mathfrak{P}$ y $\mathfrak{Q}$ son las propiedades de "ser par" y "ser impar" respectivamente, entonces la primera expresión se lee como que un número natural es par o impar (que es verdadera) y la segunda dice que todo número natural es par o todo número natural es impar (que es falsa);

2) la expresión $(\exists x : \mathfrak{P}(x)) \wedge (\exists x : \mathfrak{Q}(x))$ no equivale a $(\exists x : \mathfrak{P}(x) \wedge \mathfrak{Q}(x))$. En efecto, tomando de nuevo el ejemplo de 1), la primera expresión se lee como que existe un número natural par y existe un número natural impar (que es cierta), y la segunda significa que existe un número natural a la vez par e impar (que es falsa).

1.1.2. Los objetos del razonamiento

Definir una teoría matemática es establecer las *reglas del juego* sobre los objetos manipulados, los denominados *axiomas*.

Definición 1.3. Un *axioma* es todo enunciado que:

1) sirve de fundamento para la construcción de una teoría;

2) se admite como cierto y no es por lo tanto objeto de discusión.

Cuando un único axioma no basta para definir una teoría, se pide además:

3) que los diferentes axiomas usados no se contradigan y sean independientes los unos de los otros.

Ejemplos 1.1. Algunos ejemplos de axiomas son los siguientes:

1) primer –de los cinco que son base de la geometría euclídea– *axioma de Euclides*: por dos puntos se puede trazar una recta que los une;

2) *axioma de elección*: dado un conjunto X, existe una *función* (definición 2.8) *de elección*, $f\colon \mathcal{P}(X) - \{\emptyset\} \longrightarrow X$ (definición 2.4), que asigna a todo conjunto A no vacío, un punto distinguido $f(A) = a \in A$;

3) *lema de Zorn*: sea un conjunto parcialmente ordenado $(X, \leq)$ (definición 2.27), tal que todo conjunto bien ordenado (definición 2.29) admite una cota superior (definición 2.30); entonces $(X, \leq)$ posee un elemento maximal (definición 2.28);

4) *axioma de Zermelo*: todo conjunto puede ser bien ordenado.

Observación 1.1. 2), 3) y 4) son formulaciones equivalentes del mismo axioma.

Definición 1.4. Una *definición* es un enunciado que sirve para explicar o introducir una nueva noción.

Una vez conocidos los axiomas y algunas definiciones, *el juego* puede comenzar, puesto que las reglas ya se conocen.

Definición 1.5. Un *teorema* es un enunciado que se deduce:

1) directamente de los axiomas o

2) de los axiomas y los teoremas precedentes, y

con las reglas de deducción que se llaman *demostraciones*, que aseguran su validez.

Definición 1.6. A veces, se da únicamente el nombre de teorema a los verdaderamente importantes, a los que han pasado a la historia con un nombre, o a los que precisan una demostración muy larga, dejando el nombre de *proposición* al resto.

Definición 1.7. Un *lema* es una proposición preliminar a la demostración de un teorema.

Definición 1.8. Un *corolario* es una proposición que se deduce inmediatamente de un teorema, por una demostración si no inmediata, cuando menos corta y fácil.

1.1.3. Condiciones necesarias y suficientes

Definición 1.9. (La implicación) Sean X un conjunto y $\mathfrak{P}$ y $\mathfrak{Q}$ dos propiedades definiendo los conjuntos $A = \{x \in X : \mathfrak{P}(x)\}$ y $B = \{x \in X : \mathfrak{Q}(x)\}$ respectivamente. Si $A \subset B$ (definición 2.2), todo elemento verificando $\mathfrak{P}$, cumple también $\mathfrak{Q}$. En este caso, se dice que $\mathfrak{P}$ *implica* $\mathfrak{Q}$, y se escribe $\mathfrak{P} \Longrightarrow \mathfrak{Q}$. Se dice también que $\mathfrak{P}$ es una *condición suficiente* de $\mathfrak{Q}$ (para obtener $\mathfrak{Q}$ basta con conocer $\mathfrak{P}$) o que $\mathfrak{Q}$ es una *condición necesaria* de $\mathfrak{P}$.

Definición 1.10. (La equivalencia) En las condiciones de la definición 1.9, si $A = B$ (definición 2.2), todo elemento verificando $\mathfrak{P}$ cumple también $\mathfrak{Q}$ y viceversa. En este caso, se dice que $\mathfrak{P}$ *es equivalente* a $\mathfrak{Q}$, y se escribe $\mathfrak{P} \Longleftrightarrow \mathfrak{Q}$. Como $A = B$ es idéntico a $A \subset B$ y $B \subset A$, la equivalencia $\mathfrak{P} \Longleftrightarrow \mathfrak{Q}$ significa las dos implicaciones $\mathfrak{P} \Longrightarrow \mathfrak{Q}$ y $\mathfrak{Q} \Longrightarrow \mathfrak{P}$. Es decir, las dos propiedades equivalentes $\mathfrak{P}$ y $\mathfrak{Q}$ caracterizan el mismo conjunto. Observar que en tal caso $\mathfrak{P}$ es una *condición necesaria y suficiente* de $\mathfrak{Q}$.

1.2. Demostraciones por reducción al absurdo y por inducción

Hay muchos métodos de demostración, de los cuales citamos los más importantes a continuación, usando la notación de la definición 1.9:

(i) Ley de la no contradicción: *no puede ser cierto a la vez* $\mathfrak{P}$ *y no-*$\mathfrak{P}$.

(ii) Ley del tercio excluso: *alguna de las dos sentencias siguientes debe ser cierta* $\mathfrak{P}$ *o no-*$\mathfrak{P}$.

(iii) Método de la hipótesis auxiliar (o implicación directa): *para probar que* $\mathfrak{P} \Longrightarrow \mathfrak{Q}$*, se supone* $\mathfrak{P}$ *cierta y se argumenta hasta llegar a* $\mathfrak{Q}$.

Esta forma de razonamiento, la más directa, es también la más conocida. De manera práctica consiste en demostrar el teorema $\mathfrak{P} \Longrightarrow \mathfrak{Q}$, donde $\mathfrak{P}$ es la *hipótesis* y $\mathfrak{Q}$ la *conclusión o tesis*, suponiendo que se verifica $\mathfrak{P}$ (la hipótesis es cierta) y ayudándose de los axiomas y de los otros teoremas de la teoría demostrados anteriormente.

Ejemplo 1.1. *El cuadrado de un número impar es impar.*

Solución: En efecto, si x es impar, se escribe de la forma $x = 2n - 1$. Entonces $x^2 = 4n^2 - 4n + 1 = 4(n^2 - n) + 1$, que claramente es impar. ∎

(iv) Método "marcha atrás" (o demostración indirecta): *para probar que* $\mathfrak{P} \Longrightarrow \mathfrak{Q}$*, podemos plantear que significa la validez de* $\mathfrak{Q}$.

Ejemplo 1.2. *Si $x > 0$, entonces $x + \frac{1}{x} \geq 2$.*

Solución: Podemos argumentar del siguiente modo:

$$x + \frac{1}{x} \geq 2 \Longleftrightarrow x + \frac{1}{x} - 2 \geq 0 \Longleftrightarrow \frac{x^2 - 2x + 1}{x} \geq 0 \Longleftrightarrow \frac{(x-1)^2}{x} \geq 0,$$

lo que obviamente es cierto al ser $x > 0$. ∎

(v) Disjunción de los casos: *para probar que $\mathfrak{P} \Longrightarrow \mathfrak{Q}$, se descompone $\mathfrak{P}$ en la forma $\mathfrak{P}_1 \vee \cdots \vee \mathfrak{P}_n$, y se prueba que para cada $i \in \{1, \ldots, n\}$, es $\mathfrak{P}_i \Longrightarrow \mathcal{Q}$.*

Es decir, se descompone el conjunto A de los elementos que cumplen $\mathfrak{P}$ en una unión disjunta (definición 2.3) de subconjuntos $A_1, \cdots, A_n$. Entonces, se prueba que para cada $1 \leq i \leq n$ es $A_i \subset B$; y como $A = A_1 \cup \cdots \cup A_n$, se tendrá $A \subset B$.

Ejemplo 1.3. *Si $n \in \mathbb{N}$, entonces $n(n+1)$ es par.*

Solución: Distinguimos dos posibilidades: si n es par, existe $k \in \mathbb{N}$, tal que $n = 2k$, y entonces $n(n+1) = 2k(2k+1)$. Si n es impar, existe $k \in \mathbb{N}$, tal que $n = 2k - 1$, y entonces $n(n+1) = (2k-1)(2k) = 2k(2k-1)$, que es claramente par. ∎

(vi) Método de contraposición: *para probar que $\mathfrak{P} \Longrightarrow \mathfrak{Q}$, se demuestra el contrarrecíproco no-$\mathfrak{Q} \Longrightarrow$ no-$\mathfrak{P}$.*

Es otro método de prueba indirecta. Se basa en el hecho de que la inclusión $A \subset B$ es equivalente a decir que los conjuntos complementarios (definición 2.3) verifican la inclusión $B^c \subset A^c$.

Ejemplo 1.4. *Si $n \in \mathbb{N}$ es tal que n^2 es par, entonces n es par.*

Solución: Si $n \in \mathbb{N}$ es impar, entonces n^2 es impar (ejemplo 1.1). ∎

(vii) Demostración por reducción al absurdo: *para probar un enunciado $\mathfrak{P}$, se supone su negación no-$\mathfrak{P}$, y se busca una contradicción en la teoría en la que se trabaja.*

Como evidentemente se admite que esta teoría no admite contradicciones, la suposición no-$\mathfrak{P}$ será falsa, lo cual es equivalente a decir que $\mathfrak{P}$ es cierta. ¿A qué contradicción se debe llegar? A contradecir un axioma, un teorema anteriormente probado o la propia suposición no-$\mathfrak{P}$.

De modo similar, para probar que $\mathfrak{P} \Longrightarrow \mathfrak{Q}$ razonando por reducción al absurdo, se admite lo contrario, es decir, que no-$(\mathfrak{P} \Longrightarrow \mathfrak{Q})$, o lo que es equivalente, $\mathfrak{P}$ y no-$\mathfrak{Q}$. Y se busca entonces encontrar una contradicción.

Ejemplo 1.5. $\sqrt{2}$ *es irracional.*

Solución: Si $\sqrt{2}$ fuera racional, existirían $p \in \mathbb{Z}$ y $q \in \mathbb{N}$, tales que $\sqrt{2} = \frac{p}{q}$ como fracción irreducible. Entonces, $p^2 = 2q^2$, luego p es par, es decir, $p = 2n$ con $n \in \mathbb{Z}$. Luego, $p^2 = (2n)^2 = 4n^2 = 2q^2$, es decir, $q^2 = 2n^2$, luego q es par, lo que es imposible porque la fracción era irreducible. ∎

(viii) El contraejemplo: para probar que un propiedad matemática $\mathfrak{P}$ es cierta para un conjunto X, hay que probar que todos los elementos de X la verifican. Pero, se sabe que la negación de $(\forall x \in X, \mathfrak{P}(x))$ es $(\exists x \in X, \text{no-}\mathfrak{P}(x))$. Así, para probar que esta fórmula es falsa, basta con encontrar un elemento de X que no verifique $\mathfrak{P}$: esto es lo que se llama *dar un contraejemplo*.

Ejemplo 1.6. *Si* $x \in \mathbb{R}$*, ¿es cierto que si* $x \leq x^2$*, entonces es* $x \geq 1$*?*

Solución: La respuesta es falsa, tomando $x = -2$. ∎

(ix) La demostración por inducción: este tipo de demostración está ligada a la definición del conjunto de los enteros naturales. Es una técnica útil para probar que una propiedad $\mathfrak{P}(n)$ es cierta para todos los enteros naturales n, o para los que son iguales o superiores a un cierto n_0. Sean n_0 un entero natural y $\mathfrak{P}(n)$ una propiedad matemática que depende de un entero n. Para probar que $\mathfrak{P}(n)$ se verifica para cada $n \geq n_0$, basta con probar que:

1) $\mathfrak{P}(n_0)$ es cierta,

2) demostrar, bajo la hipótesis de que $\mathfrak{P}(n)$ se verifica para $k > n_0$, que $\mathfrak{P}(k+1)$ es cierta.

La etapa 1) es una simple verificación y la 2) es, de hecho, el objeto de una demostración.

¿Por qué es válido este sistema de demostración? Si llamamos $S = \{n \in \mathbb{N} : \mathfrak{P}(n)\}$, 1) garantiza que $n_0 \in S$. Queremos ver que $T = \{n \in \mathbb{N} : n \geq n_0\} - S = \emptyset$. Si $T \neq \emptyset$, como T está bien ordenado (ver la definición 2.29), posee un primer elemento, k_0, es decir, $k_0 \in T$ ($k_0 \neq n_0$, ya que $n_0 \in S$) y $k_0 - 1 \notin T$, es decir, $k_0 - 1 \in S$. Por 2), es $(k_0 - 1) + 1 = k_0 \in S$, en contra de lo supuesto.

Ejemplo 1.7. *Para cada* $n \in \mathbb{N}$*,* $1 + \cdots + n = \frac{n(n+1)}{2}$.

Solución: Para $n = 1$, es cierto que $1 = \frac{1(1+1)}{2}$. Si la propiedad se verifica para k, entonces: $1 + 2 + \cdots + k + (k+1)$=$(1 + 2 + \cdots + k)$+$(k+1)$=$\frac{k(k+1)}{2} + (k+1)$= $\frac{(k+2)(k+1)}{2}$. ∎

(x) La demostración por inducción fuerte: en el método de demostración por inducción, para probar que $\mathfrak{P}(k+1)$ se verifica, nos apoyamos sólo sobre la hipótesis de que $\mathfrak{P}(k)$ es cierta. Pero no siempre es posible probar un resultado de este modo. Este nuevo sistema afirma que para probar que $\mathfrak{P}(n)$ se verifica para cada $n \geq n_0$, basta con probar que:

1) $\mathfrak{P}(n_0)$ es cierta,

2) demostrar, bajo la hipótesis de que $\mathfrak{P}(n)$ se verifica para $n \in \{n_0, n_0+1, \ldots, k\}$, que $\mathfrak{P}(k+1)$ es cierta.

Ejemplo 1.8. *Para $n \in \mathbb{N}$, es $a^n - 1 = (a-1)(a^{n-1} + a^{n-2} + \cdots + a^2 + a + 1)$.*

Solución: Para $n = 1$, es cierto. Supongamos que es cierta para $n \in \mathbb{N}, n \leq k$. Se tiene que

$$a^{k+1} - 1 = (a+1)(a^k - 1) - a(a^{k-1} - 1).$$

La hipótesis de inducción dice que

$$a^k - 1 = (a-1)(a^{k-1} + a^{k-2} + \cdots + a^2 + a + 1) \text{ y}$$

$$a^{k-1} - 1 = (a-1)(a^{k-2} + a^{k-3} + \cdots + a^2 + a + 1),$$

y sustituyendo:

$$a^{k+1} - 1 = (a+1)(a^k - 1) - a(a^{k-1} - 1) =$$

$$(a+1)(a-1)(a^{k-1} + a^{k-2} + \cdots + a^2 + a + 1) - a(a-1)(a^{k-2} + a^{k-3} + \cdots + a^2 + a + 1),$$

sacando factor común a $a - 1$, quedaría

$$a^{k+1} - 1 = (a+1)(a^k - 1) - a(a^{k-1} - 1) =$$

$$(a-1)\left((a+1)(a^{k-1} + a^{k-2} + \cdots + a^2 + a + 1) - a(a^{k-2} + a^{k-3} + \cdots + a^2 + a + 1)\right) =$$

$$(a-1)((a^k + a^{k-1} + \cdots + a^2 + a) + (a^{k-1} + a^{k-2} + \cdots + a^2 + a + 1)) -$$

$$(a-1)(a^{k-1} + a^{k-2} + \cdots + a^2 + a) = (a-1)(a^k + a^{k-1} + \cdots + a^2 + a). \quad \blacksquare$$

En este ejemplo se ha usado únicamente que la fórmula es cierta para k y $k-1$. Pero hay ocasiones en las que hace falta utilizar que la propiedad es cierta para todos los valores menores o iguales a k.

1.3. Ejercicios

1.- Con ayuda del lenguaje simbólico, decidir si son correctas las siguientes deducciones:

a) Los gusanos reptan. Todo lo que repta se mancha. Luego, los gusanos están sucios.

b) Si aumenta la temperatura o cae un meteorito, los osos polares morirán de hambre. Se sabe que los osos polares van a sobrevivir, por lo tanto, caerá pronto un meteorito.

c) Ninguna pelota de tenis es de cristal. Ningún objeto de cristal es indestructible. Luego, ninguna pelota de tenis es indestructible.

d) Si se abandona la utilización de gasolina o se incrementa el uso de energía solar, la contaminación disminuirá. Si se abandona el uso de gasolina, el país entrará en crisis. La utilización de la energía solar no aumentará, a no ser que no haya crisis. Por lo tanto, la contaminación no va a disminuir.

e) Los profesores son sádicos. Algunos sádicos usan látigo. Por lo tanto, algunos profesores usan látigo.

f) Los caramelos son dulces. Ningún alimento dulce contiene sal. Luego, los caramelos no contienen sal.

g) Los pájaros silban. Algunos habitantes de Euskadi son pájaros. Luego, algunas criaturas de Euskadi silban.

h) Si no trabajo duro, me dormiré. Si estoy preocupado, no dormiré. Por lo tanto, si estoy preocupado, trabajaré duro.

i) Las nubes son esponjosas. Algunos objetos esponjosos son rosas. Luego, algunas nubes son rosas.

j) Los osos polares tocan el violín. Los violinistas no vuelan. Por lo tanto, los osos polares no vuelan.

k) Las tortugas ven CSI-Las Vegas. Algunas criaturas de Gálapagos son tortugas. Por lo tanto, algunos habitantes de Galápagos ven CSI-Las Vegas.

l) Las polillas salen de noche. Algunos caminantes nocturnos son vampíros. Por lo tanto, las polillas son vampíros.

m) Si Thor se enfada, hay tormentas. Está comenzando una tormenta. Por lo tanto, Thor está enfadado.

n) Si en Marte hubiera grandes cantidades de agua, podría haber vida. No hay grandes extensiones de agua en Marte. Por lo tanto, no hay vida en Marte.

ñ) Los buenos políticos son honestos. Juan es honesto. Juan sería un buen político.

o) Algunas personas no beben café. Los matemáticos son humanos. Por lo tanto, algunos matemáticos no beben café.

p) Ningún elefante sabe tricotar. Yo no sé tricotar. Luego, soy un elefante.

q) Algunos poetas son nerviosos. Hay gente nerviosa que se come las uñas. Luego, algunos poetas se comen las uñas.

r) Como chocolate si estoy deprimido. No estoy deprimido. Por lo tanto, no estoy comiendo chocolate.

s) Como chocolate sólo cuando estoy deprimido. No estoy deprimido. Por lo tanto, no estoy comiendo chocolate.

t) Si hago estos ejercicios, aprenderé lógica. Ya he terminado de hacerlos... ¡Sé lógica!

2.- Traducir las siguientes frases del lenguaje natural en un lenguaje simbólico utilizando una o varias propiedades $\mathfrak{P}$. Negar cada enunciado y traducirlo al lenguaje natural:

a) Los políticos son gordos y feos.

b) Hay un matemático que sabe sumar.

c) Algunas personas de Sevilla tienen paraguas.

d) El Athletic de Bilbao ganará la Liga de fútbol.

e) Nadie en Euskadi habla swahili.

f) Al menos dos faraones egipcios eran ciegos.

g) Como mucho, la mitad de los números: 1, 2, 3, 4, 5, 6, son pares.

h) A veces, llueve en El Sahara.

i) Siempre hace frío en Groenlandia.

j) Ni Alejandro Magno, ni Julio César eran pelirrojos.

k) $x \in A$ o $x \in B$.

l) $x \in A$ y $x \in B$.

m) $x \in A$, pero $x \notin B$.

n) $A \subset B$.

ñ) para cada $i \in I$, es $x \in A_i$.

o) existe $i \in I$, tal que $x \in A_i$.

p) No hay amor feliz.

q) Una puerta está abierta o cerrada.

r) Ser o no ser.

s) Las verdades son fáciles de decir.

t) Prefiero la poesía a la novela histórica.

u) Entre dos números reales cualesquiera siempre hay un racional.

3.- Cuatro compañeros han faltado a la clase de Matemáticas en el Instituto. Delante del Jefe de Estudios y en presencia de su profesor, se defienden del modo siguiente:

- **Pedro**: *No he faltado.*
- **Elena**: *Lo admito, he faltado, pero estaba con Juan.*
- **Juan**: *Yo también he faltado; pero no estaba con Elena, sino con Pedro.*
- **María**: *Yo estaba en clase, pero no he visto a Pedro.*
- **El profesor**: *Estaba concentrado en mis cosas, pero he visto a Pedro en clase.*

¿Puedes ayudar al Jefe de Estudios, sabiendo que sólo tres de estas sentencias son ciertas?

4.- Demostrar las siguientes propiedades usando los métodos de inducción o de inducción fuerte:

i) Para cada $n \in \mathbb{N}$, $1 + 3 + 5 + \cdots + (2n - 1) = n^2$.

ii) Para cada $n \geq 126$, es $n^{100} \leq n!$.

iii) Para cada $n \in \mathbb{N}$, es $1^3 + 2^3 + 3^3 + \cdots + n^3 = \frac{1}{4}n^2(n + 1)^2$. Usar esta fórmula para probar que el cubo de cualquier número natural se puede expresar como diferencia de dos cuadrados de números naturales.

iv) Para cada $n \in \mathbb{N}$, es

$$2 \cdot 6 \cdot 10 \cdot 14 \cdot \cdots \cdot (4n-2) = \frac{(2n)!}{n!}.$$

Deducir que se verifican las dos desigualdades siguientes:

$$2^n (n!)^2 \leq (2n)! \leq 2^{2n} (n!)^2$$

v) Para cada $n \in \mathbb{N}$, el cociente $\frac{(3n)!}{(3!)^n}$ es un número entero.

vi) ¿Para que valores de n se cumple la desigualdad $n! \geq n^3$? Demostrar por inducción la conjetura.

vii) Se llama *sucesión de Fibonacci* a la sucesión $\{a_n\}_{n\in\mathbb{N}}$ definida del modo siguiente: $a_1 = a_2 = 1$ y $a_{n+1} = a_n + a_{n-1}$ para $n \geq 2$. Probar la *fórmula de Binet*

$$a_n = \frac{1}{\sqrt{5}} \left(\left(\frac{1+\sqrt{5}}{2} \right)^n - \left(\frac{1-\sqrt{5}}{2} \right)^n \right).$$

5.- Demostrar por reducción al absurdo las siguientes afirmaciones:

i) Si $n \in \mathbb{N}$ y n^2 es múltiplo de 3, entonces n es múltiplo de 3.

ii) $\sqrt{2} + \sqrt{6} < \sqrt{15}$.

iii) $\sqrt{6} - \sqrt{2} > 1$.

iv) Si $n \in \mathbb{N}$ y n^2 es par, entonces n es par.

v) Si $n = k^3 - k$ para algún $k \in \mathbb{N}$, entonces n es múltiplo de 6.

6.- Se quiere probar que $\mathfrak{P} \Longrightarrow \mathfrak{Q}$. Se sabe que $\mathfrak{Q}$ es falso. ¿Qué hay que probar para $\mathfrak{P}$?

Capítulo 2

Conjuntos, aplicaciones y relaciones

La poesía es un arma cargada de mercurio,
–hay una minoría que la atrapa–.
Los demás que se apañen con la nómina,
con el vídeo, la coca, o la esperanza.

La poesía es un arma cargada de mercurio
Belén Reyes (1964–)

2.1. Operaciones con conjuntos

Definición 2.1. Un *conjunto* es una colección de objetos, llamados *elementos* o *puntos*. Si x es un elemento de X, se denota por $x \in X$. Análogamente, $x \notin X$ denota la "no pertenencia" de x a X. El *conjunto vacío* $\emptyset$ es el conjunto sin elementos.

Son conjuntos importantes los siguientes:

$$\mathbb{N} = \{1, 2, 3, 4, \dots, n, \dots\}, \text{ los naturales o enteros positivos,}$$

$$\mathbb{Z} = \{\pm n : n \in \mathbb{N}\} \cup \{0\}, \text{ los números enteros,}$$

$$\mathbb{Q} = \left\{ \frac{p}{q} : p \in \mathbb{Z}, q \in \mathbb{N} \right\} \text{ los racionales,}$$

los números reales $\mathbb{R}$, los números reales positivos $\mathbb{R}^+$, $\mathbb{R}^* = \mathbb{R} - \{0\}$, los números complejos $\mathbb{C}$, etc.

Se puede definir un conjunto:

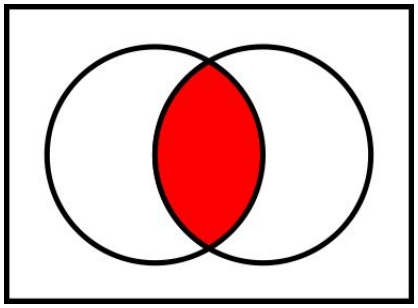
1) por *extensión*, nombrando todos sus elementos: por ejemplo, el conjunto de los números naturales pares es $\{2, 4, 6, 8, \cdots\}$;

2) a través de una *propiedad* $\mathfrak{P}$ válida en un universo $\mathfrak{U}$, que servirá para caracterizarlo $\{x \in \mathfrak{U} : \mathfrak{P}(x)\}$. Por ejemplo, el conjunto de los números naturales pares se puede expresar por $\{x \in \mathbb{N} : x \text{ es múltiplo de } 2\}$.

Definición 2.2. Dados $A, B \subset X$, se dice que A *está contenido* en B, $A \subset B$, si para cada $x \in A$, es $x \in B$. Y A es *igual* a B, $A = B$, si $A \subset B$ y $B \subset A$.

Definición 2.3. Si $A, B \subset X$, se definen:

1) la *intersección* de A y B, por $A \cap B = \{x \in X : x \in A \wedge x \in B\}$. Claramente, $A \cap B \subset A, B$. A y B se dicen *disjuntos* si $A \cap B = \emptyset$;

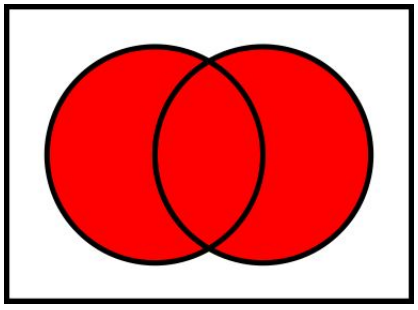


2) la *unión* de A y B, por $A \cup B = \{x \in X : x \in A \vee x \in B\}$. Es decir $x \in A \cup B$, si se verifica una (y sólo una) de las condiciones siguientes:

   (i) $x \in A$ y $x \in B$,

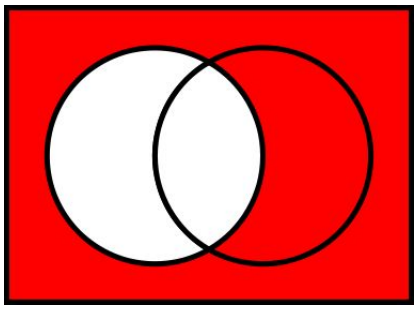
   (ii) $x \in A$ y $x \notin B$,

   (iii) $x \notin A$ y $x \in B$.

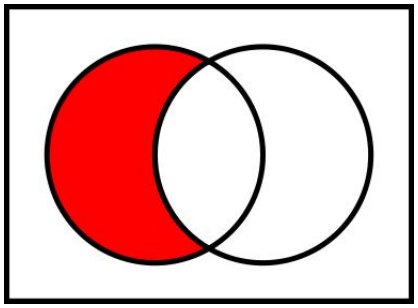


   Claramente, $A, B \subset A \cup B$;

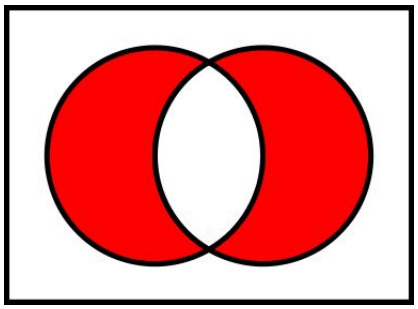
3) el *complementario* de A en X, por $X - A = \{x \in X : x \notin A\}$. Si no hay duda de respecto a que conjunto se está tomando el complementario, se denota por A^c;



4) la *diferencia* de A y B, por $A - B = A \cap B^c = \{x \in X : x \in A \wedge x \notin B\}$;



5) la *diferencia simétrica* de A y B, por $A \triangle B = (A - B) \cup (B - A)$.



Proposición 2.1. *Las anteriores operaciones verifican las siguientes propiedades:*

1) leyes idempotentes: $A \cap A = A = A \cup A$;

2) leyes asociativas: $(A \cup B) \cup C = A \cup (B \cup C)$ *y* $(A \cap B) \cap C = A \cap (B \cap C)$;

3) leyes conmutativas: $A \cup B = B \cup A$ *y* $A \cap B = B \cap A$;

4) leyes distributivas: $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$ *y* $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$;

5) identidades: $A \cap X = A = A \cup \emptyset$, $A \cup X = X$ *y* $A \cap \emptyset = \emptyset$;

6) propiedades del complementario: $A \cup A^c = X$, $A \cap A^c = \emptyset$, $(A^c)^c = A$ *y* $X^c = \emptyset$;

7) leyes de De Morgan: $(A \cup B)^c = A^c \cap B^c$ *y* $(A \cap B)^c = A^c \cup B^c$.

Definición 2.4. Se llama *partes de* X o *conjunto potencia de* X al conjunto de todos los subconjuntos de X, y se denota por $\mathcal{P}(X)$ o 2^X. Es decir, $A \subset X$ si y sólo si $A \in \mathcal{P}(X)$.

Definición 2.5. $A \times B = \{(a, b) : a \in A \wedge b \in B\}$ es el *producto cartesiano* de A por B. Sus elementos son *pares ordenados*.

Claramente, $A \times B \neq B \times A$. Y $A \times B = \emptyset$, si y sólo si $A = \emptyset$ ó $B = \emptyset$. Dos pares ordenados $(a_1, b_1), (a_2, b_2) \in A \times B$, son iguales $(a_1, b_1) = (a_2, b_2)$ si y sólo si $a_1 = a_2$ y $b_1 = b_2$. Luego, $(a_1, b_1) \neq (a_2, b_2)$ si y sólo si $a_1 \neq a_2$ o $b_1 \neq b_2$.

En general, dada una familia finita de conjuntos $\{A_1, \cdots, A_n\}$, se define su producto cartesiano por $\prod_{i=1}^{n} A_i = A_1 \times \cdots \times A_n = \{(a_1, \cdots, a_n) : a_i \in A_i, i \in \{1, \cdots, n\}\}$. Si $A_i = A$ para cada $i \in \{1, \cdots, n\}$, el producto cartesiano se denota por A^n.

Proposición 2.2. *El producto cartesiano verifica las siguientes propiedades:*

1) $A \times (B \cap C) = (A \times B) \cap (A \times C)$;

2) $A \times (B \cup C) = (A \times B) \cup (A \times C)$;

3) si $C \neq \emptyset$ *y* $A \times C = B \times C$, *entonces* $A = B$;

4) $A \times (B - C) = (A \times B) - (A \times C)$;

5) $(A \times B) \cap (C \times D) = (A \cap C) \times (B \cap D)$;

6) $(A \times B)^c = (A^c \times B^c) \cup (A^c \times B) \cup (A \times B^c)$;

7) si $B \subset C$, *entonces* $A \times B \subset A \times C$;

8) $(A \times B) \cap (C \times D) = (A \times D) \cap (C \times B)$;

9) si A, B, C *y* D *son conjuntos no vacíos, entonces* $A \times B \subset C \times D$ *si y sólo si* $A \subset C$ *y* $B \subset D$.

Definición 2.6. Sea $I \neq \emptyset$ un *conjunto de índices*. Se considera una familia de conjuntos $\{A_i : i \in I\}$, y se dice que esta familia está *indicada* por I. Los conjuntos A_i no tienen porque ser diferentes.

Definición 2.7. Dada una familia indicada $\{A_i : i \in I\}$, con $A_i \subset X$, se define:

1) la *intersección generalizada* $\bigcap_{i\in I} A_i = \{x \in X : \forall i \in I, x \in A_i\}$, y

2) la *unión generalizada* $\bigcup_{i\in I} A_i = \{x \in X : \exists i \in I \text{ tal que } x \in A_i\}$.

Si el conjunto de índices I es finito, estas definiciones coinciden con las dadas en la definición 2.3. Se cumplen también en este caso las propiedades distributivas, las leyes de De Morgan $\left(\bigcap_{i\in I} A_i\right)^c = \bigcup_{i\in I} A_i^c$ y $\left(\bigcup_{i\in I} A_i\right)^c = \bigcap_{i\in I} A_i^c$, etc.

2.2. Aplicaciones

Definición 2.8. Dados dos conjuntos X e Y, una *aplicación* o *función* $f\colon X \longrightarrow Y$, es una correspondencia que asocia a cada $x \in X$, un elemento y sólo uno de Y, que se denota por $f(x)$.

Ejemplos 2.1. Algunos ejemplos de aplicaciones son:

1) la *aplicación identidad*, $1_X\colon X \longrightarrow X$, definida por $1_X(x) = x$;

2) la *aplicación inclusión*: si $A \subset X$, $i_A\colon A \longrightarrow X$, se define por $i_A(x) = x$;

3) la *aplicación constante*, $c_{y_0}\colon X \longrightarrow Y$, definida por $c_{y_0}(x) = y_0$, donde y_0 es un punto fijo de Y;

4) la *i-ésima proyección coordenada*, $p_i\colon A_1 \times \cdots \times A_n \longrightarrow A_i$, definida por la igualdad $p_i((a_1, \cdots, a_n)) = a_i$;

5) la *inyección diagonal*, $d\colon X \longrightarrow X^n$, definida por $d(x) = (x, \cdots, x)$;

6) la *función característica de un conjunto*: si $A \subset X$, $\chi_A\colon X \longrightarrow \{0, 1\}$, definida por

$$\chi_A(x) = \begin{cases} 0 & \text{si} \quad x \notin A \\ 1 & \text{si} \quad x \in A \end{cases}$$

7) dada $f\colon X \longrightarrow Y$ y $A \subset X$, la *restricción* de f a A, $f|_A\colon A \longrightarrow Y$, está definida por $f|_A(a) = f(a)$;

8) si $g\colon A \longrightarrow Y$ y $A \subset X$, entonces $f\colon X \longrightarrow Y$ es una *extensión* de g a X, si $f|_A = g$. Observar que una aplicación puede tener varias extensiones;

9) si $f\colon A \longrightarrow Y$ y $g\colon B \longrightarrow Y$ son dos aplicaciones, donde $A \cup B = X$ y $f(x) = g(x)$, para cada $x \in A \cap B$, se puede definir la *combinada* de f y g, como la aplicación $h\colon X \longrightarrow Y$ definida por

$$h(x) = \begin{cases} f(x) & \text{si} \quad x \in A \\ g(x) & \text{si} \quad x \in B \end{cases}$$

10) si $f\colon X \longrightarrow Y$ y $g\colon Z \longrightarrow W$ son dos aplicaciones, su *producto cartesiano* se define por $f \times g\colon X \times Z \longrightarrow Y \times W$, donde $(f \times g)(x, z) = (f(x), g(z))$.

Definición 2.9. Dada una aplicación $f\colon X \longrightarrow Y$, X se llama el *dominio* de f e Y es su *codominio*. El *grafo* de f es el conjunto $G_f = \{(x, f(x)) : x \in X\} \subset X \times Y$, que en muchas ocasiones se identifica con f.

Definición 2.10. Dos aplicaciones $f\colon X \longrightarrow Y$ y $g\colon Z \longrightarrow W$ son *iguales*, cuando coinciden sus dominios ($X = Z$), sus codominios ($Y = W$) y $f(x) = g(x)$, para cada $x \in X$. Por ejemplo, si $f\colon X \longrightarrow Y$ es una aplicación y $A \subset X$, f y $f|_A$ no son iguales.

Definición 2.11. Dada $f\colon X \longrightarrow Y$, $f(A) = \{y \in Y : \exists a \in A \text{ tal que } f(a) = y\}$ es la *imagen directa* de A. $f(X)$ se llama *rango* de la aplicación.

Definición 2.12. Si $B \subset Y$, $f^{-1}(B) = \{x \in X : f(x) \in B\}$ es su *imagen recíproca*.

Proposición 2.3. *Dada $f\colon X \longrightarrow Y$, se verifica:*

1) $f(\emptyset) = \emptyset$, $f(X) \subset Y$ y si $A \neq \emptyset$, entonces $f(A) \neq \emptyset$;

2) si $A_1, A_2 \subset X$, y $A_1 \subset A_2$, entonces $f(A_1) \subset f(A_2)$;

3) Si $A_i \subset X$ para $i \in I$, $f\left(\bigcup_{i\in I} A_i\right) = \bigcup_{i\in I} f(A_i)$ y $f\left(\bigcap_{i\in I} A_i\right) \subset \bigcap_{i\in I} f(A_i)$;

4) si $A_1, A_2 \subset X$, $f(A_1) - f(A_2) \subset f(A_1 - A_2)$ y en particular $f(X) - f(A_2) \subset f(X - A_2)$. Entre $Y - f(A_2)$ y $f(X - A_2)$ no hay en general ninguna relación;

5) $f^{-1}(\emptyset) = \emptyset$, y puede existir $\emptyset \neq B \subset Y$, tal que $f^{-1}(B) = \emptyset$;

6) $f^{-1}(Y) = X$;

7) si $B_1, B_2 \subset Y$ y $B_1 \subset B_2$, entonces $f^{-1}(B_1) \subset f^{-1}(B_2)$;

8) si $B_i \subset Y$ para $i \in I$, $f^{-1}\left(\bigcap_{i\in I} B_i\right) = \bigcap_{i\in I} f^{-1}(B_i)$ y $f^{-1}\left(\bigcup_{i\in I} B_i\right) = \bigcup_{i\in I} f^{-1}(B_i)$;

9) Si $B_1, B_2 \subset Y$, $f^{-1}(B_1 - B_2) = f^{-1}(B_1) - f^{-1}(B_2)$, *y en particular,* $f^{-1}(Y - B_2) = X - f^{-1}(B_2)$;

10) si $A \subset X$, $A \subset f^{-1}(f(A))$;

11) si $B \subset Y$, $f(f^{-1}(B)) = f(X) \cap B \subset B$;

12) si $A \subset X$ *y* $B \subset Y$, $f(A \cap f^{-1}(B)) = f(A) \cap B$.

Definición 2.13. Dadas $f\colon X \longrightarrow Y$ y $g\colon Y \longrightarrow Z$, se define la *composición* de g y f, por $g \circ f\colon X \longrightarrow Z$, donde $(g \circ f)(x) = g(f(x))$, para cada $x \in X$.

Proposición 2.4. *Sean* $f\colon X \longrightarrow Y$, $g\colon Y \longrightarrow Z$ *y* $h\colon Z \longrightarrow W$ *aplicaciones, entonces:*

1) la composición de funciones es asociativa: $h \circ (g \circ f) = (h \circ g) \circ f$;

2) $f \circ 1_X = f$ *y* $1_Y \circ g = g$;

3) si $C \subset Z$, *es* $(g \circ f)^{-1}(C) = f^{-1}(g^{-1}(C))$;

4) si $f\colon X \longrightarrow Y$ *y* $g\colon Y \longrightarrow X$, *en general,* $f \circ g \neq g \circ f$.

Definición 2.14. Se dice que $f\colon X \longrightarrow Y$ es *sobreyectiva*, si $f(X) = Y$, es decir, para cada $y \in Y$, existe $x \in X$, tal que $f(x) = y$. Y es *inyectiva*, si dados $x_1 \neq x_2$ en X, es $f(x_1) \neq f(x_2)$ (o equivalentemente, si $f(x_1) = f(x_2)$, entonces $x_1 = x_2$).

Proposición 2.5. *Sea* $f\colon X \longrightarrow Y$, *entonces:*

1) $B = f(f^{-1}(B))$ *para cada* $B \subset Y$, *si y sólo si* f *es sobreyectiva;*

2) $Y - f(A) \subset f(X - A)$ *para cada* $A \subset X$ *si y sólo si* f *es sobreyectiva;*

3) si $g, h\colon Y \longrightarrow Z$ *y* f *es sobreyectiva, entonces* $g \circ f = h \circ f$ *implica que* $h = g$;

4) si $g\colon Y \longrightarrow X$ *y* $f \circ g = 1_Y$, *entonces* f *es sobreyectiva;*

5) $A = f^{-1}(f(A))$ *para cada* $A \subset X$, *si y sólo si* f *es inyectiva;*

6) $f\left(\bigcap_{i \in I} A_i\right) = \bigcap_{i \in I} f(A_i)$ *para cada familia indicada de conjuntos* $\{A_i \subset X\}_{i \in I}$ *si y sólo si* f *es inyectiva;*

7) si f *es sobreyectiva, entonces para cada* $A \subset X$ *es* $Y - f(A) = f(X - A)$ *si y sólo si* f *es inyectiva;*

8) si $g, h\colon Z \longrightarrow X$ *y* f *es inyectiva, entonces* $f \circ g = f \circ h$ *implica que* $h = g$;

9) si $g\colon Y \longrightarrow X$ *y* $g \circ f = 1_X$*, entonces* f *es inyectiva.*

Definición 2.15. $f\colon X \longrightarrow Y$ es *biyectiva* si es sobreyectiva e inyectiva a la vez. En tal caso, la correspondencia definida por $f^{-1}\colon Y \longrightarrow X$, donde $f^{-1}(y) = x$ si y sólo si $f(x) = y$, es una función.

Proposición 2.6. *Sea* $f\colon X \longrightarrow Y$*, entonces:*

1) si f *es biyectiva, entonces* f^{-1} *también lo es;*

2) si f *es biyectiva, entonces* $f^{-1} \circ f = 1_X$*,* $f \circ f^{-1} = 1_Y$ *y* $(f^{-1})^{-1} = f$*;*

3) si $g\colon Y \longrightarrow X$ *y* $g \circ f = 1_X$ *y* $f \circ g = 1_Y$*, entonces* f *es biyectiva y* $g = f^{-1}$*;*

4) si $f\colon X \longrightarrow Y$ *y* $g\colon Y \longrightarrow Z$ *son biyectivas, entonces* $g \circ f$ *lo es y además* $(g \circ f)^{-1} = f^{-1} \circ g^{-1}$.

2.3. Conjuntos numerables y no numerables

Definición 2.16. Dos conjuntos se llaman *equipotentes*, si existe una aplicación biyectiva entre ellos.

Definición 2.17. X se dice *finito* si existe $n \in \mathbb{N}$, tal que X es equipotente a $\{1, \cdots, n\}$. X es *infinito*, si no es finito, lo cual equivale a decir que es equipotente a un subconjunto propio de sí mismo. X es *numerable* si es equipotente a $\mathbb{N}$ y es *contable* si es finito o numerable.

Observación 2.1. Dos conjuntos finitos son equipotentes si y sólo si poseen el mismo número de elementos. No sucede lo mismo si X es infinito: $\mathbb{N}$ es equipotente al conjunto $\mathbb{P}$ de los números pares, y sin embargo $\mathbb{P} \subset \mathbb{N}$ y no son iguales.

Lema 2.7. *La relación de equipotencia es una relación de equivalencia (definición 2.22).*

Definición 2.18. A cada clase de equipotencia se le puede asignar un *número cardinal*, que es un objeto matemático ω tal que existe un conjunto X con $Card(X) = \omega$.

Definición 2.19. Un conjunto A es *de potencia menor o igual* que B, si existe una aplicación $f\colon A \longrightarrow B$ inyectiva, con lo cual $Card(A) \leq Card(B)$ (equivalentemente, si existe una aplicación $f\colon B \longrightarrow A$ sobreyectiva).

Definición 2.20. Dados dos números cardinales ω_1 y ω_2, se dice que $\omega_1 \leq \omega_2$, si existen conjuntos X e Y con $Card(X) = \omega_1$ y $Card(Y) = \omega_2$ y tales que la potencia de X es menor o igual a la potencia de Y. Se trata de una relación de orden. Si $\omega_1 \leq \omega_2$ y $\omega_1 \neq \omega_2$, se dice que ω_1 es estrictamente menor que ω_2.

Proposición 2.8. *Se verifican las siguientes propiedades:*

1) si X es contable y $A \subset X$, entonces A es contable;

2) si X no es contable y $X \subset Y$, entonces Y no es contable;

3) si X es infinito, existe $A \subset X$, numerable y propio.

Demostración: 1) Si X es finito y $A \subset X$, A es finito, luego contable. Si X es numerable, existe una biyección $f\colon \mathbb{N} \longrightarrow X$, es decir, se puede expresar $X = \{x_1, x_2, \ldots, x_n, \ldots\}$. Sea $A \subset X$. Si $A = \emptyset$, es contable. Si $A \neq \emptyset$, sea x_{n_1} el primer elemento de X tal que $x_{n_1} \in A$. Sea $A_1 = A - \{x_{n_1}\}$. Si $A_1 = \emptyset$, A es finito, luego contable. Si $A_1 \neq \emptyset$ sea x_{n_2} el primer elemento de X tal que $x_{n_2} \in A_1$ (observar que $n_2 > n_1$). Sea $A_2 = A_1 - \{x_{n_2}\} = A - \{x_{n_1}, x_{n_2}\}$. Si $A_2 = \emptyset$, A es finito, luego contable. Continuando de este modo, se construye $A_k = A - \{x_{n_1}, x_{n_2}, \ldots, x_{n_k}\}$ que o bien es vacío (en cuyo caso A es finito, luego contable) o existe $x_{n_{k+1}}$ el primer elemento de X tal que $x_{n_{k+1}} \in A_k$. Prosiguiendo de este modo –a no ser que en algún paso el conjunto en cuestión sea vacío– se comprueba fácilmente que $A = \{x_{n_1}, x_{n_2}, \ldots, x_{n_k} \ldots\}$.

2) Basta con aplicar 1).

3) Como X es infinito, elegimos $x_0 \neq x_1$ en X. Como $X_1 = X - \{x_0, x_1\} \neq \emptyset$, existe $x_2 \in X_1$, que es distinto de x_0 y x_1. Continuando de este modo, como $X_n = X - \{x_0, x_1, \ldots, x_n\} \neq \emptyset$, existe $x_{n+1} \in X_n$. Así, se construye el conjunto numerable $A = \{x_n : n \in \mathbb{N}\}$, que es distinto de X porque $x_0 \notin A$. ∎

Teorema 2.9. $\mathbb{N} \times \mathbb{N}$ *es numerable.*

Demostración: Se define la siguiente relación binaria sobre $\mathbb{N}\times\mathbb{N}$: dados $(m_1, n_1), (m_2, n_2) \in \mathbb{N} \times \mathbb{N}$, $(m_1, n_1) \prec (m_2, n_2)$ si:

1) $m_1 + n_1 < m_2 + n_2$, o

2) $m_1 + n_1 = m_2 + n_2$ y $m_1 < m_2$.

$\preceq$ es un orden total (definición 2.27) sobre $\mathbb{N}\times\mathbb{N}$, gracias al cual se ordenan los elementos de $\mathbb{N} \times \mathbb{N}$ en una lista. La aplicación $f\colon \mathbb{N} \times \mathbb{N} \longrightarrow \mathbb{N}$ dada por

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

asigna a cada elemento $(m, n) \in \mathbb{N} \times \mathbb{N}$ el lugar que ocupa en esta lista, y es por lo tanto una biyección. ∎

Corolario 2.10. *Del teorema 2.9 se deduce:*

1) el producto cartesiano de una familia finita de conjuntos contables, es contable;

2) la unión de una familia contable de conjuntos contables es contable;

3) $\mathbb{Z}$ y $\mathbb{Q}$ son numerables.

Demostración: 2) Si $\{A_i : i \in I\}$ fuera una familia numerable de conjuntos dos a dos disjuntos y numerables, tendríamos biyecciones $\Phi\colon \mathbb{N} \longrightarrow \mathbb{I}$ y $f_i\colon \mathbb{N} \longrightarrow A_i$. La función $f\colon \mathbb{N} \times \mathbb{N} \longrightarrow \bigcup_{i\in I} A_i$ definida por $f(m,n) = f_{\Phi(m)}(n)$ es biyectiva. Este es el caso más desfavorable (donde se obtiene una unión mayor).

3) $\mathbb{Z} = \mathbb{N} \cup \{0\} \cup -\mathbb{N}$, donde $-\mathbb{N} = \{-n : n \in \mathbb{N}\}$. Además, $\mathbb{Q}$ se puede escribir como la unión numerable $\mathbb{Q} = \bigcup_{n\in\mathbb{N}} A_n$, donde $A_n = \{\frac{m}{n} : m \in \mathbb{Z}\}$, que es obviamente equipotente a $\mathbb{Z}$. ∎

Contraejemplo 2.1. $\mathbb{R}$ no es numerable.

Demostración: Basta con demostrar que $[0,1]$ no es numerable. Si lo fuera, se escribiría $[0,1] = \{x_n\}_{n\in\mathbb{N}}$. Se construye una sucesión de intervalos encajados del modo siguiente: x_1 no puede pertenecer a los tres intervalos $\left[0, \frac{1}{3}\right]$, $\left[\frac{1}{3}, \frac{2}{3}\right]$ y $\left[\frac{2}{3}, 1\right]$. Sea $I_1 = [a_1, b_1]$ uno de estos tres intervalos, tal que $x_1 \notin I_1$. Se divide I_1 en tres intervalos de amplitud $\frac{1}{9}$: $\left[a_1, a_1 + \frac{1}{3}\right]$, $\left[a_1 + \frac{1}{3}, a_1 + \frac{2}{3}\right]$ y $\left[a_1 + \frac{1}{3}, b_1\right]$. De nuevo, existe uno de ellos $I_2 \subset I_1$, tal que $x_2 \notin I_2$. Se continúa de manera inductiva, obteniendo una sucesión de intervalos encajados $\{I_n\}_{n\in\mathbb{N}}$, cada I_n de longitud $\frac{1}{3^n}$ y tal que $x_n \notin I_n$. Por la propiedad de los intervalos de encaje (corolario 2.21), existe $p \in \bigcap_{n\in\mathbb{N}} I_n \subset [0,1]$, lo que es imposible. ∎

Observación 2.2. Se puede dar otra prueba de esta propiedad, utilizando el denominado *argumento diagonal de Cantor*: suponemos de nuevo que $[0,1] = \{x_n\}_{n\in\mathbb{N}}$, y escribimos cada uno de estos números en su forma decimal

$$x_1 = 0, a_1^1 a_1^2 a_1^3 \ldots a_1^n \ldots$$

$$x_2 = 0, a_2^1 a_2^2 a_2^3 \ldots a_2^n \ldots$$

$$x_3 = 0, a_3^1 a_3^2 a_3^3 \ldots a_3^n \ldots$$

$$\ldots$$

$$x_n = 0, a_n^1 a_n^2 a_n^3 \ldots a_n^n \ldots$$

$$\ldots$$

El número $x = 0, \alpha_1\alpha_2\alpha_3 \ldots \alpha_n \ldots$, definido por $\alpha_k = a_k^k + 1$, es claramente un número real, pero $x \neq x_k$ para cada $k \in \mathbb{N}$, pues el k-ésimo dígito de x_k es a_k^k y el k-ésimo dígito de x es $a_k^k + 1$. ∎

El $Card(\emptyset) = 0$, es el cardinal mínimo. Sin embargo no existe un cardinal máximo, ya que:

Teorema 2.11. ***(de Cantor)*** *Para cada conjunto X, $Card(X) < Card(\mathcal{P}(X))$.*

Demostración: Si $X = \emptyset$, $Card(\mathcal{P}(X)) = 1$, pues $\mathcal{P}(X) = \{\emptyset\}$. Si $X \neq \emptyset$, es obvio que $Card(X) \leq Card(\mathcal{P}(X))$, porque la aplicación $h\colon X \longrightarrow \mathcal{P}(X)$ definida por $h(x) = \{x\}$ es inyectiva. Supongamos que $Card(X) = Card(\mathcal{P}(X))$, es decir, existe una aplicación $f\colon X \longrightarrow \mathcal{P}(X)$ biyectiva. Sea $A = \{x \in X : x \notin f(x)\} \in \mathcal{P}(X)$. Como f es sobreyectiva, existe $x_0 \in X$ tal que $f(x_0) = A$. Si $x_0 \in A$, esto significaría que $x_0 \notin f(x_0) = A$, lo cual es imposible. Luego, es $x_0 \notin A$, lo cual significa que $x_0 \in f(x_0) = A$, imposible de nuevo. ∎

En particular, $Card(\mathbb{N}) = \aleph_0 < Card(\mathcal{P}(\mathbb{N})) = 2^{\aleph_0}$ (notación que proviene del hecho de que si A es un conjunto con n elementos, entonces $\mathcal{P}(A)$ tiene 2^n elementos). Puede probarse que $2^{\aleph_0} = Card(\mathbb{R}) = c$, que se llama el *cardinal del continuo*. De aquí se concluye que $\aleph_0 < c$.

Desde principios de siglo, se ha intentado en vano establecer si existe un número cardinal $\aleph_1$, entre $\aleph_0$ y c. Georg Cantor (1845-1918) hace la siguiente conjetura:

Teorema 2.12. ***(Hipótesis del continuo)*** *$c = \aleph_1$, es decir, no existe ningún conjunto A, tal que $\aleph_0 < Card(A) < c$.*

Paul Joseph Cohen (1934-2007) establece en 1963 que la hipótesis del continuo es indecidible: añadiendo como axioma su veracidad o su falsedad, los fundamentos de la Matemática siguen siendo coherentes.

2.4. Relaciones de equivalencia y orden

Definición 2.21. Dado un conjunto X, una *relación binaria* es $\mathfrak{R} \subset X \times X$. $\mathfrak{R}$ se llama:

1) *reflexiva*, si para cada $x \in X$, es $(x, x) \in \mathfrak{R}$;

2) *simétrica*, si dado $(x, y) \in \mathfrak{R}$, entonces $(y, x) \in \mathfrak{R}$;

3) *antisimétrica*, si $(x, y) \in \mathfrak{R}$ e $(y, x) \in \mathfrak{R}$ implica que $x = y$;

4) *transitiva*, si dados $(x, y), (y, z) \in \mathfrak{R}$, entonces $(x, z) \in \mathfrak{R}$.

2.4.1. Relaciones de equivalencia

Definición 2.22. Una relación de *equivalencia* sobre X es una relación binaria reflexiva, simétrica y transitiva. Se suele denotar por $x\mathfrak{R}y$ en vez de $(x, y) \in \mathfrak{R}$.

Definición 2.23. Dada $\mathfrak{R}$ una relación de equivalencia, se llama *clase de* x al conjunto $[x] = \{y \in X : x\mathfrak{R}y\}$. El *conjunto cociente* $X/\mathfrak{R}$, es el conjunto de todas las clases de equivalencia.

Proposición 2.13. *Algunas propiedades de las clases de equivalencia son:*

1) $x \in [x]$ *(*x *se llama representante de su clase), luego* $[x] \neq \emptyset$*;*

2) $x\mathfrak{R}y$ *si y sólo si* $[x] = [y]$*;*

3) $[x] \neq [y]$ *si y sólo si* $[x] \cap [y] = \emptyset$*.*

Definición 2.24. Una *partición* de X es una familia $\mathcal{P} = \{P_i : i \in I\}$ de subconjuntos no vacíos de X, tales que:

(i) $X = \bigcup_{i \in I} P_i$, y

(ii) si $P_i \neq P_j$, entonces $P_i \cap P_j = \emptyset$.

Lema 2.14. *Dar una partición de* X *equivale a dar una relación de equivalencia sobre él.*

Definición 2.25. Existe una aplicación canónica, $p\colon X \longrightarrow X/\mathfrak{R}$, que asigna a cada elemento x su clase de equivalencia $p(x) = [x]$. Se llama *aplicación cociente* y es sobreyectiva. Una vez dada la aplicación cociente, el conjunto de los elementos de X relacionados con x es precisamente $p^{-1}(p(x))$.

Definición 2.26. Con las notaciones de la definición 2.25, si $f\colon X \longrightarrow Y$ es una aplicación, se dice que f *factoriza a través de* $X/\mathfrak{R}$ si existe una aplicación $g\colon X/\mathfrak{R} \longrightarrow Y$ tal que $f = g \circ p$.

Proposición 2.15. $f\colon X \longrightarrow Y$ *factoriza a través de* $X/\mathfrak{R}$ *si y sólo si* f *es compatible con la relación de equivalencia.*

2.4.2. Relaciones de orden

Definición 2.27. Una relación de *orden parcial* sobre X es una relación binaria reflexiva, antisimétrica y transitiva. Se dice también que X está *parcialmente ordenado*. Se suele denotar por $x \leq y$ y se habla del par $(X, \leq)$. El orden se llama *total*, si dos elementos cualesquiera de X son comparables por esta relación.

Si $(X, \leq)$ es un conjunto parcialmente ordenado, se dice que $x < y$ si $x \leq y$ y $x \neq y$.

Ejemplo 2.1. Sobre $\mathbb{R}$, el orden usual es un orden total.

Ejemplo 2.2. Si $(A, \leq_A)$ y $(B, \leq_B)$ son conjuntos parcialmente ordenados, se define el *orden lexicográfico* $\leq_{lex}$ sobre $A \times B$ por: dados $(a_1, b_1), (a_2, b_2) \in A \times B$:

(i) si $a_1 <_A a_2$, es $(a_1, b_1) \leq_{lex} (a_2, b_2)$;

(ii) si $a_1 = a_2$ y $b_1 \leq_B b_2$, es $(a_1, b_1) \leq_{lex} (a_2, b_2)$.

Ejemplo 2.3. En $\mathcal{P}(X)$, la relación de inclusión entre conjuntos es un orden parcial, pero no total.

Definición 2.28. Si X está parcialmente ordenado por $\leq$, entonces:

(i) $a \in X$ se llama *elemento máximo* de X, si para cada $x \in X$, es $x \leq a$;

(ii) $a \in X$ es un *elemento maximal* de X, si $a \not\leq x$ para cada $x \neq a$;

(iii) $a \in X$ se llama *elemento mínimo* de X, si para cada $x \in X$, es $x \geq a$,

(iv) $a \in X$ es un *elemento minimal* de X, si $x \not\leq a$ para cada $x \neq a$.

Ejemplo 2.4. Si $X = \{a, b, c\}$ con el orden parcial $a \leq b$ y $a \leq c$, entonces b es un elemento maximal de X, pero no un máximo.

Definición 2.29. Un conjunto totalmente ordenado en el cual todo $A \subset X$ no vacío posee un elemento mínimo, se llama conjunto *bien ordenado*. Por ejemplo, $(\mathbb{Z}, \leq)$ no está bien ordenado.

Observación 2.3. $(A \times B, \leq_{lex})$ está bien ordenado si y sólo si $(A, \leq_A)$ y $(B, \leq_B)$ lo están.

Definición 2.30. Sea $(X, \leq)$ un conjunto totalmente ordenado y $A \subset X$:

1) si $u \in X$ es tal que $a \leq u$ para cada $a \in A$, se dice que u es una *cota superior* de A;

2) la menor de las cotas superiores de A (es decir, u es cota superior de A y para cada z cota superior de A es $z \geq u$) es el *supremo* de A, y se denota $\sup(A)$;

3) si $l \in X$ es tal que $a \geq l$ para cada $a \in A$, se dice que l es una *cota inferior* de A;

4) la mayor de las cotas inferiores de A (es decir, l es cota inferior de A y para cada z cota inferior de A es $z \leq l$) es el *ínfimo* de A, y se denota $\text{ínf}(A)$.

En el caso particular del orden usual sobre $\mathbb{R}$, se verifica:

Teorema 2.16. ***(Axioma de la cota superior)*** *Si $A \subset \mathbb{R}$ está acotado superiormente (es decir, existe $u \in \mathbb{R}$, tal que $u \geq a$, para cada $a \in A$), existe el supremo de A. Y en tal caso, $s = \sup(A)$ si y sólo si:*

(i) para cada $a \in A$, es $a \leq s$, y

(ii) para todo $\varepsilon > 0$, existe $a_\varepsilon \in A$ tal que $a_\varepsilon > s - \varepsilon$.

Del axioma anterior, se deduce que:

Corolario 2.17. *Si $A \subset \mathbb{R}$ está acotado inferiormente (es decir, existe $l \in \mathbb{R}$, tal que $l \leq a$, para cada $a \in A$), existe el ínfimo de A. Y entonces, $i = \text{ínf}(A)$ si y sólo si:*

(i) para cada $a \in A$, es $a \geq i$, y

(ii) para todo $\varepsilon > 0$, existe $a_\varepsilon \in A$ tal que $a_\varepsilon < i + \varepsilon$.

Teorema 2.18. *$\mathbb{R}$ es arquimediano, es decir, el conjunto $\mathbb{N}$ no está acotado superiormente.*

Demostración: Si lo estuviera, existiría $r_0 \in \mathbb{R}$, tal que $n \leq r_0$ para cada $n \in \mathbb{N}$. Pero $n_0 = [r_0] + 1 \in \mathbb{N}$, y $n_0 \not\leq r_0$. ∎

Del teorema 2.18 se deducen inmediatamente:

Corolario 2.19. ***(Propiedad arquimediana)*** *Para todo $x > 0$, existe $n \in \mathbb{N}$, tal que $0 < \frac{1}{n} < x$.*

Corolario 2.20. ***(Densidad de los racionales)*** *Dados dos números reales $x < y$, existe $r \in \mathbb{Q}$, tal que $x < r < y$.*

Demostración: Por la propiedad arquimediana (corolario 2.19), existe $n_0 \in \mathbb{N}$ tal que $\frac{1}{n_0} < y - x$. El conjunto $\mathbb{M} = \{m \in \mathbb{N} : x < \frac{m}{n_0}\}$ es no vacío y está bien ordenado, es decir, existe $m_0 \in \mathbb{M}$ tal que $x < \frac{m_0}{n_0}$ y $x \geq \frac{m_0 - 1}{n_0}$. Es inmediato probar que además $\frac{m_0}{n_0} < y$. ∎

Corolario 2.21. ***(Propiedad de los intervalos de encaje)*** *Dada $\{[a_n, b_n] : n \in \mathbb{N}\}$, una familia de intervalos cerrados y encajados (es decir, si $n \leq m$, es $[a_m, b_m] \subset [a_n, b_n]$), entonces $\bigcap_{n \in \mathbb{N}} [a_n, b_n] \neq \emptyset$.*

Demostración: Para cada $m, n \in \mathbb{N}$, es $a_n < b_m$, luego para todo $m \in \mathbb{N}$, b_m es cota superior del conjunto $A = \{a_n\}_{n \in \mathbb{N}}$. Si $p = \sup(A)$, es claro que $p \in \bigcap_{n \in \mathbb{N}} [a_n, b_n]$. ∎

2.5. Ejercicios

1.- Sea X el conjunto de los estudiantes de la Facultad de Ciencia y Tecnología de la UPV/EHU, H el conjunto de los hombres, M el de la mujeres, C el de los estudiantes que van en coche a la Universidad, A el de los estudiantes que van en autobús a la Universidad, E el de los estudiantes de Matemáticas y F el de los estudiantes de Físicas. Describir los siguientes conjuntos: $X - H$, $X - M$, $X - C$, $X - A$, $X - E$, $X - F$, $H \cap C$, $H \cap A$, $H \cap E$, $H \cap F$, $M \cap C$, $M \cap A$, $M \cap E$, $M \cap F$, $C \cap A$, $C \cap E$, $C \cap F$, $A \cap E$, $A \cap F$, $E \cap F$, $M \cup H$, $H - M$, $H - C$, $H - A$, $H - E$, $H - F$, $H - M$, $M - H$, $M - C$, $M - A$, $M - E$, $M - F$, $C - A$, $C - E$, $C - F$, $A - C$, $A - M$, $A - H$, $A - E$, $A - F$, $E - H$, $E - M$, $E - C$, $E - A$ y $E - F$.

2.- En un grupo de 40 personas, sea E el conjunto de las que estudian inglés, F el conjunto de las que estudian francés y C el conjunto de las que estudian castellano. Se sabe que 3 personas no estudian ningún idioma, 2 estudian los 3, 8 inglés y francés, 10 inglés y castellano, 6 francés y castellano, 13 francés y 28 inglés. ¿Cuántos estudian sólo castellano? ¿Puedes expresar este conjunto de manera simbólica?

3.- Dado el conjunto $A = \{a, b\}$, ¿son válidas las siguientes expresiones?
(i) $a \in A$; (ii) $\{a\} \in A$; (iii) $\emptyset \in A$; (iv) $\{a\} \in \mathcal{P}(A)$; (v) $\emptyset \in \mathcal{P}(A)$.

4.- Sean A, B y C tres conjuntos finitos, de cardinales a, b y c, respectivamente. Sea $p = Card(A \cap B)$, $q = Card(B \cap C)$, $r = Card(A \cap C)$ y $s = Card(A \cap B \cap C)$. Calcular el cardinal de $A \cup B$, $A \cup C$, $B \cup C$ y $A \cup B \cup C$.

5.- Se pide:

a) calcular $\mathcal{P}(X)$, si $X = \{1, 2\}$, $X = \{\emptyset\}$ y $X = \{1, 2, 3, 4\}$;

b) probar que si $Card(X) = n$, entonces $Card(\mathcal{P}(X)) = 2^n$;

c) probar que si $A \subset B$, entonces $\mathcal{P}(A) \subset \mathcal{P}(B)$. ¿Es cierto el recíproco?

d) ¿es $\mathcal{P}(A) \cup \mathcal{P}(B) = \mathcal{P}(A \cup B)$? ¿Y $\mathcal{P}(A) \cap \mathcal{P}(B) = \mathcal{P}(A \cap B)$?

6.- Si $A, B \subset X$, probar que son equivalentes las siguientes expresiones:

(i) $A \subset B$; (ii) $A \cap B = A$; (iii) $A \cup B = B$;

(iv) $B^c \subset A^c$; (v) $A \cap B^c = \emptyset$; (vi) $B \cup A^c = X$.

7.- Probar las propiedades siguientes para conjuntos, dando un contraejemplo en el caso de inclusión estricta:

a) $A \cup \left(\bigcup_{i \in I} B_i \right) = \bigcup_{i \in I} (A \cup B_i)$; b) $A \cap \left(\bigcap_{i \in I} B_i \right) = \bigcap_{i \in I} (A \cap B_i)$;

c) $A \cup \left(\bigcap_{i\in I} B_i\right) = \bigcap_{i\in I}(A \cup B_i)$; d) $\bigcap_{i\in I} A_i \cap \bigcap_{j\in J} B_j = \bigcap_{(i,j)\in I\times J}(A_i \cap B_j)$;

e) $\left(\bigcap_{i\in I} A_i\right) \cup \left(\bigcap_{j\in J} B_j\right) = \bigcap_{(i,j)\in I\times J}(A_i \cup B_j)$; f) $\bigcap_{(i,j)\in I^2}(A_i \cup B_j) \subset \bigcap_{i\in I}(A_i \cup B_i)$;

g) $\left(\bigcap_{i\in I} A_i\right) \cup \left(\bigcap_{i\in I} B_i\right) \subset \bigcap_{i\in I}(A_i \cup B_i)$; h) $\bigcup_{i\in I}(A_i \cap B_i) \subset \bigcup_{(i,j)\in I^2}(A_i \cap B_j)$;

i) $\left(\bigcup_{i\in I} A_i\right) \times \left(\bigcup_{j\in J} B_j\right) = \bigcup_{(i,j)\in I\times J}(A_i \times B_j)$. Esto no significa que $(A\cup B)\times(C\cup D) = (A \times C) \cup (B \times D)$;

j) $\left(\bigcap_{i\in I} A_i\right) \times \left(\bigcap_{j\in J} B_j\right) = \bigcap_{(i,j)\in I\times J}(A_i \times B_j)$;

k) $\left(\bigcap_{i\in I} A_i\right) \times \left(\bigcap_{i\in I} B_i\right) = \bigcap_{i\in I}(A_i \times B_i)$;

l) $\left(\bigcup_{i\in I} A_i\right) - \left(\bigcup_{j\in J} B_j\right) = \bigcup_{i\in I}\bigcap_{j\in J}(A_i - B_j)$;

m) $\left(\bigcap_{i\in I} A_i\right) - \left(\bigcap_{j\in J} B_j\right) = \bigcap_{i\in I}\bigcup_{j\in J}(A_i - B_j)$.

8.- Para cada uno de los siguientes conjuntos de índices I y cada familia dada de conjuntos indicados por I, hallar los conjuntos pedidos:

a) si $I = \mathbb{R}^2$ y para cada $p \in I$, $S_p = \{p\}$, hallar $\bigcup_{p\in I} S_p$;

b) si $I = (0, \infty)$ y para cada $x \in I$, $C_x = [0, x]$, hallar $\bigcup_{x\in I} C_x$ y $\bigcap_{x\in I} C_x$;

c) si $I = \left(\frac{1}{2}, 1\right)$ y para $r \in I$, B_r es el círculo de radio r y centro $(0, 0)$, hallar $\bigcup_{r\in I} B_r$ y $\bigcap_{r\in I} B_r$;

d) si $I = (0,1)$ y para cada $r \in I$, N_r es el interior del círculo de radio r y centro $(0,0)$, hallar $\bigcup_{r\in I} N_r$ y $\bigcap_{r\in I} N_r$;

e) si $I = [1,2]$ y para cada $x \in I$, $A_x = [\frac{x}{2}, \frac{3x}{2}]$, hallar $\bigcup_{x\in I} A_x$ y $\bigcap_{x\in I} A_x$;

f) si $I = \mathbb{N}$ y para cada $n \in I$, $A_n = \left(-\frac{1}{n}, \frac{1}{n}\right)$, hallar $\bigcup_{n\in I} A_n$ y $\bigcap_{n\in I} A_n$;

g) si $I = \mathbb{N}$ y para cada $n \in I$, $B_n = (\frac{1}{n}, 1]$, hallar $\bigcup_{n\in I} B_n$ y $\bigcap_{n\in I} B_n$;

h) si $I = \mathbb{N}$ y para cada $n \in I$, $C_n = (-n, n)$, hallar $\bigcup_{n\in I} C_n$ y $\bigcap_{n\in I} C_n$.

9.- Probar las siguientes propiedades de la diferencia simétrica:

(i) $A\triangle(B\triangle C) = (A\triangle B)\triangle C$; (ii) $A \cup B = A\triangle B\triangle(A \cap B)$;

(iii) $A \cap (B\triangle C) = (A \cap B)\triangle(A \cap C)$;

(iv) $A\triangle(B \cap C) = (A\triangle B) \cap (A\triangle C)$ si y sólo si $A \cap B = A \cap C$,

(v) calcular $A\triangle\emptyset$, $A\triangle A$ y $(A\triangle B) \cup (A\triangle B^c)$; (vi) Si $A\triangle B = \emptyset$, ¿es $A = B$?

10.- Dados $A, B \subset X$, probar:

a) $\chi_{A\cap B} = \chi_A \cdot \chi_B$; b) $\chi_{A\cup B} = \chi_A + \chi_B - \chi_{A\cap B}$;

c) $\chi_{A-B} = \chi_A - \chi_{A\cap B}$; d) $\chi_{A^c} = 1 - \chi_A$.

11.- Sean $f\colon X \longrightarrow Y$ y $g\colon Y \longrightarrow Z$ dos aplicaciones. Probar:

a) si f y g son sobreyectivas, entonces $g \circ f$ también lo es, pero el recíproco no es cierto;

b) si $g \circ f$ es sobreyectiva, entonces g también lo es, pero el recíproco no es cierto;

c) si $g \circ f$ es sobreyectiva y g es inyectiva, entonces f es sobreyectiva;

d) si f y g son inyectivas, entonces $g \circ f$ también lo es, pero el recíproco no es cierto;

e) si $g \circ f$ es inyectiva, entonces f también lo es, pero el recíproco no es cierto;

f) si $g \circ f$ es inyectiva y f es sobreyectiva, entonces g es inyectiva.

12.- Sea $f\colon X \longrightarrow Y$; probar:

a) si existe $g\colon Y \longrightarrow X$, tal que $g \circ f = 1_X$, entonces f es inyectiva;

b) si existe $h\colon Y \longrightarrow X$, tal que $f \circ h = 1_Y$, entonces f es sobreyectiva;

c) f es biyectiva si y sólo si existen $g, h\colon Y \longrightarrow X$, tales que $g \circ f = 1_X$, $f \circ h = 1_Y$ y en tal caso $h = f^{-1} = g$.

13.- Sean dos conjuntos X_1, X_2 y para cada $i \in \{1, 2\}$, $A_i \subset X_i$. Sea $p_i\colon X_1 \times X_2 \longrightarrow X_i$ la i-ésima proyección coordenada. Probar las siguientes propiedades:

a) $A_1 \times X_2 = p_1^{-1}(A_1)$, $X_1 \times A_2 = p_2^{-1}(A_2)$ y $A_1 \times A_2 = p_1^{-1}(A_1) \cap p_2^{-1}(A_2)$;

b) si $A \subset X_1 \times X_2$, entonces $A \subset p_1(A) \times p_2(A)$;

c) $p_i\,(A_1 \times A_2) = A_i$ $(i \in \{1, 2\})$.

14.- Sean $f, g\colon \mathbb{R} \longrightarrow \mathbb{R}$, dadas por:

$$f(x) = \begin{cases} x^2 & \text{si} \quad x \geq 0 \\ 2 & \text{si} \quad x < 0 \end{cases} \qquad \text{y} \qquad g(x) = \begin{cases} \sqrt{x} & \text{si} \quad x \geq 0 \\ x & \text{si} \quad x < 0 \end{cases}$$

Se pide:

a) estudiar las funciones $f \circ g$, $f \circ f$, $g \circ g$, $g \circ f$, si tienen sentido;

b) estudiar el carácter sobreyectivo e inyectivo de f, g, $f \circ g$ y $g \circ f$;

c) calcular $f(-5, 5]$, $g(-5, 5]$, $f^{-1}(-5, 5]$ y $g^{-1}(-5, 5]$.

15.- Hacer lo mismo que en el ejercicio anterior para las funciones: $f\colon \mathbb{Z}^2 \longrightarrow \mathbb{Z}$ y $g\colon \mathbb{Z} \longrightarrow \mathbb{Z}^2$ dadas por: $f(x, y) = x^2 + y$ y $g(x) = (x, -2x)$.

16.- Sea $f\colon \mathbb{R} \longrightarrow \mathbb{R}$, dada por:

$$f(x) = \begin{cases} 2 & \text{si} \quad x < 0 \\ 1 & \text{si} \quad 0 \leq x \leq 2 \\ x - 1 & \text{si} \quad x > 2 \end{cases}$$

Se pide:

a) estudiar si f es inyectiva o sobreyectiva;

b) calcular $f((1, 3))$, $f([-2, 2])$, $f^{-1}((0, 1))$, $f^{-1}([-4, 4])$;

c) si $g\colon \mathbb{R} \longrightarrow \mathbb{R}$ es la aplicación $g(x) = |x|$, determinar $f \circ g$ y calcular $(f \circ g)^{-1}((-2, 5])$.

17.- Probar que la aplicación $f\colon \mathbb{R}-\{2\}\longrightarrow\mathbb{R}-\{1\}$, definida por $f(x)=\frac{x+2}{x-2}$ es biyectiva y calcular f^{-1}.

18.- Calcular $f(A_i)$ y $f^{-1}(B_i)$ ($i\in\{1,2\}$), para $f\colon\mathbb{R}\longrightarrow\mathbb{R}$, donde:

a) $f(x)=x^2$, $A_1=(0,2)$, $B_1=(0,4)$ y $B_2=(-1,0)$;

b) $f(x)=x^4$, $A_1=(0,2)$, $A_2=\emptyset$, $B_1=(0,16]$ y $B_2=(-1,0]$;

c) $f(x)=\frac{1}{x}$ (para $x>0$), $A_1=\mathbb{N}$, $B_1=\{x\in\mathbb{R}:x>2\}$ y $B_2=\mathbb{N}$;

d) $f(x)=x^3-3x$, $A_1=[0,\infty)$, $B_1=(0,2)$ y $B_2=\{2\}$.

19.- Si $f,g,h\colon\mathbb{R}\longrightarrow\mathbb{R}$ son las funciones $f(x)=x^2$, $g(x)=2^x$ y $h(x)=\cos(x)$, escribir las siguientes expresiones como composiciones de las anteriores: $2^{\cos(x)}$, $\cos(2^{x+\cos(x)})$, $\cos(2^x)$, $\cos(\cos(x)^2)$, $(\cos(x))^2$, $\cos(x^2)$, $2^{2\cos(x)}$, $(\cos(2^{\cos(x)}))^2$, $\cos^2(x)$, $2^{x^2+2(\cos(2^x)^2)}$.

20.- Escribir $f\colon\mathbb{R}\longrightarrow\mathbb{R}$, $f(x)=(1+(1-x)^3)^{\frac{1}{3}}$ como composición de cuatro funciones.

21.- Encontrar biyecciones explícitas entre

a) $[0,1]$ y $[1,2]$; b) $(-1,1)$ y $\mathbb{R}$;

c) $[0,1]$ y $[0,1)$; d) $[-1,1]$ y $\mathbb{R}$.

22.- Probar que las siguientes funciones son biyectivas y calcular su inversa:

a) $f\colon\mathbb{Z}\longrightarrow\mathbb{Z}$ dada por

$$f(n)=\begin{cases} n+p & \text{si } n \text{ es múltiplo de } p \\ n & \text{si } n \text{ no es múltiplo de } p \end{cases}$$

b) $f\colon\mathbb{R}\longrightarrow\mathbb{R}$ dada por

$$f(x)=\begin{cases} x^4 & \text{si } x\geq 0 \\ x(2-x) & \text{si } x<0 \end{cases}$$

23.- Sea $f\colon X\longrightarrow X$ una función y la relación binaria sobre X, xRy si $f(x)=y$. Probar:

a) R es reflexiva si y sólo si $f=1_X$.

b) R es simétrica si y sólo si $f^2=1_X$.

c) R es transitiva si y sólo si $f^2=f$.

24.- Decir cuales de las siguientes relaciones sobre X son de equivalencia, y en su caso, encontrar un sistema completo de representantes de dicha relación (es decir, un subconjunto $A \subset X$ tal que cualquier elemento de X está relacionado con exactamente un elemento de A):

a) $X = \mathbb{Z}$ y $x \sim y$ si y sólo si $x - y$ es impar;

b) $X = \mathbb{Z}$ y $x \sim y$ si y sólo si $x^2 + x = y^2 + y$;

c) $X = \mathbb{R}$ y $x \sim y$ si y sólo si $x - y \in \mathbb{Z}$;

d) $X = \mathbb{R}$ y $x \sim y$ si y sólo si $xy \leq 0$;

e) $X = \mathbb{R}$ y $x \sim y$ si y sólo si $xy > 0$.

25.- Definir sobre $X = \{1, 2, 3\}$ tres relaciones binarias cada una de las cuales cumpla dos de las propiedades reflexiva, simétrica y transitiva, pero no la tercera. Esto prueba que estas tres propiedades son independientes.

26.- ¿Cuántas relaciones de equivalencia se pueden definir sobre un conjunto con dos elementos? ¿Con tres elementos? ¿Con cuatro elementos?

27.- Se define sobre $\mathbb{R}$ la relación de equivalencia $x \sim y$ si y sólo si $x - y \in \mathbb{Z}$. Determinar cuales de las siguientes funciones $f : \mathbb{R} \longrightarrow \mathbb{R}$ pasan al cociente:

a) $f(x) = x^2$; b) $f(x) = x - [x]$ ($[x]$ es la parte entera de x);

c) $f(x) = \sin(2\pi x)$; d) $f(x) = \sin(\pi x)$;

e)

$$f(x) = \begin{cases} -1 & \text{si} \quad x < 0 \\ 0 & \text{si} \quad x = 0 \\ 1 & \text{si} \quad x > 0 \end{cases}$$

28.- Dados $x, y \in \mathbb{R}$, utilizando el carácter arquimediano de $\mathbb{R}$, probar:

a) si $x > 0$ e $y > 0$, existe $n \in \mathbb{N}$, tal que $nx > y$;

b) si $x > 0$, existe $n \in \mathbb{N}$, tal que $0 < \frac{1}{n} < x$;

c) si $x > 0$, existe $n \in \mathbb{N}$, tal que $n - 1 \leq x < n$.

Capítulo 3

Elementos de combinatoria

Ahora puedo olvidarlas. Llego a mi centro,
a mi álgebra y mi clave,
a mi espejo.
Pronto sabré quién soy.

Elogio de la sombra
Jorge Luis Borges (1899–1986)

3.1. Los principios multiplicativo y aditivo

El análisis combinatorio es la técnica que permite saber cuántos elementos hay en un conjunto sin necesidad de conocerlos. En este capítulo se van a ver algunas técnicas de conteo: las dos básicas son el *principio aditivo* y el *principio multiplicativo*.

3.1.1. Principio aditivo de conteo

Es la técnica más sencilla para calcular el cardinal de un conjunto. La idea consiste en dividir el conjunto a estudiar en dos subconjuntos disjuntos cuyos cardinales sean más fáciles de calcular, y sumarlos.

Proposición 3.1. ***(Principio aditivo)*** *Si $A_1, A_2, \ldots, A_n$ son conjuntos finitos y dos a dos disjuntos, entonces*

$$Card\,(A_1 \cup A_2 \cup \cdots \cup A_n) = Card(A_1) + Card(A_2) + \cdots + Card(A_n).$$

Observación 3.1. Recordar que si para cada $i \in \{1, \ldots, n\}$ se define A_i como el conjunto de los elementos que cumplen cierta propiedad $\mathfrak{P}_i$, entonces $A_1 \cup A_2 \cup \cdots \cup A_n$ es el

conjunto de los elementos que verifican la propiedad $\mathfrak{P}_1$, o la $\mathfrak{P}_2$,... o la $\mathfrak{P}_n$, es decir, al menos una de ellas. Si las propiedades son dos a dos incompatibles (no hay ningún elemento que satisfaga ambas simultáneamente), entonces los conjuntos son dos a dos disjuntos. Se puede aplicar entonces el principio aditivo (proposición 3.1), y el número de elementos que satisfacen al menos una de las propiedades es $Card(A_1) + Card(A_2) + \cdots + Card(A_n)$.

Ejemplo 3.1. Lanzamos cuatro monedas distintas, ¿cuántas maneras hay de conseguir *al menos* dos caras?

Solución: Sea A el conjunto formado por todos los lanzamientos de cuatro monedas que contienen 2, 3 ó 4 caras. Se puede descomponer en la unión disjunta de tres conjuntos:

$$A_2 = \{\text{lanzamientos en los que se obtienen exactamente 2 caras}\} =$$

$$= \{(c,c,x,x),(c,x,c,x),(c,x,x,c),(x,c,c,x),(x,c,x,c),(x,x,c,c)\},$$

$$A_3 = \{\text{lanzamientos en los que se obtienen exactamente 3 caras}\} =$$

$$= \{(c,c,c,x),(c,c,x,c),(c,x,c,c),(x,c,c,c)\},$$

$$A_4 = \{\text{lanzamientos en los que se obtienen exactamente 4 caras}\} = \{(c,c,c,c)\}.$$

Así $Card(A) = Card(A_2) + Card(A_2) + Card(A_4) = 6 + 4 + 1 = 11$. ∎

Observación 3.2. Es muy importante recordar que el principio aditivo sólo es válido si los subconjuntos son dos a dos disjuntos. Por ejemplo, si nos piden calcular, lanzando dos dados distintos, de cuántas maneras se puede conseguir que la suma de los puntos sea múltiplo de 4 ó de 6, consideramos: sean A_1 el conjunto de todas las tiradas cuya suma es múltiplo de 4 y A_2 el conjunto de todas las tiradas cuya suma es múltiplo de 6:

$$A_1 = \{(1,3),(2,2),(2,6),(3,1),(3,5),(4,4),(5,3),(6,2),(6,6)\}$$

$$A_2 = \{(1,5),(2,4),(3,3),(4,2),(5,1),(6,6)\}$$

No podemos aplicar directamente el principio aditivo, ya que A_1 y A_2 no son conjuntos disjuntos. En tal caso, puede aplicarse el *principio de inclusión-exclusión*, que garantiza que si A_1 y A_2 son conjuntos finitos, entonces:

$$Card\,(A_1 \cup B) = Card(A_1) + Card(A_2) - Card\,(A_1 \cap A_2)\,.$$

3.1.2. Principio multiplicativo de conteo

El *principio multiplicativo* se utiliza sobre todo para contar el número de posibles listas ordenadas de longitud r, es decir, listas formadas por r objetos, en los que importa el orden de colocación.

Proposición 3.2. ***(Principio multiplicativo)*** *Se quiere hacer una lista ordenada de longitud r. Para el primer lugar de la lista se puede elegir entre n_1 objetos, para el segundo entre n_2 y así sucesivamente hasta el lugar r-ésimo, para el que se puede elegir entre n_r objetos. Entonces, el número total de listas de r objetos ordenados es $n_1 n_2 \dots n_r$.*

Ejemplo 3.2. ¿Cuántos números de cuatro cifras distintas se pueden formar con los dígitos $\{1, 2, 3, 4, 5, 6, 7\}$? ¿Y si las cifras pueden repetirse? ¿Cuántos de estos números son pares?

Solución: 1) Si pensamos el número como una 4-tupla (m, c, d, u) y las cifras no se pueden repetir, tenemos 7 posibles elecciones para m, 6 para c, 5 para d y 4 para u. Aplicando el principio multiplicativo (proposición 3.2), hay $7 \cdot 6 \cdot 5 \cdot 4 = 840$ posibles números.

2) Si las cifras se pueden repetir, hay $7 \cdot 7 \cdot 7 \cdot 7 = 2401$ posibles números.

3) Son pares aquellos cuya cifra en las unidades u es igual a 2, 4 ó 6. Es decir, hay $7 \cdot 7 \cdot 7 \cdot 3 = 1029$ posibles números. ∎

Ejemplo 3.3. Cada usuario de un servidor de Internet tiene una palabra clave para acceder a su cuenta. La palabra clave está formada por 4 caracteres, a elegir entre 26 letras mayúsculas y 10 dígitos $\{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$. Además, la clave debe tener al menos 1 dígito (es decir, 2AAA es una clave, pero AAAA, no). ¿Cuántas palabras clave se pueden formar?

Solución: Cada clave es una lista ordenada (c_1, c_2, c_3, c_4). Para los tres primeros caracteres, hay 36 posibilidades de elección, pero no así para el cuarto carácter, pues depende de las elecciones realizadas con anterioridad. Si los tres primeros caracteres son letras, el último debe ser un dígito, con lo que sólo puede elegirse entre 10 posibilidades. Sin embargo, si en los tres primero hay al menos un dígito, el cuarto carácter puede ser una letra o un dígito, es decir, se pueden elegir entre 36 posibilidades. Así, no se pude aplicar el principio multiplicativo directamente. El tener que aparecer *al menos* un dígito obliga a utilizar además el principio aditivo. El conjunto de las palabras clave con al menos un dígito se divide en 4 subconjuntos disjuntos C_1 el de las claves con exactamente un dígito, C_2 el de las claves con exactamente 2 dígitos, C_3 el de las claves con exactamente 3 dígitos y C_4 el de las claves con exactamente 4 dígitos. Si C es el conjunto de todas las posibles claves, el conjunto de las que no poseen ningún dígito es $C_0 = C - (C_1 \cup C_2 \cup C_3 \cup C_4)$, y por la proposición 3.2 $Card(C) = 36^4$ y $Card(C_0) = 26^4$, con lo que la cantidad buscada es $36^4 - 26^4$. ∎

3.1.3. Principio del palomar o de distribución de Dirichlet

Este principio se basa en este comentario obvio (y de allí su nombre): *Si $m+1$ palomas ocupan m nidos, al menos uno de ellos debe contener más de una paloma.*

Proposición 3.3. ***Principio del palomar*** *Si m objetos se distribuyen en n conjuntos y*

1) $m > n$, entonces hay al menos 2 objetos que se encuentran en el mismo conjunto;

2) $m > 2n$, entonces hay al menos 3 objetos en el mismo conjunto;

3) $m > kn$ para un cierto k, entonces hay al menos $k+1$ objetos que se encuentran en el mismo conjunto.

Proposición 3.4. ***Principio de distribución*** *Sean m, n, r enteros positivos. Si distribuimos $mn + r$ objetos en m cajas, entonces alguna caja contiene más de n objetos.*

3.2. Combinaciones y permutaciones

En esta sección abordamos el siguiente problema: dado un conjunto con n objetos ¿cuál es el número de familias de k objetos que se pueden formar eligiéndolos entre esos n? La respuesta se deduce del principio multiplicativo (proposición 3.2), y depende de dos factores:

1) ¿importa el orden en que se agrupen los k objetos?

2) ¿puede haber elementos repetidos entre esos k objetos?

Según la respuesta a las anteriores cuestiones tendremos cuatro tipos de familias: variaciones –y las permutaciones, que son un tipo especial de variaciones–, variaciones con repetición, combinaciones y combinaciones con repetición.

3.2.1. Variaciones

Definición 3.1. Una *variación de n elementos tomados de k en k* ($k \leq n$) es una lista ordenada de k objetos distintos elegidos de $A = \{a_1, a_2, \ldots, a_n\}$. El número de posibles variaciones es

$$V(n,k) = n(n-1)(n-2)\ldots(n-k+1) = \frac{n!}{(n-k)!}.$$

Ejemplo 3.4. Si A tiene k elementos y B tiene n ($k \leq n$), el número de aplicaciones inyectivas de A en B es $V(n,k)$.

Definición 3.2. Una *permutación de* n objetos distintos es una lista ordenada de esos n objetos, es decir, es una *variación de* n *elementos tomados de* n *en* n. El número de posibles permutaciones es $P(n) = V(n, n) = n!$.

Ejemplo 3.5. Si A y B tienen n elementos, el número de aplicaciones biyectivas de A en B es $P(n)$.

Definición 3.3. Una *variación con repetición de* n *elementos tomados de* k *en* k (no se impone ninguna restricción sobre k con respecto a n) es una lista ordenada de k objetos –no necesariamente distintos– elegidos de $A = \{a_1, a_2, \ldots, a_n\}$. El número de posibles variaciones con repetición es $VR(n, k) = n^k$.

Ejemplo 3.6. Si A tiene k elementos y B tiene n, el número de aplicaciones de A en B es $VR(n, k)$. Observar la diferencia con el ejemplo 3.4.

Definición 3.4. Una *permutación con repetición de* n *objetos* se define del modo siguiente: dado un conjunto $A = \{a_1, a_2, \ldots, a_n\}$, tomamos m_1 elementos iguales a a_1, m_2 elementos iguales a $a_2, \ldots, m_n$ elementos iguales a a_n, de forma que $m_1+m_2+\cdots+m_n = m$. El número de ordenaciones posibles de estos m elementos es:

$$PR_m^{m_1,m_2,\ldots,m_n} = \frac{m!}{m_1!m_2!\ldots m_n!}$$

Ejemplo 3.7. ¿Cuántas palabras se pueden formar con las letras A, B y C, si la letra "A" debe aparecer 3 veces, la letra "B" 4 y la "C" 5?

Solución: En realidad, debemos formar esas palabras con las letras AAABBBBCCCCC. La respuesta es $PR_{12}^{3,4,5} = \frac{(12)!}{3!4!5!} = 27720$. Es posible llegar a la respuesta anterior a través de otro argumento, a veces más claro: se trata de colocar 12 objetos en 12 lugares. Supongamos que colocamos primero las 3 "A", luego las 4 "B" y por último las 5 "C". Tenemos $\binom{12}{3}$ maneras de colocar las "A", una vez hecho esto $\binom{9}{4}$ de colocar las "B", y por fin $\binom{5}{5}$ de colocar las "C", es decir, las posibles palabras a formar son:

$$\binom{12}{3}\binom{9}{4}\binom{5}{5} = \frac{(12)!}{9!3!}\frac{9!}{4!5!} = 27720. \qquad \blacksquare$$

3.2.2. Combinaciones y números combinatorios

Definición 3.5. Una *combinación de* n *elementos tomados de* k *en* k ($k \leq n$) es una colección de k objetos distintos elegidos de $A = \{a_1, a_2, \ldots, a_n\}$, pero sin importar el orden en que se eligen. El número de estas posibles familias es:

$$C(n, k) = \frac{V(n, k)}{k!} = \frac{n!}{(n-k)!k!}.$$

Demostración: Los k objetos de cada una de estas combinaciones se pueden ordenar de $k!$ formas distintas, produciendo $k!$ variaciones. Si hacemos esto con cada una de las combinaciones, obtenemos todas las variaciones posibles de n elementos tomadas de k en k. Es decir, $C(n,k) \cdot P(k) = C(n,k) \cdot k! = V(n,k)$. ∎

Definición 3.6. A la expresión $C(n,k)$ se le llama *número combinatorio o coeficiente binomial*. Con el convenio $0! = 1$, se verifica que $C(n,0) = C(n,n) = 1$. Se suele denotar $C(n,k) = \binom{n}{k}$.

Ejemplo 3.8. Cada apuesta de la lotería primitiva es una combinación de 6 números elegidos entre 49. Por lo tanto, el número de apuestas posibles es de $\binom{49}{6} = 13983816$.

Ejemplo 3.9. Una sucesión binaria es una sucesión de 0 y 1. ¿Cuántas sucesiones binarias de longitud 10 hay con al menos 7 "1"?

Solución: El conjunto de las sucesiones binarias con al menos 7 "1" se descompone en la unión de cuatro conjuntos disjuntos $S_7 \cup S_8 \cup S_9 \cup S_{10}$, donde S_k denota el conjunto de las sucesiones binarias con exactamente k "1". Construir S_k consiste en elegir los lugares que van a ocupar los k "1", es decir $Card(S_k) = C(10,k)$. Así el número buscado es

$$C(10,7) + C(10,8) + C(10,9) + C(10,10) = 120 + 45 + 10 + 1 = 176.$$

Definición 3.7. Una *combinación con repetición de n elementos tomados de k en k* es una colección de k objetos elegidos –no necesariamente distintos– de $A = \{a_1, a_2, \ldots, a_n\}$ y sin importar el orden. El número de estas posibles familias es $CR(n,k) = C(n+k-1,k)$.

Demostración: En efecto, como no importa el orden, se trata de formar listas de la forma

$$a_1 \overbrace{\ldots}^{k_1} a_1, a_2 \overbrace{\ldots}^{k_2} a_2, a_n \overbrace{\ldots}^{k_n} a_n,$$

con k_i copias de a_i ($i \in \{1, \ldots, n\}$) y donde $k_1 + \cdots + k_n = k$. Es decir, se trata de colocar $n + k - 1$ objetos en k lugares, sin importar el orden. ∎

Ejemplo 3.10. ¿Cuántos productos diferentes de dos factores se pueden formar con los dígitos 2, 3 y 5, sin repetir factores? ¿Y pudiendo repetirse los factores?

Solución: Como el producto es conmutativo, no influye el orden en que se tomen, así que si no se pueden repetir hay $C(3,2) = 3$ productos (son 6, 10 y 15). Si se permiten repetir los dígitos, tendríamos $CR(3,2) = C(4,2) = 6$ posibles productos (son 4, 6, 10, 9, 15 y 25). ∎

3.3. El triángulo de Pascal y el binomio de Newton

Proposición 3.5. *Se verifican las siguientes propiedades:*

1) $\binom{n}{0} = 1 = \binom{n}{n}$*;*

2) $\binom{n}{1} = n$*;*

3) $\binom{n}{k} = \binom{n}{n-k}$*;*

4) ***Fórmula de Pascal****: si* $k < n$*, entonces* $\binom{n}{k} = \binom{n-1}{k-1} + \binom{n-1}{k}$.

Se denomina **Triángulo de Pascal** al siguiente triángulo formado por números combinatorios:

$$\binom{0}{0}$$

$$\binom{1}{0}\binom{1}{1}$$

$$\binom{2}{0}\binom{2}{1}\binom{2}{2}$$

$$\binom{3}{0}\binom{3}{1}\binom{3}{2}\binom{3}{3}$$

$$\binom{4}{0}\binom{4}{1}\binom{4}{2}\binom{4}{3}\binom{4}{4}$$

$$\binom{5}{0}\binom{5}{1}\binom{5}{2}\binom{5}{3}\binom{5}{4}\binom{5}{5}$$

$$\binom{6}{0}\binom{6}{1}\binom{6}{2}\binom{6}{3}\binom{6}{4}\binom{6}{5}\binom{6}{6}$$

Observación 3.3. La *fórmula de Pascal* dice que cada número combinatorio se obtiene sumando los dos números de la fila superior que están justo encima de él:

$$\underbrace{\binom{n-1}{k-1} + \binom{n-1}{k}}$$

$$\binom{n}{k}$$

Sustituyendo los números combinatorios por su valor, el triángulo queda:

$$1$$

$$1 \quad 1$$

$$1 \quad 2 \quad 1$$

$$1 \quad 3 \quad 3 \quad 1$$

$$1 \quad 4 \quad 6 \quad 4 \quad 1$$

$$1 \quad 5 \quad 10 \quad 10 \quad 5 \quad 1$$

$$1 \quad 6 \quad 15 \quad 20 \quad 15 \quad 6 \quad 1$$

Proposición 3.6. *Para cada $n \geq 0$, se cumple*

$$\binom{n}{0} + \binom{n}{1} + \dots \binom{n}{n-1} + \binom{n}{n} = 2^n.$$

Demostración: La prueba se hace por inducción. Para $n = 0$, $\binom{0}{0} = 1 = 2^0$. Supongamos que la propiedad es cierta para $n - 1$, es decir,

$$\binom{n-1}{0} + \binom{n-1}{1} + \dots \binom{n-1}{n-1} = 2^{n-1}.$$

Aplicando la fórmula de Pascal, queda:

$$\binom{n}{0} + \dots + \binom{n}{n} = \binom{n}{0} + \left(\binom{n-1}{0} + \binom{n-1}{1} \right) + \dots + \left(\binom{n-1}{n-2} + \binom{n-1}{n-1} \right) + \binom{n}{n}.$$

Reordenando y aplicando la hipótesis de inducción, queda:

$$\binom{n}{0} + \binom{n}{1} + \dots \binom{n}{n-1} + \binom{n}{n} =$$

$$= \binom{n}{0} + \binom{n-1}{0} + 2\binom{n-1}{1} + \dots 2\binom{n-1}{n-2} + \binom{n-1}{n-1} + \binom{n}{n} =$$

$$2\binom{n-1}{0} + 2\binom{n-1}{1} + \dots 2\binom{n-1}{n-2} + 2\binom{n-1}{n-1} = 2 \cdot 2^{n-1} = 2^n. \qquad \blacksquare$$

Teorema 3.7. ***(Teorema del binomio de Newton)*** *Para cada $n > 0$,*

$$(a+b)^n = \binom{n}{0} a^n + \binom{n}{1} a^{n-1} b + \binom{n}{2} a^{n-2} b^2 + \dots + \binom{n}{n-1} a b^{n-1} + \binom{n}{n} b^n.$$

Demostración: Se prueba por inducción. Para $n = 1$, es claro que $(a+b)^1 = \binom{1}{0}a + \binom{1}{1}b$. Supongamos la fórmula cierta para $n-1$, es decir:

$$(a+b)^{n-1} = \binom{n-1}{0}a^{n-1} + \binom{n-1}{1}a^{n-2}b + \cdots + \binom{n-1}{n-2}ab^{n-2} + \binom{n-1}{n-1}b^{n-1}.$$

Entonces, aplicando la hipótesis de inducción y la fórmula de Pascal, queda:

$$(a+b)^n = (a+b)(a+b)^{n-1} =$$

$$(a+b)\left(\binom{n-1}{0}a^{n-1} + \binom{n-1}{1}a^{n-2}b + \cdots + \binom{n-1}{n-2}ab^{n-2} + \binom{n-1}{n-1}b^{n-1}\right) =$$

$$\left(\binom{n-1}{0}a^n + \binom{n-1}{1}a^{n-1}b + \cdots + \binom{n-1}{n-2}a^2b^{n-2} + \binom{n-1}{n-1}ab^{n-1}\right) +$$

$$+\left(\binom{n-1}{0}a^{n-1}b + \binom{n-1}{1}a^{n-2}b^2 + \cdots + \binom{n-1}{n-2}ab^{n-1} + \binom{n-1}{n-1}b^n\right) =$$

$$\binom{n-1}{0}a^n + \left(\binom{n-1}{0} + \binom{n-1}{1}\right)a^{n-1}b + \cdots +$$

$$+\left(\binom{n-1}{n-2} + \binom{n-1}{n-1}\right)ab^{n-1} + \binom{n-1}{n-1}b^n =$$

$$\binom{n}{0}a^n + \binom{n}{1}a^{n-1}b + \cdots + \binom{n}{n-1}ab^{n-1} + \binom{n}{n}b^n. \qquad \blacksquare$$

3.4. Ejercicios

1.- ¿De cuántas maneras pueden sentarse 10 personas en un banco si hay 4 sitios libres?

2.- En una clase de 10 alumnos van a distribuirse 3 premios. ¿De cuántos modos puede hacerse, si los tres premios son diferentes? ¿Y si son iguales?

3.- Las diagonales de un polígono se obtienen uniendo pares de vértices no adyacentes. ¿Cuántas diagonales tiene el cuadrado? ¿Y el hexágono?

4.- Se quieren colocar a 5 hombres y 4 mujeres en una fila, de manera que las mujeres ocupen los lugares pares. ¿De cuántas maneras puede hacerse?

5.- ¿Cuántos números de 4 dígitos se pueden formar con las cifras 1, 2, 3, 4, 5, 6, 7, 8 y 9, si se permiten repeticiones? ¿sin repeticiones? ¿y si el último dígito debe ser el 1 y no se permiten repeticiones?

6.- En un grupo de 10 amigos, ¿cuántas distribuciones de fechas de cumpleaños pueden darse al año?

7.- ¿Cuántas letras de 5 signos con 3 rayas y 2 puntos podría tener el alfabeto Morse?

8.- Cuando se arrojan simultáneamente 4 monedas, ¿cuáles son los resultados posibles que se pueden obtener? ¿cuántos casos hay en que salgan 2 caras y 2 cruces?

9.- Cuatro libros de matemáticas, seis de física y dos de química deben ordenarse en una estantería, ¿cuántas colocaciones son posibles si los libros de cada materia deben estar juntos? ¿y si sólo deben estar juntos los libros de matemáticas?

10.- Un alumno debe elegir 7 entre las 10 preguntas de un examen. ¿De cuántas maneras puede elegirlas? ¿Y si las 4 primeras son obligatorias?

11.- Una línea de ferrocarril tiene 25 estaciones. ¿Cuántos billetes diferentes habrá que imprimir si cada billete lleva impresas las estaciones de origen y destino?

12.- Tres atletas toman parte en los 100 metros lisos. ¿De cuantas maneras pueden llegar –pueden llegar juntos– a la meta?

13.- En un hospital se utilizan 5 símbolos para clasificar las historias clínicas de los pacientes, de manera que los dos primeros son letras y los tres últimos son dígitos. ¿Cuántas historias clínicas podrían hacerse si no hay restricciones sobre las letras o los números? ¿Y si las dos letras no pueden ser iguales?

14.- Cada uno de los 200 delegados a un congreso de las Naciones Unidas saluda a los demás con un apretón de manos. ¿Cuántos apretones de mano se dan?

15.- Seis estudiantes forman un equipo para colaborar en un trabajo formado por 8 problemas. Dos personas deberán hacer 2 ejercicios y el resto de las personas 1 cada uno. ¿De cuántas maneras se puede hacer esta distribución?

16.- Se deben distribuir 4 naranjas, 5 manzanas y 6 peras entre 5 niños. ¿De cuántas maneras puede hacerse? (No se distinguen dos piezas de fruta de la misma clase).

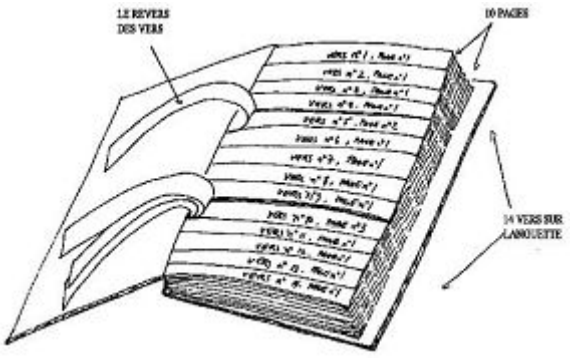
17.- Se quiere distribuir 9 libros entre 3 niños. ¿De cuántas maneras puede hacerse si los libros son todos diferentes, el niño mayor debe recibir 5 y los otros 2 cada uno? ¿Y si los libros son 9 copias idénticas del mismo título y no hay restricciones sobre el número de libros que recibe cada niño? ¿Y si los libros son 9 copias idénticas del mismo título y cada niño debe recibir al menos un libro?

18.- ¿Cuántos menús diferentes se pueden hacer si se puede elegir entre 3 primeros platos, 2 segundos platos y 4 postres?

19.- Una mujer tiene en su armario 4 faldas, 5 camisas y 3 chaquetas. Si elige al azar una falda, una blusa y una chaqueta, ¿de cuántas maneras diferentes se puede vestir?

20.- Tenemos un cuestionario con 15 preguntas que permite una sola respuesta por pregunta. Para cada pregunta se proponen 4 posibles respuestas. ¿De cuántas maneras se puede responder al cuestionario?

21.- Raymond Queneau escribió un libro titulado *Cent mille milliards de poèmes (Cien mil millardos de poemas)*. El libro está compuesto por 10 sonetos –14 versos–, que se imprimen sobre 10 páginas (uno por página), que se recortan en 14 trozos, cada uno correspondiente a una línea (verso). Un lector puede componer su propio poema de 14 versos tomando el primer verso de una de las 10 páginas, luego el segundo verso de una de las 10 páginas y así sucesivamente hasta el verso número 14. Justifica el título de la obra (un millardo es 10^9).



22.- En informática, se usa el sistema binario para codificar los caracteres. Un bit es un elemento que toma el valor 0 o el 1. Con 8 bits, ¿cuántos caracteres se pueden codificar?

23.- ¿Cuántos números de teléfono se pueden formar con 8 cifras? ¿Y si el primer dígito no puede ser 0?

24.- En una competición deportiva con 18 atletas, se atribuye una medalla de oro, una de plata y una de bronce. ¿Cuántas distribuciones de medallas son posibles?

25.- En una clase de 24 alumnos forman la asociación *Los mejores*. La asociación consta de presidente, secretario y tesorero. ¿Cuántas posibles juntas directivas hay?

26.- Seis personas eligen mentalmente un número entre el 1 y el 6. ¿cuántos resultados se pueden obtener? ¿cuántos resultados se pueden obtener sin repetir ningún número?

27.- Sea A el conjunto de los números de 4 cifras (el primero no puede ser 0). ¿Cuántos elementos tiene A? ¿Cuántos números tienen las 4 cifras diferentes? ¿Cuántos tienen al menos dos cifras idénticas? ¿Cuántos tienen 4 cifras diferentes y que no sean 5 ó 7?

28.- Un teclado formado por las letras A, B, C y los números 1, 2, 3, 4, 5 y 6 permite componer el código de entrada a una casa, formada por una letra seguida de tres cifras arbitrarias. ¿Cuántos códigos diferentes se pueden componer? ¿Cuántos sin la cifra 1? ¿Cuántos que contengan al menos una vez la cifra 1? ¿Cuántos con cifras diferentes? ¿Cuántos con al menos dos cifras iguales?

29.- ¿Cuántos anagramas existen del nombre PATRICE? ¿Cuántos empezando y terminando por consonante? ¿Cuántos empezando y terminando por vocal? ¿Cuántos empezando por consonante y terminando por vocal? ¿Cuántos empezando por vocal y terminando por consonante? Un *anagrama* de una palabra es otra palabra que resulta de la transposición de letras de la primera.

30.- ¿Cuántos anagramas tiene la palabra ANAGRAMA?

31.- Un torneo deportivo tiene 8 equipos inscritos. Cada equipo debe jugar con todos los demás una sola vez. ¿Cuántos partidos deben organizarse?

32.- ¿De cuántas maneras pueden elegirse 3 mujeres y 2 hombres entre 10 mujeres y 5 hombres?

33.- En una clase de 32 alumnos hay 19 chicos y 13 chicas. Deben elegirse dos delegados. ¿Cuántas elecciones son posibles? ¿Cuántas si debe haber un chico y una chica? ¿Cuántas si debe de haber dos chicos?

34.- Pablo y Claudia pertenecen a un club de 18 personas. Se debe elegir 5 personas para representar al club en una reunión. ¿Cuántos grupos de 5 personas se pueden formar? ¿En cuántos de estos grupos puede figurar Pablo? Pablo y Claudia no se soportan, ¿cuántos grupos de 5 personas se pueden formar sin que Pablo y Claudia coincidan?

35.- En una empresa hay 12 personas solteras entre los 30 empleados. Se quiere realizar una encuesta, para lo que se elige una muestra de 4 personas. ¿Cuántas muestras posibles se pueden realizar? ¿Cuántas de ellas no contienen a ninguna persona soltera? ¿Cuántas tienen al menos una persona soltera?

36.- Entre 25 mujeres y 32 hombres se quiere elegir un grupo de 6 personas. ¿De cuántas maneras puede hacerse si el grupo sólo consta de hombres? ¿Si consta de personas del mismo sexo? ¿Si hay al menos un hombre y al menos una mujer?

37.- Se extraen simultáneamente 5 cartas –una mano– de un juego de 32 –baraja de póker– . ¿Cuántas manos diferentes hay? ¿Cuántos *póker* –4 cartas iguales–? ¿Cuántas manos con 2 pares diferentes (no valen los póker)? ¿Cuántos *full* –3 cartas del mismo valor y otras 2 diferentes del mismo valor–? ¿Cuántos tríos (no valen los full)? ¿Cuántas escaleras de color –5 cartas del mismo color siguiéndose en orden creciente–?

38.- Un saco contiene 5 canicas verdes –numeradas del 1 al 5– y 4 rojas –numeradas del 1 al 4–. Se sacan 3 canicas del saco sin reponerlas. ¿Cuántas probabilidades hay de sacar 3 canicas verdes? ¿De no sacar ninguna verde? ¿De sacar como mucho 2 canicas verdes? ¿De sacar exactamente 1 canica verde? Responder a las mismas cuestiones si se reponen las canicas tras sacarlas.

39.- Un armario tiene 5 perchas alineadas. Si no se ponen las prendas las unas sobre las otras, ¿de cuántas maneras se pueden colocar 3 abrigos sobre las 5 perchas? ¿5 abrigos? ¿6 abrigos?

40.- Cuatro chicos y dos chicas se sientan en un banco. ¿De cuántas maneras lo pueden hacer? ¿Y si los chicos se sientan en un lado y las chicas en otro? ¿Y si cada chica se coloca entre dos chicos? ¿Y si las chicas se quieren sentar todas juntas?

41.- Un aseguradora clasifica a sus asegurados según el sexo (2 clases), el estado civil (3 clases) y el tipo de riesgo (10 clases). ¿De cuántas categorías distintas dispone la compañía?

42.- La fábrica de sidra *Sidrabon* quiere identificar sus productos. Para ello, destaca algunas de sus características:

1) según el grado de CO_2, la sidra es *espumosa*, *con gas* o *no efervescente*;

2) según el grado de azúcar, la sidra se cataloga en *dulce*, *semi-seca* o *seca*;

3) según el grado de alcohol, la sidra es *ligera* o *fuerte*.

¿Cuántos productos diferentes puede fabricar *Sidrabon*?

43.- Un artesano fabrica 5 modelos diferentes de zapatos, en 10 tallas y 3 colores. ¿Cuántas clases diferentes de zapatos puede fabricar?

44.- Se lanzan simultáneamente una moneda y un dado. ¿Cuántos resultados posibles hay?

45.- Tres carreteras unen *Ale* y *Bar* y cuatro unen *Bar* y *Cel*. ¿De cuántas maneras se puede ir de *Ale* a *Cel* pasando por *Bar*?

46.- ¿De cuántas maneras se pueden pintar las 4 paredes de tu habitación si se dispone de 6 colores?

47.- Los señores García, Gómez y Pérez llegan a una ciudad donde hay 4 hoteles. Cada uno elige uno de ellos al azar. ¿De cuántas maneras pueden alojarse? ¿De cuántas maneras si deben ir a hoteles diferentes?

48.- ¿Cuántos números de 3 cifras y menores a 500 se pueden formar con los dígitos 1, 2, 3, 4, 5, 6 y 7? ¿Y si las cifras deben ser todas diferentes?

49.- Se administran 5 drogas para buscar el tratamiento de una enfermedad. Se realiza un test para observar si el orden de administración de estas drogas es importante. ¿De cuántas maneras diferentes pueden administrarse estas 5 drogas?

50.- ¿De cuántas maneras pueden pintarse 7 circunferencias concéntricas con los 7 colores blanco, negro, rojo, amarillo, azul, verde y marrón (usando todos los colores) si el negro y el blanco deben colorear circunferencias vecinas, pero el negro debe colorear una circunferencia mayor que el blanco? ¿Y si el negro y el blanco nunca deben estar juntos?

51.- Cinco parejas compran los billetes para la temporada de fútbol en San Mamés. Consiguen 10 bancos en la fila H de la zona norte. ¿De cuántas maneras diferentes pueden ocupar sus asientos si se conocen y por lo tanto no les importa donde sentarse? ¿Y si quieren sentarse por parejas? ¿Y si alternan hombres y mujeres? ¿Y si las mujeres se sientan juntas? ¿Y si las mujeres se sientan juntas y los hombres también?

52.- Se pide al tenor Franco Barettini que interprete 8 canciones en una gala benéfica. Elige interpretar 2 obras de Verdi, 2 de Bizet, 2 de Wagner y 2 de Puccini. ¿De cuántas maneras puede hacerlo si quiere comenzar por una obra de Verdi y terminar por una de Puccini? ¿Si quiere interpretar consecutivamente las dos obras de cada autor? ¿Si quiere que las cuatro primeras canciones sean de compositores diferentes?

53.- Un grupo de 12 estudiantes que comparte casa necesita elegir a sus 3 cocineros y a las 4 personas que lavarán los platos. ¿De cuántas maneras pueden hacer esta elección si 3 de los estudiantes no saben cocinar?

54.- La capacidad de un minibús es de 14 pasajeros. Ocho de los asientos dan a una ventana. ¿De cuántas maneras pueden sentarse 6 pasajeros si 3 de ellos quieren sentarse cerca de una ventana y otros 2 no quieren un asiento de ventana?

55.- ¿De cuántas maneras se puede transportar a 16 personas en dos furgonetas, si una furgoneta tiene capacidad para 8 personas y la otra para 10? Se supone que el orden en el interior de cada furgoneta no tiene importancia.

56.- Un gobierno debe elegir entre 70 diputados a sus 25 ministros. ¿Cuántos Consejos de Ministros diferentes hay si se eligen los ministros al azar? ¿Si 10 ministros estaban previamente impuestos antes de la elección? ¿Si esos 10 elegidos tenían ya asignados ministerios específicos?

57.- Se organiza una fiesta donde hay 7 chicos y 10 chicas. A la hora de bailar, los chicos eligen una chica al azar. ¿De cuántas formas pueden hacerlo? ¿Y si Mónica y Luisa están seguras de que van a bailar (aunque no saben con quien)? ¿Y si Mónica está segura de que Juan le invitará a bailar y Luisa sabe que Pedro hará lo propio?

58.- El director del Museo Guggenheim desea disponer en fila 7 cuadros, 3 de Monet

y 4 de Picasso. Los Picasso están datados y el director quiere que aparezcan en orden cronológico. ¿De cuántas maneras diferentes pueden colocarse los cuadros?

59.- Antonio dispone de las siguientes guarniciones: pepperoni, champiñón, pimiento, cebolla, anchoa, salami, jamón y gambas. Si una pizza puede contener ninguna, parte de o todas estas guarniciones, ¿cuántas pizzas diferentes puede hacer Antonio?

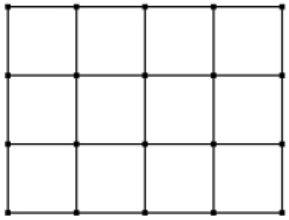
60.- Un sastre confecciona camisas de 12 colores, cada color en 8 tallas de cuello diferentes y cada talla de cuello en 3 longitudes de mangas distintas. ¿Cuántas clases de camisas confecciona?

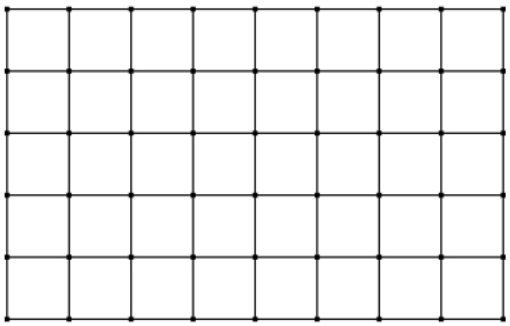
61.- En una tienda los clientes tienen la opción de pagar en diferentes cajas. ¿De cuántas maneras pueden pagar 5 clientes en 3 cajas? ¿Y 2 clientes en 6 cajas?

62.- Un hombre adinerado lega 9 cuadros a sus 3 hijos. ¿De cuántas maneras puede repartir los cuadros si cada hijo debe tener 3 pinturas?

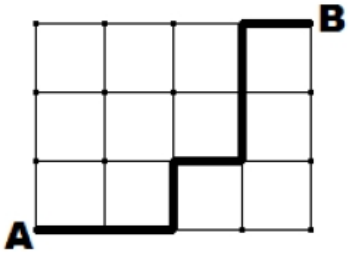
63.- Determinar el número de palabras de tres letras que se pueden formar con A, M y E, usando cada letra exactamente una vez.

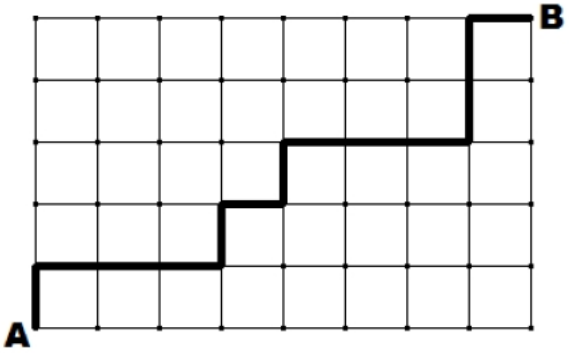
64.- Determinar el número de rectángulos diferentes (los cuadrados son rectángulos) que se pueden observar en las figuras de debajo. Se considera que dos rectángulos son diferentes si tienen distintas dimensiones y están colocados en un lugar diferente en el retículo.





65.- Las calles de una ciudad son todas perpendiculares, como en los dibujos de debajo. Calcular el número de caminos diferentes que se pueden trazar para unir los puntos A y B desplazándose únicamente hacia la derecha y hacia arriba (se ven ejemplos de tales caminos en las figuras).





66.- Se fijan 6 puntos sobre una circunferencia. ¿Cuántos segmentos se pueden trazar al unirlos de dos en dos? ¿Cuántos triángulos se pueden formar con esos 6 puntos?

67.- Las franjas de una diana están numeradas del 1 al 17. Si tiras 3 dardos y anotas las puntuaciones, ¿cuántas puntuaciones diferentes puedes tener?

68.- ¿Cuántas matrículas diferentes se pueden formar con 3 letras seguidas de 4 números?

69.- En un plano se marcan 4 puntos rojos, 5 verdes y 6 azules, entre los cuales no hay tres alineados. ¿Cuántas rectas se pueden pasan por dos puntos rojos? ¿Y por dos puntos del mismo color? ¿Y por dos puntos de distinto color? ¿Y por un punto rojo y otro de color verde o azul?

70.- ¿Cuántos números de 5 cifras existen en el sistema decimal que sean capicúas? ¿Y de 6 cifras?

71.- Con los números 1, 2, 3, 4 y 5, ¿cuántos números de tres cifras se pueden escribir? ¿cuántos son capicúas? Calcular la suma de todos ellos.

72.- Simplificar las siguientes expresiones:

a) $\dfrac{(n+5)!}{(n+3)!}$; b) $\dfrac{(n^2)!}{(n-2)!(n+1)!}$; c) $\dfrac{(n+1)!}{n!}$;

d) $\dfrac{(n-1)!-n!}{n!+(n-1)!}$; e) $\dfrac{(n-2)!}{(n-1)!}$; f) $\dfrac{n!-(n-1)(n-1)!}{(n-1)n!-(n-1)!}$.

73.- Demostrar las siguientes igualdades:

a) $\dfrac{((2n)!)^2}{(2n-1)!(2n+1)!}=\dfrac{2n}{2n+1}$; b) $\dfrac{(n+1)!}{n!}-\dfrac{(n-1)!}{(n-2)!}=2$;

c) $\dfrac{r(n-1)!}{(n-r)!}+\dfrac{(n-1)!}{(n-r-1)!}=\dfrac{n!}{(n-r)!}$; d) $\binom{2n}{2}=2\binom{n}{2}+n^2$.

74.- Resolver las siguientes ecuaciones:

a) $\dfrac{n!}{(n-4)!} = \dfrac{20n!}{(n-2)!}$; b) $n! = (n-2)!$;

c) $n! = 12\sqrt{n! - 20}$; d) $n! - 7 + \dfrac{6}{n!} = 0$.

75.- Desarrollar las siguientes fórmulas usando el binomio de Newton:

a) $(x+2)^7$; b) $\left(x + \dfrac{1}{x}\right)^6$;

c) $(2a^2 - 3)^6$; d) $\left(\dfrac{a}{b^2} - \dfrac{b}{a^2}\right)^5$.

76.- Hallar los valores indicados:

a) el quinto término de $(2a - b)^7$;

b) el término independiente de a y de b de $\left(\dfrac{a}{b} - \dfrac{b}{a}\right)^{10}$;

c) el coeficiente de x^2y^4 al desarrollar $(3x - 4y^2)^4$.

77.- Si los términos 6^0 y 16^0 de $(a-b)^n$ son iguales, encontrar el tercero.

78.- Escribir en forma de binomio y evaluar 101^3 y 99^4.

79.- Probar la identidad:

$$\binom{n}{0} - \binom{n}{1} + \binom{n}{2} - \binom{n}{3} + \cdots + (-1)^n \binom{n}{n} = 0.$$

80.- Usar el ejercicio anterior y la proposición 3.6 para probar que:

$$\binom{n}{0} + \binom{n}{2} + \binom{n}{4} + \cdots = \binom{n}{1} + \binom{n}{3} + \binom{n}{5} + \cdots = 2^{n-1}\binom{n}{n} = 0.$$

81.- Usar el teorema del binomio 3.7 y la igualdad $(1+x)^{2n} = (1+x)^n(1+x)^n$ para probar que:

$$\binom{2n}{n} = \binom{n}{0}^2 + \binom{n}{1}^2 + \binom{n}{2}^2 + \cdots + \binom{n}{n}^2.$$

82.- Encontrar el valor de n si:

a) $\binom{n-1}{6} + \binom{n-1}{5} = \binom{n}{12}$; b) $\frac{2(n-1)!}{(n-2)!} + \frac{(n-1)!}{(n-3)!} = 56$;

c) $3\left(\binom{n}{0} + \binom{n}{1} + \binom{n}{2} + \cdots + \binom{n}{n}\right) = 2^{n-1}\left(\binom{n-1}{1} + \binom{n-1}{2}\right)$;

d) $\binom{n}{3} = 4\binom{n-2}{2}$; e) $\binom{n}{41} = \binom{n}{94}$.

Capítulo 4

Divisibilidad

Día, noche, ponientes, madrugadas, espacios,
ondas nuevas, antiguas, fugitivas, perpetuas,
mar o tierra, navío, lecho, pluma, cristal,
metal, música, labio, silencio, vegetal,
mundo, quietud, su forma. Se querían, sabedlo.

Se querían
Vicente Aleixandre (1898–1984)

4.1. Los números enteros

Uno de los conceptos básicos en la teoría elemental de números es el de *divisibilidad*. La división con resto de números enteros es la idea fundamental de este capítulo.

Definición 4.1. Dados dos enteros $a, b \in \mathbb{Z}$, con $a \neq 0$, se dice que a *divide a* b, y se escribe $a \mid b$, si existe $c \in \mathbb{Z}$ tal que $b = ac$. Se dice que a *es factor o divisor de* b y que b *es múltiplo de* a o que b *es divisible por* a. En caso contrario, se escribe $a \nmid b$.

Se demuestran de manera inmediata las siguientes propiedades:

Proposición 4.1. *Si* $a, b, c, d \in \mathbb{Z}$*, se cumplen las siguientes propiedades:*

1) $a \mid b$ *si y sólo si* $|a| \mid |b|$*, donde* $|x| = \begin{cases} x & \text{si} \quad x \geq 0 \\ -x & \text{si} \quad x < 0 \end{cases}$

2) $a \mid 0$ *y* $1 \mid a$*.*

3) $a \mid 1$ *si y sólo si* $a = \pm 1$*.*

4) $a \mid a$.

5) Si $a \mid b$ *y* $b \mid a$, *entonces* $a = \pm b$.

6) Si $a \mid b$ *y* $b \mid c$, *entonces* $a \mid c$ *(transitividad de la división).*

7) Si $a \mid b$ *y ambos números son enteros positivos, entonces* $a \leq b$.

8) Si $a \mid b$ *y* $a \mid c$, *entonces* $a \mid (bx - cy)$, *para cualesquiera* $x, y \in \mathbb{Z}$.

4.2. El algoritmo de la división

La idea fundamental en la que se basa nuestro estudio de números enteros es el algoritmo de la división:

Proposición 4.2. *Dados dos enteros* a *y* b, *con* $b \neq 0$, *existen enteros* q *y* r *tales que* $a = qb + r$, *con* $0 \leq r < |b|$. *Tanto* q *como* r *son únicos. Se dice que* a *es el dividendo,* b *es el divisor,* q *el cociente y* r *el resto de la división de* a *entre* b.

Demostración: Sea el número racional $\frac{a}{b}$ (si a y b son de distinto signo, se pasa el signo negativo a a, y se supone que $b > 0$ durante la demostración). Existe un entero q tal que $q \leq \frac{a}{b} < q + 1$. Multiplicando por b, queda $qb \leq a < (q + 1)b$. Y entonces $r = a - qb$, que verifica claramente las propiedades pedidas. ∎

Observación 4.1. Se verifican las siguientes propiedades de demostración inmediata:

1) En el caso particular en que $r = 0$, a es divisible por b.

2) la condición $0 \leq r < |b|$ es la que caracteriza el algortimo de la división. Una expresión del tipo $21 = (-3)(-5) + 6$ no es fruto del algoritmo de la división.

3) Fijado el divisor b, sólo hay una cantidad finita de restos. En efecto, sólo hay $|b|$ restos posibles, que son $0, 1, 2, \ldots |b| - 1$. Esto nos permitirá clasificar los infinitos números enteros en una cantidad finita de clases –$|b|$ clases– según los restos que se obtengan al dividirlos por b.

Ejemplo 4.1. El cuadrado de todo número entero a es de la forma $3k$ ó $3k + 1$. De otra manera, al dividir a^2 por 3, el resto obtenido es 0 ó 1.

Demostración: En efecto, si se divide a entre 3, los únicos restos posibles son 0, 1 ó 2, es decir, hay tres posibilidades:

1) $a = 3q$, entonces $a^2 = 9q^2 = 3(3q^2) = 3k$;

2) $a = 3q + 1$, entonces $a^2 = 9q^2 + 6q + 1 = 3(3q^2 + 2q) + 1 = 3k + 1$;

3) $a = 3q + 2$, entonces $a^2 = 9q^2 + 12q + 4 = 3(3q^2 + 4q + 1) + 1 = 3k + 1$. ∎

4.3. Sistemas de numeración

Nuestra forma habitual de representar los números es mediante el *sistema decimal*, en el que manejamos los diez dígitos: 0, 1, 2, 3, 4, 5, 6, 7, 8 y 9. Cuando tenemos diez unidades –unidad = primer dígito por la derecha antes de la coma, si la hubiera–, las agrupamos en una decena (10^1) –decena = dígito a la izquierda de la unidad–, cuando tenemos diez decenas las agrupamos en una centena (10^2) –centena = dígito a la izquierda de la decena–, y así sucesivamente. De esta manera el número que consta de 1 centena, 0 decenas y 8 unidades se representa en el sistema decimal por la siguiente suma de potencias de diez:

$$1 \cdot 10^2 + 0 \cdot 10^1 + 8 \cdot 10^0,$$

o en su forma habitual 108.

Observación 4.2. Aquí nos vamos a limitar a números enteros, pero en el caso general, el primer número a la derecha de la coma es uno de esos diez dígitos multiplicado por 10^{-1}, la segunda cifra tras la coma es uno de ellos mutiplicado por 10^{-2}, etc.

No hay ningún motivo por el que limitarse al sistema decimal. Por ejemplo, los ordenadores usan los sistemas binario (base 2), octal (base 8) y hexadecimal (base 16). Para hacer cálculos numéricos, un ordenador utiliza la siguiente expresión de 108 como potencias de 2:

$$108 = 1 \cdot 2^6 + 1 \cdot 2^5 + 0 \cdot 2^4 + 1 \cdot 2^3 + 1 \cdot 2^2 + 0 \cdot 2^1 + 0 \cdot 2^0.$$

En realidad el ordenador utiliza sólo los coeficientes de dichas potencias (como hacemos en base 10), que sustituyen a la expresión 108 en el sistema binario, que se expresa del modo $(1101100)_2$. Si expresamos 108 como potencias de 4, queda:

$$108 = 1 \cdot 4^3 + 2 \cdot 4^2 + 3 \cdot 4^1 + 0 \cdot 4^0,$$

que se representa por $(1230)_4$. O en base 9:

$$108 = 1 \cdot 9^2 + 3 \cdot 9^1 + 0 \cdot 9^0,$$

es decir, $(130)_9$.

Para obtener estas expresiones se utiliza el algoritmo de la división (proposición 4.2).

Observación 4.3. El número 108 puede también obtenerse de otra manera como suma de potencias de 2:

$$108 = 3 \cdot 2^5 + 0 \cdot 2^4 + 0 \cdot 2^3 + 3 \cdot 2^2 + 0 \cdot 2^1 + 0 \cdot 2^0.$$

Lo que caracteriza la primera escritura

$$108 = 1 \cdot 2^6 + 1 \cdot 2^5 + 0 \cdot 2^4 + 1 \cdot 2^3 + 1 \cdot 2^2 + 0 \cdot 2^1 + 0 \cdot 2^0,$$

es que todos los coeficientes son menores que 2, lo que garantiza la unicidad de esta expresión.

Proposición 4.3. *Sea un entero $b \geq 2$, al que llamaremos base. Todo número natural $n \in \mathbb{N}$ se puede escribir de forma única como suma de potencias de b de la siguiente manera:*

$$n = a_m b^m + a_{m-1} b^{m-1} + \cdots + a_2 b^2 + a_1 b + a_0,$$

donde $0 \leq a_i < b$ para cada i y $a_m \neq 0$.

Demostración: Basta con aplicar la proposición 4.2 de manera sucesiva, empezando por $n = n_1 b + a_0$, después $n_1 = n_2 b + a_1$, y así hasta llegar a una expresión $n_{m-1} = a_m b + a_{m-1}$, con $a_m < b$. Sustituyendo estos valores en $n = n_1 b + a_0$, se obtiene finalmente:

$$n = (((a_m b + a_{m-1} \ldots) b + a_2) b + a_1) b + a_0 = a_m b^m + a_{m-1} b^{m-1} + \cdots + a_2 b^2 + a_1 b + a_0. \quad \blacksquare$$

Observación 4.4. La escritura en base b del número n se denotará por

$$n = (a_m a_{m-1} \ldots a_2 a_1 a_0)_b.$$

Ejemplo 4.2. ¿Cómo se pasa de base b a base 10?

Solución: Basta con desarrollar las potencias de b en la escritura dada. Observar que el exponente de la mayor potencia de b es uno menos que el número de dígitos que aparecen en la escritura. Por ejemplo:

$$(3043)_5 = 3 \cdot 5^3 + 0 \cdot 5^2 + 4 \cdot 5 + 3 = 398. \quad \blacksquare$$

Ejemplo 4.3. ¿Cómo se pasa de base 10 a base b?

Solución: Basta con dividir sucesivas veces por b, es decir, seguir el procedimiento de la proposición 4.3. Por ejemplo, para pasar 1025 a base 7, si se divide entre 7, se obtiene: $1025 = 146 \cdot 7 + 3$. Pero $146 = 20 \cdot 7 + 6$ y $20 = 2 \cdot 7 + 6$. Así:

$$1025 = 146 \cdot 7 + 3 = (20 \cdot 7 + 6) \cdot 7 + 3 = ((2 \cdot 7 + 6) \cdot 7 + 6) \cdot 7 + 3,$$

y sacando factor común a las potencias de 7, se tiene:

$$1025 = 2 \cdot 7^3 + 6 \cdot 7^2 + 6 \cdot 7 + 3 = (2663)_7.$$

Observar que los dígitos 2, 6, 6 y 3 son precisamente los restos que hemos obtenido al ir dividiendo entre la base $b = 7$. $\blacksquare$

Observación 4.5. En el sistema hexadecimal necesitamos 16 símbolos, por lo que a 0, 1, 2, ..., 9, se les añaden las letras A (=10), B (=11), C (=12), D (=13), E (=14) y F (=15) como símbolos adicionales.

Ejemplo 4.4. ¿Cómo se pasa de base 10 a base 16?

Solución: Basta con repetir el proceso anterior, por ejemplo: $3027 = 189 \cdot 16 + 3$ y $189 = 11 \cdot 16 + 13$, con lo que $3027 = (BD3)_{16}$. ∎

4.4. Máximo común divisor y algoritmo de Euclides

4.4.1. El máximo común divisor de dos números

Entre las aplicaciones más importantes del algoritmo de la división (proposición 4.2), tenemos dos problemas relacionados con el máximo común divisor de dos números:

1) su cálculo efectivo y

2) su expresión como combinación lineal entera de dichos números.

Definición 4.2. Sean a y b dos enteros, al menos uno de ellos distinto de cero. El máximo común divisor de a y b, MCD(a, b), es el único entero positivo d tal que:

1) $d \mid a$ y $d \mid b$ (es decir, d es divisor común de a y de b), y

2) si $c \mid a$ y $c \mid b$, entonces $c \leq d$ (es decir, d es el mayor de los divisores comunes de a y de b).

Ejemplo 4.5. MCD$(-12, 18) = 6$.

Demostración: Los divisores de -12 son ± 1, ± 2, ± 3, ± 4, ± 6 y ± 12 y los de 18 son ± 1, ± 2, ± 3, ± 6 y ± 18. ∎

Observación 4.6. Se verifican las siguientes propiedades de demostración inmediata:

1) MCD$(a, b) =$ MCD(b, a);

2) si $a = 0 = b$, no existiría MCD(a, b);

3) MCD(a, b) existe ya que el conjunto de los divisores comunes de a y b es no vacío (al menos, 1 es divisor común de a y b) y es finito (pues a o b es no nulo), y por lo tanto dicho conjunto tiene un máximo, que es MCD(a, b);

4) MCD(a, b) es siempre positivo, de hecho MCD(a, b) = MCD$(-a, b)$ = MCD$(a, -b)$ = MCD$(-a, -b)$ = MCD$(|a|, |b|)$;

5) MCD$(a, 0) = |a|$, ya que todo número divide a 0.

El máximo común divisor de dos números se puede expresar como combinación lineal entera de éstos, expresión que se conoce como *identidad de Bezout*:

Proposición 4.4. *Si a y b son dos enteros (al menos uno distinto de cero) , existen otros dos enteros x_0 y y_0 tales que MCD$(a, b) = ax_0 + by_0$.*

Demostración: Sea el conjunto $C = \{ax + by : ax + by > 0, x, y \in \mathbb{Z}\}$. $C \subset \mathbb{N}$ es no vacío, pues por ejemplo $a^2 + b^2 \in C$. Como C está bien ordenado (definición 2.29), llamemos d a su primer elemento, es decir, existen $x_0, y_0 \in \mathbb{Z}$ tales que $d = ax_0 + by_0$. Veamos que d es el máximo común divisor.

1) Usando el algoritmo de la división, puede escribirse $a = qd + r$ con $0 \leq r < d$. Luego

$$r = a - qd = a - q(ax_0 + by_0) = a(1 - qx_0) + b(-qy_0).$$

Si fuese $r > 0$, sería $r \in C$ y $r < d$, en contra de la definición de d. Luego $r = 0$, y por lo tanto $d \mid a$. De manera similar se prueba que $d \mid b$.

2) Si $c \mid a$ y $c \mid b$, sabemos que c divide a cualquier combinación lineal de a y de b, por lo que $c \mid d$, luego $c \leq |c| \leq d$. ∎

Observación 4.7. Se verifican las siguientes propiedades de demostración inmediata:

1) Si $c \mid a$ y $c \mid b$, no sólo es $c \leq$ MCD(a, b), sino que $c \mid$ MCD(a, b).

2) La expresión de MCD(a, b) como combinación lineal de a y de b no es necesariamente única. Por ejemplo, $3 =$ MCD$(6, 9) = 6 \cdot (-1) + 9 \cdot 1 = 6 \cdot 5 + 9 \cdot (-3)$.

Corolario 4.5. *Si a y b son dos enteros (al menos uno distinto de cero), el conjunto $T = \{ax + by : x, y \in \mathbb{Z}\}$ de las combinaciones lineales enteras de a y b es el conjunto de los múltiplos de $d =$ MCD(a, b).*

Demostración: Como a y b son múltiplos de d, cualquier combinación lineal suya también lo es. Recíprocamente, cualquier múltiplo de d es de la forma

$$kd = k(ax_0 + by_0) = kax_0 + kby_0 \in T. \quad ∎$$

Definición 4.3. Si a y b son dos enteros no nulos, se dice que son *primos entre sí*, si MCD$(a, b) = 1$. También se dice que a y b son *coprimos* o *primos relativos*.

Corolario 4.6. *Si a y b son dos enteros no nulos, son primos entre sí, si y sólo si existen $x_0, y_0 \in \mathbb{Z}$ tales que $1 = ax_0 + by_0$.*

Ejemplo 4.6. Para cualquier $n \in \mathbb{Z}$, los enteros $5n + 2$ y $7n + 3$ son coprimos.

Solución: Según el corolario 4.6, basta con encontrar $x_0, y_0 \in \mathbb{Z}$ tales que

$$(5n + 2)x_0 + (7n + 3)y_0 = 1.$$

Pensando en el lado izquierdo como un polinomio en n, tenemos para cada $n \in \mathbb{Z}$

$$n(5x_0 + 7y_0) + (2x_0 + 3y_0) = 1.$$

Así, tenemos las dos igualdades

$$\begin{cases} 5x_0 + 7y_0 &= 0 \\ 2x_0 + 3y_0 &= 1 \end{cases}$$

Y resolviendo el sistema de ecuaciones lineales, encontramos la solución $x_0 = -7$ e $y_0 = 5$. Luego $-7(5n + 2) + 5(7n + 3) = 1$. ∎

Lema 4.7. ***(de Euclides)*** *Si $a \mid bc$ y MCD$(a, b) = 1$, entonces $a \mid c$.*

Demostración: Por el corolario 4.6, existen $x_0, y_0 \in \mathbb{Z}$ tales que $ax_0 + by_0 = 1$. Multiplicando por c, se obtiene $acx_0 + bcy_0 = c$. Como $a \mid bc$ y claramente $a \mid acx_0$, se deduce que $a \mid c$. ∎

¿Cómo calcular el máximo común divisor de dos números? El *algoritmo de Euclides* va a permitir calcular el máximo común divisor de dos números enteros y expresarlo como combinación lineal entera de dichos números. Este algoritmo se basa en la llamada *reducción de Euclides*:

Lema 4.8. ***(Reducción de Euclides)*** *Si $a = qb + r$, entonces MCD$(a, b) =$ MCD(b, r).*

Demostración: Sea $d = \text{MCD}(a, b)$; $d \mid r$ al ser r combinación lineal entera de a y b. Y es el mayor divisor común de b y r, ya que si $c \mid b$ y $c \mid r$, entonces $c \mid a$, con lo que $c \leq \text{MCD}(a, b) = d$. ∎

Así, para calcular el máximo común divisor de dos números, podemos sustituir el mayor de ellos por el resto que se obtiene al dividirlo por el menor.

Ejemplo 4.7. Calcular MCD$(1479, 272)$.

Solución: Dividimos 1479 entre 272, y obtenemos $1479 = 5 \cdot 272 + 119$. Así,

$$\text{MCD}(1479, 272) = \text{MCD}(272, 119),$$

que es más sencillo de calcular. Repetimos la operación, y $272 = 2 \cdot 119 + 34$, con lo que

$$\text{MCD}(1479, 272) = \text{MCD}(272, 119) = \text{MCD}(119, 34).$$

De nuevo, $119 = 3 \cdot 34 + 17$, y así

$$\text{MCD}(1479, 272) = \text{MCD}(272, 119) = \text{MCD}(119, 34) = \text{MCD}(34, 17).$$

Y finalmente, $34 = 2 \cdot 17 + 0$, con lo que

$$\text{MCD}(1479, 272) = \text{MCD}(272, 119) = \cdots = \text{MCD}(17, 0) = 17.$$

Es decir, el último resto no nulo es el máximo común divisor buscado.

4.4.2. El algoritmo de Euclides

Sean $a, b \in \mathbb{Z}$, que podemos considerar positivos, sin pérdida de generalidad (pues $\text{MCD}(a, b) = \text{MCD}(|a|, |b|)$). Supongamos $a \geq b$, dividiendo a entre b, obtenemos

$$a = q_1 b + r_1, \quad \text{con} \quad 0 \leq r_1 < b.$$

La reducción de Euclides (lema 4.8) garantiza que $\text{MCD}(a, b) = \text{MCD}(b, r_1)$. Si $r_1 = 0$, $\text{MCD}(a, b) = \text{MCD}(b, r_1) = b$, y hemos acabado. En caso contrario, dividimos b entre r_1:

$$b = q_2 r_1 + r_2, \quad \text{con} \quad 0 \leq r_2 < r_1.$$

La reducción de Euclides garantiza que $\text{MCD}(a, b) = \text{MCD}(b, r_1) = \text{MCD}(r_1, r_2)$. Si $r_2 = 0$, $\text{MCD}(a, b) = \text{MCD}(r_1, r_2) = r_1$, y hemos acabado. En caso contrario, dividimos r_1 entre r_2:

$$r_1 = q_3 r_2 + r_3, \quad \text{con} \quad 0 \leq r_3 < r_2.$$

El proceso continúa hasta que lleguemos a una división con resto 0. Esto ocurre tras una cantidad finita de divisiones, ya que la sucesión de restos es finita por ser estrictamemte decreciente $r_1 > r_2 > r_3 > \cdots \geq 0$. El último resto no nulo es entonces el máximo común divisor buscado.

Si suponemos que la primera división que da resto no nulo es la $(n+1)$-ésima, tendríamos

$$r_{n-1} = q_{n+1} r_n + 0, \quad \text{y}$$

$$\text{MCD}(a, b) = \text{MCD}(b, r_1) = \text{MCD}(r_1, r_2) = \cdots = \text{MCD}(r_{n-1}, r_n) = \text{MCD}(r_n, 0) = r_n.$$

Observación 4.8. Este método es mucho más rápido que el de factorizar cada número para encontrar el máximo común divisor.

¿Cómo usar el algoritmo de Euclides para encontrar una identidad de Bezout (proposición 4.4)? Tenemos

$$\begin{aligned} a &= q_1 b + r_1, \quad \text{con} \quad 0 \leq r_1 < b \\ b &= q_2 r_1 + r_2, \quad \text{con} \quad 0 \leq r_2 < r_1 \\ r_1 &= q_3 r_2 + r_3, \quad \text{con} \quad 0 \leq r_3 < r_2 \\ &\dots \\ r_{n-3} &= q_{n-1} r_{n-2} + r_{n-1}, \quad \text{con} \quad 0 \leq r_{n-1} < r_{n-2} \\ r_{n-2} &= q_n r_{n-1} + r_n, \quad \text{con} \quad 0 \leq r_n < r_{n-1} \\ r_{n-1} &= q_{n+1} r_n + 0. \end{aligned}$$

Despejando r_n de la penúltima igualdad, es $r_n = r_{n-2} - q_n r_{n-1}$, es decir, una combinación lineal de r_{n-2} y r_{n-1}. Despejando a su vez r_{n-1} de la anterior igualdad, es

$$r_{n-1} = r_{n-3} - q_{n-1} r_{n-2},$$

combinación lineal de r_{n-3} y r_{n-2}. Sustituyendo en la expresión lineal anterior, es

$$r_n = r_{n-2} - q_n (r_{n-3} - q_{n-1} r_{n-2}),$$

es decir, una expresión de r_n como combinación lineal de r_{n-3} y r_{n-2}. Si continuamos de este modo subiendo por la columna de igualdades, llegaremos finalmente a expresar r_n como combinación lineal de a y b.

Ejemplo 4.8. Expresar $\text{MCD}(1479, 272)$ como una combinación lineal de 1479 y 272.

Solución: Tenemos

$$\begin{aligned} 1479 &= 5 \cdot 272 + 119, \\ 272 &= 2 \cdot 119 + 34, \\ 119 &= 3 \cdot 34 + 17, \\ 34 &= 2 \cdot 17 + 0. \end{aligned}$$

Sabemos que $\text{MCD}(1479, 272) = 17$. Si vamos despejando los restos de cada división desde la penúltima ecuación hacia arriba, tenemos:

$$17 = 119 - 3 \cdot 34 = 119 - 3 \cdot (272 - 2 \cdot 119) =$$

$$7 \cdot 119 - 3 \cdot 272 = 7 \cdot (1479 - 5 \cdot 272) - 3 \cdot 272 = 7 \cdot 1479 - 38 \cdot 272. \qquad \blacksquare$$

A veces es mejor aplicar el algoritmo de Euclides a números más pequeños que los inicialmente dados. Por ejemplo, si nos piden calcular $\text{MCD}(56, 72) = \text{MCD}(8 \cdot 7, 8 \cdot 9) = 8 \cdot \text{MCD}(7, 9) = 8$.

Proposición 4.9. *Para todo entero $k \neq 0$, es MCD$(ka, kb) = |k|$MCD(a, b).*

Demostración: Si $k > 0$, hay que ver MCD$(ka, kb) = k$.MCD(a, b). Se debe comparar la columna de igualdades que aparecen al aplicar el algoritmo de Euclides a los números positivos ka y kb, con la que aparece al aplicársela a a y b. La primera columna es el resultado de multiplicar por k la segunda. En particular, el último resto no nulo de la primera es el resultado de multiplicar por k el último resto no nulo de la segunda. Si $k < 0$, hay que ver MCD$(ka, kb) = -k$.MCD(a, b). Pero

$$\text{MCD}(ka, kb) = \text{MCD}(|k|a, |k|b) = |k|\text{MCD}(a, b) = -k.\text{MCD}(a, b). \qquad \blacksquare$$

Corolario 4.10. *Si MCD$(a, b) = d$, entonces $a = da'$ y $b = db'$, con MCD$(a', b') = 1$.*

Existe un concepto paralelo el de máximo común divisor de dos números:

Definición 4.4. Si a y b son dos enteros no nulos, el *mínimo común múltiplo de a y b* mcm(a, b) es el único entero positivo m tal que:

1) $a \mid m$ y $b \mid m$ (es decir, m es múltiplo común de a y de b),

2) si $a \mid c$ y $b \mid c$, con $c > 0$, entonces $m \leq c$ (es decir, m es el menor de los múltiplos positivos de a y de b).

Observación 4.9. Se verifican las siguientes propiedades de demostración inmediata:

1) mcm$(a, b) =$ mcm(b, a);

2) la condición de que ambos sean distintos de cero es necesaria para la existencia múltiplos;

3) mcm(a, b) existe ya que el conjunto de los múltiplos comunes de a y b es no vacío ($|ab|$ es múltiplo común de a y b) y como cualquier subconjunto de $\mathbb{N}$ está bien ordenado (definición 2.29), este conjunto tiene un menor elemento, que es mcm(a, b);

4) mcm(a, b) es siempre positivo, de hecho mcm$(a, b) =$ mcm$(-a, b) =$ mcm$(a, -b) =$ mcm$(-a, -b) =$ mcm$(|a|, |b|)$.

Una forma de calcular el mínimo común múltiplo de dos números es realizar la factorización en primos, pero es un método complicado para números grandes. Existe una relación entre el máximo común divisor y el mínimo común múltiplo de dos números, que puede ayudar a calcular el uno a partir del otro:

Proposición 4.11. *Si a y b son dos enteros no nulos, es MCD(a, b)mcm$(a, b) = |ab|$.*

Demostración: Como MCD(a, b) y mcm(a, b) son siempre positivos, podemos suponer que $a > 0$ y $b > 0$. Sea $d =$ MCD(a, b). Entonces $a = da'$ y $b = db'$ con a' y b' primos entre sí. Sea $m = \frac{ab}{d}$. Se trata de ver que $m =$ mcm(a, b).

1) m es múltiplo de a, pues $m = ab'$ y es múltiplo de b al ser $m = a'b$.

2) Si $c > 0$ es un múltiplo común de a y de b, existen enteros r y s tales que $c = ar = bs$. Por la identidad de Bezout (proposición 4.4), existen enteros x_0, y_0 tales que $d = ax_0 + by_0$. Dividiendo c entre $m = \frac{ab}{d}$, queda:

$$\frac{c}{m} = \frac{cd}{md} = \frac{cd}{ab} = \frac{c(ax_0 + by_0)}{ab} = \frac{c}{b}x_0 + \frac{c}{a}y_0 = sx_0 + ry_0,$$

que es un número entero. Luego $m \mid c$, y efectivamente $m \leq c$. ∎

4.5. Los números primos y la criba de Eratóstenes

Definición 4.5. Un entero $p > 1$ es un *número primo* si sus únicos divisores son 1 y p. En caso contrario se llama compuesto.

Observación 4.10. Se cumplen las siguientes propiedades de demostración inmediata:

1) Todo entero n admite a 1 y n como divisores, son los llamados *divisores triviales*. Los demás (si los tiene) son los *divisores propios*. Así un número p es primo si sólo no posee divisores propios;

2) 1 no es primo;

3) el menor primo es el 2, que es además el único primo par;

4) los números primos son los que no se pueden factorizar, es decir, los que no se pueden escribir como producto $p = ab$ con $1 < a < p$ y $1 < b < p$;

5) si p es primo y a es un entero cualquiera,

$$\text{MCD}(a, p) = \begin{cases} p & \text{si} \quad p \mid a \\ 1 & \text{si} \quad p \nmid a \end{cases}$$

Lema 4.12. *Si p es primo y a y b son enteros tales que $p \mid ab$, entonces $p \mid a$ o $p \mid b$.*

Demostración: Si $p \nmid a$, es MCD$(a, p) = 1$. El lema 4.7 de Euclides garantiza que $p \mid b$. ∎

Observación 4.11. Esto sólo sucede para primos; por ejemplo $6 \mid 2 \cdot 3$, pero $6 \nmid 2$ y $6 \nmid 3$.

Corolario 4.13. ***(Teorema de Pitágoras)*** *El número $\sqrt{2}$ es irracional.*

Demostración: Si $\sqrt{2}$ fuera racional, sería $\sqrt{2} = \frac{a}{b}$ con a y b enteros, $b > 0$. Simplificando la fracción si es necesario, podemos suponer que a y b son primos entre sí. Elevando al cuadrado, queda $2b^2 = a^2$, por lo que $2 \mid a^2 = aa$. Como 2 es primo, se deduce que $2 \mid a$. Luego existe un entero r tal que $a = 2r$. Sustituyendo, es $2b^2 = a^2 = 4r^2$, es decir, $b^2 = 2r^2$, por lo que $2 \mid b$, lo que contradice que a y b sean coprimos. ∎

Corolario 4.14. *Si p es primo y $a_1, \ldots, a_n$ son enteros tales que $p \mid a_1 \ldots a_n$, entonces $p \mid a_i$ para algún $i \in \{1, \ldots, n\}$.*

Corolario 4.15. *Si p es primo y $p_1, \ldots, p_n$ son primos tales que $p \mid p_1 \ldots p_n$, entonces p es igual a, al menos, uno de los factores $p_1, \ldots, p_n$.*

La criba de Eratóstenes para $n = 150$

El problema de encontrar los primos menores que un número dado n se hace difícil cuando n es grande. Una técnica llamada la *criba de Eratóstenes* representa un método razonable para obtener una lista completa de los primos menores o iguales que n cuando

n es relativamente pequeño. Consiste en escribir la lista completa de los enteros entre 2 y n, para después ir tachando cada segundo número después del 2 –los múltiplos de 2, que son compuestos–, cada tercer número después del 3 –los múltiplos de 3, que son compuestos–, etc. En esta pasada, muchos números se tachan más de una vez. El proceso termina cuando se han eliminado todos los múltiplos de p para p primo y $p \leq \sqrt{n}$ – la razón se explica en la proposición 4.21– se han eliminado. Los enteros que quedan después de esta criba son todos los primos menores o iguales a n.

Ejemplo 4.9. La criba de Eratóstenes para $n = 150$. Los primos buscados están rodeados con un círculo. Observar que, excepto para los primos 2 y 3, todo primo de la tabla está en la primera o la quinta columna. Los enteros localizados en estas columnas son de la forma $6k + 1$ ó $6k - 1$, donde k es un entero positivo. Esto no es casualidad.

Solución: En efecto, si p es primo $p > 3$, debe ser impar, por lo tanto de la forma $6k + 1$, $6k + 3$ ó $6k + 5$. Pero un número de la forma $6k + 3$ no es primo, y $6k + 5 = 6(k + 1) - 1$. ∎

4.6. El Teorema Fundamental de la Aritmética

Teorema 4.16. *Todo entero $n > 1$ se puede escribir como producto de primos $n = p_1 p_2 \dots p_r$. Además, esta expresión es única salvo el orden de los factores.*

Demostración: 1) Existencia de la factorización: sea S el conjunto de los enteros mayores que 1 que no son producto de primos, y supongamos que es no vacío. Como $S \subset \mathbb{N}$ está bien ordenado, sea a su primer elemento. Pero a no puede ser primo, pues si $a = p$, a sería una factorización de a como producto de primos. Luego $a = mn$ con $1 < m < a$ y $1 < n < a$. Pero a es el menor elemento de S, con lo que $m \notin S$ y $n \notin S$, es decir, m y n si pueden factorizarse en productos de primos $m = p_1 p_2 \dots p_r$ y $n = q_1 q_2 \dots q_s$. Entonces, $a = p_1 p_2 \dots p_r q_1 q_2 \dots q_s$, que es un producto de primos, con lo que llegamos a un absurdo. Luego $S = \emptyset$.

2) Unicidad salvo el orden de los factores: supongamos que tenemos dos factorizaciones $n = p_1 p_2 \dots p_r$ y $n = q_1 q_2 \dots q_s$, donde ordenamos los primos en orden creciente: $p_1 \leq p_2 \leq \dots \leq p_r$ y $q_1 \leq q_2 \leq \dots \leq q_s$. Se trata de probar que $r = s$ y para cada índice $p_i = q_i$. Como $n = p_1 p_2 \dots p_r = q_1 q_2 \dots q_s$, p_1 divide a $q_1 q_2 \dots q_s$, luego $p_1 = q_k$ para algún k. En particular, $p_1 \geq q_1$. Del mismo modo, q_1 divide a $p_1 p_2 \dots p_r$, con lo que $q_1 = p_i$ para algún i, y en particular, $q_1 \geq p_1$. Así, $p_1 = q_1$. Eliminando este factor en la factorización de n, se deduce que $p_2 \dots p_r = q_2 \dots q_s$. Repitiendo el argumento, se llega a que $p_2 = q_2$. Por lo tanto, $p_3 \dots p_r = q_3 \dots q_s$. Si por ejemplo fuese $r < s$, tras sucesivas cancelaciones llegaríamos a $1 = q_{r+1} q_{r+2} \dots q_s$, lo que es imposible porque todos los primos son mayores que 1. ∎

El Teorema Fundamental de la Aritmética se ha demostrado para $n > 1$. Si $n < -1$, como $-n > 1$, obtenemos una factorización de la forma $-n = p_1 p_2 \dots p_r$, con lo que $n = -p_1 p_2 \dots p_r$. En ambas factorizaciones, los primos pueden estar repetidos. Si agrupamos los que son iguales entre sí, se obtiene lo que se llama la *factorización canónica* de un entero n:

Teorema 4.17. ***(Teorema Fundamental de la Aritmética)*** *Todo entero $n \neq 0, \pm 1$ se puede escribir de manera única de la forma*

$$n = \pm p_1^{k_1} p_2^{k_2} \dots p_r^{k_r},$$

donde $p_1 < p_2 < \cdots < p_r$ son primos y $k_i > 0$ para cada índice.

Proposición 4.18. *Si $n = p_1^{k_1} p_2^{k_2} \dots p_r^{k_r}$ donde $p_1 < p_2 < \cdots < p_r$ son primos y $k_i > 0$ para cada índice, y $m \mid n$, entonces $m = p_1^{h_1} p_2^{h_2} \dots p_r^{h_r}$, con $h_i \leq k_i$ para cada i.*

Demostración: Si $m \mid n$, es $n = cm$ para algún entero c. Consideremos las factorizaciones en primos $m = q_1^{h_1} q_2^{h_2} \dots q_s^{h_r}$ y $c = r_1^{l_1} r_2^{l_2} \dots r_t^{l_t}$. Entonces

$$p_1^{k_1} p_2^{k_2} \dots p_r^{k_r} = q_1^{h_1} q_2^{h_2} \dots q_s^{h_r} r_1^{l_1} r_2^{l_2} \dots q_t^{l_t}$$

Por el teorema 4.17 fundamental de la aritmética, los primos y las potencias a cada lado deben ser iguales. Así, cada q_j debe coincidir con algún p_i y su potencia $h_j \leq k_i$. ∎

La técnica de la factorización puede utilizarse para calcular máximos comunes divisores y mínimos comunes múltiplos, evitando el algoritmo de Euclides:

Proposición 4.19. *Si $n = p_1^{k_1} p_2^{k_2} \dots p_r^{k_r}$ y $m = p_1^{h_1} p_2^{h_2} \dots p_r^{h_r}$ donde $p_1 < p_2 < \cdots < p_r$ son primos y $k_i, h_i \geq 0$ para cada índice, entonces:*

(i) $\mathit{MCD}(m,n) = p_1^{\min(k_1,h_1)} p_2^{\min(k_2,h_2)} \dots p_r^{\min(k_r,h_r)}$;

(ii) $\mathit{mcm}(m,n) = p_1^{\max(k_1,h_1)} p_2^{\max(k_2,h_2)} \dots p_r^{\max(k_r,h_r)}$;

(iii) $mn = \mathit{mcm}(m,n) \cdot \mathit{MCD}(m,n)$.

El sistema para factorizar es ir probando de manera creciente si los primos 2, 3, 5, 7, etc. dividen n. Pero hay un truco para ahorrar comprobaciones: cuando la sucesión creciente de divisores "se cruza" con la sucesión decreciente de cocientes, se puede parar. Esto sucede cuando llegamos al primo más cercano –y menor que– a $\sqrt{n}$:

Proposición 4.20. *Si un entero n no es primo (es compuesto), admite un divisor primo $p \leq \sqrt{n}$.*

Demostración: Sea p el menor divisor primo de n, entonces $n = pa$ con a un producto de primos mayores o iguales que p. Luego, $p \leq a$, es decir, $p^2 \leq pa$, con lo que

$$\sqrt{p^2} = p \leq \sqrt{pa} = \sqrt{n}. \qquad \blacksquare$$

Esta proposición puede reformularse del siguiente modo:

Proposición 4.21. *Si n es un entero tal que ningún primo $p \leq \sqrt{n}$ lo divide, entonces n es primo.*

A pesar de que la anterior propiedad simplifica la factorización de un número en primos, el cálculo de los factores puede ser muy complicado, incluso para ordenadores potentes. En esta propiedad se basa precisamente la criptografía, en encriptar mensajes por medio de enteros, de manera que sea "imposible" encontrar la factorización en un tiempo razonable.

Corolario 4.22. *Existen infinitos números primos.*

Demostración: Consideremos la familia de los primos en orden creciente y supongamos que es finita:

$$p_1 = 2, p_2 = 3, p_3 = 5, \ldots p_n.$$

Sea el entero $N = p_1 p_2 p_3 \ldots p_n + 1$. Como $N > 1$, el Teorema Fundamental de la Artimética asegura que N puede factorizarse en producto de primos. Sea p uno de ellos. Como $p_1, p_2, p_3, \ldots p_n$ es la lista de todos ellos, debe existir un índice i tal que $p = p_i$. Así, $p \mid p_1 p_2 p_3 \ldots p_n$ y $p \mid p_1 p_2 p_3 \ldots p_n + 1$, luego $p \mid 1$, lo que es imposible. $\blacksquare$

4.7. Ejercicios

1.- Sea a un entero. Demostrar que:

1) $2 \mid a(a+1)$ y $6 \mid a(a+1)(a+2)$;

2) $2 \mid a(2a^2+7)$;

3) si a es impar, $32 \mid (a^2+3)(a^2+7)$.

2.- Sean a y b dos enteros primos entre sí. Se pide:

1) demostrar que si $d \mid b$, entonces MCD$(a, d) = 1$;

2) probar que MCD$(ac, b) =$ MCD(c, b) y usarlo para calcular MCD$(5000, 31768)$;

3) hallar un entero a tal que MCD$(4, a) = 2$ y mcm$(8, a) = 56$.

3.- Sea $p > 3$ un número primo. Probar:

1) p es de la forma $6q + 1$ ó $6q + 5$;

2) $p^2 + 2$ no es primo.

4.- Calcular la factorización canónica de 120497 y de 111111.

5.- Se pide probar las siguientes propiedades:

1) un entero $n > 1$ es un cuadrado perfecto (es decir, $n = a^2$) si y sólo si todos los exponentes que aparecen en su factorización canónica son pares;

2) un entero $n > 1$ es un producto de un cuadrado perfecto y de un cubo perfecto si y sólo si todos los exponentes que aparecen en su factorización son mayores o iguales a 2.

6.- Encontrar todos los enteros positivos a y b tales que MCD$(a, b) = 12$ y mcm$(a, b) = 504$.

7.- Si n es un entero positivo, probar que $\sqrt{n}$ es racional si y sólo si n es un cuadrado perfecto.

8.- Si n y m son enteros positivos primos entre sí, probar que si mn es una potencia k-ésima de algún entero, entonces ambos n y m son potencias k-ésimas de enteros.

9.- Probar que todo primo impar es de la forma $4k + 1$ ó $4k - 1$.

10.- Probar que existe un número infinito de primos de la forma $6k - 1$.

11.- Aunque el número de primos es infinito (corolario 4.22), se puede probar –excede los contenidos de este curso– que la distribución de los primos disminuye constantemente, es decir, si denotamos por $\pi(n)$ al número de primos menores o iguales a n, entonces $\dfrac{\pi(n)}{n}$ decrece si n crece. De hecho, se puede probar que $\lim\limits_{n\to\infty} \dfrac{\pi(n)\log_e(n)}{n} = 1$, propiedad que se llama *teorema del número primo*. Se pide:

1) encontrar una sucesión de 10 enteros consecutivos todos ellos compuestos;

2) probar que para cada $n \in \mathbb{N}$, la sucesión

$$(n+1)! + 2, (n+1)! + 3, \ldots, (n+1)! + n, (n+1)! + (n+1)$$

consta de n enteros compuestos consecutivos.

12.- Dos enteros impares consecutivos se llaman *primos gemelos*, si ambos son primos. Se pide:

1) probar que 1997 y 1999 son primos gemelos;

2) encontrar un par de primos gemelos entre 400 y 500;

3) no se sabe aún si existen infinitos pares de primos gemelos. Probar que el número de primos triples (tres impares consecutivos, todos ellos primos) es uno; de hecho, esa única familia es $\{3, 5, 7\}$. Indicación: usar el ejemplo 4.9.

13.- Usar la criba de Eratóstenes para construir la lista de todos los primos menores que 200 y que 300.

14.- Si $n \in \mathbb{N}$, llamamos $\sigma(n)$ a la suma de sus divisores positivos. Se pide:

1) si $n = p_1^{k_1} p_2^{k_2} \dots p_r^{k_r}$ es la factorización canónica de n, probar que

$$\sigma(n) = \frac{p^{k_1+1} - 1}{p_1 - 1} \cdot \frac{p^{k_2+1} - 1}{p_2 - 1} \dots \frac{p^{k_r+1} - 1}{p_r - 1};$$

2) resolver la ecuación $\sigma(n) = 60$;

3) probar que $\sigma \colon \mathbb{N} \longrightarrow \mathbb{N}$ es una *función numérica multiplicativa*, es decir, $\sigma(mn) = \sigma(m)\sigma(n)$ si m y n son coprimos;

4) una función numérica $f \colon \mathbb{N} \longrightarrow \mathbb{N}$ se llama *multiplicativa completa* si $f(mn) = f(m)f(n)$ para cualquier par de enteros. Probar que σ no es una función multiplicativa completa.

15.- Si $n \in \mathbb{N}$, llamamos $\nu(n)$ a su número de divisores positivos. Se pide:

1) si $n = p_1^{k_1} p_2^{k_2} \dots p_r^{k_r}$ es la factorización canónica de n, probar que

$$\nu(n) = (k_1 + 1) \cdot (k_2 + 1) \dots (k_r + 1);$$

2) encontrar el menor entero positivo n que tiene 10 divisores positivos;

3) demostrar que si $\nu(n) = 2$, entonces n es primo;

4) demostrar que la ecuación $\nu(n) = m$, donde m es un entero positivo mayor que 1 tiene infinitas soluciones;

5) demostrar que $\nu(n)$ es impar si y sólo si n es un cuadrado perfecto;

6)probar que $\nu\colon \mathbb{N} \longrightarrow \mathbb{N}$ es una función numérica multiplicativa, pero no es multiplicativa completa.

16.- Un entero positivo n se llama *número perfecto* si es igual a la suma de todos sus divisores positivos diferentes de sí mismo, de otro modo, $\sigma(n) = 2n$. Se denota por p_n al n-ésimo número perfecto. Observar que:

$$p_1 = 6 = (110)_2 = 2(2^2 - 1), \quad p_2 = 28 = (11100)_2 = 2^2(2^3 - 1),$$

$$p_3 = 496 = (111110000)_2 = 2^4(2^5 - 1), \quad p_4 = 8128 = (1111111000000)_2 = 2^6(2^7 - 1),$$

donde los factores de la forma $2^n - 1$ son primos (3, 7, 31 y 127 en los casos anteriores). Se pide probar:

1) un entero par es un número perfecto si y sólo si es de la forma $2^{p-1}(2^p - 1)$, donde $2^p - 1$ es un primo;

2) demostrar que 130816 no es un número perfecto;

3) demostrar que la suma de los recíprocos de los divisores positivos de un número perfecto par es 2.

17.- Dos enteros positivos m y n se llaman *números amigos* si su suma es igual a la suma de los divisores positivos de cada uno de ellos, es decir, $\sigma(m) = m + n = \sigma(n)$. Comprobar que los siguientes pares son de números amigos $\{220, 284\}$ y $\{17296, 18416\}$.

18.- Probar que si un número de la forma $2^p - 1$ es primo, entonces p es primo. Los números de la forma denominan $2^p - 1$ con p primo se llaman *números de Mersenne* y se denotan por M_p. Si además $M_p = 2^p - 1$ es primo, se habla de un *primo de Mersenne*. A cada primo de Mersenne M_p se le puede asociar un número perfecto par $2^{p-1}M_p$, por ejemplo,

$$M_2 = 2^2 - 1 = 3 \text{ le corresponde el número perfecto par } 2(2^2 - 1) = 6,$$

$$M_3 = 2^3 - 1 = 7 \text{ le corresponde el número perfecto par } 2^2(2^3 - 1) = 28,$$

$$M_4 = 2^4 - 1 = 31 \text{ le corresponde el número perfecto par } 2^3(2^4 - 1) = 496,$$

$$M_5 = 2^5 - 1 = 127 \text{ le corresponde el número perfecto par } 2^4(2^5 - 1) = 8128, \text{ etc.}$$

Se pide comprobar:

1) todo número perfecto par termina en 6 u 8. Indicación: usar el ejercicio **9** y probar previamente que si $n \in \mathbb{N}$, entonces 16^n termina en 6;

2) un número primo no puede ser un número perfecto;

3) ninguna potencia de un primo es un número perfecto.

Capítulo 5

Congruencias

Se equivocó la paloma,
se equivocaba.
Por ir al norte, fue al sur.
Creyó que el trigo era agua.
Se equivocaba.

Metamorfosis del clavel
Rafael Alberti (1902–1999)

5.1. Congruencias

Una de las herramientas más potentes para abordar cuestiones de divisibilidad es el lenguaje de las *congruencias*, introducido por Gauss en sus *Disquisitiones Arithmaticae* en 1801.

Definición 5.1. Sea n un entero positivo. Diremos que los enteros a y b son *congruentes módulo* n, y se representa como $a \equiv b (\text{mód } n)$, si al dividirlos por n dan el mismo resto. Al número n se le llama *módulo* de la congruencia.

Ejemplo 5.1. Algunos casos particulares son los siguientes:

1) al dividir cualquier entero por $n = 1$ se obtiene resto 0, es decir, todos los enteros son congruentes módulo 1;

2) si $n = 2$, los dos únicos restos posibles son 0 y 1. Los que dan resto 0 son los pares y los que dan resto 1 son los impares;

3) para $n = 5$, es $9 \equiv 19 (\text{mód } 5)$, $-13 \equiv 2 (\text{mód } 5)$ ó $5 \equiv -5 (\text{mód } 5)$. En general, se pueden clasificar los infinitos números enteros en 5 clases $(\text{mód } 5)$.

Lema 5.1. *$a \equiv b$(mód n) si y sólo si $a - b$ es múltiplo de n.*

Demostración: Si $a \equiv b$(mód n), podemos escribir

$$a = q_1 n + r \quad \text{y} \quad b = q_2 n + r \quad \text{con } 0 \leq r < n.$$

Restando ambas expresiones, se obtiene $a - b = (q_1 - q_2)n$. Y recíprocamente, supongamos que $a - b$ es múltiplo de n y que

$$a = q_1 n + r_1 \quad \text{y} \quad b = q_2 n + r_2 \quad \text{con } 0 \leq r_1, r_2 < n.$$

Restando ambas expresiones, se obtiene $a - b = (q_1 - q_2)n + (r_1 - r_2)$ y despejando, $r_1 - r_2 = (a - b) - (q_1 - q_2)n$, que es múltiplo de n, es decir, es $r_1 - r_2 = 0$. ∎

Proposición 5.2. *Sean un entero $n > 1$ y a, b, c, d, k enteros. Se cumplen las siguientes propiedades:*

1) propiedad reflexiva: $a \equiv a$(mód n);

2) propiedad simétrica: si $a \equiv b$(mód n), entonces $b \equiv a$(mód n);

3) propiedad transitiva: si $a \equiv b$(mód n) y $b \equiv c$(mód n), entonces $a \equiv c$(mód n);

4) si $a \equiv b$(mód n) y $c \equiv d$(mód n), entonces

$$a + c \equiv b + d(\text{mód } n) \quad y \quad ac \equiv bd(\text{mód } n);$$

5) Si $a \equiv b$(mód n), entonces

$$a \pm k \equiv b \pm k(\text{mód } n) \quad y \quad ak \equiv bk(\text{mód } n);$$

6) Si $a \equiv b$(mód n), entonces $a^m \equiv b^m$(mód n) para todo entero positivo m;

7) Si $a \equiv b$(mód n) y $p(x)$ es una función polinómica en x con coeficientes enteros, entonces $p(a) \equiv p(b)$(mód n).

Demostración: 1), 2) y 3) son triviales y dicen que la relación "ser congruente módulo n" es una relación de equivalencia sobre el conjunto $\mathbb{Z}$. 4) Si $a \equiv b$(mód n) y $c \equiv d$(mód n), entonces $a - b = q_1 n$ y $c - d = q_2 n$. Sumando ambas ecuaciones $(a + c) - (b + d) = (q_1 + q_2)n$, que es múltiplo de n, o lo que es lo mismo $a + c \equiv b + d$(mód n). Del mismo modo, como $a = b + q_1 n$ y $c = d + q_2 n$, multiplicando ambas igualdades queda

$$ac = (b + q_1 n)(d + q_2 n) = bd + (bq_2 + dq_1 + q_1 q_2 n)n,$$

es decir $ac - db$ es múltiplo de n. 5) es consecuencia de 4) al ser $k \equiv k$(mód n). 6) se deduce de 4) al multiplicar la congruencia $a \equiv b$(mód n) por sí misma m veces. Y 7) es una consecuencia de 4), 5) y 6). ∎

Ejemplo 5.2. Calcular el resto de la división entre 12 del número

$$n = 1! + 2! + 3! + \cdots + 99! + 100!.$$

Solución: En el lenguaje de las congruencias, se trata de encontrar un entero r entre 0 y 12 tal que $n \equiv r(\text{mód } 12)$, es decir, hay que *reducir* n módulo 12. En primer lugar, $4! = 24 \equiv 0(\text{mód } 12)$, por lo que si $k \geq 4$, es

$$k! = k(k-1)\ldots 6 \cdot 5 \cdot 4! \equiv k(k-1)\ldots 6 \cdot 5 \cdot 0 \equiv 0(\text{mód } 12).$$

Así, $n \equiv 1! + 2! + 3!(\text{mód } 12)$, luego $n \equiv 9(\text{mód } 12)$. ∎

Ejemplo 5.3. Para todo $k \geq 1$, $7 \mid (5^{2k} + 3 \cdot 2^{5k-2})$.

Solución: Hay que probar que al dividir $5^{2k} + 3 \cdot 2^{5k-2}$ por 7 sale resto 0. Tenemos las siguientes congruencias módulo 7:

$$5^{2k} + 3 \cdot 2^{5k-2} \equiv 5^{2k} + (-2^2) \cdot 2^{5k-2} \equiv 5^{2k} - 2^{5k} \equiv 25^k - 32^k(\text{mód } 7)$$

al ser $3 \equiv -2^2(\text{mód } 7)$ y aplicando 4) de la proposición 5.2. Como $25 \equiv 4(\text{mód } 7)$ y $32 \equiv 4(\text{mód } 7)$, aplicando 6) de la proposición 5.2, se deduce que:

$$5^{2k} + 3 \cdot 2^{5k-2} \equiv 25^k - 32^k \equiv 4^k - 4^k \equiv 0(\text{mód } 7). \quad ∎$$

Las propiedades anteriores prueban que se pueden pensar las congruencias practicamente como igualdades. Aunque no se puede usar la propiedad de cancelación en los productos, existen resultados parciales:

Proposición 5.3. *Si $ak \equiv bk(\text{mód } n)$, entonces $a \equiv b(\text{mód } \frac{n}{d})$, donde $d = MCD(k, n)$.*

Demostración: Como $d = \text{MCD}(k, n)$, se puede escribir $k = dk'$ y $n = dn'$, con $\text{MCD}(k', n') = 1$. Por hipótesis, $ka - kb = qn$ para algún entero q, de otra manera es $dk'a - dk'b = qdn'$, y dividiendo por d, es $k'a - k'b = qn'$. Luego, $n' \mid k'(a-b)$, es decir, $a \equiv b(\text{mód } n')$. ∎

Corolario 5.4. *Si $ak \equiv bk(\text{mód } n)$ y k y n son primos entre sí, entonces $a \equiv b(\text{mód } n)$.*

Corolario 5.5. *Si $ak \equiv bk(\text{mód } p)$ con p primo y $p \nmid k$, entonces $a \equiv b(\text{mód } p)$.*

Ejemplos 5.1. Algunas aplicaciones de los anteriores resultados son:

1) $6 \equiv 4(\text{mód } 4)$ se puede cambiar por $3 \equiv 2(\text{mód } \frac{4}{d})$, donde $d = \text{MCD}(2, 4)$; es decir, $3 \equiv 2(\text{mód } 2)$.

2) $44 \equiv 8(\text{mód } 9)$ se puede cambiar por $11 \equiv 2(\text{mód } \frac{9}{d})$, donde $d = \text{MCD}(11, 9)$, es decir, $11 \equiv 2(\text{mód } 9)$.

Ejemplo 5.4. Un entero en numeración decimal es divisible por 9 si y sólo si la suma de sus dígitos es divisible por 9.

Solución: En efecto, sea la representación decimal

$$n = a_0 + a_1 \cdot 10 + a_2 \cdot 10^2 + \cdots + a_k \cdot 10^k,$$

donde a_i es un entero $0 \leq a_i \leq 9$. Como $10 \equiv 1(\text{mód } 9)$, por 6) de la proposición 5.2, es $10^i \equiv 1(\text{mód } 9)$ y $a_i \cdot 10^i \equiv a_i(\text{mód } 9)$, luego $n \equiv a_1 + a_2 + \cdots + a_n(\text{mód } 9)$. ∎

5.2. Criterios de divisibilidad

Teorema 5.6. ***(Pequeño teorema de Fermat)*** *Si p es primo y $p \nmid a$, entonces*

$$a^{p-1} \equiv 1(\textit{mód } p).$$

Demostración: Sean los primeros $p-1$ múltiplos positivos de a: $a, 2a, \ldots, (p-1)a$. Éstos son dos a dos no congruentes entre sí módulo p. En efecto, si fuese $sa \equiv ta(\text{mód } p)$ con $s \neq t$, cancelando a, sería $s \equiv t(\text{mód } p)$, lo cual es imposible al ser s y t menores que p. Al ser dos a dos no congruentes, dan $p-1$ restos diferentes al dividirlos por p. Ninguno de ellos puede ser 0, ya que si $sa \equiv 0(\text{mód } p)$, cancelando a, sería $s \equiv 0(\text{mód } p)$, lo que es imposible al ser $1 \leq s \leq p-1$. Por lo tanto, con esos $p-1$ números obtenemos los restos $1, 2, \ldots p-1$. Luego los números $a, 2a, \ldots (p-1)a$ son congruentes, en algún orden, con $1, 2, \ldots p-1$. Multiplicando todas estas congruencias, obtenemos:

$$a \cdot 2a \cdot 3a \ldots (p-1)a \equiv 1 \cdot 2 \cdot 3 \ldots (p-1)(\text{mód } p),$$

es decir,

$$1 \cdot 2 \cdot 3 \ldots (p-1)a^{p-1} \equiv 1 \cdot 2 \cdot 3 \ldots (p-1)(\text{mód } p),$$

y cancelando, $a^{p-1} \equiv 1(\text{mód } p)$.

Ejemplo 5.5. Calcular el resto de la división de 614^{6943} entre 17.

Solución: Como $614 \equiv 2(\text{mód } 17)$ $(614 = 36 \cdot 17 + 2)$, es $614^{6943} \equiv 2^{6943}(\text{mód } 17)$. Como $17 \nmid 2$, el teorema 5.6 garantiza que $2^{16} \equiv 1(\text{mód } 17)$. Como $6943 = 433 \cdot 16 + 15$,

$$2^{6943} \equiv 2^{433 \cdot 16 + 15} \equiv (2^{16})^{433} 2^{15} \equiv 1^{433} 2^{15} \equiv 2^{15}(\text{mód } 17).$$

Y finalmente, como $2^4 \equiv 16 \equiv -1(\text{mód } 17)$, es

$$2^{15} \equiv 2^{4 \cdot 3 + 3} \equiv (2^4)^3 2^3 \equiv (-1)^3 2^3 \equiv -8 \equiv 9(\text{mód } 17).$$

Así, el resto buscado es 9. ∎

Proposición 5.7. *Si p y q son números primos distintos y a un entero tal que $p \nmid a$ y $q \nmid a$, entonces $a^{(p-1)(q-1)} \equiv 1 (\text{mód } pq)$.*

Demostración: Por el pequeño teorema de Fermat (teorema 5.6), sabemos que $a^{p-1} \equiv 1(\text{mód } p)$. Aplicando 6) de la proposición 5.2, se deduce que $a^{(p-1)(q-1)} \equiv 1(\text{mód } p)$. De manera similar, al ser $a^{q-1} \equiv 1(\text{mód } q)$, se deduce que $a^{(p-1)(q-1)} \equiv 1(\text{mód } q)$. Como $p \mid a^{(p-1)(q-1)} - 1$ y $q \mid a^{(p-1)(q-1)} - 1$ y ambos son primos distintos, $pq \mid a^{(p-1)(q-1)} - 1$, o lo que es lo mismo, $a^{(p-1)(q-1)} \equiv 1(\text{mód } pq)$. ∎

5.3. Congruencias lineales

Definición 5.2. Si m es un entero positivo y $a, b \in \mathbb{Z}$, la ecuación $ax \equiv b(\text{mód } m)$ con incógnita $x \in \mathbb{Z}$, se llama una *congruencia lineal*.

Ejemplo 5.6. Resolver la congruencia lineal $4x \equiv 2(\text{mód } 28)$.

Solución: Si $x \in \mathbb{Z}$ es solución de esta ecuación, entonces $4x = 2+28n$ para algún $n \in \mathbb{Z}$, lo que es obviamente imposible porque la parte izquierda de la igualdad es divisible por 4, pero la derecha no lo es. ∎

Ejemplo 5.7. Resolver la congruencia lineal $13x \equiv 2(\text{mód } 31)$.

Solución: Si $x \in \mathbb{Z}$ es solución de esta ecuación, entonces $13x = 2 + 31n$ para algún $n \in \mathbb{Z}$. Observemos que MCD$(13, 31) = 1$, luego por el corolario 4.6, existen enteros s, t tales que $1 = 13s + 31t$. Luego, $13s \equiv 1(\text{mód } 31)$, y multiplicando esta congruencia por 2, queda $13(2s) \equiv 2(\text{mód } 31)$, luego $x = 2s$ ($s \in \mathbb{Z}$) es una solución de la congruencia planteada. ∎

El ejemplo anterior da la clave de la solución de las congruencias lineales:

Proposición 5.8. *La congruencia lineal $ax \equiv b(\text{mód } m)$ tiene solución $x \in \mathbb{Z}$ si y sólo si $d = MCD(a, m)$ divide a b. En tal caso, hay exactamente d soluciones no congruentes.*

Demostración: Supongamos que $x \in \mathbb{Z}$ es una solución de la congruencia lineal. Entonces $ax = qm + b$ para algún $q \in \mathbb{Z}$. Como $d \mid a$ y $d \mid m$, se deduce que $d \mid b$. Recíprocamente, supongamos que $d \mid b$ y sea $b = kd$ con $k \in \mathbb{Z}$. Por la proposición 4.4, existen enteros s, t tales que $d = sa + tm$. Multiplicando por k, queda $b = kd = ksa + ktm$, luego $aks = b - ktm \equiv b(\text{mód } m)$. Si x_0 y x_1 son dos soluciones de $ax \equiv b(\text{mód } m)$, aplicando la proposición 5.3, es $x_1 \equiv x_0(\text{mód } \frac{m}{d})$. Las d soluciones incongruentes de la congruencia dada son:

$$\{x_0, x_0 + \frac{m}{d}, x_0 + 2\frac{m}{d}, \ldots, x_0 + (d-1)\frac{m}{d}\}. \qquad \blacksquare$$

Ejemplo 5.8. Probar el **teorema de Wilson**: *si p es primo, se verifica la congruencia* $(p-1)!+1 \equiv 0(\textit{mód}\ p)$.

Solución: En efecto, por el pequeño teorema de Fermat (teorema 5.6) la congruencia $x^{p-1} \equiv 1(\text{mód}\ p)$ (equivalentemente, $x^{p-1}-1 \equiv 0(\text{mód}\ p)$) tiene $p-1$ soluciones diferentes $1, 2, \ldots, p-1$. Luego,

$$x^{p-1}-1 \equiv (x-1)(x-2)\ldots(x-(p-1))(\text{mód}\ p).$$

Como cualquier valor de x satisface esta congruencia, si hacemos $x=0$, será

$$-1 \equiv (-1)(-2)\ldots(-(p-1))(\text{mód}\ p) \equiv (-1)^{p-1}1\cdot 2\ldots(p-1)(\text{mód}\ p),$$

es decir, $(-1)^{p-1}\cdot(p-1)!+1 \equiv 0(\text{mód}\ p)$. Si $p=2$, queda $-1+1 \equiv 0(\text{mód}\ 2)$ y si p es impar, queda que $(p-1)!+1 \equiv 0(\text{mód}\ p)$. ∎

5.4. La función ϕ de Euler

Definición 5.3. Si $n \in \mathbb{N}$, denotamos por $\phi(n)$ al número de enteros positivos menores o iguales que n y que son coprimos con n (por definición, $\phi(1)=1$), y se llama la *función ϕ de Euler*.

Proposición 5.9. *Si p primo, $\phi(p)=p-1$.*

Proposición 5.10. *Si p primo y $n \in \mathbb{N}$, es $\phi(p^n)=p^n-p^{n-1}$.*

Demostración: Los enteros positivos menores o iguales a p^n y que no son coprimos con p^n son

$$p, 2p, 3p, \ldots p^2, 2p^2, 3p^2, \ldots, p^{n-2}, 2p^{n-2}, 3p^{n-2}, \ldots p^{n-1}p,$$

es decir, hay p^{n-1} de tales enteros. Por lo tanto, $\phi(p^n)=p^n-p^{n-1}=p^{n-1}(p-1)=p^n(p-\frac{1}{p})$. ∎

Corolario 5.11. *Si p primo y $n \in \mathbb{N}$,* $\displaystyle\sum_{i=0}^{n}\phi(p^i)=p^n$.

Demostración: Aplicando la proposición 5.10

$$\sum_{i=0}^{n}\phi(p^i)=\phi(p^0)+\sum_{i=1}^{n}\left(p^i-p^{i-1}\right)=1+(p-1)\sum_{i=1}^{n}p^{i-1}=$$

$$\phi(1)+(p-1)\frac{p^n-1}{p-1}=1+p^n-1=p^n. \qquad \blacksquare$$

Teorema 5.12. *Si $n = p_1^{k_1} p_2^{k_2} \dots p_r^{k_r}$ es la factorización canónica de $n \in \mathbb{N}$, entonces*

$$\phi(n) = \prod_{i=1}^{r} (p_i^{k_i} - p_i^{k_i - 1}) = n \prod_{i=1}^{r} (1 - \frac{1}{p_i}).$$

Demostración: Se demuestra por inducción. El número de enteros positivos menores o iguales a n que no son divisibles por p_1 está dado claramente por la expresión $n - \frac{n}{p_1}$. Supongamos que el números de enteros positivos menores o iguales a n y que no son divisibles por $p_1, p_2, \dots, p_s$ (con $s < r$) viene dado por la expresión:

$$n(1 - \frac{1}{p_1})(1 - \frac{1}{p_2}) \dots (1 - \frac{1}{p_s}).$$

Los múltiplos de p_{s+1} menores o iguales a n son $p_{s+1}, 2p_{s+1}, \dots, \frac{n}{p_{s+1}} p_{s+1}$. De éstos, los números que no son múltiplos de $p_1, p_2, \dots, p_s$ son aquellos en los que los coeficientes de p_{s+1} (es decir, $1, 2, 3, \dots, \frac{n}{p_{s+1}}$) no son divisibles por $p_1, p_2, \dots, p_s$. Por la hipótesis de inducción, el número de tales enteros positivos está dado por la expresión:

$$\frac{n}{p_{s+1}}(1 - \frac{1}{p_1})(1 - \frac{1}{p_2}) \dots (1 - \frac{1}{p_s}).$$

Por lo tanto, el número de enteros positivos menores o iguales a n que no son divisibles por $p_1, p_2, \dots p_{s+1}$ está dado por la expresión:

$$n(1 - \frac{1}{p_1})(1 - \frac{1}{p_2}) \dots (1 - \frac{1}{p_s}) - \frac{n}{p_{s+1}}(1 - \frac{1}{p_1})(1 - \frac{1}{p_2}) \dots (1 - \frac{1}{p_s}) =$$

$$n(1 - \frac{1}{p_1})(1 - \frac{1}{p_2}) \dots (1 - \frac{1}{p_{s+1}}). \qquad \blacksquare$$

Proposición 5.13. *Si $n > 1$, la suma de los enteros positivos menores o iguales a n y coprimos con n es $\frac{1}{2} n\phi(n)$.*

Demostración: Sean $m_1, m_2, \dots, m_{\phi(n)}$ los enteros positivos menores o iguales a n y coprimos con n. La suma de estos enteros es:

$$S = m_1 + m_2 + \dots + m_{\phi(n)}.$$

Para cada $i \in \{1, \dots, \phi(n)\}$, $n - m_i$ y n son primos entre sí, luego los enteros positivos menores o iguales a n y coprimos con n se pueden expresar también del modo:

$$(n - m_1), (n - m_2), \dots, (n - m_{\phi(n)}),$$

luego

$$S = (n - m_1) + (n - m_2) + \dots + (n - m_{\phi(n)}).$$

Sumando ambas expresiones para S, se obtiene:

$$2S = n + \overbrace{\dots}^{\phi(n)} + n = n\phi(n). \qquad \blacksquare$$

Lema 5.14. *La función ϕ de Euler es una función numérica multiplicativa, es decir, si m y n son primos entre sí, entonces $\phi(mn) = \phi(m)\phi(n)$.*

Demostración: Sean $m = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_r^{\alpha_r}$ y $n = q_1^{\beta_1} q_2^{\beta_2} \dots q_s^{\beta_s}$ las factorizaciones canónicas de estos enteros, donde $p_i \neq q_j$ para cada valor de los índices. Entonces:

$$mn = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_r^{\alpha_r} q_1^{\beta_1} q_2^{\beta_2} \dots q_s^{\beta_s},$$

y aplicando el teorema 5.12:

$$\phi(mn) = mn(1 - \frac{1}{p_1})(1 - \frac{1}{p_2}) \dots (1 - \frac{1}{p_r})(1 - \frac{1}{q_1})(1 - \frac{1}{q_2}) \dots (1 - \frac{1}{q_s}) =$$

$$\left(m(1 - \frac{1}{p_1}) \dots (1 - \frac{1}{p_r})\right) \left(n(1 - \frac{1}{q_1}) \dots (1 - \frac{1}{q_s})\right) = \phi(m)\phi(n). \qquad \blacksquare$$

Observación 5.1. Sin embargo, no es una función multiplicativa completa: $\phi(3) = 2$ y $\phi(6) = 6(1 - \frac{1}{2})(1 - \frac{1}{3}) = 2$. Pero $\phi(3 \cdot 6) = \phi(18) = 18(1 - \frac{1}{2})(1 - \frac{1}{3}) = 6 \neq \phi(3)\phi(6)$.

5.5. El teorema chino de los restos

Proposición 5.15. *Existe solución del sistema de congruencias lineales*

$$\begin{cases} x & \equiv & a_1 (\textit{mód } m_1) \\ x & \equiv & a_2 (\textit{mód } m_2) \end{cases}$$

si y sólo si MCD$(m_1, m_2) \mid (a_2 - a_1)$. Si existe una solución x_1, cualquier otra solución es de la forma $x \equiv x_1 (\textit{mód mcm}(m_1, m_2))$.

Demostración: Si $x \equiv a_1 (\text{mód } m_1)$, entonces $x = a_1 + km_1$ con k un entero. Sustituyendo en la segunda ecuación lineal, tenemos $a_1 + km_1 \equiv a_2 (\text{mód } m_2)$, con lo que $km_1 \equiv (a_1 - a_2) (\text{mód } m_2)$. Por la proposición 5.8, esta congruencia tiene solución si y sólo si $\text{MCD}(m_1, m_2) \mid (a_2 - a_1)$. Supongamos que existe una solución x_0; cualquier otra solución es de la forma $x_0 + \frac{m_2}{d} t$, donde $d = \text{MCD}(m_1, m_2)$ y t es un entero. Por lo tanto,

$$x = a_1 + km_1 = a_1 + (x_0 + \frac{m_2}{d} t)m_1 = a_1 + x_0 m_1 + \frac{m_1 m_2}{d} t.$$

Como $x_1 = a_1 + x_0 m_1$ es un entero y $\text{MCD}(m_1, m_2) \cdot \text{mcm}(m_1, m_2) = m_1 m_2$, se tiene que $x \equiv x_1 (\text{mód mcm}(m_1, m_2))$. $\blacksquare$

Teorema 5.16. ***(Teorema chino de los restos)*** *Si MCD*$(m_i, m_j) = 1$ *para* $i \neq j$*, el sistema de congruencias lineales*

$$\begin{cases} x & \equiv & a_1 (\textit{mód}\ m_1) \\ x & \equiv & a_2 (\textit{mód}\ m_2) \\ & \cdots & \\ x & \equiv & a_n (\textit{mód}\ m_n) \end{cases}$$

tiene una solución única módulo $m = m_1 \ldots m_n$*.*

Demostración: Sea $M_i = \frac{m}{m_i}$ para cada $i \in \{1, \ldots, n\}$. Entonces, MCD$(M_i, m_i) = 1$. Por la proposición 5.8 existen soluciones únicas para las congruencias lineales

$$M_1 x_1 \equiv 1 (\text{mód}\ m_1), M_2 x_2 \equiv 1 (\text{mód}\ m_2), \ldots, M_n x_n \equiv 1 (\text{mód}\ m_n).$$

Multiplicando cada una de ellas por el factor correspondiente, queda:

$$M_1 x_1 a_1 \equiv a_1 (\text{mód}\ m_1), M_2 x_2 a_2 \equiv a_2 (\text{mód}\ m_2), \ldots, M_n x_n a_n \equiv a_n (\text{mód}\ m_n).$$

Cada una de las congruencias lineales del enunciado se cumple si

$$x = M_1 x_1 a_1 + M_2 x_2 a_2 + \cdots + M_n x_n a_n,$$

ya que M_j contiene el factor m_i si $i \neq j$. Luego el sistema de congruencias lineales tiene solución. Si x' es cualquier otra solución del sistema, es $x' \equiv a_i (\text{mód}\ m_i)$ para cada i, luego $x' \equiv x (\text{mód}\ m_i)$ y como MCD$(m_i, m_j) = 1$ para $i \neq j$, aplicando iteradamente la proposición 5.15, se llega a que $x' \equiv x (\text{mód}\ m)$. ∎

5.6. Ejercicios

1.- Sea n un entero. Demostrar que:

1) $6 \mid (n^3 - n)$; 2) $30 \mid (n^5 - n)$;

3) si n es impar, $8 \mid (n^2 - 1)$; 4) $24 \mid (n^4 + 2n^3 - n^2 - 2n)$.

5) si n es impar y no es múltiplo de 5, entonces $n^2 - 1$ ó $n^2 + 1$ es múltiplo de 10.

2.- Responder a las siguientes cuestiones:

1) hallar el resto de dividir 23^{84292} entre 7 y el de dividir 113^{34291} entre 5;

2) probar que $53^{103} + 103^{53}$ es divisible por 39 y que $111^{333} + 333^{111}$ es divisible por 7;

3) calcular el resto de dividir el número $23^{3n+2} - 7n + 4$ entre 7;

4) demostrar que para todo $n \in \mathbb{N}$, el número $7^{2n+1} + 11^{2n+1}$ es múltiplo de 18;

5) demostrar que para todo $n \in \mathbb{N}$, el número $3^{3n+2} + 5^{3n+1}$ es múltiplo de 14;

6) calcular el resto de la división de 6^{82} entre 7 y entre 13.

3.- Sea p un primo impar. Demostrar que:

1) $1^{p-1} + 2^{p-1} + \cdots + (p-1)^{p-1} \equiv -1 (\text{mód } p)$;

2) $a^p \equiv a (\text{mód } p)$ para todo a;

3) $1^p + 2^p + \cdots + (p-1)^p \equiv 0 (\text{mód } p)$.

4.- Demostrar que la suma de los dígitos de $n \in \mathbb{N}$ (escrito en sistema decimal) es congruente $(\text{mód } 9)$ con el propio n. Deducir un criterio de divisibilidad por 9.

5.- Se pide demostrar:

1) si $n \in \mathbb{N}$, n^2 no es congruente con 2 módulo 3;

2) si $n \in \mathbb{N}$ es impar, $n^2 \equiv 1 (\text{mód } 4)$;

3) si p es primo y a es un entero, $(a+1)^p \equiv (a^p + 1) (\text{mód } p)$.

6.- Demostrar las siguientes propiedades de la función ϕ de Euler:

1) $\phi(n^2) = n\phi(n)$;

2) si $n > 2$, entonces $\phi(n)$ es par;

3) si $n \geq 1$, entonces $\displaystyle\sum_{d|n} \phi(d) = n$.

7.- Si $n = a_0 + a_1 \cdot 10 + a_2 \cdot 10^2 + \cdots + a_k \cdot 10^k$ es la representación decimal de un entero positivo, probar:

1) n es divisible por 11 si y sólo si $\displaystyle\sum_{i=0}^{k} (-1)^i a_i$ es divisible por 11;

2) n es divisible por 7 si y sólo si

$$a_0 + 3a_1 + 2a_2 - a_3 - 3a_4 - 2a_5 + a_6 + 3a_7 + 2a_8 - a_9 - 2a_{11} \ldots$$

es divisible por 7.

8.- Resolver el sistema de congruencias lineales:

$$\begin{cases} x & \equiv & 8(\text{mód } 5) \\ x & \equiv & 5(\text{mód } 3) \\ x & \equiv & 11(\text{mód } 7) \\ x & \equiv & 2(\text{mód } 4) \end{cases}$$

9.- Resolver las congruencias lineales:

1) $13x \equiv 17(\text{mód } 42)$;

2) $36x \equiv 53(\text{mód } 131)$;

3) $11x \equiv 25(\text{mód } 60)$;

4) $64x \equiv 16(\text{mód } 84)$;

5) $21x \equiv 15(\text{mód } 39)$.

10.- Probar el recíproco del teorema de Wilson (ejemplo 5.8): si $(n-1)!+1 \equiv 0(\text{mód } n)$, entonces n es primo.

11.- Demostrar que si n no es un primo, entonces $(n-1)!+1$ no es una potencia de n.

12.- Probar que si MCD$(a, m) = 1$, entonces la congruencia lineal $ax \equiv b(\text{mód } m)$ tiene exactamente una solución.

13.- Sean a y b dos enteros no nulos, $a \equiv b(\text{mód } 6)$. Decidir si las afirmaciones siguientes son ciertas o falsas, demostrándolas o dando un contraejemplo:

1) a y b son de la misma paridad;

2) $a \equiv b(\text{mód } 3)$;

3) si a y b son pares, entonces $a \equiv b(\text{mód } 12)$;

4) $2a \equiv 2b(\text{mód } 12)$;

5) si a y b son divisibles por 3, entonces $\frac{a}{3} \equiv \frac{b}{3}(\text{mód } 6)$.

14.- Sean a_1, a_2, a_3, a_4, a_5, a_6, a_7 y a_8 enteros positivos distintos. Se pide probar:

1) entre ellos, existen al menos dos cuya diferencia es un múltiplo de 7;

2) probar que existe un múltiplo de 7 cuya escritura decimal no contiene más que 0s y 1s. Indicación: Basta con elegir adecuadamente los 8 enteros.

15.- Se dice que un entero a es *inversible* $(mód\ n)$, si existe otro entero b, tal que $ab \equiv 1(\text{mód } n)$. Se pide:

1) encontrar los elementos inversibles $(\text{mód } 5)$, $(\text{mód } 6)$, $(\text{mód } 9)$ y $(\text{mód } 11)$;

2) encontrar el inverso de 107 $(\text{mód } 281)$ y el inverso de 281 $(\text{mód } 107)$. Indicación: Calcular antes MCD$(107, 281)$ y encontrar su representación lineal;

3) probar que a es inversible $(\text{mód } n)$ si y sólo si MCD$(a, n) = 1$.

16.- Sean a, b, c y d enteros no nulos. Decidir si son ciertas o falsas las siguientes afirmaciones, demostrándolas o dando un contraejemplo:

1) si $a \mid b$ y $a \mid c$, entonces $c^2 - 2b$ es múltiplo de a;

2) si existen dos enteros u y v tales que $au + bv = d$, entonces mcm$(a, b) = |d|$;

3) si a y b son coprimos, también los son a y b^3;

4) si $a \mid (b + c)$ y $a \mid (b - c)$, entonces $a \mid b$ y $a \mid c$;

5) si $19 \mid ab$, entonces $19 \mid a$ o $19 \mid b$;

6) si a es múltiplo de b y c es múltiplo de d, entonces $a + b$ es múltiplo de $c + d$;

7) si $4 \not| bc$, entonces b o c es impar;

8) si $a \mid b$ y $b \not| c$, entonces $a \not| c$;

9) si $6 \mid b^2$, entonces $36 \mid b^2$;

10) si $5 \mid b^2$, entonces $25 \mid b^2$;

11) si $12 \mid b^2$, entonces $9 \mid b^2$;

12) si $91 \mid ab$, entonces $91 \mid a$ o $91 \mid b$.

Capítulo 6

Polinomios

La poesía con anemia,
con tisis el ideal,
bajo la capa el puñal
y en la boca la blasfemia.

Abrojos
Rubén Darío (1867–1916)

En este capítulo, vamos a considerar el conjunto de los polinomios en una variable, y vamos a ver que posee propiedades análogas a las de los enteros, como el algoritmo de la división, el de Euclides o la factorización única en primos.

6.1. Los algoritmos de la división y de Euclides

Definición 6.1. Denotamos por $\mathbb{R}[x]$ al conjunto de los polinomios en una variable, es decir, $p(x) \in \mathbb{R}[x]$ si es de la forma $p(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$, donde los *coeficientes* $a_0, \cdots, a_n \in \mathbb{R}$. Dos polinomios son *iguales* si coinciden todos sus coeficientes.

Definición 6.2. Dado $p(x) \in \mathbb{R}[x]$, si todos sus coeficientes son cero, $p(x)$ es el *polinomio nulo*. Si para cada $k \geq 1$ es $a_k = 0$, $p(x)$ es un polinomio *constante*.

Definición 6.3. Si $p(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 \in \mathbb{R}[x]$ y $a_n \neq 0$, se dice que $p(x)$ tiene *grado* n y se denota por $\text{grad}(p(x)) = n$. Los polinomios constantes tienen grado 0.

Definición 6.4. Dos polinomios $p(x), q(x) \in \mathbb{R}[x]$ se suman y multiplican de la manera natural. Si

$$p(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 \quad \text{y}$$
$$q(x) = b_m x^m + b_{m-1}x^{m-1} + \cdots + b_1 x + b_0,$$

(suponemos grad$(p(x)) = n$, grad$(q(x)) = m$ y $m \geq n$):

$$(p+q)(x) = b_m x^m + \ldots b_{n+1}x^{n+1} + (a_n + b_n)x^n + + \cdots + (a_1 + b_1)x + (a_0 + b_0)$$

$$(p \cdot q)(x) = a_n b_m x^{n+m} + \cdots + (a_0 b_2 + a_1 b_1 + a_2 b_0)x^2 + (a_0 b_1 + a_1 b_0)x + a_0 b_0 =$$
$$= \sum_{j=0}^{n+m} \left(\sum_{k=0}^{j} a_k b_{j-k} \right) x^j.$$

Observación 6.1. grad$((p+q)(x)) \leq$ máx$\{$grad$(p(x))$, grad$(q(x))\}$ y grad$((p \cdot q)(x)) =$ grad$(p(x))$ + grad$(q(x))$.

Observación 6.2. Se denota por $\mathbb{Z}[x]$ (respectivamente, $\mathbb{Q}[x]$) al subconjunto de $\mathbb{R}[x]$ formado por los polinomios con coeficientes enteros (respectivamente, racionales). La suma y la multiplicación de polinomios son operaciones binarias sobre $\mathbb{R}[x]$, $\mathbb{Z}[x]$ y $\mathbb{Q}[x]$. Los polinomios nulo y constante $p(x) = 1$ son las identidades aditiva y multiplicativa, respectivamente.

6.1.1. Algoritmo de la división

Teorema 6.1. *Si $p(x), q(x) \in \mathbb{R}[x]$ y $q(x) \neq 0$, existen dos polinomios únicos $c(x), r(x) \in \mathbb{R}[x]$ –el cociente y resto, respectivamente– tales que:*

$$p(x) = c(x)q(x) + r(x), \quad \textit{grad}(r(x)) < \textit{grad}(q(x)) \quad \textit{ó} \quad r(x) = 0.$$

Demostración: Vamos a hacer la prueba por inducción (fuerte) sobre el grado de $p(x)$. Sean $p(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$, $q(x) = b_m x^m + b_{m-1}x^{m-1} + \cdots + b_1 x + b_0$, grad$(p(x)) = n$ y grad$(q(x)) = m$. Si $n < m$ se deduce la propiedad tomando $c(x) = 0$ y $r(x) = p(x)$; es decir, el teorema se cumple para $n < m$. Sea ahora $n \geq m$, y suponemos que la propiedad se cumple para cualquier polinomio de grado menor que n. Sea $h(x) = \dfrac{a_n}{b_m} x^{n-m}$. Observemos que $h(x) \cdot q(x) - p(x)$ no posee término de grado n; se puede entonces escribir $p(x) = h(x) \cdot q(x) + r(x)$, donde grad$(r(x)) <$ grad$(p(x))$. Si $r(x) = 0$, se cumple el teorema tomando $c(x) = h(x)$ y $r(x) = 0$. Si $r(x) \neq 0$, la hipótesis de inducción nos permite escribir $r(x) = C(x)q(x) + R(x)$, donde grad$(R(x)) < m =$ grad$(q(x))$. Y entonces,

$$p(x) = C(x)q(x) + R(x) + h(x)q(x) = (C(x) + h(x))q(x) + R(x),$$

y se obtiene el resultado tomando $c(x) = C(x) + h(x)$ y $r(x) = R(x)$.
Si $c_0(x), r_0(x) \in \mathbb{R}[x]$, grad$(r_0(x)) <$ grad$(q(x))$ (o $r_0(x) = 0$) y $p(x) = c_0(x)q(x) + r_0(x)$, entonces $(c_0(x) - c(x))q(x) + r_0(x) - r(x) = 0$. Igualando coeficientes, se deduce que $r_0(x) - r(x)$ y $c_0(x) - c(x)$. ∎

Corolario 6.2. *Si $p(x) \in \mathbb{R}[x]$ y $a \in \mathbb{R}$, existe $c(x) \in \mathbb{R}[x]$ tal que*

$$p(x) = (x - a)c(x) + p(a).$$

Demostración: Se aplica el teorema 6.1 al polinomio $q(x) = x - a$. El resto debe ser una constante –pues grad$(c(x)) = 1$–, que se determina evaluando $p(x)$ en $x = a$. ∎

Definición 6.5. Dados $p(x), q(x) \in \mathbb{R}[x]$, diremos que $p(x)$ *divide* a $q(x)$ –se denota $p \mid q$– si existe $c(x) \in \mathbb{R}[x]$ tal que $q(x) = p(x)c(x)$.

Definición 6.6. Dado $p(x) \in \mathbb{R}[x]$, si $p(a) = 0$, se dice que a es una *raíz* de $p(x)$.

Teorema 6.3. *Sean $p(x) \in \mathbb{R}[x]$ y $a \in \mathbb{R}$. a es una raíz de $p(x)$ si y sólo si $(x - a) \mid p(x)$.*

Demostración: Si $(x - a) \mid p(x)$, a es claramente una raíz. Y si a es una raíz, como $p(a) = 0$, el corolario 6.2 garantiza que $(x - a) \mid p(x)$. ∎

Teorema 6.4. *Si $p(x) = a_n x^n + \cdots + a_1 x + a_0 \in \mathbb{R}[x]$ y $a_n \neq 0$, $p(x)$ tiene a lo sumo n raíces.*

Demostración: Lo haremos por inducción sobre el grado de $p(x)$. Si $n = 0$ ($p(x) \neq 0$), entonces $p(x) = a_0 \neq 0$ y no posee raíces. Si $n \geq 1$ y no tiene raíces, hemos terminado; si a es una raíz, $(x - a) \mid p(x)$ y entonces $p(x) = (x - a)q(x)$, con grad$(q(x)) < n$. En el anterior producto de polinomios, el primero tiene exactamente una raíz y la hipótesis de inducción garantiza que el segundo tiene a lo sumo $n - 1$ raíces. ∎

Definición 6.7. Dados $p(x), q(x) \in \mathbb{R}[x] - \{0\}$, se llama *máximo comun divisor* de $p(x)$ y $q(x)$ a $d(x) \in \mathbb{R}[x]$ –y se denota MCD$(p(x), q(x))$–, verificando:

1) $d(x) \mid p(x)$ y $d(x) \mid q(x)$ (es decir, d es divisor común de p y de q);

2) si $c(x) \in \mathbb{R}[x]$ es tal que $c(x) \mid p(x)$ y $c(x) \mid q(x)$, entonces $c(x) \mid d(x)$ (es decir, $d(x)$ es el mayor en grado entre los divisores comunes de p y de q).

Teorema 6.5. *Dados $p(x), q(x) \in \mathbb{R}[x] - \{0\}$, existe MCD$(p(x), q(x))$ y es único, salvo factores multiplicativos. Además, existen $a(x), b(x) \in \mathbb{R}[x]$ tales que MCD$(p(x), q(x)) = a(x)p(x) + b(x)q(x)$.*

Demostración: Sea $S \subset \mathbb{R}[x]$ el conjunto de los polinomios que se pueden escribir de la forma $a(x)p(x)+b(x)q(x)$, para $a(x), b(x) \in \mathbb{R}[x]$. Se puede demostrar que es el conjunto de todos los múltiplos de un cierto $d(x) \in \mathbb{R}[x]$ (ver, por ejemplo teorema 6.27 en [AW]). Además, $p(x), q(x) \in S$ ya que $p(x) = 1 \cdot p(x) + 0 \cdot q(x)$ y $q(x) = 0 \cdot p(x) + 1 \cdot q(x)$. Luego $d \mid p$ y $d \mid q$. Si $c(x) \in \mathbb{R}$ es tal que $c \mid p$ y $c \mid q$, entonces $c \mid d$, al ser $d \in S$. Es decir, $d(x) = \text{MCD}(p(x), q(x))$. ∎

Observación 6.3. Los polinomios $a(x), b(x) \in \mathbb{R}[x]$ del teorema 6.5 que proporcionan la identidad de Bezout no son únicos.

Observación 6.4. Se verifican –y generalizan a las propiedades análogas para números enteros– las siguientes propiedades:

1) si $p(x) \mid q(x)$, entonces $\text{MCD}(p(x), q(x)) = p(x)$;

2) $p(x) = c(x)q(x) + r(x)$, con $\text{grad}(r(x)) < \text{grad}(q(x))$, entonces $\text{MCD}(p(x), q(x)) = \text{MCD}(q(x), r(x))$.

6.1.2. Algoritmo de Euclides

El *algoritmo de Euclides* permite calcular el máximo común divisor de dos polinomios de manera sencilla.

Sean $p(x), q(x) \in \mathbb{R}[x] - \{0\}$ con $\text{grad}(p(x)) \geq \text{grad}(q(x)) > 0$. Aplicando el teorema 6.1 de manera reiterada, es posible encontrar $c_1(x), c_2(x), \ldots, c_n(x), c_{n+1}(x) \in \mathbb{R}[x]$ y $r_1(x), r_2(x), \ldots, r_n(x) \in \mathbb{R}[x] - \{0\}$ verificando:

$$p(x) = c_1(x)q(x) + r_1(x), \quad \text{grad}(r_1(x)) < \text{grad}(q(x)),$$

$$q(x) = c_2(x)r_1(x) + r_2(x), \quad \text{grad}(r_2(x)) < \text{grad}(r_1(x)),$$

$$r_1(x) = c_3(x)r_2(x) + r_3(x), \quad \text{grad}(r_3(x)) < \text{grad}(r_2(x)),$$

$$\ldots$$

$$r_{n-2}(x) = c_n(x)r_{n-1}(x) + r_n(x), \quad \text{grad}(r_n(x)) < \text{grad}(r_{n-1}(x)),$$

$$r_{n-1}(x) = c_{n+1}(x)r_n(x).$$

Por la observación 6.4, se deduce que

$$\text{MCD}(p(x), q(x)) = \text{MCD}(q(x), r_1(x)) = \cdots = \text{MCD}(r_n(x), 0) = r_n(x).$$

Ejemplo 6.1. Calcular $\text{MCD}(p(x), q(x))$, donde $p(x) = 3x^3 + x + 1$ y $q(x) = x^2$.

Solución: Aplicando el algoritmo de Euclides,

$$p(x) = 3x^3 + x + 1 = 3x \cdot x^2 + (x-1) = c_1(x)q(x) + r_1(x),$$
$$q(x) = x^2 = (x+1)(x-1) + 1 = c_2(x)r_1(x) + r_2(x),$$
$$r_1(x) = x - 1 = (x-1) \cdot 1 = c_3(x)r_2(x).$$

Luego,

$$\text{MCD}(p(x), q(x)) = \text{MCD}(q(x), r_1(x)) = \text{MCD}(r_1(x), r_2(x)) = \text{MCD}(r_2(x), 0) = 1.$$

Ejemplo 6.2. Calcular $\text{MCD}(p(x), q(x))$, donde $p(x) = x^3+2x^2+2x+1$ y $q(x) = x^2+x$.

Solución: Aplicando el algoritmo de Euclides,

$$p(x) = x^3 + 2x^2 + 2x + 1 = (x+1)(x^2+x) + (x+1) = c_1(x)q(x) + r_1(x),$$
$$q(x) = x^2 + x = x(x+1) = c_2(x)r_1(x).$$

Luego,

$$\text{MCD}(p(x), q(x)) = \text{MCD}(q(x), r_1(x)) = \text{MCD}(r_1(x), 0) = x + 1.$$

6.2. Factorización

Definición 6.8. $p(x) \in \mathbb{R}[x] - \{0\}$ es *reducible*, si existen $q(x), h(x) \in \mathbb{R}[x]$ tales que $p(x) = q(x)h(x)$, siendo $1 \leq \text{grad}(q(x)), \text{grad}(h(x))$. Se llama *irreducible* en caso contrario.

Observación 6.5. Se verifican las siguientes propiedades:

1) los polinomios de grado 1 son irreducibles;

2) si $p(x) \in \mathbb{R}[x] - \{0\}$ es irreducible y $\text{grad}(p(x)) \geq 2$, entonces $p(x)$ no tiene raíces. Pero el recíproco no es cierto: por ejemplo $p(x) = (x^2+1)^2$ no tiene raíces y es reducible.

Lema 6.6. *Si $p(x) \in \mathbb{R}[x]$ es irreducible y divide a un producto de polinomios $a(x)b(x)$, entonces $p(x) \mid a(x)$ o $p(x) \mid b(x)$.*

Demostración: Si $p(x) \nmid a(x)$, es $\text{MCD}(p(x), a(x)) = 1$. Por el teorema 6.5, existen $s(x), t(x) \in \mathbb{R}[x]$, tales que $1 = s(x)p(x) + t(x)a(x)$, y por lo tanto

$$b(x) = s(x)p(x)b(x) + t(x)a(x)b(x).$$

Pero $p(x) \mid t(x)a(x)b(x)$ y $p(x) \mid s(x)p(x)b(x)$, luego $p(x) \mid b(x)$. ∎

Teorema 6.7. *Si $p(x) \in \mathbb{R}[x]$ es reducible, se puede escribir como un producto de polinomios irreducibles. La descomposición es única, salvo el orden de los factores y la multiplicación por constantes.*

Demostración: Por hipótesis, existen $q(x), h(x) \in \mathbb{R}[x]$ tales que $p(x) = q(x)h(x)$, con $\text{grad}(q(x)), \text{grad}(h(x)) < \text{grad}(p(x))$. La prueba se hace entonces por inducción fuerte sobre el grado. La unicidad se obtiene a partir del lema 6.6. ∎

6.3. Raíces y multiplicidades

Definición 6.9. Sea $p(x) \in \mathbb{R}[x]$ y $a \in \mathbb{R}$ una raíz de este polinomio. Se dice que a tiene *multiplicidad* $m \in \mathbb{N}$, si $(x-a)^m \mid p(x)$ y $(x-a)^{m+1} \nmid p(x)$. Si $m = 1$ diremos que a es una *raíz simple*, y es *múltiple* en caso contrario.

Definición 6.10. Si $p(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 \in \mathbb{R}[x]$, llamamos *polinomio derivado* a:

$$p'(x) = na_n x^{n-1} + \cdots + 2a_2 x + a_1.$$

De manera similar, se pueden definir los polinomios derivados de cualquier orden $p''(x)$, $p'''(x)$, ..., $p^{(k)}(x)$.

Lema 6.8. ***Fórmula de Taylor*** *Sea $p(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 \in \mathbb{R}[x]$, entonces*

$$p(x) = \frac{p^{(n)}(a)}{n!}(x-a)^n + \cdots + \frac{p''(a)}{2}(x-a)^2 + p'(a)(x-a) + p(a).$$

Demostración: La prueba de hace por inducción sobre el grado de $p(x)$. ∎

Teorema 6.9. *Sea $p(x) \in \mathbb{R}[x]$ y $a \in \mathbb{R}$ una raíz. Su multiplicidad es m si y sólo si $p(a) = p'(a) = \ldots = p^{(m-1)}(a) = 0$ y $p^{(m)}(a) \neq 0$.*

Demostración: Si la multiplicidad es m, es $(x-a)^m \mid p(x)$ y $(x-a)^{m+1} \nmid p(x)$. Por la fórmula de Taylor (lema 6.8), debe ser $p(a) = p'(a) = \ldots = p^{(m-1)}(a) = 0$ y $p^m(a) \neq 0$. Y recíprocamente, si $p(a) = p'(a) = \ldots = p^{(m-1)}(a) = 0$ y $p^{(m)}(a) \neq 0$, es

$$p(x) = \frac{p^{(n)}(a)}{n!}(x-a)^n + \cdots + \frac{p^{(m)}(a)}{m!}(x-a)^m =$$

$$= (x-a)^m \left(\frac{p^{(n)}(a)}{n!}(x-a)^{n-m} + \cdots + \frac{p^{(m)}(a)}{m!} \right). \quad \blacksquare$$

6.4. Descomposición en fracciones simples de las funciones racionales

Definición 6.11. Una *fracción simple* es una expresión de la forma $\dfrac{p(x)}{q(x)^k}$, donde $p(x), q(x) \in \mathbb{R}[x]$, $q(x)$ es irreducible y grad$(p(x)) <$ grad$(q(x))$.

Lema 6.10. *Sean $p(x), q(x), q_1(x), q_2(x) \in \mathbb{R}[x]$, de modo que $q(x) = q_1(x)q_2(x)$, con MCD$(q_1(x), q_2(x)) = 1$. Entonces:*

$$\frac{p(x)}{q(x)} = c(x) + \frac{r_1(x)}{q_1(x)} + \frac{r_2(x)}{q_2(x)},$$

donde $c(x), r_1(x), r_2(x) \in \mathbb{R}[x]$, grad$(r_1(x)) <$ grad$(q_1(x))$ y grad$(r_2(x)) <$ grad$(q_2(x))$.

Demostración: Por el teorema 6.1, $p(x) = c(x)q(x)+r(x)$, con grad$(r(x)) <$ grad$(q(x))$. Como MCD$(q_1(x), q_2(x)) = 1$, el teorema 6.5 garantiza que existen $a(x), b(x) \in \mathbb{R}[x]$ tales que $a(x)q_1(x) + b(x)q_2(x) = 1$. Multiplicando por $r(x)$, se tiene que

$$r(x)a(x)q_1(x) + r(x)b(x)q_2(x) = r(x), \quad \text{luego:}$$

$$\frac{p(x)}{q(x)} = c(x) + \frac{r(x)}{q(x)} = c(x) + \frac{r(x)b(x)q_2(x) + r(x)a(x)q_1(x)}{q(x)} =$$

$$= c(x) + \frac{r(x)b(x)}{q_1(x)} + \frac{r(x)a(x)}{q_2(x)} = c(x) + \frac{r_1(x)}{q_1(x)} + \frac{r_2(x)}{q_2(x)}.$$

Y como MCD$(q_1(x), q_2(x)) = 1$ y grad$(q(x)) =$ grad$(q_1(x))+$grad$(q_2(x))$, es grad$(a(x)) =$ grad$(q_2(x))$ y grad$(b(x)) =$ grad$(q_1(x))$, de donde se deduce que grad$(r_1(x)) <$ grad$(q_1(x))$ y grad$(r_2(x)) <$ grad$(q_2(x))$. ∎

La siguiente descomposición se usa –entre otras cosas– para integrar fracciones racionales, ya que las integrales de fracciones simples son más fáciles de calcular.

Teorema 6.11. *Sean $p(x), q(x) \in \mathbb{R}[x]$, MCD$(p(x), q(x)) = 1$ y $q(x) = q_1(x)^{k_1} \cdots q_r(x)^{k_r}$ la factorización en polinomios irreducibles de $q(x)$. Si $c(x), r(x) \in \mathbb{R}[x]$ son el cociente y el resto de la división de $p(x)$ entre $q(x)$, es decir,*

$$\frac{p(x)}{q(x)} = c(x) + \frac{r(x)}{q(x)},$$

existe una única descomposición de $\frac{r(x)}{q(x)}$ como suma de fracciones simples con denominadores de la forma $q_j(x)^m$, para $1 \leq m \leq k_j$.

Ejemplo 6.3. Si $p(x) = -50x - 10 = -10(5x + 1)$ y $q(x) = (x - 1)^2(x + 2)(x^2 + 1)$, entonces MCD$(p(x), q(x)) = 1$ y

$$\frac{p(x)}{q(x)} = \frac{-10}{(x-1)^2} + \frac{5}{x-1} + \frac{2}{x+2} + \frac{9-7x}{x^2+1}.$$

6.5. Ejercicios

1.- Factorizar los siguientes polinomios:

(i) $x^3 - 6x^2 + 11x - 6$.

(ii) $x^3 - 3x^2 - 9x - 5$.

(iii) $x^3 - 2x^2 - 49x + 98$.

(iv) $3x^4 - 9x^3 + 3x^2 + 9x - 6$.

(v)$x^4 + 12x^3 + 54x^2 + 108x + 81$.

(vi) $4x^3 - 12x^2 + 11x - 3$.

(vii) $x^3 + x2 - 5x + 3$.

(viii) $x^3 + 7x2 - 9x - 63$.

(ix) $x^4 + -2x^2 + 1$.

(x) $x^3 + 7x^2 + 15x + 9$.

2.- Calcular el cociente y el resto de las divisiones de $p(x)$ entre $q(x)$, donde:

(i) $p(x) = 3x^2 + 6x - 9$ y $q(x) = x - 3$.

(ii) $p(x) = 3x^3 - 2x^2 + 3x + 3$ y $q(x) = x^2 + 1$.

(iii) $p(x) = x^{52} + 6x - 1$ y $q(x) = x - 1$.

(iv) $p(x) = 3x^3 - 2x^2 + 3x + 3$ y $q(x) = x + 1$.

(v) $p(x) = x^5 - x^3 + 2x - 3$ y $q(x) = x + 2$.

(vi) $p(x) = x^{59} + x^3 + x$ y $q(x) = x + 1$.

(vii) $p(x) = 3x^7 - 2x^5 + x^3 - 4$ y $q(x) = 2x^2 - x + 3$.

3.- Calcular el valor de m para que el polinomio $3x^3 - 2x^2 + mx + 3$ sea divisible por: (i) $x - 1$, (ii) $x + 2$ y (iii) $x + 3$.

4.- Encontrar los polinomios $p(x)$ tales que $p(x) + 1$ sea divisible por $(x - 1)^4$ y $p(x) - 1$ por $(x + 1)^4$.

5.- Calcular MCD$(p(x), q(x))$ y encontrar una identidad de Bezout, en los siguientes casos:

(i) $p(x) = x^4 + x^3 - 2x^2 - 4x - 1$ y $q(x) = x^3 + x^2 - x - 1$.

(ii) $p(x) = x^4 - 10x^2 + 1$ y $q(x) = x^4 - 4x^3 + 6x^2 - 4x + 1$.

(iii) $p(x) = x^4 - x^3 - 2x + 1$ y $q(x) = x^2 + x + 1$.

(iv) $p(x) = x^3 - x^2 - x - 2$ y $q(x) = x^5 - 2x^4 + x^2 - x - 2$.

(v) $p(x) = x^6 - 2x^5 + 2x^4 - 3x^3 + 3x^2 - 2x$ y $q(x) = x^4 - 2x^3 + x^2 - x - 1$.

6.- Para $n \in \mathbb{N}$, ¿cuál es la multiplicidad de 2 como raíz del polinomio

$$nx^{n+2} - (4n+1)x^{n+1} + 4(n+1)x^n - 4x^{n-1}?$$

7.- ¿Para que valores de $a \in \mathbb{R}$, el polinomio $(x+1)^7 - x^7 - a$ admite una raíz múltiple real?

8.- Descomponer los siguientes polinomios en productos de polinomios irreducibles:

(i) $x^4 + x^2 + 4$.

(ii) $x^8 + x^4 + 1$.

(iii) $x^4 - 6x^3 + 7x^2 + 6x - 8$.

(iv) $x^{2n+1} + 1$, con $n \in \mathbb{N}$.

(v) $x^4 + 1$.

9.- Descomponer en fracciones simples los siguientes polinomios:

(i) $\dfrac{6}{2x^2 - 1}$.

(ii) $\dfrac{x^2 + 1}{(x-2)^3(x-1)^2(x^2 + 7x + 12)}$.

(iii) $\dfrac{x+2}{(x^2 + x + 1)(x-1)}$.

(iv) $\dfrac{x+1}{x^5 - x^4 + 2x^3 - 2x^2 + x - 1}$.

(v) $\dfrac{x^2+3x+5}{x^2+x-2}$.

(vi) $\dfrac{x^2}{(x-1)(x-2)(x-3)}$.

(vii) $\dfrac{1}{x+x^3}$.

(viii) $\dfrac{1}{x^3+6x^2+11x+6}$.

(ix) $\dfrac{x}{x^3-4x^2+5x-2}$.

(x) $\dfrac{x}{(x-1)^3(x-2)}$.

(xi) $\dfrac{x^3}{(x^2+1)(x^2+x+1)}$.

(xii) $\dfrac{x^2}{x^4+1}$.

Capítulo 7

Desigualdades

El viento no escucha.
No escuchan las piedras,
pero hay que hablar, comunicar,
con las piedras, con el viento.

Con las piedras, con el viento
José Hierro (1922–2002)

Una desigualdad es un enunciado sobre números reales que envuelve alguno de los símbolos $<$, $\leq$, $>$ o $\geq$.

Proposición 7.1. *Se verifican las siguientes reglas básicas referentes al orden de los números reales:*

1) si $x \in \mathbb{R}$*, se da una de las tres propiedades mutuamente excluyentes:* $x > 0$*,* $x < 0$ *o* $x = 0$*;*

2) si $x > y$*, entonces* $-x < -y$*,*

3) si $x > y$ *y* $c \in \mathbb{R}$*, entonces* $x + c > y + c$*,*

4) si $x > 0$ *e* $y > 0$*, entonces* $xy > 0$*,*

5) Si $x > y$ *e* $y > z$*, entonces* $x > z$*,*

6) si $0 < x < y$ *, es* $x^2 < xy < y^2$ *y* $\sqrt{x} < \sqrt{y}$*,*

7) si $a \geq 0$*, es* $|x| \leq a$ *si y sólo si* $-a \leq x \leq a$*,*

8) si $a \geq 0$*, es* $|x| \geq a$ *si y sólo si* $x \geq a$ *o* $-x \leq -a$*,*

9) $-|x| \leq x \leq |x|$*.*

7.1. Inecuaciones polinómicas

Definición 7.1. Una *inecuación* es una desigualdad entre dos expresiones algebraicas en las que hay una o más cantidades desconocidas (incógnitas) y que sólo se verifica para determinados valores de la incógnita o incógnitas.

Ejemplo 7.1. Un ejemplo de inecuación es: $|x-3| < 2|x+3|$.

Definición 7.2. Dos inecuaciones son *equivalentes* si tienen las mismas soluciones.

Observación 7.1. Se obtienen inecuaciones equivalentes si:

1) se suma o se resta un mismo número a los dos miembros de la desigualdad,

2) se multiplican o dividen los dos miembros de la desigualdad por un mismo número positivo,

3) se multiplican o dividen los dos miembros de la desigualdad por un mismo número negativo y la desigualdad cambia de sentido.

Definición 7.3. Una *inecuación lineal o de primer grado* es aquella cuyos miembros son polinomios de primer grado.

Observación 7.2. En su resolución se sigue un proceso análogo al de resolución de ecuaciones de primer grado.

Definición 7.4. Una *inecuación de segundo grado* es aquella cuyos miembros son polinomios de segundo grado.

Observación 7.3. Para resolverlas se dan los siguientes pasos:

1) se opera hasta obtener una inecuación equivalente en la que uno de los miembros sea 0, y el otro, un polinomio,

2) se factoriza el polinomio (si es posible),

3) se estudia el signo de cada factor en las zonas inducidas por las raíces y se determina el signo del polinomio,

4) se escribe la solución incluyendo o no las raíces dependiendo del tipo de desigualdad.

Definición 7.5. Una *inecuación polinómica* es aquella cuyos miembros son polinomios de grado superior a 2.

Observación 7.4. Para resolverlas se sigue un proceso análogo al de resolución de inecuaciones de segundo grado: dada la inecuación $a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 \sim 0$, donde $\sim$ es cualquier signo de estos $<, >, \leq, \geq$.

1) hallamos sus raíces, que son a lo sumo n raíces reales $a_1, \dots a_n$,

2) se estudian los signos en cada zona definida por las raíces y se deduce la solución de la inecuación.

Ejemplo 7.2. Resolver la desigualdad $x^3 + x \leq 4x^2 - 6$.

Solución: La escribimos de la forma $x^3 + x - 4x^2 + 6 \leq 0$, que factoriza del modo $x^3 + x - 4x^2 + 6 = (x+1)(x-2)(x-3)$, con lo que la inecuación del principio es equivalente a $(x+1)(x-2)(x-3) \leq 0$. Estudiamos los signos, ayudándonos de la siguiente tabla –donde se excluyen los ceros del polinomio–:

	$(-\infty, -1)$	$(-1, 2)$	$(2, 3)$	$(3, \infty)$
$x+1$	$-$	$+$	$+$	$+$
$x-2$	$-$	$-$	$+$	$+$
$x-3$	$-$	$-$	$-$	$+$
$(x+1)(x-2)(x-3)$	$-$	$+$	$-$	$+$

Así $x^3 + x \leq 4x^2 - 6$ si y sólo si $x \in (-\infty, -1] \cup [2, 3]$. ∎

7.2. Algunas desigualdades clásicas

Lema 7.2. ***(Desigualdad de Cauchy-Schwartz)*** *Dadas dos familias de números reales* $\{a_i\}_{i=1}^n, \{b_i\}_{i=1}^n$, *se cumple:*

$$\sum_{i=1}^{n} (a_i b_i) \leq \sqrt{\sum_{i=1}^{n} a_i^2} \sqrt{\sum_{i=1}^{n} b_i^2}.$$

Se da la igualdad si y sólo si existe λ *tal que* $a_i = \lambda b_i$ *para cada* i.

Demostración: Suponemos que $\sum_{i=1}^{n} a_i^2 \neq 0 \neq \sum_{i=1}^{n} b_i^2$; en caso contrario, para todo i sería $a_i = 0 = b_i$, y la desigualdad sería trivial. Sean $\alpha, \beta \in \mathbb{R}$, entonces:

$$0 \leq \sum_{i=1}^{n} (\alpha a_i - \beta b_i)^2 = \sum_{i=1}^{n} \left(\alpha^2 a_i^2 + \beta^2 b_i^2 - 2\alpha\beta a_i b_i \right),$$

es decir, $2\alpha\beta \sum_{i=1}^{n} a_i b_i \leq \alpha^2 \sum_{i=1}^{n} a_i^2 + \beta^2 \sum_{i=1}^{n} b_i^2$. Tomando $\alpha = \sqrt{\sum_{i=1}^{n} b_i^2}$ y $\beta = \sqrt{\sum_{i=1}^{n} a_i^2}$, queda probado el resultado. ∎

Lema 7.3. ***(Desigualdad de Minkowski)*** *En las condiciones del lema 7.2, es*

$$\sqrt{\sum_{i=1}^{n}(a_i+b_i)^2} \leq \sqrt{\sum_{i=1}^{n} a_i^2} + \sqrt{\sum_{i=1}^{n} b_i^2}$$

Demostración: Lo que se desea probar equivale a demostrar que

$$\sum_{i=1}^{n}(a_i+b_i)^2 \leq \sum_{i=1}^{n} a_i^2 + \sum_{i=1}^{n} b_i^2 + 2\sqrt{\sum_{i=1}^{n} a_i^2}\sqrt{\sum_{i=1}^{n} b_i^2},$$

es decir, simplificando $\sum_{i=1}^{n}(a_i b_i) \leq \sqrt{\sum_{i=1}^{n} a_i^2}\sqrt{\sum_{i=1}^{n} b_i^2}$, que es el lema 7.2. ∎

Lema 7.4. ***(Desigualdad triangular)*** *Dada una familia de números reales $\{a_i\}_{i=1}^n$, es*

$$|a_1 + \cdots + a_n| \leq |a_1| + \cdots + |a_n|.$$

Demostración: Como $-|a_i| \leq |a_i|$ para cada $i \in \{1, \ldots, n\}$, sumando se deduce que

$$-(|a_1| + |a_2| + \cdots + |a_n|) \leq a_1 + a_2 + \cdots + a_n \leq (|a_1| + |a_2| + \cdots + |a_n|). \quad ∎$$

Lema 7.5. ***(Series de fracciones desiguales)*** *Dadas dos familias de números reales $\{a_i\}_{i=1}^n, \{b_i > 0\}_{i=1}^n$, si*

$$\frac{a_1}{b_1} \leq \frac{a_2}{b_2} \leq \cdots \leq \frac{a_n}{b_n} \quad \Rightarrow \quad \frac{a_1}{b_1} \leq \frac{a_1 + \cdots + a_n}{b_1 + \cdots + b_n} \leq \frac{a_n}{b_n}.$$

Demostración: Si para cada $i \in \{1, \ldots, n\}$ es $\alpha_i = \frac{a_i}{b_i}$ (es decir, $\alpha_i b_i = a_i$), tenemos $\alpha_1 \leq \cdots \leq \alpha_n$. Así, se deduce que:

$$\alpha_1 b_1 \leq \alpha_1 b_1 \leq \alpha_n b_1$$

$$\alpha_1 b_2 \leq \alpha_2 b_2 \leq \alpha_n b_2$$

$$\cdots$$

$$\alpha_1 b_n \leq \alpha_n b_n \leq \alpha_n b_n$$

Luego, sumando miembro a miembro cada desigualdad, queda:

$$\alpha_1(b_1 + \cdots + b_n) \leq a_1 + \cdots + a_n \leq \alpha_n(b_1 + \cdots + b_n),$$

y dividiendo por $b_1 + \cdots + b_n$ se sigue el resultado. En el caso particular en que $b_1 = b_2 = \cdots = b_n = 1$, se obtiene que

$$a_1 \leq a_2 \leq \cdots \leq a_n \quad \Rightarrow \quad a_1 \leq \frac{a_1 + a_2 + \cdots + a_n}{n} \leq a_n,$$

es decir, la media aritmética de varios números está comprendida entre el mayor y el menor de ellos. ∎

Lema 7.6. ***(Desigualdad de Bernoulli)*** *Si $h > -1$ y $n \in \mathbb{N}$, es $(1+h)^n \geq 1 + nh$.*

Demostración: Se demuestra por inducción sobre n. Si $n = 1$ es trivial. Supongamos que es cierta para $n \in \mathbb{N}$, veámoslo para $n+1$: por hipótesis de inducción es $(1+h)^n \geq 1+nh$, y como $1 + h > 0$, multiplicando queda que:

$$(1+h)^{n+1} \geq (1+nh)(1+h) = 1 + (n+1)h + nh^2 \geq 1 + (n+1)h.$$

Si fuese $h > 0$, en vez de hacerlo por inducción, bastaría con desarrollar aplicando la fórmula de la potencia de un binomio:

$$\begin{aligned}(1+h)^n &= \binom{n}{0}h^n + \binom{n}{1}h^{n-1} + \binom{n}{2}h^{n-2} + \cdots + \binom{n}{n-1}h + \binom{n}{n} \\ &\geq \binom{n}{n-1}h + \binom{n}{n} = nh + 1.\end{aligned}$$

∎

Lema 7.7. ***(Desigualdades con las medias)*** *Si $\{a_i\}_{i=1}^n$ son números reales positivos,*

$$\sqrt{\frac{a_1^2 + a_2^2 + \cdots + a_n^2}{n}} \geq \frac{a_1 + a_2 + \cdots + a_n}{n} \geq \sqrt[n]{a_1 a_2 \ldots a_n} \geq \frac{n}{\frac{1}{a_1} + \cdots + \frac{1}{a_n}}.$$

*Las anteriores expresiones se llaman respectivamente, media cuadrática **(1)**, media aritmética **(2)**, media geométrica **(3)** y media armónica **(4)**.*

Demostración: **(1)**$\geq$ **(2)** Basta con tomar la desigualdad de Cauchy-Schwarz (lema 7.2) con todos los coeficientes $b_i = 1$, y queda que

$$\left(\sum_{i=1}^n a_i\right)^2 \leq n\left(\sum_{i=1}^n a_i^2\right).$$

La igualdad sólo se da si y sólo si los a_i son iguales, ya que deben ser proporcionales a los b_i que valen todos 1.

(2)$\geq$ **(3)** Sean A la media aritmética y G la geométrica; es claro si $a_1 = \cdots = a_n$, entonces $A = G$. En caso contrario existen a_i, a_j tales que $a_i < A < a_j$. Si sustituímos a_j por A y a_i por $a_i + a_j - A$, es claro que la media aritmética no cambia. En cambio la media geométrica aumenta estrictamente ya que

$$A(a_i + a_j - A) - a_i a_j = (A - a_i)(a_j - A) > 0.$$

Repitiendo este proceso suficientes veces, llegaremos a un conjunto de n números iguales, cuya media aritmética A será igual a su media geométrica, y ésta estrictamente mayor que G.

(3)$\geq$ **(4)** Si tomamos los números $\left\{\dfrac{1}{a_i}\right\}_{i=1}^{n}$, como ya se ha probado, sus medias aritmética y geométrica verifican la siguiente desigualdad:

$$\frac{\frac{1}{a_1} + \frac{1}{a_2} + \cdots + \frac{1}{a_n}}{n} \geq \sqrt[n]{\frac{1}{a_1}\frac{1}{a_2}\cdots\frac{1}{a_n}},$$

luego inviertiendo la desigualdad, es:

$$\sqrt[n]{a_1 a_2 \ldots a_n} \geq \frac{n}{\frac{1}{a_1} + \cdots + \frac{1}{a_n}}. \qquad \blacksquare$$

7.3. Ejercicios

1.- Resolver la inecuaciones siguientes:

(i) $3 - 2x \geq 8 - 7x$.

(ii) $\frac{1}{5}(6 - 2x) > \frac{1}{10}(1 - x)$.

(iii) $x^2 + 6x - 1 \leq 3x^2 + 3x - 6$.

(iv) $3x^2 + 4 < x^4 + 3x^3 + 3x$.

(v) $\frac{4x+x^2-2}{x^2+x} > \frac{x^2-2}{x}$.

(vi) $2(x + 3) > 3(x + 2)$.

(vii) $\frac{x-1}{4} - \frac{x+2}{3} > \frac{3x-1}{6} - x$.

(vii) $x^3 - 5x^2 + 6x \leq 0$.

(viii) $\frac{x^2+4}{x^2-4} - \frac{1}{x-2} > \frac{x+3}{x+2}$.

(ix) $|x-3| \geq 4$.

(x)$|x-4| < x-2$.

(xi)$|2+\frac{5}{x}| > 1$.

(xii) $\frac{-x^2+x+6}{x^2+1} \leq 0$.

2.- Sea una familia de números reales positivos $\{a_i\}_{i=1}^n$, tal que $a_1 a_2 \dots a_n = 1$. Probar que $a_1 + a_2 + \cdots + a_n \geq n$.

3.- Sea una familia de números reales positivos $\{a_i\}_{i=1}^n$. Probar que

$$\frac{a_1}{a_2} + \frac{a_2}{a_3} + \cdots + \frac{a_{n-1}}{a_n} + \frac{a_n}{a_1} \geq n.$$

4.- Para $n \in \mathbb{N}$, $n \geq 2$, probar que

$$n! < \left(\frac{n+1}{2}\right)^n.$$

5.- Sea una familia de números reales positivos $\{a_i\}_{i=1}^n$. Probar que:

$$(a_1 + a_2 + \cdots + a_n)\left(\frac{1}{a_1} + \cdots + \frac{1}{a_n}\right) \geq n^2.$$

6.- Sea una familia de números reales positivos $\{a_i\}_{i=1}^n$. Probar que:

$$n a_1 a_2 \dots a_n \leq a_1^n + a_2^n + \cdots + a_n^n.$$

7.- Probar la *desigualdad del reordenamiento*: dadas dos familias de números reales positivos $\{a_i\}_{i=1}^n$ y $\{b_i\}_{i=1}^n$, tales que:

$$a_1 \leq a_2 \leq \dots a_n \text{ y } b_1 \leq b_2 \leq \dots b_n,$$

si σ es una permutación de $\{1, \dots, n\}$, probar que:

$$a_1 b_n + a_2 b_{n-1} + \cdots + a_n b_1 \leq a_1 b_{\sigma(1)} + a_2 b_{\sigma(2)} + \cdots + a_n b_{\sigma(n)} \leq a_1 b_1 + a_2 b_2 + \cdots + a_n b_n.$$

8.- Probar la *desigualdad de Chebyshev*: dadas dos familias de números reales $\{a_i\}_{i=1}^n$ y $\{b_i\}_{i=1}^n$, es:

$$\frac{a_1 + a_2 + \cdots + a_n}{n} \frac{b_1 + b_2 + \cdots + b_n}{n} \leq \frac{a_1 b_1 + a_2 b_2 + \cdots + a_n b_n}{n}.$$

9.- Probar la *desigualdad de Hölder*: dadas dos familias de números reales $\{a_i\}_{i=1}^n$ y $\{b_i\}_{i=1}^n$ y $p, q > 0$ tales que $\frac{1}{p} + \frac{1}{q} = 1$, entonces es:

$$\sum_{i=1}^{n} |a_i b_i| \leq \left(\sum_{i=1}^{n} |a_i|^p \right)^{\frac{1}{p}} \left(\sum_{i=1}^{n} |b_i|^q \right)^{\frac{1}{q}}.$$

10.- Probar la *desigualdad de Minkowski*: dadas dos familias de números reales $\{a_i\}_{i=1}^n$ y $\{b_i\}_{i=1}^n$ y $p \geq 1$, entonces es:

$$\left(\sum_{i=1}^{n} |a_i + b_i|^p \right)^{\frac{1}{p}} \leq \left(\sum_{i=1}^{n} |a_i|^p \right)^{\frac{1}{p}} \left(\sum_{i=1}^{n} |b_i|^p \right)^{\frac{1}{p}}.$$

11.- Si $a, b, c > 0$, probar que:

$$\left(1 + \frac{a}{b}\right)\left(1 + \frac{b}{c}\right)\left(1 + \frac{c}{a}\right) \geq 2\left(1 + \frac{a+b+c}{\sqrt[3]{abc}}\right).$$

Capítulo 8

Trigonometría y números complejos

¿Hay algo, pregunto yo
Más noble que una botella
De vino bien conversado
Entre dos almas gemelas?

Coplas del vino
Nicanor Parra (1914–)

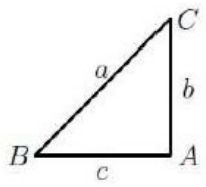
Como ya sabemos, no todo polinomio con coeficientes reales posee raíces (reales); por ejemplo, $x^2 + 1 = 0$ no se anula para ningún valor real. Si denotamos por el símbolo i a aquel que verifica la igualdad $i^2 = -1$, se llama *número complejo* a aquel que es de la forma $z = a + ib$, con $a, b \in \mathbb{R}$, donde $a = \text{Re}z$ se denomina la *parte real* y $b = \text{Im}z$ la *parte imaginaria*.

Al identificar $a \in \mathbb{R}$ con el número complejo $a = a + i0$, podemos pensar que $\mathbb{R} \subset \mathbb{C}$. A veces se identifica $z = a + ib$ con el par $(a, b) \in \mathbb{R}^2$, y por eso se suele hablar del *plano complejo*.

8.1. Trigonometría

La palabra *trigonometría* procede de las voces griegas *tri-gonon-metron*, es decir, "medida de tres ángulos".

La relación entre los lados y los ángulos de un triángulo vienen dadas a través de las razones trigonométricas, que son cocientes entre los diversos lados del triángulo:



RAZONES TRIGONOMÉTRICAS			
Directas		Inversas	
SENO	$\frac{\text{cateto opuesto}}{\text{hipotenusa}}$	COSECANTE	$\frac{\text{hipotenusa}}{\text{cateto opuesto}}$
COSENO	$\frac{\text{cateto contiguo}}{\text{hipotenusa}}$	SECANTE	$\frac{\text{hipotenusa}}{\text{cateto contiguo}}$
TANGENTE	$\frac{\text{cateto opuesto}}{\text{cateto contiguo}}$	COTANGENTE	$\frac{\text{cateto contiguo}}{\text{cateto opuesto}}$

Por ejemplo, las razones trigonométricas del ángulo B vienen dadas por:

$$\operatorname{sen}(B) = \frac{b}{a}, \quad \cos(B) = \frac{c}{a}, \quad \tan(B) = \frac{b}{c},$$

$$\operatorname{cosec}(B) = \frac{a}{b} = \frac{1}{\operatorname{sen}(B)}, \quad \sec(B) = \frac{a}{c} = \frac{1}{\cos(B)}, \quad \operatorname{cotan}(B) = \frac{c}{b} = \frac{1}{\tan(B)}.$$

Se suponen conocidas las fórmulas trigonométricas de sumas de ángulos, ángulos dobles, etc.

8.2. Operaciones con los números complejos

Definición 8.1. El conjunto de los *números complejos* $\mathbb{C}$ es el conjunto de pares ordenados de números reales $\mathbb{R}^2$, provisto de dos operaciones:

(i) la *suma*: $(a, b) + (c, d) = (a + c, b + d)$, y

(ii) el *producto*: $(a, b) \cdot (c, d) = (ac - bd, ad + bc)$.

Definición 8.2. Si $z = (a, b) \in \mathbb{C}$, a es la *parte real* de z y b es su *parte imaginaria*. Se escribe $\mathrm{Re}z = a$ e $\mathrm{Im}z = b$. Como $(a, 0) + (c, 0) = (a + c, 0)$ y $(a, 0) \cdot (c, 0) = (ac, 0)$ –es decir, este tipo de números se comportan respecto a la suma y producto de números como los números reales respecto a sus propias operaciones– se identifica $(a, 0)$ con el número real a y se considera que $\mathbb{R} \subset \mathbb{C}$.

Proposición 8.1. *Dados $(a, b), (c, d), (e, f) \in \mathbb{C}$, se verifican las siguientes propiedades:*

(i) asociatividad de la suma: $((a, b) + (c, d)) + (e, f) = (a, b) + ((c, d) + (e, f))$,

(ii) conmutatividad de la suma: $(a, b) + (c, d) = (c, d) + (a, b)$,

(iii) existencia de neutro: existe un número complejo $(0, 0)$*, tal que para cada* $z = (a, b) \in \mathbb{C}$ *es* $(a, b) + (0, 0) = (a, b)$,

(iv) existencia de opuesto: para cada $z = (a, b) \in \mathbb{C}$ *existe* $-z = (-a, -b) \in \mathbb{C}$ *tal que* $(a, b) + (-a, -b) = (0, 0)$*,*

(v) asociatividad del producto: $((a, b) \cdot (c, d)) \cdot (e, f) = (a, b) \cdot ((c, d) \cdot (e, f))$*,*

(vi) conmutatividad del producto: $(a, b) \cdot (c, d) = (c, d) \cdot (a, b)$*,*

(vii) existencia de unidad: existe un número complejo $(1, 0)$*, tal que para cada* $z = (a, b) \in \mathbb{C}$ *es* $(a, b) \cdot (1, 0) = (a, b)$*,*

(viii) existencia de inverso: para cualquier $z = (a, b) \in \mathbb{C}$ *distinto de* $(0, 0)$*, existe su inverso* $z^{-1} \in \mathbb{C}$*, que verifica que* $z \cdot z^{-1} = (1, 0)$*, y está dado por la expresión* $z^{-1} = \left(\dfrac{a}{a^2 + b^2}, \dfrac{-b}{a^2 + b^2}\right)$*,*

(ix) distributividad: $(a, b) \cdot ((c, d) + (e, f)) = (a, b) \cdot (c, d) + (a, b) \cdot (e, f)$*.*

Definición 8.3. La notación usual –se trata de un convenio de escritura, y suele llamarse también *forma algebraica*– para el número complejo $z = (a, b)$ es $a+bi$, donde $i = (0, 1)$ es la denominada *unidad imaginaria*. Su nombre proviene de que

$$i^2 = (0, 1) \cdot (0, 1) = (-1, 0) = -1,$$

es decir, la ecuación $x^2 + 1 = 0$ tiene solución compleja.

Observación 8.1. Además $(a, b) = (a, 0) + (0, b) = (a, 0) + (b, 0) \cdot (0, 1) = a + bi$, usando la identificación de $(a, 0)$ con a y la unidad imaginaria $i = (0, 1)$.

Observación 8.2. Con esta nueva notación, el producto de dos números complejos se escribe del modo: $(a + ib) \cdot (c + id) = (ac - bd) + i(ad + bc)$.

8.3. Conjugación

Definición 8.4. Si $z = a + ib \in \mathbb{C}$, su *complejo conjugado* es $\overline{z} = a - ib \in \mathbb{C}$.

Definición 8.5. Se llama *módulo* de $z = a + ib \in \mathbb{C}$ –y se denota por $|z|$– a la distancia de (a, b) al origen de coordenadas en $\mathbb{R}^2$, es decir, $|z| = \sqrt{a^2 + b^2}$.

Como consecuencia de las propiedades análogas de números reales, se deduce:

Proposición 8.2. *Dados* $z = a + ib, w = c + id \in \mathbb{C}$*, se verifica:*

(i) $\overline{\overline{z}} = z$*,*

(ii) $\overline{z} = z$ *si y sólo si* $z \in \mathbb{R}$,

(iii) $\overline{z+w} = \overline{z} + \overline{w}$ *y* $\overline{z \cdot w} = \overline{z} \cdot \overline{w}$,

(iv) $\overline{-z} = -\overline{z}$ *y* $\overline{z^{-1}} = \overline{z}^{-1}$,

(v) $|z|^2 = z \cdot \overline{z}$,

(vi) $|z \cdot w| = |z| \cdot |w|$ *y* $|z+w| \leq |z| + |w|$.

8.4. Forma polar

Si $z = a + ib$, su *argumento* es el ángulo θ entre el eje OX y la línea que une el origen de coordenadas con z, es decir, $a = r\cos(\theta)$ y $b = r\,\mathrm{sen}(\theta)$, siendo $r = |z|$. Se puede escribir $z = r\,(\cos(\theta) + i\,\mathrm{sen}(\theta))$ y se llama la *forma polar* de z. Existe un único valor del argumento con $-\pi < \theta \leq \pi$, que se llama el *argumento principal* de z, $\arg(z)$.

Teorema 8.3. ***(Teorema de De Moivre)*** *Dados dos números complejos en forma polar*

$$z_1 = r_1\,(\cos(\theta_1) + i\,\mathrm{sen}(\theta_1)) \quad y \quad z_2 = r_2\,(\cos(\theta_2) + i\,\mathrm{sen}(\theta_2))\,,$$

entonces es $z_1 \cdot z_2 = r_1 r_2\,(\cos(\theta_1 + \theta_2) + i\,\mathrm{sen}(\theta_1 + \theta_2))$.

Demostración: $z_1 \cdot z_2 = r_1 r_2\,(\cos(\theta_1) + i\,\mathrm{sen}(\theta_1))\,(\cos(\theta_2) + i\,\mathrm{sen}(\theta_2)) =$
$= r_1 r_2\,((\cos(\theta_1)\cos(\theta_2) - \mathrm{sen}(\theta_1)\,\mathrm{sen}(\theta_2)) + i(\cos(\theta_1)\,\mathrm{sen}(\theta_2) + \mathrm{sen}(\theta_1)\cos(\theta_2))) =$
$= r_1 r_2\,(\cos(\theta_1 + \theta_2) + i\,\mathrm{sen}(\theta_1 + \theta_2))$, usando las fórmulas del seno y el coseno de una suma de ángulos. ∎

Corolario 8.4. *Si* $z = r\,(\cos(\theta) + i\,\mathrm{sen}(\theta))$, *entonces* $z^n = r^n\,(\cos(n\theta) + i\,\mathrm{sen}(n\theta))$ *y* $z^{-n} = r^{-n}\,(\cos(n\theta) - i\,\mathrm{sen}(n\theta))$.

Demostración: Basta con usar que

$$z^{-1} = \frac{1}{z} = \frac{1}{r\,(\cos(\theta) + i\,\mathrm{sen}(\theta))} = \frac{1}{r}\,(\cos(\theta) - i\,\mathrm{sen}(\theta))\,. \qquad \blacksquare$$

Ejemplo 8.1. Calcular $(-\sqrt{3} + i)^7$.

Solución: Pasando a la forma polar $z = -\sqrt{3} + i$, es $z = 2(\cos(\frac{5\pi}{6}) + i\,\mathrm{sen}(\frac{5\pi}{6}))$. Luego,

$$z^7 = 2^7\left(\cos\left(\frac{35\pi}{6}\right) + i\,\mathrm{sen}\left(\frac{35\pi}{6}\right)\right) = 2^7\left(\cos\left(\frac{-\pi}{6}\right) + i\,\mathrm{sen}\left(\frac{-\pi}{6}\right)\right) =$$

$$= 2^7\left(\frac{\sqrt{3}}{2} + i\frac{-1}{2}\right) = 2^6(\sqrt{3} - i) = 64(\sqrt{3} - i).$$

Ejemplo 8.2. Encontrar la fórmula de $\cos(3\theta)$ en términos de $\cos(\theta)$.

Solución: Comenzamos con la ecuación $\cos(3\theta) + i\sin(3\theta) = (\cos(\theta) + i\sin(\theta))^3$. Igualando las partes real e imaginaria, se deduce que $\cos(3\theta) = 4\cos^3(\theta) - 3\cos(\theta)$.

8.5. Extracción de raíces y raíces de la unidad

Por comodidad, se usa a menudo la notación exponencial compleja

$$e^{i\theta} = \cos(\theta) + i\,\mathrm{sen}(\theta).$$

Con esta notación, si $z = re^{i\theta}$, es $\overline{z} = re^{-i\theta}$. Y además, $z_1 = r_1e^{i\theta_1} = r_2e^{i\theta_2} = z_2$ si y sólo si $r_1 = r_2$ y $\theta_1 = \theta_2 + 2k\pi$, con $k \in \mathbb{Z}$.

Si queremos resolver la ecuación $z^3 = 1$, podemos hacer

$$0 = z^3 - 1 = (z-1)(z^2 + z + 1),$$

que tiene como raíces 1, $-\frac{1}{2} + i\frac{\sqrt{3}}{2}$ y $-\frac{1}{2} - i\frac{\sqrt{3}}{2}$ es decir, 1, $e^{i\frac{2\pi}{3}}$ y $e^{i\frac{4\pi}{3}}$, que se denominan *raíces cúbicas de la unidad*.

En general, un número complejo z que satisface la ecuación $z^n = 1$ es una *raíz n-ésima de la unidad*.

Proposición 8.5. *Si $n \in \mathbb{N}$ y $w = e^{i\frac{2\pi}{n}}$, las raíces n-ésimas de la unidad son*

$$1, w, w^2, \ldots, w^{n-1}.$$

Demostración: Sea $z = re^{i\theta}$ una de las raíces n-ésimas de la unidad. Entonces, $z^n = r^ne^{in\theta}$, con lo que $r = 1$ y $n\theta = 2k\pi$, con $k \in \mathbb{Z}$. Por lo tanto, $\theta = \frac{2k\pi}{n}$ y $z = e^{i\frac{2k\pi}{n}} = w^k$. Luego, cada raíz n-ésima de la unidad es una potencia de w. Y recíprocamente, cada potencia de w es una raíz n-ésima de la unidad, ya que $(w^k)^n = w^{kn} = (e^{i\frac{2\pi}{n}})^{kn} = (e^{i2\pi})^k = 1$. ∎

Ejemplo 8.3. Las raíces cuartas de la unidad son $1, e^{i\frac{\pi}{2}}, e^{i\pi}$ y $e^{i\frac{3\pi}{2}}$, que son justamente $1, i, -1, -i$. Las raíces sextas de la unidad son $1, e^{i\frac{\pi}{3}}, e^{i\frac{2\pi}{3}}, -1, e^{i\frac{4\pi}{3}}$ y $e^{i\frac{5\pi}{3}}$, que son los vértices de un hexágono regular inscrito en un círculo.

Se pueden usar las raíces n-ésimas de la unidad para calcular las raíces n-ésimas de cualquier número complejo.

Ejemplo 8.4. Se pide calcular las soluciones de la ecuación $z^5 = -\sqrt{3} + i$, es decir, calcular las raíces quintas de $p = -\sqrt{3} + i = 2e^{i\frac{5\pi}{6}}$. Una raíz quinta de p es $\alpha = 2^{\frac{1}{5}}e^{i\frac{\pi}{6}}$. Si w es una raíz quinta de la unidad, entonces $(\alpha.w)^5 = \alpha^5 w^5 = \alpha^5 = p$, luego $\alpha.w$ es también una raíz quinta de p. Así, hemos encontrado las cinco raíces quintas de $-\sqrt{3}+i$, que son

$$\alpha, \alpha e^{i\frac{2\pi}{5}}, \alpha e^{i\frac{4\pi}{5}}, \alpha e^{i\frac{6\pi}{5}}, \alpha e^{i\frac{8\pi}{5}}.$$

Son de hecho las cinco raíces para p: si β es otra raíz quinta de p, entonces $\beta^5 = \alpha^5 = p$, con lo que $\left(\frac{\beta}{\alpha}\right)^5 = 1$, lo que significa que $\frac{\beta}{\alpha} = w$ es una raíz quinta de la unidad y por lo tanto $\beta = \alpha w$ está en la lista anterior. Así, las cinco raíces quintas de $-\sqrt{3} + i$ son:

$$2^{\frac{1}{5}}e^{i\frac{\pi}{6}}, 2^{\frac{1}{5}}e^{i\frac{17\pi}{30}}, 2^{\frac{1}{5}}e^{i\frac{29\pi}{30}}, 2^{\frac{1}{5}}e^{i\frac{41\pi}{30}}, 2^{\frac{1}{5}}e^{i\frac{53\pi}{30}}.$$

En general, el método anterior prueba que si una de las raíces n-ésimas de un número complejo es β, entonces el resto son $\beta w, \beta w^2, \ldots \beta w^{n-1}$, donde $w = e^{i\frac{2\pi}{n}}$.

8.6. El Teorema fundamental del Álgebra

Una ecuación polinómica es de la forma $p(x) = 0$, donde $p(x)$ es un polinomio con coeficientes complejos

$$p(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0.$$

Teorema 8.6. *Toda ecuación polinómica de al menos grado 1 tiene una raíz en* $\mathbb{C}$.

Corolario 8.7. ***(Teorema fundamental del Álgebra)*** *Todo polinomio de grado* n *factoriza como un producto de polinomios lineales y posee exactamente* n *raíces en* $\mathbb{C}$ *(aunque sean múltiples).*

Demostración: Si $p(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$ es un polinomio de grado n, por el teorema 8.6, $p(x)$ posee una raíz en $\mathbb{C}$, sea α_1. Entonces

$$p(x) = (x - \alpha_1)p_1(x),$$

donde $p_1(x)$ es un polinomio de grado $n-1$. Aplicando de nuevo el teorema 8.6 a $p_1(x)$, éste posee otra raíz en $\mathbb{C}$, sea α_2. Así, existe $p_2(x)$ un polinomio de grado $n-2$ tal que

$$p(x) = (x - \alpha_1)(x - \alpha_2)p_2(x).$$

Se puede reiterar este argumento hasta obtener un polinomio de grado 1, con lo que se deduce la factorización:

$$p(x) = a_n(x - \alpha_1)(x - \alpha_2)\ldots(x - \alpha_n). \qquad \blacksquare$$

Si consideramos ecuaciones polinómicas reales $p(x) = a_n x^n + \cdots + a_1 x + a_0$, el teorema 6.4 afirmaba que tenía a lo sumo n raíces reales. El corolario 8.7 nos permite probar la siguiente propiedad:

Corolario 8.8. *Todo polinomio real factoriza en un producto de polinomios reales lineales y cuadráticos, y sus raíces no reales son pares de números complejos conjugados.*

Demostración: Si $\alpha \in \mathbb{C}$ es una solución de la ecuación $p(x) = 0$, entonces

$$p(\alpha) = a_n\alpha^n + a_{n-1}\alpha^{n-1} + \cdots + a_1\alpha + a_0 = 0.$$

Consideremos su complejo conjugado $\overline{\alpha}$. Vamos a ver que también es una raíz. Observar primero que $\overline{\alpha}^n = \overline{\alpha^n}$ y como los coeficientes son reales $\overline{a_k} = a_k$. Luego

$$p(\overline{\alpha}) = a_n\overline{\alpha}^n + a_{n-1}\overline{\alpha}^{n-1} + \cdots + a_1\overline{\alpha} + a_0 =$$

$$a_n\overline{\alpha^n} + a_{n-1}\overline{\alpha^{n-1}} + \cdots + a_1\overline{\alpha} + a_0 = \overline{a_n\alpha^n} + \overline{a_{n-1}\alpha^{n-1}} + \cdots + \overline{a_1\alpha} + a_0 = \overline{p(\alpha)} = 0.$$

Luego, para una ecuación polinómica real $p(x) = 0$, las raíces complejas no reales aparecen a pares, un número complejo y su conjugado. Es decir,

$$p(x) = (x - \beta_1)\dots(x - \beta_k)(x - \alpha_1)(x - \overline{\alpha_1})\dots(x - \alpha_l)(x - \overline{\alpha_l}).$$

Observar además que $(x - \alpha_n)(x - \overline{\alpha_n}) = x^2 - (\alpha_n + \overline{\alpha_n})x + \alpha_n\overline{\alpha_n}$, que es una ecuación polinómica cuadrática con coeficientes reales. ∎

8.7. Ejercicios

1.- Representar gráficamente los siguientes números complejos: $3 + 4i$, -4, $-2i$, $2 + 3i$, $1 - 4i$ y $7 + 5i$.

2.- Pasar a forma polar los siguientes números complejos: $(1 + i)^4$, $i + \sqrt{3}$, $\dfrac{1 - i}{(1 + i)^2}$, $\dfrac{1 - \sqrt{3}}{(1 + \sqrt{3})^5}$.

3.- Calcular el módulo y el argumento de los siguientes números complejos: $\dfrac{1 + i}{1 - i}$, $1 + i\sqrt{3}$, $(1 + i) \cdot (2i)$, $1 + i(1 + \sqrt{2})$, $\left(\dfrac{1 + i\sqrt{3}}{\sqrt{3} + i}\right)^2$.

4.- Efectuar las siguientes operaciones:

(i) $(2 + 3i) + (4 - i)$, (ii) $(3 + 3i) - (6 + 2i)$,

(iii) $(3 - 2i) + (2 + i) - 2(-2 + i)$, (iv) $(2 - i) - (5 + 3i) + \frac{1}{2}(4 - 4i)$,

(v) $(1 + 2i)(3 - 2i)$, (vi) $(2 + i)(5 - 2i)$,

(vii) $(i+1)(3-2i)(2+2i)$, (viii) $3(2-i)(2+3i)i$,

(ix) $(2+i)/(1-2i)$, (x) $(7-i)/(3+i)$

(xi) $(5+5i)/(3-i)$, (xii) $(18-i)/(3+4i)$.

5.- Resolver las siguientes ecuaciones en $\mathbb{C}$:

(i) $x^3-27=0$, (ii) $x^5+32=0$,

(iii) $x^2+4=0$, (iv) $x^2-9=0$,

(v) $x^2+1=0$, (vi) $x^2-10x+29=0$,

(vii) $x^2-6x+10=0$ (viii) $x^2-4x+13=0$,

(ix) $x^3+27=0$, (x) $x^2-4x+5=0$,

(xi) $x^6+64=0$, (xii) $x^2-3x+4=0$,

(xiii) $x^2-(3+4i)x-1+5i=0$, (xiv) $(1-i)x^2+(1+7i)x+4-10i=0$.

6.- Calcular $(2-3i)^3$, $(3+i)^2, i^{23}$, $(1+2i)^3$, $(-3-i)^4$, $(1-3i)^2$, $(1+i)^8$, $(-1+i)^6$, $(1+\sqrt{3}i)^2$ y $(2+2i)^4$.

7.- Sean z y w dos números complejos de módulo 1, tales que $z\cdot w\neq -1$. Probar que $\dfrac{z+w}{1+z\cdot w}$ es un número real.

8.- Encontrar un polinomio cuadrático de coeficientes reales, tal que $2-5i$ sea una raíz.

9.- Probar la propiedad o dar un contraejemplo para las siguientes afirmaciones:

(i) si $z,w\in\mathbb{C}$ y $z^2+w^2=0$, entonces es $z=0$ y $w=0$,

(ii) si $|z|=1$, entonces $z=1,-1,i$ o $-i$,

(iii) si $\overline{z}=-z$, entonces z es imaginario puro.

10.- Resolver la ecuación $\left|\dfrac{z}{\overline{z}}+\dfrac{\overline{z}}{z}\right|=1$.

11.- Si $z,w\in\mathbb{C}$, probar que:

$$\frac{|z+w|}{1+|z+w|}\leq\frac{|z|}{1+|z|}+\frac{|w|}{1+|w|}.$$

12.- Demostrar la *identidad del paralelogramo*: para $z, w \in \mathbb{C}$, es

$$|z+w|^2 + |z-w|^2 = 2|z|^2 + 2|w|^2.$$

13.- Encontrar las raíces cúbicas de $2-2i$ y $11+2i$.

14.- Encontrar los puntos z del plano complejo que verifican las siguientes propiedades:

(i) $z^2 + 2z - 3 \in \mathbb{R}$, (ii) $|1-z| \leq 1/2$,

(iii) $\text{Re}(1-z) \leq 1/2$, (iv) $\left|\dfrac{z-3}{z+3}\right| < 2$,

(v) $\dfrac{2z-4}{z-i} \in \mathbb{R}$, (vi) $|(1-i)z - 3i| = 3$,

(vii) $\text{Re}(iz) \leq 1/2$, (viii) $\left|1 - \dfrac{1}{z}\right|^2 = 2$.

15.- Sea $z \in \mathbb{C}$, $z \neq 1$. Probar que $\dfrac{1+z}{1-z}$ es imaginario puro si y sólo si $|z| = 1$.

16.- ¿Para que enteros entre 2006, 2007, 2008 y 2009, el número complejo $(1+i)^n$ es imaginario puro?

17.- Sea $z = e^{\frac{2\pi i}{5}}$. Se pide:

(i) calcular $1 + z + z^2 + z^3 + z^4$,

(ii) deducir, utilizando $z + z^4$ y $z^2 + z^3$ el valor de $\cos\left(\frac{2\pi i}{5}\right)$ y de $\text{sen}\left(\frac{2\pi i}{5}\right)$.

18.- Resolver la ecuación $(z-i)^n = (z+i)^n$, para $n \in \mathbb{N}$. ¿Cuántas soluciones tiene?

19.- Dados $z, w, x \in \mathbb{C}$, probar que si $|z| = |w| = |x| = 1$, entonces $|zw + zx + wx| = |z + w + x|$.

20.- Se pide:

(i) probar que $1 + e^{it} + \cdots + e^{int} = \dfrac{\text{sen}\left(\frac{(n+1)t}{2}\right)}{\text{sen}\left(\frac{t}{2}\right)} \cdot e^{\frac{int}{2}}$,

(ii) deducir la fórmula de la suma $1 + \cos(t) + \ldots \cos(nt)$.

Bibliografía

[AW] J.P. D'Angelo y D.B. West, *Mathematical Thinking: Problem-Solving and Proofs*, Prentice Hall, 2000.

[BR] T.S. Blyth y E.F. Robertson, *Sets, Relations and Mappings*, Cambridge University Press, 1984.

[R] K.H. Rosen, *Matemática discreta y sus aplicaciones*, McGraw-Hill, 2004.

Que un gran tropel de ceros
asalte nuestras dichas
esbeltas, al pasar,
y las lleve a su cima.
Que se rompan las cifras,
sin poder calcular
ni el tiempo ni los besos.

La voz a tí debida
Pedro Salinas (1892–1951)