



Curso Iberoamericano de formación permanente de profesores de matemática

Tema 1: Números naturales

Números naturales

Contenido de este documento:

Introducción

Definición

Operaciones

Divisibilidad

Ordenación en N

Sistemas de numeración

Operaciones en cualquier sistema de numeración

Introducción

“La Matemática moderna lleva a cabo una actividad intelectual muy sofisticada difícil de definir, pero una gran parte de lo que hoy se conoce como matemática es el resultado de un pensamiento que originalmente se centró en los conceptos de número, magnitud y forma.

Las nociones primitivas relacionadas con los conceptos de número, magnitud y forma se remontan al origen de la raza humana, y estarían, en un principio, relacionadas más bien con diferencias y contrastes que con semejanzas, tales como la diferencia entre un lobo y muchos. Después, y de una forma gradual, debe haber surgido, la constatación de que las diferencias mismas están apuntando ya a las semejanzas, puesto que el contraste que se observa entre un lobo y muchos, una oveja y un rebaño, vienen a sugerir que un lobo y una oveja tienen algo en común, su unidad.”

Extracto de “Historia de la matemática”. Carl B. Boyer

Nota: *En este tema va a encontrar una introducción formal del número natural. Por tanto se utilizará un lenguaje al que, tal vez, esté poco habituado. La introducción axiomática, como es sabido, tiene una estructura según la cual, partiendo de unas verdades indiscutibles (axiomas) se construye luego todo un entramado de propiedades y teoremas que siguen un estricto razonamiento lógico deductivo que es, entre otras virtudes, una de las grandezas de las matemáticas. Aconsejamos, por tanto, una lectura pausada, sin pretender memorizar los diferentes pasos de las demostraciones sino tratar de seguir los razonamientos y saber que, en este tema, tiene un tratamiento riguroso de la introducción del número natural.*

El concepto de número surge de la propiedad abstracta que tienen en común los grupos de un lobo, oveja, etc., o bien de dos lobos, ovejas, etc. y es a lo que llamamos **número**. Los números son objetos abstractos

que indican cantidad.

En esta unidad analizaremos el conjunto de los Números Naturales y la aritmética definida sobre él. Los números naturales son los números que usamos para contar; uno, dos, tres, cuatro, etc. y también para ordenar: 1^o , 2^o , 3^o , 4^o , ... Les damos un nombre, "Números naturales". El hombre primitivo solo necesitó algunos cuantos números, los cuales representó mediante marcas en huesos o madera, este hecho queda constatado por el dato de que algunas lenguas han conservado en su gramática una distinción entre uno, dos y más de dos, que se llamaba muchos.

La conciencia del número se extendió lo suficiente para necesitar expresar esta propiedad en lenguaje simbólico, primero a través de objetos como piedras, luego mediante muescas, después a través de los dedos de la mano y, posteriormente empleando lo que nos distingue de los animales: el lenguaje, cuyo desarrollo es esencial para el pensamiento matemático abstracto.

A través de este pensamiento abstracto vamos a abordar la construcción del conjunto de los números naturales que se puede dar en dos sentidos:

1. **Desde un punto de vista axiomático**, esto es, estableciendo un número de axiomas, y a partir de ellos probar una serie de teoremas que no son otra cosa que sus propiedades (método seguido por Peano y Hilbert).
2. **A través del cálculo de clases de equivalencia obtenidas por la relación de coordinabilidad** entre conjuntos (método iniciado por Cantor, Frege y perfeccionado por Russell).

En este tema abordaremos la construcción del conjunto de los números naturales desde el punto de vista axiomático.

1. Definición

Definición | Un **número natural** es cualquiera de los símbolos que se usan para contar los elementos de un conjunto. Reciben ese nombre porque fueron los primeros que utilizó el ser humano para contar objetos.

Algunos matemáticos, dependiendo de la construcción del conjunto que utilicen, prefieren reconocer el cero (0) como un número natural como los que se basan en la definición axiomática, otros, especialmente los de Teoría de conjuntos, Lógica e Informática, sostienen la postura opuesta. Nosotros vamos a considerar el 0 dentro del conjunto de

números naturales. La construcción sin el 0 es similar considerando que el primer elemento del conjunto de los naturales es el 1.

Definición axiomática

El conjunto de los números naturales se representa por N y corresponde al siguiente conjunto numérico infinito de objetos distintos llamados números naturales:

$$N = \{0, 1, 2, 3, 4, 5, 6, 7, \dots\}$$

En el que cada número menos el primero es el siguiente del que le precede:

Axiomas de Peano

Los axiomas de Peano rigen la estructura de los números naturales sin necesidad de otra teoría (por ejemplo, la de conjuntos) ni de las nociones aritméticas de suma o equivalencia. Requiere, eso sí, de la noción previa de sucesor. Los cinco axiomas de Peano son:

1) El 0 es un número natural.

$(0 \in N)$ y queda definido el primer elemento del conjunto y por tanto,

$$N \neq \emptyset$$

2) Si n es un número natural, entonces el sucesor de n también es un número natural.

$$\forall n \in N \Rightarrow \exists s(n) \in N / \forall n \in N \text{ y } \forall m \in N, \text{ si } n=m \Rightarrow s(n)=s(m)$$

La relación así definida entre los elementos del conjunto de naturales es aplicación, es decir, a cada elemento de los naturales le corresponde un único siguiente.

3) El 0 no es el sucesor de ningún número natural.

$$\forall n \in N \Rightarrow s(n) > 0$$

Queda definido el primer elemento del conjunto de los naturales.

4) Si hay dos números naturales n y m con el mismo sucesor, entonces n y m son el mismo número natural.

$$s(n)=s(m) \Rightarrow n=m. \text{ La aplicación definida es inyectiva.}$$

5) Si el 0 pertenece a un conjunto, y dado un número natural cualquiera, el sucesor de ese número también pertenece a ese conjunto, entonces todos los números naturales pertenecen a ese conjunto.

Éste es el axioma de inducción matemática y se formula:

$$\left. \begin{array}{l} \forall \mathbf{K} \subseteq \mathbb{N} \text{ con } 0 \in \mathbf{K} \\ \forall n \in \mathbf{K} \Rightarrow s(n) \in \mathbf{K} \end{array} \right\} \Rightarrow \mathbf{K} = \mathbb{N}$$

De los axiomas se deducen los siguientes teoremas necesarios para definir la suma y la multiplicación de \mathbb{N} .

Teorema 1 Si dos números naturales cualesquiera son distintos entonces sus siguientes también son distintos:

$$\forall n, m \in \mathbb{N} \text{ si } n \neq m \Rightarrow s(n) \neq s(m)$$

Demostración:

Por reducción al absurdo, supongamos que $n \neq m$ pero $s(n) = s(m)$, por el axioma 4 obtendríamos que $n = m$, que es una contradicción y por tanto es cierta la afirmación del teorema.

■

Teorema 2 Todo número natural es distinto de su siguiente:

$$\forall n \in \mathbb{N} \quad n \neq s(n)$$

Demostración:

Consideremos el conjunto de los números que verifican esta condición, sea éste $\mathbf{K} = \{n / n \in \mathbb{N} \text{ y } n \neq s(n)\}$

Veamos que $\mathbf{K} = \mathbb{N}$

Por la propia definición del conjunto se tiene: $\mathbf{K} \subseteq \mathbb{N}$.

Por el axioma 3, $0 \in \mathbf{K}$

Supongamos un número $n \in \mathbf{K}$, entonces $n \neq s(n)$; aplicando el teorema 1 sabemos que: $s(n) \neq s(s(n))$

Por definición del conjunto \mathbf{K} , $s(n) \in \mathbf{K} \Rightarrow$ aplicando el axioma 5 concluimos en que $\mathbf{K} = \mathbb{N}$ ■

Teorema 3 Todo número natural distinto de 0 es el siguiente de otro número natural

$$\forall n \in \mathbb{N} \quad n \neq 0 \Rightarrow \exists m \in \mathbb{N} / n = s(m)$$

Demostración:

Tal y como se hizo en la demostración anterior consideremos el siguiente conjunto:

$$K = \{0\} \cup \{n \in \mathbb{N} / \exists m \in \mathbb{N} \text{ y } n = s(m)\}$$

Veamos que $K = \mathbb{N}$

Por la propia construcción del conjunto $K \neq \emptyset$, ya que el $0 \in K$. Consideremos un elemento $n \in K \Rightarrow$ como el conjunto K contiene a todos los siguientes $s(n) \in K \Rightarrow K = \mathbb{N}$ ■

2. Operaciones

2.1. Suma

Consideramos la suma de números naturales como la aplicación

$$f: \mathbb{N} \times \mathbb{N} \rightarrow \mathbb{N}$$

que verifica:

- 1) $f(n, 0) = n + 0 = n, \forall n \in \mathbb{N}$
- 2) $f(n, s(m)) = s[f(n, m)], \forall n, m \in \mathbb{N}$

Veamos que la aplicación está bien definida.

Demostración:

Como en teoremas anteriores, vamos a construir un conjunto

$$K = \left\{ n \in \mathbb{N} / \exists \text{ la aplicación } f_n : \{n\} \times \mathbb{N} \rightarrow \mathbb{N} / \begin{array}{l} f_n(n, 0) = n \\ f_n(n, s(m)) = s[f_n(n, m)] \end{array}, \text{ con } m \in \mathbb{N} \right\}$$

Y comprobar que $K = \mathbb{N}$

- 3) Por la propia construcción del conjunto se tiene que no es vacío, es decir, $K \neq \emptyset$, ya que el $0 \in K$ puesto que:

$$\begin{cases} f_0(0, 0) = 0 + 0 = 0 \\ f_0(0, s(n)) = s(n) = s[f_0(0, n)], \forall n \in \mathbb{N} \end{cases}$$

Sigamos aplicando el método de inducción:

Suponemos que para un valor $a \in K$ existe la aplicación $f_a : \{a\} \times \mathbb{N} \rightarrow \mathbb{N}$ verificando:

$$\begin{cases} f_a(a, 0) = a \\ f_a(a, s(n)) = s[f_a(a, n)], \forall n \in \mathbb{N} \end{cases}$$

Veamos que si se verifica para a también se consigue para el $s(a)$. Definimos la siguiente aplicación

$$\begin{aligned} f_{s(a)} : \{s(a)\} \times \mathbb{N} &\rightarrow \mathbb{N} \\ f_{s(a)}(s(a), n) &= s[f_a(a, n)], \forall n \in \mathbb{N} \end{aligned}$$

verificando:

$$f_{s(a)}(s(a), 0) = s(a)$$

Comprobemos finalmente que $s(a) \in K$:

$$f_{s(a)}(s(a), s(n)) = s[f_a(a, s(n))] = s[s(f_a(a, n))] = s[f_{s(a)}(s(a), n)] \Rightarrow s(a) \in K$$

y por consiguiente: $K = \mathbb{N}$

Como se verifica para todo $a \in \mathbb{N}$, se puede afirmar que existe la aplicación que define la suma. ■

Mediante el método de reducción al absurdo. se puede demostrar además, **la unicidad de esta aplicación que define la suma de números naturales.**

Propiedades

Asociativa: $\forall a, b, c \in \mathbb{N}, (a + b) + c = a + (b + c)$

Demostración: Construimos el conjunto

$$K = \{n \in \mathbb{N} / (a + b) + n = a + (b + n)\} \forall a, b \in \mathbb{N}$$

para demostrar que $K = \mathbb{N}$

El $0 \in K$ ya que $(a + b) + 0 = (a + b) = a + (b + 0)$ por la propiedad 1 de la suma.

Ahora consideramos un número $c \in K$, por tanto, verificará:

$$(a + b) + c = a + (b + c)$$

y veamos que $s(c)$ también pertenece a K .

Por la definición de la suma se tiene:

$$(a + b) + s(c) = s((a + b) + c)$$

y como $c \in K$, tenemos que:

$$s((a + b) + c) = s(a + (b + c)) = a + s(b + c) = a + (b + s(c))$$

comprobándose así que $s(c) \in K$.

Aplicando el axioma 5 de Peano se llega a que $K = \mathbb{N}$ y queda demostrada la propiedad asociativa. ■

Conmutativa: $\forall a, b \in \mathbb{N}, a + b = b + a$

Demostración: Construimos el conjunto

$$K = \{n \in \mathbb{N} / n + 1 = 1 + n\}$$

y demostraremos que $K = \mathbb{N}$

El $0 \in K$ ya que $0 + 1 = 1 = 1 + 0$ por la propiedad 1 de la suma.

Sea ahora un número $a \in K$ lo que significa que $a + 1 = 1 + a$.

comprobemos que $s(a) \in K$

En efecto:

$$s(a) + 1 = (a + 1) + 1$$

por la propiedad 1 de la suma y, además como $a \in K$ entonces

$$(a + 1) + 1 = (1 + a) + 1 = s(1 + a) = 1 + (a + 1) = 1 + s(a)$$

Con lo que podemos concluir que $s(a) \in K$.

Según el axioma 5 de Peano si el $0 \in K$ y de $a \in K$ se sigue que también $s(a) \in K$ entonces se llega a la igualdad $K = \mathbb{N}$.

Con esto hemos demostrado que todos los números naturales poseen la propiedad conmutativa con el 1. Para que la demostración esté completa hay que probar que conmutan todos entre sí y para ello consideremos un nuevo conjunto $M = \{n \in \mathbb{N} / a + n = n + a\}$.

Seguimos el mismo esquema:

$$0 \in M \text{ ya que } a + 0 = 0 + a.$$

Consideremos un número $b \in M$ entonces se verifica: $a + b = b + a$ y tratemos de probar si $s(b) \in M$.

$$a + s(b) = a + (b + 1)$$

Aplicando la condición 2 de la suma:

$$a + (b + 1) = s(a + b)$$

Como $b \in M \Rightarrow s(a+b) = s(b+a) = b+(a+1) = b+(1+a)$ aplicando ahora la propiedad asociativa $\Rightarrow b+(1+a) = (b+1)+a = s(b)+a$.

Por tanto $a+s(b) = s(b)+a$.

Puesto que se verifican las dos condiciones del axioma 5 de Peano podemos concluir que el conjunto $M = \mathbb{N}$ y, en consecuencia, todo par de números naturales con la suma verifican la propiedad conmutativa. ■

Elemento neutro: $\exists 0 \in \mathbb{N}, \forall n \in \mathbb{N}, n+0 = 0+n = n$

Demostración: Aplicamos el axioma 5 de inducción como en las anteriores demostraciones.

Definimos el conjunto $K = \{n \in \mathbb{N} / n+0 = 0+n\}$ y demostraremos que $K = \mathbb{N}$.

El $0 \in K$ ya que $n+0 = n = 0+n$ por la propiedad 1 de la suma.

Consideremos un número $a \in K$ y por tanto $a+0 = 0+a$, veamos si $s(a) \in K$

$$s(a)+0 = s(a) = s(a+0)$$

Como $a \in K$

$$s(a+0) = s(0+a) = 0+s(a)$$

y por la propiedad 1 de la suma:

$$0+s(a) = s(a) \Rightarrow s(a) \in K \quad \blacksquare$$

Con la demostración de estas propiedades para la suma, hemos probado que el par formado por el conjunto \mathbb{N} y la operación interna $+$, es decir, $(\mathbb{N}, +)$ tiene estructura de **semigrupo conmutativo con elemento neutro**.

2.2. Multiplicación

Consideramos la multiplicación de números naturales como la aplicación $f: \mathbb{N} \times \mathbb{N} \rightarrow \mathbb{N}$ que verifica:

$$1) f(n, 0) = n \times 0 = 0, \forall n \in \mathbb{N}$$

$$2) f(n, s(m)) = f(n, m) + n, \forall n, m \in \mathbb{N}$$

Esta aplicación así definida se puede demostrar que existe y está definida de forma única siguiendo los mismos pasos que para la suma.

La multiplicación de dos números naturales $a, b \in \mathbb{N}$ queda definida de la siguiente manera usando el símbolo habitual del punto: " \cdot "

$$\forall a, b \in \mathbb{N}, a \cdot b = \cdot(a, b) / \left\{ \begin{array}{l} \cdot(a, 0) = a \cdot 0 = 0 \\ \cdot(a, s(b)) = a \cdot b + a \end{array} \right\} \begin{array}{l} \rightarrow \text{propiedad 1} \\ \rightarrow \text{propiedad 2} \end{array}$$

Propiedades:

Siguiendo pasos similares a los utilizados para demostrar las propiedades de la suma se pueden demostrar las propiedades para la multiplicación. Sólo demostraremos en este apartado la propiedad distributiva.

Asociativa: $\forall a, b, c \in \mathbb{N}, (a \cdot b) \cdot c = a \cdot (b \cdot c)$

Conmutativa: $\forall a, b \in \mathbb{N}, a \cdot b = b \cdot a$

Elemento neutro: \exists un número $1 \in \mathbb{N} / \forall n \in \mathbb{N}, 1 \cdot n = n = n \cdot 1$

Distributiva de la multiplicación respecto a la suma:

$$\forall a, b, c \in \mathbb{N}, (a + b) \cdot c = a \cdot c + b \cdot c \quad \text{y} \quad \forall a, b, c \in \mathbb{N}, c \cdot (a + b) = c \cdot a + c \cdot b$$

Demostración: Vamos a demostrar la propiedad distributiva por la derecha; por la izquierda se haría de forma análoga:

Consideremos el conjunto:

$$\mathbf{K} = \{n \in \mathbb{N} / (a + b) \cdot n = a \cdot n + b \cdot n\} \forall a, b \in \mathbb{N}$$

Demostraremos por el principio de inducción, como en casos anteriores, que $\mathbf{K} = \mathbb{N}$

Primero: $0 \in \mathbf{K}$. En efecto, por definición de la multiplicación $(a + b) \cdot 0 = 0$ y $a \cdot 0 + b \cdot 0 = 0 + 0 = 0$

Ahora consideramos un número $c \in \mathbf{K}$, por tanto verificará: $(a + b) \cdot c = a \cdot c + b \cdot c$ y veamos que $s(c)$ también pertenece a \mathbf{K} .

$$(a + b) \cdot s(c) = (a + b) \cdot c + (a + b)$$

por definición de la multiplicación y puesto que $c \in \mathbf{K}$

$$(a + b) \cdot c + (a + b) = a \cdot c + b \cdot c + a + b$$

aplicando sobre esta expresión las propiedades conmutativa y asociativa de la suma obtenemos la siguiente expresión:

$$a \cdot c + a + b \cdot c + b = a \cdot s(c) + b \cdot s(c).$$

Hemos aplicado el axioma 5 de Peano ya que vemos que si $0 \in \mathbf{K}$ y que

$$c \in \mathbf{K} \Rightarrow s(c) \in \mathbf{K} \Rightarrow \mathbf{K} = \mathbb{N}$$

Con lo que queda demostrada la propiedad distributiva de la multiplicación respecto de la suma. ■

El conjunto \mathbb{N} con las operaciones internas suma (+) y multiplicación (\cdot) es decir, la terna $(\mathbb{N}, +, \cdot)$ cumpliendo las propiedades expuestas, le da estructura de **semianillo conmutativo con elemento neutro**.

3. Divisibilidad

Dados dos números naturales $a \neq 0$ y $b \neq 0$, decimos que **a es divisible por b** o que **b es divisor de a** si \exists un número $c \in \mathbb{N}/a = b \cdot c$, es decir, cuando la división del primero por el segundo es exacta. También se puede decir que **a es múltiplo de b**.

- La relación "a es divisible por b" es una relación binaria de orden parcial.

La forma simbólica de definir la relación entre el par (a,b) es:

$$a/b \Leftrightarrow \exists c \in \mathbb{N}/b = a \cdot c, \quad a, b, c \in \mathbb{N} \text{ y } a \neq 0$$

Esta relación binaria define sobre \mathbb{N} un orden parcial porque hay números naturales no relacionados, por ejemplo: $(2,3)$, $(5,17)$, etc.

Verifica las propiedades:

- Reflexiva: $\forall a \in \mathbb{N}, a/a$, pues $a = a \cdot 1$
- Antisimétrica: Si a/b y $b/a \Rightarrow a = b$

pues $\left. \begin{array}{l} \text{Si } a/b \Rightarrow \exists c \in \mathbb{N}/b = a \cdot c \\ \text{Si } b/a \Rightarrow \exists d \in \mathbb{N}/a = b \cdot d \end{array} \right\} \Rightarrow$ sustituyendo en la primera igualdad

el valor de la segunda se tiene que: $b = b \cdot d \cdot c \Rightarrow d = 1 \text{ y } c = 1 \Rightarrow a = b$

- Transitiva: Si a/b y $b/c \Rightarrow a/c$

Si $\left. \begin{array}{l} \text{Si } a/b \Rightarrow \exists d_1 \in \mathbb{N}/b = a \cdot d_1 \\ \text{Si } b/c \Rightarrow \exists d_2 \in \mathbb{N}/c = b \cdot d_2 \end{array} \right\} \Rightarrow$ sustituimos el valor de b en la

segunda igualdad, teniendo que: $c = a \cdot d_1 \cdot d_2$ por tanto

$\exists z = d_1 \cdot d_2 / c = a \cdot z$ y a/c

Propiedades

- El 1 es divisor de cualquier número natural: $1/n, \forall n \in \mathbb{N}$

3.1. Múltiplo

El conjunto de todos los múltiplos de un número natural n , se simboliza $\overset{\circ}{a}$

$$\overset{\circ}{a} = \{a \cdot n, \forall n \in \mathbb{N}\}$$

- Todo número es múltiplo de sí mismo y de la unidad:
- Los múltiplos son compatibles con la suma, es decir, si dos números son múltiplos de un mismo número, su suma también lo es.
- Si un número a es múltiplo de uno b entonces todos los múltiplos de a lo son también de b .

3.2. Divisor

Denotamos por $D(a)$ al conjunto de los divisores de cualquier número natural a , de forma simbólica:

$$D(a) = \{n \in \mathbb{N}, n \neq 0; \exists c \in \mathbb{N}/a = c \cdot n\}$$

- El cero no es divisor de ningún número natural
- El 1 es divisor de cualquier número natural.
- Todo número natural distinto de cero es divisor de sí mismo.
- Los divisores son compatibles con la suma, es decir, si un número natural a es divisor de otros b, c, \dots , lo es también de su suma $b + c + \dots$
- Todo número natural divisor de otro, también lo será de sus múltiplos.

Para calcular los divisores de un número, lo dividimos entre los números naturales menores que él, y anotamos los que den división exacta, es decir, resto cero. Veremos procedimientos que simplifican este método.

Definición | Un número es **primo** si sólo es divisible por sí mismo y por 1.

Definición | Si un número no es primo entonces diremos que es **compuesto**.

Propiedades

- Todo número compuesto puede ser descompuesto en factores primos. Si $n \in \mathbb{N}$ es primo, entonces $n = n \cdot 1$
- Siendo $n \in \mathbb{N}$ es compuesto $\Rightarrow n = a^k \cdot b^l \cdot c^r \cdot \dots$ con a, b, c, \dots primos (Teorema fundamental de la aritmética)

Ejemplo

$$\begin{array}{r|l}
 90 & 2 \\
 45 & 3 \\
 15 & 3 \Rightarrow 90 = 2 \cdot 3^2 \cdot 5 \\
 5 & 5 \\
 1 &
 \end{array}$$

Para simplificar este proceso y saber cuándo un número es divisible por otro número, generalmente primo, sin necesidad de realizar la división, se utilizan los criterios de divisibilidad. Los más usados son los siguientes:

Número	Criterio
2	Acaba en 0 o en cifra par
3	La suma de sus dígitos es un múltiplo de 3
4	Lo es el número formado por los dos últimos dígitos
5	Acaba en 0 o en 5
6	Lo es de 2 y de 3 al mismo tiempo.
8	Lo es el número formado por los tres últimos dígitos
9	La suma de sus dígitos es un múltiplo de 9
10	Acaba en cero

11	La diferencia entre la suma de las cifras que ocupan lugar impar y la suma de las que ocupan lugar par ha de ser múltiplo de 11
25	Si acaba en 00, 24, 50, 75

Nota: En un documento aparte se explicará el procedimiento para obtener los criterios de divisibilidad de los diferentes números.

Definición Se define el **máximo común divisor** (m.c.d.) de dos o más números naturales como el mayor divisor posible de todos ellos.

Ejemplo

Calcular el m.c.d. (18, 30)

Para ello obtenemos los divisores de cada uno de los números:

Divisores de 18: 1, 2, 3, 6, 9, 18

Divisores de 30: 1, 2, 3, 5, 6, 10, 15, 30.

Observamos que los divisores 1, 2, 3, 6 son comunes a ambos números. El mayor es 6 y por tanto se tiene que:

$$\text{m.c.d. (18, 30)} = 6$$

Para números muy grandes esta forma de obtener el m.c.d. puede llegar a ser muy laboriosa, existe otro método de aplicación más rápida aplicando la descomposición en factores primos y es el siguiente:

- Se descomponen los números en factores primos.
- El m.c.d. de esos números se obtiene tomando los factores primos comunes, elevados al menor exponente.

Ejemplo

Vamos a calcular el m.c.d. (90, 75)

Descomponemos en factores primos

$$\begin{array}{r|l} 90 & 2 \\ 45 & 3 \\ 15 & 3 \Rightarrow 90 = 2 \cdot 3^2 \cdot 5 \\ 5 & 5 \\ 1 & \end{array} \quad \begin{array}{r|l} 75 & 3 \\ 25 & 5 \\ 5 & 5 \\ 1 & \end{array} \Rightarrow 75 = 3 \cdot 5^2$$

El m.c.d (90,75) = $3 \cdot 5 = 15$

El algoritmo de Euclides

El algoritmo de Euclides es un método para calcular el máximo común divisor (**m.c.d.**) de dos números mediante divisiones sucesivas.

En la primera división, se toma como dividendo el mayor de los números y como divisor el otro. En una siguiente división se dividen el divisor y el resto. El proceso se continúa y finalizará cuando se obtenga un resto nulo. El **m.c.d.** será el penúltimo resto del algoritmo.

Teorema Si dos números a y b ($a > b$) no son divisibles el uno por el otro, los divisores comunes de a y b son los mismos que los de b y r , siendo r el resto de la división entera de a entre b , por tanto:

$$\text{m.c.d.}(a, b) = \text{m.c.d.}(b, r),$$

Demostración

Sea $d = \text{m.c.d.}(a, b)$ y $t = \text{m.c.d.}(b, r)$, vamos a demostrar que $d = t$.

Si $d = \text{m.c.d.}(a, b) \Rightarrow d/a$ y d/b entonces

$$a = a_1 \cdot d \quad \text{y} \quad b = b_1 \cdot d.$$

Por otro lado, por el algoritmo de la división se tiene que

$$a = b \cdot q + r, \quad 0 \leq r < b \quad (1)$$

De donde llegamos a:

$$r = a - b \cdot q = a_1 \cdot d - b_1 \cdot d + r = (a_1 - b_1) \cdot d + r$$

Por tanto $d/(a - qb)$. Luego d es divisor común de b y r . Como ya teníamos que también es un divisor de d entonces divide a su **m.c.d.**, esto es d es un divisor de t .

Por otra parte, t es un divisor común de b y r , por ello luego $b = b_2 \cdot t$ y $r = r_1 \cdot t$. Sustituyendo estas igualdades en la expresión (1):

$$a = b \cdot q + r = b_2 t \cdot q + r_1 \cdot t = (b_2 q + r_1) \cdot t$$

De lo anterior tenemos que t es un divisor común de a y b , entonces también lo es de su **m.c.d.**, es decir t es divisor de d .

Como t es divisor de d y también d es divisor de $t \Rightarrow t = d$ ■

Ejemplo

Vamos a calcular el m.c.d.(90, 75) utilizando el algoritmo de Euclides

$$\begin{array}{r} 90 \overline{) 75} \\ \underline{15} \\ 15 \end{array}$$

$$\begin{array}{r} 75 \overline{) 15} \\ \underline{0} \\ 0 \end{array}$$

→ El m.c.d (90,75)=15

Ejemplo

Vamos a calcular ahora el m.c.m.(90, 25)

$$\begin{array}{r} 90 \overline{) 25} \\ \underline{15} \\ 15 \end{array}$$

$$\begin{array}{r} 25 \overline{) 15} \\ \underline{10} \\ 10 \end{array}$$

$$\begin{array}{r} 15 \overline{) 10} \\ \underline{5} \\ 5 \end{array}$$

$$\begin{array}{r} 10 \overline{) 5} \\ \underline{0} \\ 0 \end{array}$$

→ El m.c.d (90,25)=5

Definición El **mínimo común múltiplo** (m.c.m.) de varios números es el menor de sus múltiplos comunes.

Ejemplo

Calcular el m.c.m.(6, 8)

Múltiplos de 6: 6, 12, 18, 24, 30, 36, 42, 48, 54, ..

Múltiplos de 8: 8, 16, 24, 32, 40, 48, 56, ...

Observamos que el 24 es el mas pequeño de los múltiplos comunes y por eso escribimos:

m.c.m.(6, 8) = 24

También para calcular el m.c.m. de dos o más números se puede seguir un procedimiento que simplifica el anterior que consta de los siguientes pasos:

- se descomponen los números en factores primos

- el m.c.m de esos números se obtiene tomando los factores comunes y no comunes siempre los de mayor exponente.

Ejemplo

Vamos a calcular el m.c.m.(90, 75)

$$\begin{array}{r|l}
 90 & 2 \\
 45 & 3 \\
 15 & 3 \Rightarrow 90 = 2 \cdot 3^2 \cdot 5 \\
 5 & 5 \\
 1 &
 \end{array}
 \qquad
 \begin{array}{r|l}
 75 & 3 \\
 25 & 5 \\
 5 & 5 \Rightarrow 75 = 3 \cdot 5^2 \\
 1 &
 \end{array}$$

El **m.c.m. (90,75)** = $2 \cdot 3^2 \cdot 5^2 = 450$

4.Ordenación en N

Un número natural **a es menor que un número natural b** si existe un número natural c tal que $a + c = b$. En este caso se escribe $a < b$ o también $b > a$.

En lenguaje simbólico se escribe así:

$$a < b \Leftrightarrow \exists c \in \mathbb{N} / a + c = b$$

Esta es una relación binaria definida sobre el conjunto de los números naturales: $(a,b) \in \mathbb{N}$ que verifica lo siguiente:

Teorema 4 Todo número distinto del 0 es mayor que él, es decir:

$$\forall n \in \mathbb{N}, n \neq 0 \Rightarrow 0 < n$$

Demostración:

Sea $n \in \mathbb{N}, n \neq 0 \Rightarrow n = n + 0 > 0$ pues $n \neq 0 \Rightarrow 0 < n$ ■

Teorema 5 $\forall a, n \in \mathbb{N}$ sólo se verifica una de las siguientes relaciones:

a) $n = a$

b) $n < a$

c) $a < n$

Demostración:

Vamos a considerar el siguiente conjunto auxiliar K_n tal y como hemos hecho en demostraciones anteriores:

$$K_n = \{a/n = a \text{ ó } n < a \text{ ó } a < n\}$$

y veamos que $K_n = \mathbb{N}$

Primero demostremos que $0 \in K_n$

Si $n = 0 \Rightarrow 0 = 0 = n$ se verifica a) y $0 \in K_n$

Si $n \neq 0 \Rightarrow$ por el teorema 4 $0 < n$ se cumple c) y $0 \in K_n$

Supongamos ahora un valor $a \in K_n$ y demostremos que $s(a) \in K_n$

$a \in K_n \Rightarrow$ se verifica que $n = a$ ó $n < a$ ó $a < n$

$n = a \Rightarrow s(a) = a + 1 > a \Rightarrow s(a) > n$ verifica b) y $s(a) \in K_n$

$n < a \Rightarrow \exists b \neq 0/n + b = a$

$s(a) = a + 1 = (n + b) + 1 = n + (b + 1) = n + s(b) > n$ pues $s(b) \neq 0$

$\Rightarrow s(a) > n$, es decir, $n < s(a)$ se cumple b) y $s(a) \in K_n$

$a < n \Rightarrow \exists c \neq 0/a + c = n$

Como $c \neq 0$

$\exists z \in \mathbb{N}/c = s(z)$ entonces:

$$a + c = a + s(z) = n$$

y

$$a + s(z) = a + (1 + z) = (a + 1) + z = s(a) + z$$

y por la propiedad conmutativa

$$s(a) + z = n \Rightarrow s(a) < n.$$

Puede ocurrir que

$$z = 0 \Rightarrow s(a) = n \text{ o bien que } z \neq 0 \Rightarrow s(a) < n$$

En cualquier caso $s(a) \in K_n$

Con esto tenemos que, aplicando el axioma de inducción $K_n = \mathbb{N}$



- Además vamos a ver que **la relación es excluyente, si se verifica $n < a$, entonces no se puede verificar $a < n$.**

Demostración: Supongamos por reducción al absurdo que se pueden dar las dos a la vez:

$$\left. \begin{array}{l} n < a \Rightarrow \exists b \neq 0 / n + b = a \\ a < n \Rightarrow \exists c \neq 0 / a + c = n \end{array} \right\} \Rightarrow \text{sumando "c" en ambos miembros de la 1ª igualdad}$$

$$\Rightarrow n + b + c = a + c \Rightarrow n + b + c = n \text{ con } b \neq 0 \text{ y } c \neq 0 \text{ absurdo pues } n = n \blacksquare$$

- **La relación de orden " $<$ " es compatible con la suma y producto de números naturales**

Esto significa que:

$$\text{Si } a < b \Rightarrow a + c < b + c, \forall c \in \mathbb{N}$$

$$\text{Si } a < b \Rightarrow a \cdot c < b \cdot c, \forall c \in \mathbb{N}$$

4.1. $(\mathbb{N}, <)$ es un conjunto estrictamente ordenado

La relación " $<$ " es de orden estricto porque verifica las propiedades:

- Antirreflexiva: $\forall a \in \mathbb{N}, a \not< a$,
- Antisimétrica: Si $a < b$ y $b < a \Rightarrow a = b$
- Transitiva: Si $a < b$ y $b < c \Rightarrow a < c$

4.2. (\mathbb{N}, \leq) La relación " \leq " sobre \mathbb{N} es de orden total

La relación " \leq " es de orden pues verifica las propiedades:

- Reflexiva: $\forall a \in \mathbb{N}, a \leq a$, pues $a = a$
- Antisimétrica: Si $a \leq b$ y $b \leq a \Rightarrow a = b$
- Transitiva: Si $a \leq b$ y $b \leq c \Rightarrow a \leq c$

Y además para que sea de orden total debe verificar que dos elementos cualesquiera del conjunto \mathbb{N} están relacionados

Con todo esto podemos afirmar que $(\mathbb{N}, +, \cdot, \leq)$ es un semianillo totalmente ordenado llamado, **semianillo ordenado** de los números naturales

5. Sistemas de numeración

“La conciencia del número se hizo lo suficientemente extendida y clara como para que se llegase a sentir la necesidad de expresar esta propiedad en un lenguaje simbólico. Los dedos de la mano pueden usarse fácilmente para representar un conjunto de dos, tres, cuatro o cinco objetos. Cuando el uso de los dedos resultaba ya inadecuado, podían utilizarse pequeños montones de piedras, y cuando el hombre primitivo utilizaba este sistema de representación, a menudo amontonaba las piedras por grupos de cinco en cinco, debido a que antes se había familiarizado con los quíntuplos de objetos por observación de su propia mano o pie. Como hizo observar Aristóteles, lo extendido que se halla el uso del sistema decimal no es sino la consecuencia del accidente anatómico de que la mayor parte de nosotros nacemos con diez dedos en las manos y otros diez en el pie. Lo que distingue de manera más notable al hombre del resto de los animales es el lenguaje articulado, lenguaje cuyo desarrollo fue esencial para el nacimiento del pensamiento matemático abstracto. Sin embargo, las palabras para expresar ideas numéricas aparecieron muy lentamente, los signos para representar números precedieron con toda probabilidad a las palabras para representar números. Las lenguas modernas están construidas casi sin excepción sobre la base de numeración diez, de manera que un número como diecisiete, se describe como diez y siete.

Extracto de “Historia de la matemática”. Carl B. Boyer

El conjunto de números naturales es infinito; para nombrarlos necesitaríamos infinitas palabras y para escribirlos infinitos signos o símbolos. De aquí surge la necesidad de buscar un conjunto finito de palabras, símbolos y reglas que nos permitan determinar todos los números naturales con precisión y comodidad.

Definición | Un **sistema de numeración** es un par $\{S, R\}$ donde S es un conjunto de símbolos y R un conjunto de reglas y convenios que utilizamos para nombrar y escribir los números empleando la menor cantidad posible de palabras y símbolos.

Los símbolos de S se llaman **cifras** y el cardinal del conjunto S es la **base** del sistema de numeración.

El actual sistema de numeración que utilizamos en nuestro entorno cultural y que llamamos usualmente el sistema hindú, no consiste más que en una combinación de tres principios básicos:

- 1) una forma cifrada para cada uno de los diez numerales básicos.

- 2) una base decimal
- 3) una notación posicional

Al-Khowarizmo escribió dos libros sobre Aritmética y Álgebra que jugaron un papel muy importante en la historia de las matemáticas. El primero de ellos nos ha llegado sólo a través de una copia única de una traducción latina con el título “De numero indorum” (o “Sobre el arte de calcular hindú). En esta obra, que estaba basada presumiblemente en una traducción árabe de Brahmagupta, daba Al-Khowarizmi una exposición tan completa del sistema de numeración hindú, que es probablemente el responsable de la extendida aunque falsa impresión de que nuestro sistema de numeración es de origen árabe.

Extracto de “Historia de la matemática”. Carl B. Boyer

El **sistema de numeración decimal**, al tener base 10 contiene 10 cifras que se llaman también **dígitos**:

- 1) $S = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$ los 10 primeros números naturales
- 2) Cada 10 unidades de un orden determinado constituyen una unidad de orden inmediatamente superior, así:
10 unidades de orden $n-1 = 1$ unidad de orden $n = 10^{n-1}$
- 3) Escribimos cada número de derecha a izquierda como una secuencia finita formada a partir de los símbolos anteriores de manera que, el valor de dichos símbolos depende de la posición que ocupe:

$$23\ 710 = 20\ 000 + 3\ 000 + 700 + 10 + 0 = 2 \cdot 10^4 + 3 \cdot 10^3 + 7 \cdot 10^2 + 1 \cdot 10^1 + 0 \cdot 10^0$$

Mediante estos tres principios podemos construir sistemas de numeración usando otras bases.

Los Babilonios usaron un sistema de numeración de base 60 que ha llegado hasta hoy aplicado a la medida de ángulos o del tiempo; los Mayas otro con base 20 y con la aparición de ordenadores se ha dado mucho auge a los sistemas binario (base 2), octal (base 8) y hexadecimal (base 16).

Cuando la base del sistema es mayor de 10, se añaden las primeras letras del alfabeto, así para el sistema hexadecimal el conjunto S viene dado por:

$$S = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, A, B, C, D, E, F\}$$

de manera que $A = 10, B = 11, \dots, F = 15$.

5.1. Teorema fundamental de la numeración

Todo $n \in \mathbb{N}$ se puede escribir de forma única en base $b, b \in \mathbb{N}$, y $b > 1$ como:

$$n = r_0 b^0 + r_1 b^1 + r_2 b^2 + \dots + r_{k-1} b^{k-1} + r_k b^k, \text{ con } r_0, r_1, \dots, r_k \in \mathbb{N} \text{ y } r_0, r_1, \dots, r_k < b$$

Para abreviar escribiremos:

$$n = \sum_{i=1}^k r_i b^i, \text{ con } r_i \in \mathbb{N} \text{ y } r_i < b \quad \forall i = 1, \dots, k$$

Demostración: Consideremos dos casos:

- Si $n \leq b \Rightarrow n = n \cdot b^0$ de forma única
- Si $n > b \Rightarrow$ dividimos n entre b , y si el cociente $c_i \geq b$, volvemos a repetir el proceso hasta obtener un cociente $c_i < b$. Es decir:

$\begin{array}{r} n \mid b \\ r_0 \quad c_1 \quad \swarrow b \\ \quad r_1 \quad c_2 \quad \swarrow b \\ \quad \quad r_2 \quad c_3 \quad \dots \end{array}$	$n = b \cdot c_1 + r_0, \quad r_0 < n$
	$c_1 = b \cdot c_2 + r_1, \quad r_1 < n$
	$c_2 = b \cdot c_3 + r_2, \quad r_2 < n$
	...
$\begin{array}{r} c_{k-1} \mid b \\ r_{k-1} \quad c_k = r_k \end{array}$	$c_{k-1} = b \cdot c_k + r_{k-1}, \quad r_{k-1} < n$
	$c_k = r_k, \quad r_k < n$

De la primera igualdad tenemos que $n = b \cdot c_1 + r_0$, y sustituyendo las demás igualdades llegamos a la expresión:

$$n = r_0 b^0 + r_1 b^1 + r_2 b^2 + \dots + r_{k-1} b^{k-1} + r_k b^k \quad \blacksquare$$

• **Principio del valor relativo**

Para escribir un número natural n en una base b

$$n = r_0 b^0 + r_1 b^1 + r_2 b^2 + \dots + r_{k-1} b^{k-1} + r_k b^k, \text{ con } r_0, r_1, \dots, r_k \in \mathbb{N} \text{ y } r_0, r_1, \dots, r_k < b$$

escribimos sus cifras de manera ordenada de la siguiente manera:

$$n = r_k r_{k-1} \dots r_2 r_1 r_0$$

teniendo en cuenta que el valor de una cifra viene determinado por el lugar que ésta ocupa. (Principio del valor relativo)

Ejemplo

Vamos a calcular cómo sería la expresión de 253 en base 4:

253	4				
1	83	4			
	3	20	4		
		0	5	4	
			1	1	

$$253_{(10)} = 11031_{(4)}$$

5.2. Representación de números en diferentes bases

Las conversiones entre números de bases diferentes se efectúan por medio de operaciones aritméticas simples.

- **Conversión de la base decimal a otra base b**

Para esta conversión se emplea el método de **divisiones sucesivas**.

Se va dividiendo la cantidad decimal por b, apuntando los restos, hasta obtener un cociente cero. El último resto obtenido es la primera cifra del número en base b y el primero es la última.

Ejemplo

Convertir el número 250 a binario.

250	2						
0	125	2					
	1	62	2				
		0	31	2			
			1	15	2		
				1	7	2	
					1	3	2
						1	1

$$250_{(10)} = 11111010_{(2)}$$

- **Conversión de base b a la base decimal**

Hay que realizar las operaciones de la expresión polinómica del número:

$$n = r_0b^0 + r_1b^1 + r_2b^2 + \dots + r_{k-1}b^{k-1} + r_kb^k$$

De forma práctica es suficiente con realizar el cálculo del valor numérico de un polinomio.

Ejemplo

Convertir el número $240_{(5)}$ a decimal.

	2	4	0
5		10	70
	2	14	70

$$240_{(5)} = 70_{(10)}$$

6. Operaciones en cualquier sistema de numeración

6.1. Suma

Tanto en el sistema decimal como en otro cualquiera, sumamos primero las unidades, pasamos luego al orden siguiente, etc., hasta llegar al mayor de los órdenes, teniendo en cuenta que, pasamos al orden siguiente cada vez que en un orden se obtiene una suma mayor o igual a la base del sistema empleado.

Ejemplo

Vamos a sumar los números $230_{(4)}$ y $113_{(4)}$.

	1		
	2	3	0
+	1	1	3
1	0	0	3

$$230_{(4)} + 113_{(4)} = 1003_{(4)}$$

Como $3+1=4$ que es la base ponemos 0 y añadimos 1 unidad al siguiente orden

6.2. Multiplicación

La multiplicación de los números se basa en la tabla de multiplicar que ofrece el producto de los números menores que la base del sistema de numeración, es decir en base b , para todo $n < b$, ésta se construye mediante la suma reiterada.

Por ejemplo, en el sistema en base 6, comprobar que la tabla de multiplicar del sistema senario es:

	0	1	2	3	4	5
0	0	0	0	0	0	0
1	0	1	2	3	4	5
2	0	2	4	10	12	14
3	0	3	10	13	20	23
4	0	4	12	20	24	32
5	0	5	14	23	32	41

En cada celda aparece el producto de los números que corresponden a la

fila y a la columna de esa celda, con la particularidad de que todos los números se escriben en base 6. Valiéndonos de esta tabla podemos multiplicar fácilmente "en columna" dos números cualesquiera:

Ejemplo

Vamos a multiplicar los números $154_{(6)}$ y $352_{(6)}$.

				1	5	$4_{(6)}$
			X	3	5	$2_{(6)}$
				3	5	$2_{(6)}$
	1	3		4	$2_{(6)}$	
	5	5	$0_{(6)}$			
1	1	3		2	6	$2_{(6)}$

$$154_{(6)} \times 352_{(6)} = 113262_{(6)}$$

6.3.División

Para realizar la división de dos números cualesquiera en un sistema de numeración de base "b" hacemos la división «en ángulo» apoyándonos en la tabla de multiplicar de dicha base. Veamos el siguiente ejemplo con números en base 4, por lo que usaremos la siguiente tabla de multiplicación correspondiente a esta base:

	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	10	12
3	0	3	12	21

Ejemplo

Vamos a dividir el número $2103_{(4)}$ entre $12_{(4)}$.

$2103_{(4)}$	$12_{(4)}$						
030	$120_{(4)}$						
003 $_{(4)}$							

$$2103_{(4)} : 12_{(4)} = 120_{(4)} \times 12_{(4)} + 3_{(4)}$$