Tema 2: Conjuntos numéricos

A. Méndez, C. Ortiz, E. Martín y J. Sendra

Marzo de 2012

Índice

Guía del tema 2

Asignatura:	Matemática Discreta
Titulo de la Unidad:	Conjuntos numéricos
Semanas de impartición en el cuatrimestre:	2 semanas

Requisitos para seguir con aprovechamiento el tema

- Conocer y distinguir los conjuntos de números naturales, enteros, racionales y reales.
- Reconocer el efecto que tienen las operaciones básicas sobre los números.
- Reconocer las relaciones y propiedades de los números en diferentes contextos.
- Analizar y explicar las distintas representaciones de un mismo número.
- Comparar y contrastar las propiedades de los números, sus relaciones y operaciones.

Objetivos

Objetivo general: Conocer más profundamente las matemáticas elementales, formulando y resolviendo problemas con las propiedades fundamentales de la teoría de números.

Objetivos Específicos:

- Justificar operaciones aritméticas utilizando las relaciones y propiedades de las operaciones.
- Capacidad para modelizar de una forma matemática una situación del mundo real y transferir los conocimientos matemáticos a otros contextos.
- Hacer conjeturas sobre propiedades y relaciones de los números.
- Justificar la elección de métodos e instrumentos de cálculo en la resolución de problemas.
- Capacidad para construir y desarrollar argumentaciones lógicas y matemáticas con una identificación clara de hipótesis y conclusiones.
- Resolver y formular problemas cuya estrategia de solución requiera de las relaciones y propiedades de los números naturales, enteros y racionales, y sus operaciones.
- Formular y resolver problemas aplicando conceptos de números primos, múltiplos, etc. en contextos reales y matemáticos.
- Destreza en razonamientos cuantitativos.

- Capacidad para utilizar herramientas computacionales como ayuda para los procesos matemáticos.
- Capacidad para presentar los razonamientos matemáticos.

Evaluación Se entregarán los ejercicios propuestos antes de la fecha límite

Con este tema queremos que el estudiante se familiarice con la Teoría de Números, que es una antigua parcela de los desarrollos de las Matemáticas ya que está fundamentada en los números que se utilizan el recuento. Contar, anotar las cuentas y realizar operaciones con ellas es bastante lejana en el tiempo. Los números han derivado de simples marcas: $|$ para el 1, $\|$ para el 2, etc. En ciertas culturas las primeras cifras fueron expresada con diferentes partes del cuerpo, por ejemplo: dedos de una mano (5), de las dos (10), de las manos y los pies (20), etc., y los sistemas de numeración se correspondían con las mismas.

1. Números naturales y enteros

Una forma de introducir los números naturales es como la representación de los elementos que forman una agrupación. Supondremos que se está familiarizado con los números naturales, también llamados enteros positivos, representados por $\mathbb{N}$, o por $\mathbb{Z}^+$, y que está formado por $\{1,\ 2,\ 3,\ 4, \ldots\}$, pero pondremos de manifiesto alguna de sus características.

- Existe un elemento menor que todos los demás, denotado por 1.
- No existe ningún valor mayor que todos los demás, es decir $\mathbb{N}$ no está acotado.
- Existe un sucesor de cada elemento, con lo que entre un número natural n y el sucesor $n+1$ no hay ningún número natural. El primer elemento es 1, 2 es su sucesor, 3 es el sucesor de 2 y así sucesivamente.
- Todo subconjunto A de $\mathbb{N}$ que contenga al elemento n y que contenga al sucesor de cada uno de sus elementos tiene el mismo número de elementos que $\mathbb{N}$, es decir existe una aplicación biyectiva, $f : \mathbb{N} \mapsto A$.

Antes de introducir los enteros enunciaremos el Principio de la Buena Ordenación, que además es un resultado que se utilizará en diversas demostraciones.

Teorema 1.1. (Principio de la Buena Ordenación)
Para todo subconjunto de los números naturales, diferente del vacío, existe un primer elemento, es decir tiene un elemento menor que todos los demás.

El conjunto de los números enteros, denotado por $\mathbb{Z}$, está formado por $\{\ldots, -2,\ -1,\ 0,\ 1,\ 2, \ldots\}$. Dados dos números enteros, x e y, se pueden definir dos operaciones internas, la suma $(x + y)$ y el producto $(x \cdot y)$. Enunciamos a continuación un resultado para recordar las principales propiedades de estas operaciones.

Teorema 1.2. *El conjunto* $\mathbb{Z}$ *para la suma verifica*

1. *Es asociativa:* $\forall x,\ y,\ z \in \mathbb{Z}$ *se cumple* $x + (y + z) = (x + y) + z$
2. *Tiene elemento neutro:* $\forall x \in \mathbb{Z}$ *se cumple* $x + 0 = 0 + x = x$
3. *Tiene elemento simétrico:* $\forall x \in \mathbb{Z} \quad \exists - x \in \mathbb{Z}$ *con* $x + (-x) = (-x) + x = 0$
4. *Es conmutativa:* $\forall x,\ y \in \mathbb{Z}$ *se cumple* $x + y = y + x$

El conjunto $\mathbb{Z}$ *para el producto verifica*

1. *Es asociativa:* $\forall x,\ y,\ z \in \mathbb{Z}$ *se cumple* $x\ (y\ z) = (x\ y)\ z$
2. *Tiene elemento unidad:* $\forall x \in \mathbb{Z}$ *se cumple* $x\ 1 = 1\ x = x$
3. *Es conmutativa:* $\forall x,\ y \in \mathbb{Z}$ *se cumple* $x\ y = y\ x$

Además, se verifica la propiedad distributiva: $\forall x,\ y,\ z \in \mathbb{Z}$ *se cumple* $x \cdot (y + z) = x \cdot y + x \cdot z$

Por cumplir todas las operaciones anteriores se dice que la terna $(\mathbb{Z},\ +,\ \cdot)$ *tiene estructura de anillo conmutativo con elemento unidad, que denominaremos el anillo de los enteros.*

También tendremos en cuenta el valor absoluto en los números enteros.

Definición 1.1. *Llamaremos valor absoluto a la función* $|\ | : \mathbb{Z} \mapsto \mathbb{Z}^+ \bigcup \{0\}$ *definida por*

$$|n| = \sup(n,\ -n),\ \textit{así} \qquad |n| = \begin{cases} -n & \textit{si } n < 0 \\ 0 & \textit{si } n = 0 \\ n & \textit{si } n > 0 \end{cases}$$

Algunas de sus propiedades son:

Proposición 1.1. *La función valor absoluto tiene las siguientes propiedades:*

1. $\forall n \in \mathbb{Z}$ *se verifica* $|n| \geq 0$, *es decir* $|n| \in \mathbb{N} \bigcup \{0\}$
2. $|n| = 0 \Longleftrightarrow n = 0$
3. $\forall n \in \mathbb{Z}$ *se verifica* $-|n| \leq n \leq |n|$
4. $\forall n,\ m \in \mathbb{Z}$ *se verifica* $|n \pm m| \leq |n| + |m|$
5. $\forall n,\ m \in \mathbb{Z}$ *se verifica* $|n\ m| = |n|\ |m|$

6. *$\forall n,\ m \in \mathbb{Z}$ se verifica $|\ |n| - |m|\ | \leq |n \pm m|$*

En $\mathbb{Z}$ se define la relación "ser menor o igual que", '$\leq$', que se define en términos de los enteros positivos, $\mathbb{N}$. Agrupamos en el siguiente resultado la definición y ciertas propiedades que nos aseguran que '$\leq$' es una relación de orden total.

Proposición 1.2. *La relación '$\leq$' definida por $n \leq m$ si y solo si $0 \leq m - n$ verifica:*

1. *$\forall n \in \mathbb{Z}$ se verifica $n \leq n$ (propiedad reflexiva).*

2. *Si $n \leq m$ y $m \leq n$ entonces $n = m$ (propiedad antisimétrica).*

3. *Si $n \leq m$ y $m \leq l$ entonces $n \leq l$ (propiedad transitiva).*

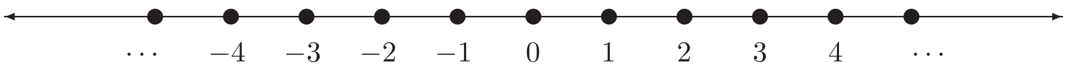
4. *$\forall n,\ m \in \mathbb{Z}$ se verifica una y solo una de las siguientes afirmaciones: $n < m$, $n = m$, o $n > m$.*

5. *Supongamos que $n \leq m$, con $n,\ m \in \mathbb{Z}$ y sea $l \in \mathbb{Z}$. Entonces:*

   a) *$n + l \leq m + l$*

   b) *Si $l > 0$ se cumple $n\, l \leq m\, l$; pero si $l < 0$ se cumple $n\, l \geq m\, l$.*

Habitualmente la representación sobre la recta real de los enteros es como puntos aislados de dicha recta, suponemos que los alumnos estáis familiarizados con esta representación gráfica.



2. El Principio de Inducción

En esta sección incluimos un resultado que muestra un método para establecer si un enunciado acerca de todos los números naturales es cierto cuando ciertos casos de ese enunciado sugieren un patrón general.

Teorema 2.1. (Principio de Inducción)
Supongamos que $P(n)$ es un enunciado matemático que implica una o más ocurrencias de la variable n, que representa a un entero positivo. Además, se verifica:

a) (Paso base) *$P(1)$ es verdadera. (Esta condición se puede sustituir por "$P(n)$ es cierta para un primer elemento n_0", por lo que el siguiente paso tiene un primer caso diferente de 1.)*

b) (Paso de inducción) *Siempre que $P(k)$ es cierta, para algún k particular pero elegido arbitrariamente, $k \in \mathbb{N}$, se cumple que $P(k+1)$ es cierta.*

Entonces, $P(n)$ es cierta para para todo n, con $n \in \mathbb{N}$.

Demostración. Supongamos que $P(n)$ es una proposición cumpliendo las dos hipótesis a) y b). Consideremos el siguiente conjunto $F = \{h \in \mathbb{Z}^+ \ / \ P(h) \text{ es falsa}\}$ y supongamos que $F \neq \emptyset$. Entonces, por el Principio de la Buena Ordenación, F tiene un primer elemento que denotamos por h_0. Puesto que $P(1)$ es verdadera $1 \neq \emptyset$, así $h_0 > 1$, por tanto $h_0 - 1 \in \mathbb{N}$. Por la definición de h_0 se cumple que $h_0 - 1 \notin F$, tenemos que $P(h_0 - 1)$ es cierta. Aplicando la hipótesis b), se sigue que $P(h_0 - 1 + 1) = P(h_0)$ es cierta, dando lugar a una contradicción con que $P(h_0)$ era falsa. La contradicción surge de la hipótesis $F \neq \emptyset$, por tanto, $F = \emptyset$. □

Otra forma de establecer este principio, llamado forma fuerte del principio de inducción, es el enunciado como

Proposición 2.1. (Forma fuerte del principio de inducción)
Supongamos que $P(n)$ es un enunciado matemático que implica una o más ocurrencias de la variable n, que representa a un entero positivo. Además, se verifica:

a) *$P(1)$ es verdadera. Esta condición se puede sustituir por "$P(n)$ es cierta para un primer elemento n_0".*

b) *Si $P(1),\ P(2), \ldots, P(k)$ son ciertas, se cumple que $P(k+1)$ es cierta.*

Entonces, $P(n)$ es cierta para para todo n, con $n \in \mathbb{N}$.

Ejemplo 2.1. Veamos algunos ejemplos que ilustran la aplicación de este resultado.

1. Para cualquier entero positivo n se verifica $\displaystyle\sum_{i=1}^{n} i = \frac{n(n+1)}{2} \equiv P(n)$.

   (Paso base): $\displaystyle\sum_{i=1}^{1} i = 1 = \frac{1(1+1)}{2}$, luego se cumple para $n = 1$.

   (Paso de inducción): Supongamos que para k se cumple $\displaystyle\sum_{i=1}^{k} i = \frac{k(k+1)}{2}$. Entonces,

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

   donde en la última igualdad se saca factor común $k+1$. Consecuentemente, por el Principio de Inducción $P(n)$ es cierta para todo $n \in \mathbb{Z}^+$.

2. Demostrar por inducción matemática que $n! \geq 2^{n-1}$ para $n = 1,\ 2,\ 3, \ldots$.
   Sea $P(n) \equiv n! \geq 2^{n-1}$
   (Paso base): $1! = 1 = 2^{1-1} = 2^0$, luego se cumple para $n = 1$.
   (Paso de inducción): Supongamos que se cumple para k, es decir $k! \geq 2^{k-1}$. Entonces,
   $$(k+1)! = (k+1) \cdot k! \geq (k+1) \cdot 2^{k-1} \geq 2 \cdot 2^{k-1} = 2^k$$
   donde la primera desigualdad es consecuencia de la hipótesis de inducción.

3. Una de las sucesiones de números que aparecen en la matemática discreta son los números armónicos, que se definen como $H_n = 1 + \frac{1}{2} + \ldots + \frac{1}{n}$, para $n \in \mathbb{N}$. Demuéstrese por inducción que $H_{2^n} \geq 1 + \frac{n}{2} \quad \forall n \in \mathbb{N}$.
   Sea $P(n) \equiv H_{2^n} \geq 1 + \frac{n}{2}$
   (Paso base): $H_{2^1} = H_2 = 1 + \frac{1}{2} \geq 1 + \frac{1}{2}$, luego se cumple para $n = 1$.
   (Paso de inducción): Supongamos que se cumple para k, es decir $H_{2^k} \geq 1 + \frac{k}{2}$. Entonces,
   $$H_{2^{k+1}} = \left(1 + \frac{1}{2} + \ldots + \frac{1}{2^k}\right) + \left(\frac{1}{2^k+1} + \ldots + \frac{1}{2^{k+1}}\right) = H_{2^k} + \left(\frac{1}{2^k+1} + \ldots + \frac{1}{2^k+2^k}\right)$$
   Puesto que $\frac{1}{2^k+j} \geq \frac{1}{2^{k+1}} \quad \forall\ 1 \leq j \leq 2^k$, se verifica $\left(\frac{1}{2^k+1} + \ldots + \frac{1}{2^k+2^k}\right) \geq 2^k \cdot \frac{1}{2^{k+1}} = \frac{1}{2}$.
   Aplicando la hipótesis de inducción se cumple que
   $$H_{2^{k+1}} \geq \left(1 + \frac{1}{2} + \ldots + \frac{1}{2^k}\right) + \frac{1}{2} \geq \left(1 + \frac{k}{2}\right) + \frac{1}{2} = 1 + \frac{k+1}{2}$$

4. Se deja como ejercicio demostrar por inducción que $H_{2^n} \leq 1 + n \quad \forall n \in \mathbb{N}$, con lo que $\forall n \in \mathbb{N}$ los números armónicos verifican $1 + \frac{n}{2} \leq H_{2^n} \leq 1 + n$.

3. El algoritmo de la división. Números primos

El resultado de realizar algunas operaciones con números enteros, como son la suma, resta y multiplicación, es otro número entero pero no ocurre lo mismo con la división, aunque existen casos en que un entero divide exactamente a otro, por ejemplo 5 divide 10, lo que implica la existencia de un cociente –en este caso 2– tal que $10 = 5 \cdot 2$.

Definición 3.1. *Dados dos enteros n y m, con $n \neq 0$, se dice que n divide a m, o que m es divisible por n, denotándose por $n|m$, si existe un entero c tal que $m = c\, n$.*
El entero c es el cociente de m dividido por n y se dice que n es divisor, o factor, de m y que m es múltiplo de n.

Nótese que si n divide a m, entonces $-n$ también divide a m y que el cociente es $-c$. En el siguiente teorema incluimos algunas resultados que pueden comprobarse fácilmente.

Teorema 3.1. *Sean $l,\ m,\ n \in \mathbb{Z}$. Entonces,*

1. $1|n$ *y* $n|0$.
2. *Si $n|l$ y $n|m$, entonces $n|(a\ l + b\ m)$ $\forall a,\ b \in \mathbb{Z}$, o equivalentemente*
   a) *Si $n|l$ y $n|m$ se cumple $n|(l+m)$.*
   b) *Si $n|m$, entonces $n|a\ m$ para cualquier a entero.*
3. *Si $n|m$ y $m|l$ se cumple $n|l$.*

Teorema 3.2. *Para cualquier par de números enteros, m y n, con $n > 0$, existen enteros únicos, c y r, tales que $m = c\ n + r$, con $0 \leq r < n$.*

Este teorema es conocido como el algoritmo de la división, el entero c se llama *cociente*, y el entero r *resto*, de la división de m (*dividendo*) entre n (*divisor*).

Cuando n es un entero cualquiera diferente de cero el algoritmo de la división establece que, dado m, existen enteros únicos, d y r, tales que $m = d\ n + r$, con $0 \leq r < |n|$.

Definición 3.2. *Un número entero positivo $p > 1$ se dice que es primo si los únicos divisores positivos de p son 1 y p. Un entero que no es primo se denomina compuesto.*

El número 1 no es ni primo ni compuesto.

Ejemplo 3.1. Veamos que si $p > 3$ es primo entonces $p^2 + 2$ es compuesto.

Cualquier entero se puede expresar como: $6k,\ 6k+1,\ 6k+2,\ 6k+3,\ 6k+4,\ 6k+5$ para algún entero k. Puesto que $6k,\ 6k+2$, y $6k+4$ son pares y $6k+3$ es múltiplo de 3, p debe ser de la forma $6k+1$ o $6k+5$.

Si $p = 6k+1 \Rightarrow p^2+2 = (6k+1)^2+2 = 36k^2+12k+1+2 = 3(12k^2+4k+1)$, luego es múltiplo de 3.

Si $p = 6k+5 \Rightarrow p^2+2 = (6k+5)^2+2 = 36k^2+60k+25+2 = 3(12k^2+20k+9)$, luego es múltiplo de 3.

Teorema 3.3. (Teorema Fundamental de la Aritmética)
Todo entero $n > 1$ puede escribirse como producto de números primos de forma única, es decir existen unos únicos números primos $p_1 < p_2 < \ldots < p_k$ y existen $\alpha_1,\ \alpha_2, \ldots, \alpha_k \in \mathbb{Z}^+$ tal que

$$n = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \ldots p_k^{\alpha_k}$$

Demostración. La demostración por inducción es:

(Paso base): Si $n = 2$ entonces n es primo y producto, con un único factor, de primos.

(Paso de inducción): Para k se verifica que puede factorizar como producto de primos de forma única.

Sea $k + 1$, si es primo entonces es producto de un solo factor. Si $k + 1$ es compuesto existen enteros positivos, a y b, menores que $k + 1$ tal que $k + 1 = a\ b$. Por la hipótesis de inducción a y b pueden expresarse de forma única como producto de primos, luego $k + 1$ se puede expresar de forma única como producto de primos. □

La única expresión de un entero n como producto de primos la llamaremos *descomposición en factores primos de n.*

La criba de Eratóstenes es un método para dilucidar si un entero es primo y se basa en el siguiente resultado.

Proposición 3.1. *Si $n > 1$ es un entero compuesto existe p un factor que aparece en la descomposición en factores primos de n con $p \leq \sqrt{n}$.*

Observación 3.1. (La criba de Eratóstenes)

Este método se utiliza para encontrar todos los primos que no exceden de un entero positivo específico. Supongamos que deseamos encontrar todos los primos inferiores a 101. Se procede como sigue:

1. Escribimos todos los enteros de 2 hasta 101.

2. Los enteros divisibles por 2, diferentes del 2, se eliminan de la lista.

3. Al ser el 3 es el primer entero mayor que 2 que no se elimina, se suprimen los múltiplos de 3 mayores que 3.

4. Se continua este procedimiento hasta los enteros primos menores o iguales que 10 ya que $10 \leq \sqrt{101} \leq 11$.

2	3	~~4~~	5	~~6~~	7	~~8~~	~~9~~	~~10~~	11	~~12~~	13	~~14~~	~~15~~	~~16~~	17	~~18~~	19	~~20~~	~~21~~
~~22~~	23	~~24~~	~~25~~	~~26~~	~~27~~	~~28~~	29	~~30~~	31	~~32~~	~~33~~	~~34~~	~~35~~	~~36~~	37	~~38~~	~~39~~	~~40~~	41
~~42~~	43	~~44~~	~~45~~	~~46~~	47	~~48~~	~~49~~	~~50~~	~~51~~	~~52~~	53	~~54~~	~~55~~	~~56~~	~~57~~	~~58~~	59	~~60~~	61
~~62~~	~~63~~	~~64~~	~~65~~	~~66~~	67	~~68~~	~~69~~	~~70~~	71	~~72~~	73	~~74~~	~~75~~	~~76~~	~~77~~	~~78~~	79	~~80~~	~~81~~
~~82~~	83	~~84~~	~~85~~	~~86~~	~~87~~	~~88~~	89	~~90~~	~~91~~	~~92~~	~~93~~	~~94~~	~~95~~	~~96~~	97	~~98~~	~~99~~	~~100~~	101

Aunque la posibilidad de que un entero no sea divisible por alguno de los que le preceden disminuye según crece dicho entero desde los tiempos de la Antigua Grecia se conoce el siguiente resultado.

Teorema 3.4. *El conjunto de números primos es infinito.*

4. Máximo común divisor y mínimo común múltiplo

Definición 4.1. *Dados m y n dos enteros no nulos, se dice un entero $d \neq 0$ es divisor común de m y n si d divide a m y a n, es decir $d|m$ y $d|n$.*
Un divisor común de m y n se llama máximo común divisor de m y n, denotándose por $m.c.d.(m,\ n)$, si $d > 0$ y todo divisor común de m y n divide a d. Por lo que $m.c.d.(m,\ n) = m.c.d.(|m|,\ |n|)$.
Si $m.c.d.(m,\ n) = 1$ se dice que m y n son primos entre sí.
Sean $n_1, \ldots, n_k$ enteros. Llamaremos máximo común divisor de $n_1, \ldots, n_k$ al divisor común $d > 0$ tal que para cualquier otro divisor común de $n_1, \ldots, n_k$, d‘, también divide a d, es decir d‘$|d$, y escribiremos $m.c.d.(n_1, \ldots, n_k) = d$.
Si $m.c.d.(n_1, \ldots, n_k) = 1$ diremos que $n_1, \ldots, n_k$ son primos entre sí.

Proposición 4.1. *Propiedades relativas al máximo común divisor.*

1. *Sean m y n enteros, con $n \neq 0$, entonces los divisores comunes de m y n son divisores del resto r de la división de m entre n.*

2. *Sean m y n enteros, con $n \neq 0$, entonces los divisores comunes de n y del resto r de la división de m entre n son divisores de m.*

3. *Sean m y n enteros diferentes de cero, entonces el máximo común divisor de m y n es único.*

4. *Sean m y n enteros, donde $n \neq 0$, y $m = c\ n + r$, con $0 \leq r < n$. Entonces se verifica, $m.c.d.(m,\ n) = m.c.d.(n,\ r)$.*

5. *Sean m y n enteros diferentes de cero y $m.c.d.(m,\ n) = d$, entonces d es el menor entero positivo que puede expresarse como $d = x\ m + y\ n$, con $x,\ y \in \mathbb{Z}$. Por tanto, $m.c.d.(m,\ n) = 1$ si y solo si $\exists\ s,\ t \in \mathbb{Z}$ tales que $s\ m + t\ n = 1$.*

6. *Si k divide a mn y, m y k son primos entre sí, entonces $k|n$.*

7. *Si l y m son primos entre si y, l y n también son primos entre sí, entonces l y mn son primos entre si.*

8. *Si $m,\ n \in \mathbb{Z}$ no son simultáneamente cero y $k \in \mathbb{Z}^+$, entonces*

$$m.c.d.(km,\ kn) = k \cdot m.c.d.(m,\ n)$$

9. *Si* $m.c.d.(m,\ n) = d \Rightarrow m.c.d.(\frac{m}{d},\ \frac{n}{d}) = 1$.

10. *Si* $m.c.d.(m,\ n) = 1 \Rightarrow m.c.d.(km,\ n) = m.c.d.(k,\ n)$.

A continuación enunciamos el algoritmo de Euclides para hallar el máximo común divisor de dos enteros.

Teorema 4.1. (Algoritmo de Euclides)
Dados dos enteros m y n, con $m > n$, si r_1 es el resto de la división de m entre n, r_2 es el resto de dividir n entre r_1, r_3 es el resto de dividir r_1 entre r_2, y $r_k = 0$ el último resto de esta secuencia, entonces $r_{k-1} = m.c.d.(m,\ n)$.

Observación 4.1. Se puede dar una definición alternativa del máximo común divisor a partir de las propiedades dadas previamente.
Sean m y n dos enteros y $\{p_1,\ p_2, \ldots, p_k\}$ los factores primos de ambos números, entonces existen $\alpha_1, \ldots, \alpha_k,\ \beta_1, \ldots, \beta_k$ enteros no negativos (algunos pueden ser cero) tales que $m = p_1^{\alpha_1} \cdot \ldots \cdot p_k^{\alpha_k}$ y $n = p_1^{\beta_1} \cdot \ldots \cdot p_k^{\beta_k}$, entonces

$$m.c.d.(m,\ n) = p_1^{\text{mín}(\alpha_1,\ \beta_1)} \cdot \ldots \cdot p_k^{\text{mín}(\alpha_k,\ \beta_k)}$$

Es decir el máximo común divisor de dos números es el producto de los factores primos comunes elevados al menor exponente.

Definición 4.2. *Dados los números enteros m y n llamaremos mínimo común múltiplo de m y n, designándolo por $m.c.m.(m,\ n)$, al menor entero positivo que sea múltiplo de ambos.*
Sean $n_1, \ldots, n_k$ enteros. Llamaremos mínimo común múltiplo de $n_1, \ldots, n_k$ al entero positivo más pequeño que sea múltiplo de todos ellos, escribiremos $m.c.m.(n_1, \ldots, n_k)$.

Observación 4.2. Al igual que en el caso del máximo común divisor se puede dar una definición alternativa del mínimo común múltiplo basada en la descomposición en factores primos. Si $\{p_1,\ p_2, \ldots, p_k\}$ son los factores primos de ambos números y estos se pueden escribir como $m = p_1^{\alpha_1} \cdot \ldots \cdot p_k^{\alpha_k}$ y $n = p_1^{\beta_1} \cdot \ldots \cdot p_k^{\beta_k}$, con $\alpha_1, \ldots, \alpha_k,\ \beta_1, \ldots, \beta_k \in \mathbb{Z}^+ \bigcup \{0\}$, entonces

$$m.c.m.(m,\ n) = p_1^{\text{máx}(\alpha_1,\ \beta_1)} \cdot \ldots \cdot p_k^{\text{máx}(\alpha_k,\ \beta_k)}$$

Es decir el mínimo común múltiplo de dos números es el producto de los factores primos comunes, y no comunes, elevados al mayor exponente.

Proposición 4.2. *Si m y n son enteros positivos, entonces $m.c.d.(m,\ n) \cdot m.c.m.(m,\ n) = m \cdot n$.*

Demostración. Si consideramos la descomposición en factores primos de m y n, entonces

$$m.c.d.(m,\ n)\cdot m.c.m.(m,\ n) = p_1^{\text{mín}(\alpha_1,\ \beta_1)}\cdot\ldots\cdot p_k^{\text{mín}(\alpha_k,\ \beta_k)}\cdot p_1^{\text{máx}(\alpha_1,\ \beta_1)}\cdot\ldots\cdot p_k^{\text{máx}(\alpha_k,\ \beta_k)} =$$
$$= p_1^{\text{mín}(\alpha_1,\ \beta_1)+\text{máx}(\alpha_1,\ \beta_1)}\cdot\ldots\cdot p_k^{\text{mín}(\alpha_k,\ \beta_k)+\text{máx}(\alpha_k,\ \beta_k)} = p_1^{\alpha_1}\cdot p_1^{\beta_1}\cdot\ldots\cdot p_k^{\alpha_k}\cdot p_k^{\beta_k} = m\cdot n$$

□

Resumen

1. Propiedades de los números naturales y enteros. Operaciones (suma y producto) con enteros. El valor absoluto y la relación "ser menor o igual".

2. Establecer el Principio de Inducción y uso del mismo.

3. Formulación de la división y sus propiedades. Números primos; relación entre la división de enteros.

4. Definición y propiedades del máximo común divisor y del mínimo común múltiplo.

Referencias

[1] E. Bujalance, J.A. Bujalance, A.F. Costa, E. Martínez, *Elementos de Matemática Discreta*, Sanz y Torres, Madrid, 1993.

[2] E. Bujalance, J.A. Bujalance, A.F. Costa, E. Martínez, *Problemas de Elementos de Matemática Discreta*, Sanz y Torres, Madrid, 1993.

[3] R.L. Grimaldi, *Matemática discreta y combinatoria. Una introducción con aplicaciones*, Prentice-Hall, México, 1998.

[4] R.L. Grimaldi, *Matemática discreta y combinatoria*, Addison-Wesley Iberoamericana, 1989.

[5] P. Henrici, *Elementos de análisis numérico*, Ed. Trillas, México, 1972.

[6] K. H. Rosen, *Matemática discreta y sus aplicaciones*, 5ª ed., McGraw-Hill Iberoamericana, 2004.

[7] A.A. Samarski, E.S. Nikolaev, *Métodos de solución de las ecuaciones reticulares*, Ed. Mir, 1982.

[8] T. Veerarajan, *Matemática Discreta con teoría de gráficas y combinatoria*, Ed. McGraw-Hill Interamericana, 2008.

[9] F. García-Merayo, G. Hernández, A. Nevot, *Problemas resueltos de matemática discreta*, Paraninfo, Madrid, 2003.

[10] C. García, J.M. López, D. Puigjaner, *Matemática discreta. Problemas y ejercicios resueltos*, Pearson Educación-Prentice Hall, 2002.

[11] M. Abellanas, D. Lodares, *Matemática Discreta*, Ed. Ra-Ma, 1990.

[12] S. Lipschutz, *Matemática Discreta*, McGraw-Hill (Serie Schaum), 1989.

[13] R. Johnsonbaugh, *Matemática Discreta*, 6ª ed., Pearson Prentice Hall, 2005.