Universidad
Carlos III de Madrid

ESCUELA POLITÉCNICA SUPERIOR
UNIVERSIDAD CARLOS III DE MADRID

Curso Cero
Grado en Ingeniería Informática

Primera Parte

Conjuntos y funciones. Combinatoria. Teoría de números.

Juan Diego ÁLVAREZ ROMÁN
Manuel CARRETERO CERRAJERO
Pedro José HERNANDO OTER
Natalia IRISHINA
Jesús SALAS MARTÍNEZ
Eduardo Jesús SÁNCHEZ VILLASEÑOR (coordinador)

Grupo de Modelización, Simulación Numérica y Matemática Industrial
Universidad Carlos III de Madrid
Avda. de la Universidad, 30
28911 Leganés

Curso 2011/2012

Índice general

Capítulo 1

Conjuntos y funciones

Uno de los conceptos fundamentales de la Matemática es el concepto de conjunto. Intuitivamente, un conjunto es una colección de objetos denominados **elementos** del conjunto. En concreto, dado un conjunto X y un cierto objeto x una y sólo una de las siguientes afirmaciones debe ser cierta:

- o bien $x \in X$, es decir el objeto x pertenece al conjunto X,
- o bien no pertenece, $x \notin X$.

Sin embargo, nótese que no hemos definido lo que es una "colección" ni lo que es un "objeto". Generalmente utilizaremos las llaves $\{\}$ para denotar los conjuntos.

Definir conjuntos. Los conjuntos pueden ser definidos de diversas maneras:

- Por **extensión**, en el caso de que sea posible enumerar todos los elementos de un conjunto:
$$X = \{1, 2\} = \{2, 1\} = \{1, 2, 2, 1, 1\}\,.$$
Es importante recordar que los conjuntos no poseen una ordenación privilegiada de sus elementos ni admiten elementos múltiples.

- Por **comprensión**, en el caso de que su definición se realice atendiendo a la propiedad común que poseen todos los elementos del conjunto:
$$Y = \{y \,:\, y \text{ es una provincia de Andalucía}\}\,.$$
Evidentemente en el ejemplo anterior también podíamos haber definido Y por extensión:
$$Y = \{\text{Almería, Cádiz, Córdoba, Granada, Huelva, Jaén, Málaga, Sevilla}\}.$$

- En la práctica se utilizan notaciones "mixtas". Por ejemplo, es habitual introducir el conjunto $\mathbb{N}$ de los números naturales en la forma $\mathbb{N} = \{1, 2, 3, \dots\}$. Sin embargo, la expresión anterior no es una definición de $\mathbb{N}$ (¿Por qué?).

- Lo más habitual es definir un conjunto utilizando otro ya conocido a través de alguna regla de formación. Por ejemplo, el conjunto C de los cubos se puede escribir de varias formas equivalentes:

$$C = \{n^3 : n \in \mathbb{N}\} = \{m \in \mathbb{N} : \exists k \in \mathbb{N} \text{ tal que } m = k^3\}.$$

  En este ejemplo es evidente que todos los elementos de C son a su vez elementos de $\mathbb{N}$, es decir C es un **subconjunto** de $\mathbb{N}$ o, en símbolos, $C \subset \mathbb{N}$.

El único conjunto que no contiene ningún elemento se llama **conjunto vacío** y normalmente se denota por $\varnothing$. Aunque $\varnothing$ es el único conjunto que no contiene elementos, admite infinitas representationes alternativas, por ejemplo:

$$\begin{aligned}\varnothing &= \{n \in \mathbb{N} : n^2 = -1\} \\ &= \{x : x \in \mathbb{N},\, x \notin \mathbb{N}\} \\ &= \{x : x \text{ es una provincia de Andalucía}\} \cap \{y : y \text{ es una provincia de Galicia}\}.\end{aligned}$$

Operaciones elementales con conjuntos. Puesto que en los primeros cursos de carrera se profundizará más en las operaciones entre conjuntos, aquí nos limitaremos a recordar las cuatro operaciones más elementales:

Unión: $X \cup Y = \{z : z \in X \text{ ó } z \in Y\} = \{z : (z \in X) \vee (z \in Y)\}$.

Intersección: $X \cap Y = \{z : z \in X,\, z \in Y\} = \{z : (z \in X) \wedge (z \in Y)\}$.

Diferencia: $X \setminus Y = \{z : z \in X,\, z \notin Y\}$.

Producto cartesiano: $X \times Y = \{(x, y) : x \in X,\, y \in Y\}$.

Ejemplo: Si $X = \{1, 2, a, c\}$, $Y = \{a, b\}$ se cumplen las siguientes igualdades:

$$\begin{aligned}X \cup Y &= \{1, 2, a, b, c\}, \\ X \cap Y &= \{a\}, \\ X \setminus Y &= \{1, 2, c\}, \\ X \times Y &= \{(1, a), (1, b), (2, a), (2, b), (a, a), (a, b), (c, a), (c, b)\}.\end{aligned}$$

Observación: Es importante señalar la diferencia entre usar $\{\}$ y usar $(\,)$. En concreto $\{1, 2\}$ denota un conjunto y por tanto $\{1, 2\} = \{2, 1\}$. Sin embargo $(1, 2)$ es un par ordenado y por tanto $(1, 2) \neq (2, 1)$.

Funciones: Puesto que conviene haber leído al menos una vez la definición de función, empezaremos dando su definición formal:

Definición de función:
Una función $f \subset X \times Y$ de un conjunto X en un conjunto Y es un subconjunto del producto cartesiano $X \times Y$ tal que para cualquier $x \in X$, f contiene exactamente un par de la forma (x, y). Al conjunto X se le denomina **dominio** de la función f.

En otras palabras, dados dos conjuntos X e Y, una función es un objeto que a cada elemento $x \in X$ le asigna un único elemento $y \in Y$ al que se suele denominar $y = f(x)$. Habitualmente las funciones se denotan mediante

$$\begin{aligned} f : X &\to Y \\ x &\mapsto f(x) \end{aligned}$$

e incluso, cuando no hay duda acerca de los conjuntos X e Y, la notación se suele reducir a expresiones del tipo $x \mapsto f(x)$ o simplemente a $y = y(x)$.

Tipos importantes de funciones:

Sea $f : X \to Y$ una función. Diremos que:

- f es **inyectiva** si $x_1 \neq x_2$ implica $f(x_1) \neq f(x_2)$.
- f es **sobreyectiva** si para cada $y \in Y$ existe al menos un $x \in X$ tal que $y = f(x)$.
- f es **biyectiva** si es inyectiva y sobreyectiva.

Si $f : X \to Y$ es una biyección, podemos definir su **función inversa** $f^{-1} : Y \to X$ a través de la regla (bien definida)

$$f^{-1}(y) = x \Leftrightarrow y = f(x)\,.$$

Ejercicio: Sea $f : \mathbb{N} \setminus \{0\} \to \mathbb{Z} = \{0, \pm 1, \pm 2, \dots\}$

$$n \mapsto f(n) = \begin{cases} n/2 & \text{si } n \text{ par} \\ (1-n)/2 & \text{si } n \text{ impar} \end{cases}$$

¿Es f inyectiva? ¿Es f sobreyectiva? En el caso de que f sea biyectiva, calcula su inversa. Repite el estudio anterior para la función $g : \mathbb{N} \to \mathbb{Z} = \{0, \pm 1, \pm 2, \dots\}$ definida mediante

$$n \mapsto g(n) = \begin{cases} n/2 & \text{si } n \text{ par } (n = 0 \text{ es par}) \\ (1-n)/2 & \text{si } n \text{ impar} \end{cases}$$

Composición de funciones:
Dadas dos funciones $f : X \to Y$, $g : Y \to Z$, es posible definir una nueva función

$$g \circ f : X \to Z$$

mediante la expresión:

$$\big(g \circ f\big)(x) = g(f(x))\,.$$

La función $g \circ f$ es la **composición** de las funciones f y g.

Ejemplo: Sean

$$f(x) = \alpha x + \beta\,, \quad g(x) = \frac{\gamma x + \delta}{\epsilon x + \rho}$$

dos funciones reales de variable real. (Los símbolos α, β, γ, δ, ϵ y ρ denotan ciertos números reales y la función g está definida para aquellos x tales que $\epsilon x + \rho \neq 0$.) Un cálculo directo permite obtener:

$$\begin{aligned} \big(g \circ f\big)(x) &= g(f(x)) = \frac{\alpha\gamma x + \beta\gamma + \delta}{\alpha\epsilon x + \beta\epsilon + \rho}\,, \\ \big(f \circ g\big)(x) &= f(g(x)) = \frac{(\alpha\gamma + \beta\epsilon)x + \alpha\delta + \beta\rho}{\epsilon x + \rho}\,. \end{aligned}$$

¿Qué elecciones de los parámetros α, β, γ, δ, ϵ y ρ hacen que $g \circ f = f \circ g$?

Capítulo 2

Combinatoria

La combinatoria es una disciplina matemática que (entre otras cosas) se ocupa de desarrollar técnicas que permiten determinar el número de elementos de un conjunto definido por comprensión, sin necesidad de enumerar uno a uno todos sus elementos (una tarea generalmente inhumana).

El número de elementos de un conjunto X se denomina **cardinal** de X y habitualmente se denota mediante $|X|$. Por ejemplo si

$$X = \{x \,:\, x \text{ es una provincia de Andalucía}\} \Rightarrow |X| = 8\,.$$

Las mayoría de las técnicas combinatorias elementales en se basan en las siguientes dos reglas (obvias):

- **Principio del producto:** $|X \times Y| = |X| \cdot |Y|$
- **Principio de la suma:** Si $X \cap Y = \varnothing$ se cumple que $|X \cup Y| = |X| + |Y|$

Ejemplo: Sean

$$\begin{aligned} X &= \{x \,:\, x \text{ es una provincia de Andalucía}\}\,, \\ Y &= \{y \,:\, y \text{ es una provincia de Galicia}\}\,, \end{aligned}$$

entonces

$$|X \cup Y| = 12\,, \quad |X \times Y| = 32\,.$$

Explícitamente

$$\begin{aligned} X \cup Y &= \{\text{Almería, Cádiz, Córdoba, Granada, Huelva, Jaén, Málaga, Sevilla,} \\ &\quad \text{La Coruña, Lugo, Orense, Pontevedra}\}, \\ X \times Y &= \{(\text{Almería, La Coruña}), (\text{Cádiz, La Coruña}), (\text{Córdoba, La Coruña}), (\text{Granada, La Coruña}), \\ &\quad (\text{Huelva, La Coruña}), (\text{Jaén, La Coruña}), (\text{Málaga, La Coruña}), (\text{Sevilla, La Coruña}), \\ &\quad (\text{Almería, Lugo}), (\text{Cádiz, Lugo}), (\text{Córdoba, Lugo}), (\text{Granada, Lugo}), \\ &\quad (\text{Huelva,Lugo}), (\text{Jaén, Lugo}), (\text{Málaga, Lugo}), (\text{Sevilla, Lugo}), \\ &\quad (\text{Almería, Orense}), (\text{Cádiz, Orense}), (\text{Córdoba, Orense}), (\text{Granada, Orense}), \\ &\quad (\text{Huelva, Orense}), (\text{Jaén, Orense}), (\text{Málaga, Orense}), (\text{Sevilla, Orense}), \\ &\quad (\text{Almería, Pontevedra}), (\text{Cádiz, Pontevedra}), (\text{Córdoba, Pontevedra}), (\text{Granada, Pontevedra}), \\ &\quad (\text{Huelva, Pontevedra}), (\text{Jaén, Pontevedra}), (\text{Málaga, Pontevedra}), (\text{Sevilla, Pontevedra})\}. \end{aligned}$$

Ejercicio: Haciendo uso del principio del producto (y algo de ingenio) debería ser relativamente directo responder a las siguientes preguntas:

- Si para crear una cierta contraseña hay que elegir secuencialmente 5 dígitos, ¿cuál es el número posible de contraseñas? ¿Cuál es el número de contraseñas posibles si los dígitos tienen que ser distintos? ¿Cuál es el número de contraseñas si cada dígito tiene que ser distinto del anterior?
- ¿De cuántas maneras se pueden ordenar 7 personas en fila?
- ¿Cuántas palabras de 11 letras se pueden formar con $a, a, a, a, a, b, b, b, c, d, d$?

Técnicas usuales de recuento:

Muchos problemas de recuento pueden ser resueltos utilizando alguno de los siguientes patrones (cuyas fórmulas pueden ser fácilmente deducidas usando el principio del producto):

Permutaciones de n objetos:
Los elementos de un conjunto de cardinal n se pueden ordenar de

$$n! = n \cdot (n-1) \cdot (n-2) \cdots 2 \cdot 1$$

maneras distintas.

Ejemplo: ¿De cuántas maneras distintas se pueden ordenar las letras de la palabra "hiperblanduzcos"?

Permutaciones con repetición de n objetos:
El número de maneras distintas de ordenar n objetos clasificados en k grupos de objetos idénticos entre sí (con n_1 elementos en el primero, n_2 en el segundo, etc.) es

$$\binom{n}{n_1, n_2, \ldots, n_k} = \frac{n!}{n_1! n_2! \cdots n_k!}, \qquad \text{con } n_1 + \cdots + n_k = n\,.$$

Ejemplo: ¿De cuántas maneras distintas se pueden ordenar las letras de la palabra "anticonstitucionalmente"?

Variaciones de r objetos tomados de entre n:
A partir de un conjunto de cardinal n es posible construir un total de

$$V(n,r) = n(n-1)(n-2)\cdots(n-r+1) = \frac{n!}{(n-r)!}$$

listas ordenadas formadas por $r \leq n$ elementos distintos.
[Nota: $0! = 1$]

Ejemplo: ¿De cuántas maneras diferentes se pueden cubrir los puestos de presidente, vicepresidente y tesorero de un Club de Gourmets sabiendo que hay 15 posibles candidatos?

Variaciones con repetición de r objetos tomados de entre n:
Dado un conjunto de cardinal n es posible construir un total de n^r listas ordenadas formadas por r elementos no necesariamente distintos.

Ejemplo: ¿Cuántas quinielas distintas de fútbol se pueden hacer?

Ejercicios:

- De los números comprendidos entre 1000 y 9999, ¿en cuántos no aparece el número 3?, ¿en cuántos aparece uno y sólo un dígito 3?

- Dos amigos son testigos de un robo, así como de la posterior fuga de los ladrones en un coche. Al ser interrogados por la policía acerca de la matrícula del coche (que está formada por dos letras seguidas por cuatro cifras), uno de ellos asegura que la segunda letra era una O o una Q, y que la última cifra era un 8 ó un 3. El otro afirma que la primera letra era una C o una G y que la primera cifra era con toda seguridad un 7. ¿Cuántas matrículas diferentes tendrá que investigar la policía?

- ¿De cuántas maneras puede el fotógrafo de una boda disponer en fila a 6 personas de un grupo de 10 invitados, entre los cuales están el novio y la novia, si

  a) la novia tiene que estar en la foto?

  b) tanto el novio como la novia tienen que estar en la foto?

  c) exactamente uno de los dos (novio/a) tiene que estar en la foto?

  d) el novio y la novia están en la foto y deben aparecer juntos?

  e) el novio y la novia están en la foto y deben aparecer en posiciones separadas?

  f) el novio y la novia están en la foto y la novia debe aparecer a la izquierda del novio?

- Los ordenadores representan la información mediante unidades de información llamadas bits. Un bit tiene dos valores posibles: 0 ó 1. Una cadena de bits de longitud n es una sucesión de bits $b_1 b_2 b_3 \cdots b_n$ de n bits.

  a) ¿Cuántas cadenas de bits de longitud 8 hay?

  b) ¿Cuántas cadenas de bits de longitud 10 empiezan y terminan con 1?

  c) ¿Cuántas cadenas de bits tienen longitud menor o igual que 6?

  d) ¿Cuántas cadenas de bits de longitud 10 contienen al menos tres ceros y tres unos?

  e) ¿Cuántas cadenas de bits de longitud 7 o bien empiezan por dos ceros o bien acaban por tres unos?

  f) Un palíndromo es una cadena de bits que al invertirse es idéntica a sí misma (por ejemplo 0010110100). ¿Cuántas cadenas de bits de longitud n son palíndromos?

Capítulo 3

Teoría de números

Hay varias clases comunes de números que es conveniente manejar con soltura. De manera *informal* definimos los siguientes conjuntos:

- **Números naturales**:
$$\mathbb{N} \;=\; \{1, 2, 3, \ldots\}\,.$$
- **Números enteros**:
$$\mathbb{Z} \;=\; \{0, \pm 1, \pm 2, \pm 3, \ldots\}\,.$$
A veces es útil definir el conjunto de los *enteros no negativos* como
$$\mathbb{Z}_+ \;=\; \mathbb{N}_0 \;=\; \{0\} \cup \mathbb{N} \;=\; \{0, 1, 2, 3, \ldots\}\,.$$
- **Números racionales**:
$$\mathbb{Q} \;=\; \left\{ \frac{p}{q} :\; p, q \in \mathbb{Z}\,, q \neq 0 \right\}\,.$$
En realidad, cada número racional p/q se puede representar de infinitas maneras: $1/2 = 2/4 = 3/6 = \cdots$
- $\mathbb{N} \subset \mathbb{Z}_+ \subset \mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R}$, donde $\mathbb{R}$ denota el conjunto de los números reales.

El conjunto de los enteros $\mathbb{Z}$ es *cerrado* bajo las operaciones de suma, diferencia y producto. Es decir, para todo $a, b \in \mathbb{Z}$, $a \pm b \in \mathbb{Z}$ y $a \cdot b \in \mathbb{Z}$. Además satisfacen que

- 0 es el elemento neutro de la suma: $a + 0 = a$ para todo $a \in \mathbb{Z}$.

- 1 es el elemento neutro del producto: $a \cdot 1 = a$ para todo $a \in \mathbb{Z}$.
- Para todo $a \in \mathbb{Z}$, existe un único elemento inverso $-a \in \mathbb{Z}$ tal que $a + (-a) = 0$.

Sin embargo, el cociente de los enteros puede no ser entero. Por ello debemos definir con cuidado cuándo un número entero divide a otro.

Definición 3.1
Dados dos enteros $a \neq 0$ y b, se dice de $\boldsymbol{a}$ **divide a** $\boldsymbol{b}$ *si existe un entero $q \in \mathbb{Z}$ tal que $b = a \cdot q$. Cuando a divide a b, se dice que a es un* **factor** *o* **divisor** *de b y que b es un* **múltiplo** *de a. Si a divide a b, lo denotamos por* $\boldsymbol{a \mid b}$ *y si a no divide a b, por* $\boldsymbol{a \nmid b}$.

Observaciones:

- Cualquier entero $a \in \mathbb{Z}$ divide a 0: $0 = a \cdot 0$.
- 1 divide a cualquier entero $a \in \mathbb{Z}$: $a = 1 \cdot a$.
- Cualquier entero $a \in \mathbb{Z}$ se divide a sí mismo: $a = a \cdot 1$.

La división usual de dos enteros dando lugar a un cociente y un resto nos la garantiza el siguiente teorema:

Teorema 3.2 (Algoritmo de divisibilidad) *Sean a y $b \neq 0$ dos enteros, entonces existe un* **único** *par de enteros q y r tales que*

$$a \;=\; q \cdot b + r \qquad con \quad 0 \leq r < |b| \,.$$

Observación: Lo más importante del teorema es que garantiza que los enteros q y r son únicos.

Notación:

- Los números a y b se denominan respectivamente **dividendo** y **divisor**.
- El número r se denomina **resto de la división**: $r \;=\; a$ mód b.
- El número q se denomina **cociente de la división**:

$$q \;=\; a \operatorname{div} b \;=\; \begin{cases} \lfloor a/b \rfloor & \text{si } b > 0 \\ \lceil a/b \rceil & \text{si } b < 0 \end{cases} \tag{3.1}$$

  dónde las funciones $\lfloor \cdot \rfloor$ y $\lceil \cdot \rceil$ se denominan, respectivamente, **función suelo** y **función techo**.

Definición 3.3
La **función suelo** $\lfloor \cdot \rfloor : \mathbb{R} \to \mathbb{Z}$ *es la función que asigna a cada real* $x \in \mathbb{R}$ *el entero menor que* x *y más próximo a* x*.*

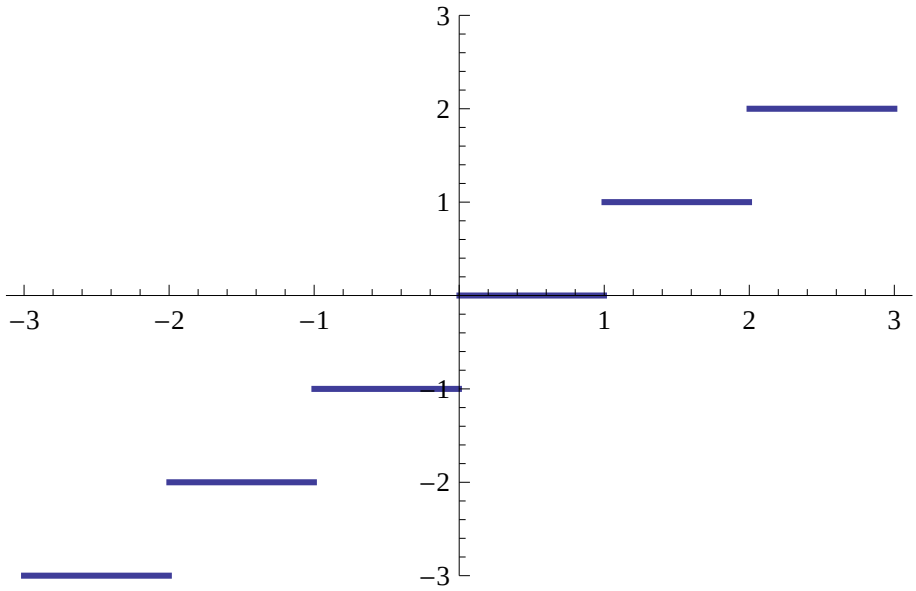

Figura 3.1: Gráfica de la función suelo $\lfloor \cdot \rfloor$. La función es discontinua en todos los enteros: si $0 < \epsilon \ll 1$, entonces $\lfloor n - \epsilon \rfloor = n - 1$ mientras que $\lfloor n \rfloor = n$ para todo $n \in \mathbb{Z}$.

Problema 3.4 Calcular el cociente y el resto de las siguientes divisiones de números enteros

1. 17 dividido por 5.
2. -17 dividido por 5.

Definición 3.5
La **función techo** $\lceil \cdot \rceil : \mathbb{R} \to \mathbb{Z}$ *es la función que asigna a cada real* $x \in \mathbb{R}$ *el entero mayor que* x *y más próximo a* x*.*

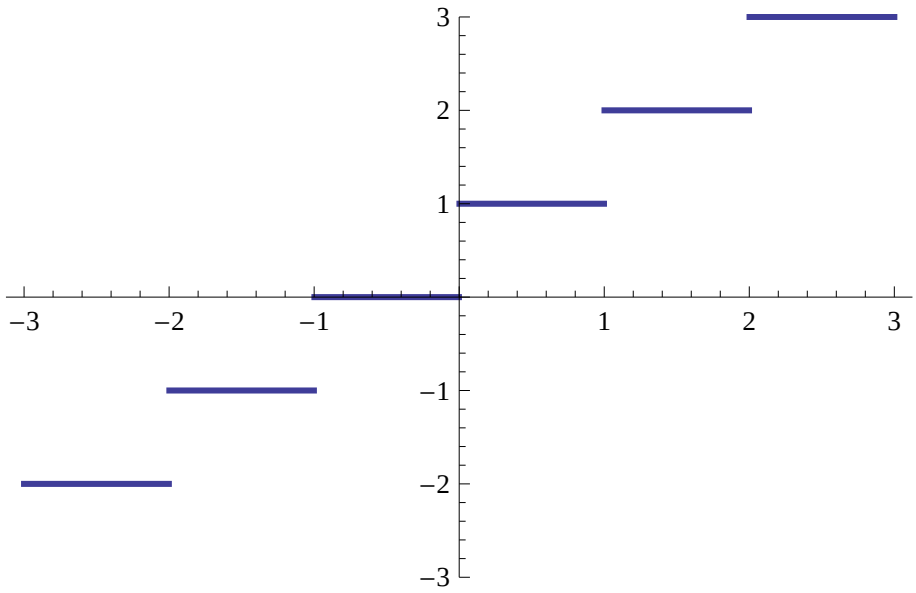

Figura 3.2: Gráfica de la función techo $\lceil \cdot \rceil$. La función es discontinua en todos los enteros: si $0 < \epsilon \ll 1$, entonces $\lceil n + \epsilon \rceil = n + 1$ mientras que $\lceil n \rceil = n$ para todo $n \in \mathbb{Z}$.

Problema 3.6 Calcular el cociente y el resto de las siguientes divisiones de números enteros

1. 17 dividido por -5.
2. -17 dividido por -5.

Problema 3.7 ¿Cuál es el cociente y el resto cuando

- 44 se divide entre 8?
- 19 se divide entre 7?
- -1 se divide entre 3?
- -123 se divide entre 19?
- -100 se divide entre 101?

El siguiente concepto importante es:

Definición 3.8
Dados dos enteros $a, b \neq 0$, se denomina **máximo común divisor** *de a y b [denotado por* $\mathrm{mcd}(a, b)$*] al mayor entero d tal que $d \mid a$ y $d \mid b$.*

Observación: El caso $a = b = 0$ hay que excluirlo porque cualquier número divide al 0.

Teorema 3.9 *El máximo común divisor de dos números enteros es único.*

Un concepto asociado al de máximo común divisor de dos números es el de mínimo común múltiplo:

Definición 3.10
Dados dos números a, b enteros no nulos, se define el **mínimo común múltiplo** *de a y b [y se denota por* $\mathrm{mcm}(a, b)$*] al menor número natural m tal que $a \mid m$ y $b \mid m$.*

Una clase muy importante de números naturales son los números primos:

Definición 3.11
Un número natural $p > 1$ se denomina **primo** *si los únicos divisores naturales de p son 1 y p. Un natural $p > 1$ que no sea primo se denomina* **compuesto**.

Observación: El número natural 1 **no** es primo. El primer primo es el número 2 y todos los demás primos son naturales impares $(3, 5, 7, 11, \ldots)$.

Problema 3.12 Encontrar los primeros 20 números primos.

Los números primos son muy importantes porque constituyen los "bloques" fundamentales con que construir los demás naturales:

Teorema 3.13 (Teorema fundamental de la aritmética) *Todo número natural $n > 1$ se puede descomponer de manera única en* **factores primos**

$$n = p_1^{n_1} \cdot p_2^{n_2} \cdot p_3^{n_3} \cdot \ldots \cdot p_k^{n_k},$$

donde los p_i son primos distintos entre sí y escritos en orden creciente y los exponentes n_i son números naturales.

Es decir, cada número natural (mayor que 1) tiene una descomposición única en números primos. Por ejemplo, $100 = 2^2 \cdot 5^2$.

Problema 3.14 Encontrar la descomposición en números primos de los naturales 81, 144, 272, y 113.

Una vez conocida la descomposición en factores primos de dos números es muy fácil calcular su máximo común divisor y su mínimo común múltiplo:

Teorema 3.15 *Si $a, b \in \mathbb{N}$ se factorizan de la forma*

$$\begin{aligned} a &= p_1^{n_1} \cdot p_2^{n_2} \cdots p_k^{n_k}, \\ b &= p_1^{m_1} \cdot p_2^{m_2} \cdots p_k^{m_k}, \end{aligned}$$

con $n_i, m_i \geq 0$ y donde todos los factores primos de a y b aparecen en ambas factorizaciones, se cumple que:

$$\begin{aligned} \text{mcd}(a,b) &= p_1^{\text{mín}(n_1,m_1)} \cdot p_2^{\text{mín}(n_2,m_2)} \cdots p_k^{\text{mín}(n_k,m_k)}, \\ \text{mcm}(a,b) &= p_1^{\text{máx}(n_1,m_1)} \cdot p_2^{\text{máx}(n_2,m_2)} \cdots p_k^{\text{máx}(n_k,m_k)}. \end{aligned}$$

Problema 3.16 Calcular el máximo común divisor y el mínimo común múltiplo de 144 y 66.

Problema 3.17 Calcular el máximo común divisor y el mínimo común múltiplo de 144, 66 y 10.

Un resultado muy importante y conocido desde la antigüedad es que el conjunto de los números primos tiene cardinal infinito:

Teorema 3.18 (Euclides) *Existen infinitos números primos.*

Es importante no confundir el concepto de número primo con el de números coprimos o primos entre sí:

Definición 3.19
Dos números a y b son **coprimos** *(o* **primos entre sí** *o* **primos relativos***) si* $\text{mcd}(a,b) = 1$. *Se dice que un conjunto de enteros $\{a_1, \cdots, a_n\}$ es un conjunto de números coprimos si* $\text{mcd}(a_1, a_2, \ldots, a_n) = 1$.

Ejemplos:

- Los números $25 = 5^2$ y $16 = 2^4$ son coprimos entre sí (ya que $\text{mcd}(25, 16) = 1$), pero ninguno de ellos es un número primo.
- Los números 5 y 17 son primos y también son coprimos.