Tema 1: Números naturales. Sistemas de numeración

Javier Martín-García

E-mail: , javier@javiermg.com

Abstract

Contents

1 Introducción

1.1 Historia

Contar fue la primera aproximación a las matemáticas del ser humano. Varias civilizaciones de la edad antigua desarrollan técnicas para operar y representar números.

Las primeras formas surgen básicamente por la necesidad de transmitir información acerca de la cantidad de elementos de un conjunto concreto; utilizando en algunos casos partes del cuerpo humano, palos, piedras, muescas, nudos en cuerdas, etc. Sin embargo, hasta que no se introduce la escritura no encontramos los primeros vestigios de los primeros sistemas de numeración que abstraían el concepto de número natural.

La definición formal de los números naturales, no obstante, no llega hasta el siglo XIX. En este momento se propondrían dos formalizaciones diferentes desde dos puntos de vista: el axiomático, impulsado por Dedekin y Peano; y aquel basado en su estudio a través de clases de equivalencia, propuesto por Frege y Russel.

1.2 Marco curricular

El tema que nos ocupa se engloba dentro del bloque correspondiente a la aritmética y la teoría de números, rama esta una de las más antiguas y esenciales de la matemática desde un punto de vista histórico. A nivel curricular, y tal y como se detalla en el *DECRETO 39/2022 y el DECRETO 40/2022 de 29 de septiembre, por por los que se establece la ordenación y el currículo de la educación secundaria obligatoria y bachillerato en la Comunidad de Castilla y León*, los fundamentos de la aritmética tienen cabida en el bloque de contenidos 'A. Sentido numérico' que comprende aspectos como el conteo, el estudio de las cantidades, el sentido de las operaciones, el estudio de relaciones, el razonamiento proporcional o la educación financiera.

1.3 Notación y convenciones

A lo largo de este tema, consideraremos el conjunto de los números naturales incluyendo el cero, y que denotaremos $\mathbb{N}$. En caso de que queramos excluir el cero utilizaremos la notación

$\mathbb{N}^* = \mathbb{N} - \{0\}$.

2 Los números naturales $\mathbb{N}$. Definición

De las dos opciones mencionadas en la introducción optaremos en lo sucesivo por la definición axiomática. Así pues, el siguiente conjunto de axiomas define el conjunto de los naturales

2.1 Axiomas de Peano

1. El 0 es un número natural.
2. Si n es un número natural, entonces el sucesor de n también es un número natural.
3. El 0 no es el sucesor de ningún número natural.
4. Si hay dos números naturales n y m con el mismo sucesor, entonces $n = m$.
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.

Una forma equivalente y más moderna de presentar estos axiomas es la siguiente: denominamos conjunto de los números naturales al par $(\mathbb{N}, s)$, donde $\mathbb{N}$ es un conjunto no vacío con un elemento distinguido $0 \in \mathbb{N}$ y s es una aplicación biyectiva

$$s : \mathbb{N} \to \mathbb{N}^*; n \to s(n)\,, \tag{1}$$

donde se suele denotar $s(n)$ como el *sucesor* de n. Dicha aplicación se define de tal modo que posee la siguiente propiedad (que es equivalente al axioma 5 de Peano):

Axioma de inducción *El único subconjunto de* $\mathbb{N}$ *que contiene al* 0 *y a todos los sucesores de cada uno de sus elementos es el propio* $\mathbb{N}$.

De estas propiedades se deduce que el conjunto $\mathbb{N}$ es infinito (por tratarse s de una biyección).

2.2 Pruebas por inducción

El axioma de inducción nos servirá en las próximas secciones para diversas pruebas y definiciones. La estrategia de las mismas será la siguiente: dada una propiedad $P(n)$ con $n \in \mathbb{N}$

- Consideramos el subcojunto $S_P \subseteq \mathbb{N}$ tal que $P(n)$ con $n \in S_P$ es cierta
- Comprobamos que $0 \in S_P$
- Comprobamos que para todo $k \in S_P$ su sucesor $s(k) \in S_P$

Si estas dos proposiciones son ciertas, se seguirá del axioma de inducción que $S_P = \mathbb{N}$ y que por tanto P es una propiedad de $\mathbb{N}$.

3 Operaciones en $\mathbb{N}$: suma y producto. Estructura algebraica de $\mathbb{N}$

Una vez definido un conjunto, el siguiente paso natural es definir operaciones internas en el mismo. A continuación por tanto definiremos dos de ellas (suma y producto) y estudiaremos sus propiedades.

3.1 Suma o adición en $\mathbb{N}$

Definición: Podemos definir de forma única la aplicación suma σ

$$\sigma \quad : \quad \mathbb{N} \times \mathbb{N} \to \mathbb{N}\,; \forall p, q \in \mathbb{N}; \tag{2}$$

$$i) \quad \sigma(p, 0) = p\,, \tag{3}$$

$$ii) \quad \sigma(p, s(q)) = s(\sigma(p, q))\,. \tag{4}$$

cuya notación convencional es $\sigma(p, q) = p + q$.

Demostración. Existencia y unicidad de la suma Demostremos la existencia y unicidad de esta operación. Para la existencia, consideramos el subconjunto de los naturales S_σ para los cuales existe la suma con las propiedades definidas arriba

$$S_\sigma = \{p \in \mathbb{N} : \exists\, \sigma(p, q)\ \forall q \in \mathbb{N}\} \tag{5}$$

Es obvio que $0 \in S_\sigma$, pues basta con escoger $\sigma(0,q)$ como la aplicación identidad para comprobar que se cumplen ambas propiedades. Por otro lado, si asumimos que existe un cierto $p \in S_\sigma$, esto es, existe $\sigma(p,q)$ tal que cumple las propiedades (3) y (4), entonces podemos comprobar que $s(p) \in S_\sigma$ ya que[1]

$$i) \quad \sigma(s(p),0) = \sigma(0,s(p)) = s(\sigma(0,p)) = s(p)\,, \tag{6}$$

$$ii) \quad \sigma(s(p),s(q)) = \sigma(s(q),s(p)) = s(\sigma(s(q),p)) = s[s(\sigma(q,p))] = s(\sigma(s(p),q))\,. \tag{7}$$

Para la unicidad, supondremos que existen dos aplicaciones diferentes $\sigma(p,q)$ y $\tau(p,q)$ tales que cumplen las propiedades de la definición. La estrategia será construir para cada p el subconjunto $S_p \subseteq \mathbb{N}$ en el cual $\sigma(p,q) \equiv \tau(p,q)$ y demostrar por inducción que $S_p = \mathbb{N}$. Esto es

$$S_p : \{q \in \mathbb{N} : \sigma(p,q) \equiv \tau(p,q)\}\,. \tag{8}$$

Resulta obvio que $0 \in S_p$ puesto que

$$\sigma(p,0) = \tau(p,0) = p \;\; \text{(por cumplir ambas la condición (3))}\,. \tag{9}$$

Y dado un $q \in S_p$, se tiene que $\sigma(p,q) = \tau(p,q)$, de modo que

$$\sigma(p,s(q)) = s(\sigma(p,q)) = s(\tau(p,q)) = \tau(p,s(q))\,, \tag{10}$$

donde hemos usado que ambas aplicaciones cumplen la propiedad (4). Así pues, $s(q) \in S_p$ y por lo tanto $S_p = \mathbb{N}$, con lo que queda demostrada la unicidad. ■

Propiedades de la suma Para cualesquiera $m, n, p \in \mathbb{N}$ se cumplen las siguientes propiedades

1. Asociativa: $(m+n)+p = m+(n+p)$
2. Conmutativa: $m+n = n+m$
3. Existencia del elemento neutro 0: $n+0 = n$

[1] Estrictamente aquí uso la propiedad conmutativa antes de demostrarla. Para ser totalmente rigurosos deberíamos ir demostrando ciertas propiedades en orden, pero puede ser un tanto tedioso así que decidí aquí tomar esa propiedad por cierta. No obstante, la demuestro en el apéndice B.1

Demostración. Para probar las dos primeras propiedades, basta de nuevo con usar el principio de inducción, demostrando que para cada $n, m \in \mathbb{N}$ los conjuntos

$$M_{n,m} = \{p \in \mathbb{N} : (m+n)+p = m+(n+p)\}, \tag{11}$$

$$M_n = \{m \in \mathbb{N} : m+n = n+m\}, \tag{12}$$

son iguales a $\mathbb{N}$. La última propiedad resulta evidente, pues basta escoger $\sigma(0,n)$ como la aplicación identidad.

Las propiedades enunciadas dotan al par $(\mathbb{N}, +)$ de estructura de semigrupo conmutativo (o abeliano) con elemento neutro, es decir, propiedades de monoide abeliano.

3.2 Multiplicación o producto en $\mathbb{N}$

Además de la suma, podemos definir la operación producto π como sigue

Definición: definimos el producto como la aplicación $\pi : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ tal que para todo $n, m \in \mathbb{N}$

$$\pi(n,0) = 0, \tag{13}$$

$$\pi(n, s(m)) = \pi(n,m) + n. \tag{14}$$

Algunas notaciones usuales de esta operación son $\pi(n,m) = n \cdot m = mn$.

De forma análoga a las pruebas de la sección anterior, es posible demostrar por inducción la existencia y unicidad de esta operación, así como las siguientes propiedades

Propiedades de la multiplicación. Para cualesquiera $n, m, p \in \mathbb{N}$ se cumple las siguientes propiedades

1. Existencia del elemento neutro $s(0) = 1$: $\pi(n,1) = n$.
2. Distributiva por la derecha: $\pi(n+m,p) = \pi(n,p) + \pi(m,p)$.
3. Conmutativa: $\pi(n,m) = \pi(m,n)$.
4. Distributiva por la izquierda: $\pi(n,m+p) = \pi(n,m) + \pi(n,p)$.
5. Asociativa: $\pi(nm,p) = \pi(n,mp)$.

Demostración. La primera propiedad se sigue de forma trivial de la construcción del producto. Para la segunda es necesario probar que el conjunto

$$S_{m,n} = \{p \in \mathbb{N} : \pi(n+m,p) = \pi(n,p) + \pi(m,p)\} \tag{15}$$

coincide con $\mathbb{N}$, y de forma similar para las propiedadas conmutativa y asociativa. Demostraremos tan sólo la distributiva por la derecha a modo de ejemplo.

En primer lugar, resulta evidente que $0 \in S_{m,n}$ puesto que $\pi(n+m,0) = 0 = \pi(n,0) + \pi(m,0) = 0$. En segundo lugar para un cierto $p \in \mathbb{N}$

$$\begin{aligned} \pi(n+m,s(p)) &= \pi(n+m,p) + n + m & (16)\\ &= \pi(n,p) + \pi(m,p) + n + m & (17)\\ &= \pi(n,s(p)) + \pi(m,s(p)) & (18) \end{aligned}$$

de modo que queda demostrado que $s(p) \in S_{m,n}$ y que por tanto $S_{m,n} = \mathbb{N}$ y la propiedad es cierta. ■

Estas propiedades hacen del par $(\mathbb{N},\cdot)$ otro semigrupo abeliano con elemento neutro (o monoide abeliano) de modo que la 3-tupla $(\mathbb{N},+,\cdot)$ tiene estructura de semianillo abeliano.

3.3 Potenciación en $\mathbb{N}$

A partir de la multiplicación, podemos definir de forma recursiva la potencia de números naturales

Definición: sean $b, e \in \mathbb{N}$, definimos la operación potencia como la aplicación $\rho : \mathbb{N}\times\mathbb{N} \to \mathbb{N}$ tal que para todo $b, e \in \mathbb{N}$

$$\begin{aligned} \rho &: \mathbb{N}\times\mathbb{N} \to \mathbb{N}\,, & (19)\\ \rho(b,1) &= b\,, & (20)\\ \rho(b,s(e)) &= \rho(b,e)b\,. & (21) \end{aligned}$$

Los números b y e se denotan usualmente como 'base' y 'exponente' y se utiliza la notación $\rho(b,e) = b^e$.

4 Ordenación de números naturales

Los números naturales tienen la propiedad de admitir una relación de orden, la cual puede ser definida a partir de las operaciones que hemos construido en la sección anterior. En particular

Definición: orden en $\mathbb{N}$. Sean $m, n \in \mathbb{N}$, definimos la relación '$\leq$' entre elementos de $\mathbb{N}$ como

$$m \leq n \text{ si existe } p \in \mathbb{N} \text{ tal que } m + p = n \tag{22}$$

en cuyo caso diremos que m es menor o igual que n. Si $m \leq n$ y $m \neq n$ diremos que m es *estrictamente menor* que n y se denota $m < n$. Las relaciones mayor o igual '$\geq$' y estrictamente mayor '$>$' se definen mediante

$$m \geq n \iff n \leq m\,, \tag{23}$$

$$m > n \iff n < m\,. \tag{24}$$

Proposición La relación $\leq$ es una relación de orden total en $\mathbb{N}$ compatible con la suma y el producto, esto es, cumple las siguientes propiedades para cualesquiera $m, n, p \in \mathbb{N}$

1. **Reflexiva:** $n \leq n$.
2. **Transitiva:** si $m \leq n$ y $n \leq p$ entonces $m \leq p$.
3. **Antisimétrica:** si $m \leq n$ y $n \leq m$ entonces $n = m$.
4. **Total:** para todo n, m, o bien $m \leq n$ o bien $n \leq m$.
5. **Compatible con suma y producto:** si $m \leq n$ entonces $m + p \leq n + p$ y $mp \leq np$

De la relación de orden total en los naturales se pueden deducir los siguientes teoremas

Teorema del buen orden Todo subconjunto $S \subseteq \mathbb{N}$ no vacío tiene elemento mínimo. Es decir existe $m \in S$ tal que $m \leq n$ para todo $n \in S$.

Demostración. De nuevo podemos demostrar este teorema por inducción. Supongamos que existe un cierto subconjunto $S \subseteq \mathbb{N}$ no vacío que no tiene elemento mínimo, y consideremos el subconjunto $\bar{S} \subseteq \mathbb{N}$ complementario, esto es, tal que $S \cup \bar{S} = \mathbb{N}$.

El 0 es menor que cualquier otro número así que no puede pertenecer a S y por tanto $0 \in \bar{S}$. Supogamos ahora que $\bar{S}$ contiene a todos los elementos menores de un cierto n. Entonces $n+1$ tendrá que pertenecer también a $\bar{S}$ puesto que si no lo hiciese entonces sería el elemento mínimo de S. Por el principio de inducción entonces $\bar{S} = \mathbb{N}$ y por lo tanto $S = \emptyset$, lo que contradice nuestra hipótesis de partida y demuestra así que S debe tener un elemento mínimo. ■

Principio fuerte de inducción Sea $S \subseteq \mathbb{N}$ un subconjunto de $\mathbb{N}$, solamente $S = \mathbb{N}$ cumple con la siguiente propiedad

Para cada $n \in \mathbb{N}$, si todo $m \in \mathbb{N}$ con $m < n$ es tal que $m \in S$, entonces $n \in S$.

Demostración. Para la demostración, supongamos que $S \subset \mathbb{N}$ cumpliendo la propiedad. Si $S \neq \mathbb{N}$ entonces su complementario $\bar{S} = \mathbb{N} - S$ es no vacío y por el teorema del buen orden existe un elemento mínimo $p = \min(\bar{S})$ y podemos asegurar que '*todo $n < p$ está en S*' de modo que aplicando el principio fuerte de inducción $p \in S$ y llegamos a una contradicción.

■

5 División de números naturales

Por su utilidad en la siguiente sección, resulta conveniente establecer la siguiente

Proposición: división de naturales Sea $n \in \mathbb{N}^*$, para todo $m \in \mathbb{N}$ existen $q, r \in \mathbb{N}$ tales que

$$m = nq + r \tag{25}$$

y además $r < n$, con q, r únicos. Llamamos dividir un número m por n a encontrar el par q, r, denominados cociente y resto de la división respectivamente.

Demostración Para demostrar que la descomposición existe, utilizamos como de costumbre el principio de inducción. Sea el conjunto

$$S_n = \{m \in \mathbb{N} : \exists\, q, r \in \mathbb{N}; r < n,\, m = nq + r\}\,, \tag{26}$$

es fácil ver que $0 \in S_n$ puesto que basta escoger $q = r = 0$. Asumiendo $m \in S$ podemos probar

$$s(m) = s(nq + r) = nq + r + 1\,. \tag{27}$$

Existen ahora dos posibilides. O bien $r + 1 < n$ en cuyo caso el par $(q, r + 1)$ admite la descomposición, o bien $r + 1 = n$ en cuyo caso podemos reescribir

$$s(m) = n(q + 1) + 0\,, \tag{28}$$

y por tanto la descomposición es válida para el par $(q + 1, 0)$. Queda demostrado por tanto que $s(m) \in S_n$ y por tanto $S_n = \mathbb{N}$. Para la unicidad podemos suponer que existen dos pares (q_1, r_1) y (q_2, r_2) tales que

$$q_1 n + r_1 = q_2 n + r_2 \tag{29}$$

Probemos en primer lugar que $r_1 = r_2$. En caso contrario podemos escoger $r_1 < r_2$ y esto implica que $q_1 > q_2$, de modo que

$$n(q_1 - q_2) = r_2 - r_1\,, \tag{30}$$

pero tanto r_2 como r_1 son menores que n y por tanto $n(q_1 - q_2) < n$ y $(q_1 - q_2) < 1$ con lo que llegamos a contradicción. Se sigue por tanto que $r_2 = r_1$ y en consecuencia $nq_1 = nq_2$ y por tanto $q_1 = q_2$. ■

6 Sistemas de numeración

Por ser $\mathbb{N}$ un conjunto infinito, la representación de todos sus elementos a partir de símbolos especiales resulta imposible, hecho que ha forzado a diversas civilizaciones a desarrollar sistemas que sean capaces de codificar todos los elementos a partir de un número finito de

símbolos. A cada conjunto de símbolos junto con sus reglas de representación se le llama *sistema de numeración*. Si bien diversas culturas desarrollaron sistemas de tipo aditivo, serían los sistemas posicionales (utilizados por culturas como la babilónica, la maya o la china) los que finalmente se extenderían por todo el mundo. A continuación describimos estos sistemas.

6.1 Sistemas de numeración posicional

En un sistema de numeración posicional en base $b \in \mathbb{N} - \{0,1\}$, se emplean b símbolos que representan los números naturales $A_b = \{0,1,2...,b-1\}$. Para cada $n \in \mathbb{N}$ existe una representación en términos de k dígitos $d_i \in A_b$, de tal modo que

$$n = d_k d_{k-1} ... d_1 d_0 = d_0 + d_1 b + ... + d_k b^k \,. \tag{31}$$

Para que este sistema sea útil y sea capaz de nombrar elementos de $\mathbb{N}$ de forma unívoca, es fundamental establecer el siguiente teorema

Teorema de numeración Sean $b \in \mathbb{N} - \{0,1\}$ y $n \in \mathbb{N}$. Existe un conjunto de dígitos $\{d_0, ..., d_k\}$ con $d_i < b$, tales que

$$n = d_0 + d_1 b + ... + d_k b^k \,. \tag{32}$$

Además, si $d_k \neq 0$, esta colección de dígitos es única.

Demostración Demostraremos la existencia por inducción sobre k de modo que construimos el subconjunto $S \subseteq \mathbb{N}$

$$S = \left\{ k \in \mathbb{N} : \forall n \in \mathbb{N},\, n < b^{k+1};\, \exists\, d_1, ..., d_k :\; n = \sum_{i=0}^{k} d_i b^i \right\} . \tag{33}$$

Resulta obvio que $0 \in S$ puesto que todo $n < b$ admite una escritura de la forma (32) con $a_0 = n$. Sea ahora $k \in S$, debemos demostrar que $s(k) \in S$, es decir que para todo $n < b^{k+2}$ tenemos

$$n = \sum_{i=0}^{k+1} d_i b^i \,, \tag{34}$$

para unos ciertos $\{b_i\}$. Si dividimos n entre b^{k+1} tenemos que, en virtud de (25) podremos reescribir

$$n = qb^{k+1} + r\,, \tag{35}$$

con $r < b^{k+1}$. Dado que $k \in S$, r admite la descomposición

$$r = \sum_{i=0}^{k} d_i b^i\,, \tag{36}$$

y además por ser $n < b^{k+2}$ sabemos que $q < b$ de modo que denotando $d_{k+1} = q$ tendremos

$$n = \sum_{i=0}^{k+1} d_i b^i\,, \tag{37}$$

lo que demuestra que la descomposición existe. Para demostrar la unicidad, supongamos que existen dos descomposiciones $\{d_i\}$ y $\{f_i\}$

$$n = \sum_{i=0}^{k} d_i b^i = \sum_{i=0}^{l} f_i b^i\,. \tag{38}$$

Probemos en primer lugar que $k = l$. Si fuese por ejemplo $k < l$ tendríamos

$$\sum_{i=0}^{k} d_i b^i \leq \sum_{i=0}^{k} (b-1) b^i = b^{k+1} - 1 < b^l \leq \sum_{i=0}^{l} f_i b^i\,, \tag{39}$$

lo cual implica $n < n$ y por tanto es una contradicción. Así pues $k = l$ y tenemos que

$$n = \sum_{i=0}^{k} d_i b^i = \sum_{i=0}^{k} f_i b^i\,. \tag{40}$$

De nuevo, podemos expresar n como una división entre b^k

$$n = d_k b^k + r_1 = f_k b^k + r_2\,, \tag{41}$$

con $r_1 = \sum_{i=0}^{k-1} d_i b^i$ y $r_2 = \sum_{i=0}^{k-1} f_i b^i$. Pero sabemos que los coeficientes esta división son únicos, de modo que $d_k = f_k$ y $r_1 = r_2 = r$. Procediendo de forma recursiva con r se concluye que $d_i = f_i$ para todo $i \in [0, k]$. ■

A Cosas pendientes o posibles modificaciones

Hay muchas cosas que se podrían añadir o quitar al tema en función de lo que busquemos. Se trata de un tema que puede ser muy extenso si se demuestran todas las propiedades de las operaciones así que por ello he decidido mostrar sólo algunas de las demostraciones a modo de ejemplo e indicar brevemente el procedimiento para algunas otras. Otra de las cosas que ha quedado sin demostrar es que la relación de orden definida cumple las propiedades necesarias.

B Algunas demostraciones más

B.1 Propiedad conmutativa de la suma

Definimos el conjunto para el cual es cierta la propiedad

$$S_c = \{p \in \mathbb{N} : \exists \sigma(p,q); \sigma(p,q) = \sigma(q,p)\ \forall q \in \mathbb{N}\} \tag{42}$$

Es obvio que $0 \in S_c$ puesto que

- $\sigma(0,0) = 0$ (y la conmutatividad es obvia por simetría de intercambio $0 \leftrightarrow 0$)
- $\sigma(0, s(q)) = s(\sigma(0,q)) = s(q) = \sigma(s(q), 0)$ (usando las propiedades i) y ii))

Así mismo, dado un $k \in S_c$ se comprueba que

- $\sigma(s(k), 0) = s(k) = s(\sigma(0,k)) = \sigma(0, s(k)$ (usando las propiedades i) y ii))
- $\sigma(q, s(k)) = s(\sigma(q,k)) = s(\sigma(k,q)) = \sigma()$ (usando las propiedades i) y ii))

con lo que demostramos que $S_c = \mathbb{N}$ y por tanto queda demostrada la propiedad conmutativa para la aplicación σ.