Capítulo 3

Naturales, inducción, sumas y productos

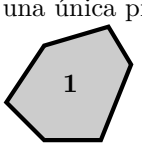
El objetivo del capítulo será construir la representación usual de número natural, así como de las operaciones suma y producto.

3.1 Naturales

3.1.1 Intuición

Visualización 3.1.1. Vamos a visualizar (ver/dibujar imágenes que asemejen conceptos, o a partir de los cuales los construimos) el proceso de formación y las propiedades de los naturales

Empecemos tomando a los objetos de forma arbitraria, por ejemplo, piedras. Empecemos un una única piedra:



Ahora bien, en la realidad no hay una única piedra, sino que hay distintas piedras, en la realidad las distinguimos por la ubicación de éstas ("ésta piedra es distinta de aquella otra" señalando con el dedo una piedra y luego la otra, y si no se pudiese, se palpan ambas con la mano, o por medio de algún otro sentido se perciben su olor, su sonido al impactar con otro objeto, etc). Por tanto, el proceso de contar está íntimamente relacionado con el de agrupar o coleccionar (señalar lo semejante o parecido de los objetos), tanto como con la propiedad de los objetos de existir en el tiempo (Debe haber la posibilidad de transitar entre un estado de cosas para que podamos decir que una es distinta de otra).

Así, nadie con un sano sentido común se atrevería a decir que como son objetos distintos, no existe forma legítima de decir que no puedan agruparse, ni clasificarse, ni tan siquiera hablar de éstos objetos por ser distintos, este ente debería ser lo suficientemente sofisticado para distinguir todo objeto posible como una unidad (haciendo inútil cualquier diálogo por estar en otro nivel de percepción que el de nuestra intuición natural) o es incapaz de distinguir cualquier objeto de la realidad, haciendo que para éste todos sean lo mismo.

Tales entes, si los hubiera, o están muy por encima de nosotros, o muy por debajo, haciendo implausible cualquier comunicación en este aspecto. En lo sucesivo, asumiremos que el lector entiende la noción de coleccionar las cosas que se ha venido discutiendo durante el capítulo 2.

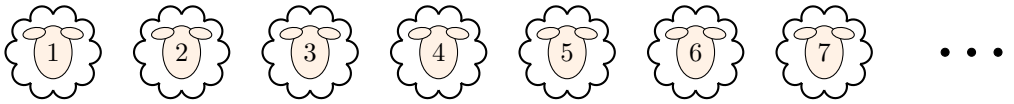
Ahora bien, si identifico algo (un objeto), que yo llamo roca, y también otro objeto, con el suficiente parecido al primero como para merecer el mismo nombre, pero que no necesariamente es el mismo objeto, también le llamaré roca, pero sabiendo que no son la misma. Por tanto, he identificado una roca y otra roca. Por tanto puedo decir que "Hay una roca y el siguiente objeto de este tipo (roca)". Por consiguiente, "Hay una roca y su sucesor (esto es, el siguiente objeto de su tipo: roca)"

De donde concluimos: "Hay roca $\equiv 1$ y su sucesor $\equiv S(1) = 2$"

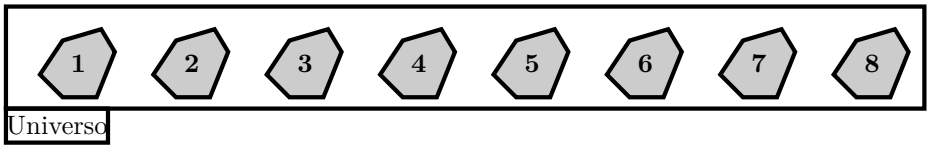
Así, queda completamente caracterizado el proceso mediante el cuál se produce el conteo, por tanto, obtendremos la siguiente imágen que representa una cantidad (no determinada) de rocas:

Ahora bien, esto es un ejemplo, bien podríamos haber usado monedas:

También Ovejas:

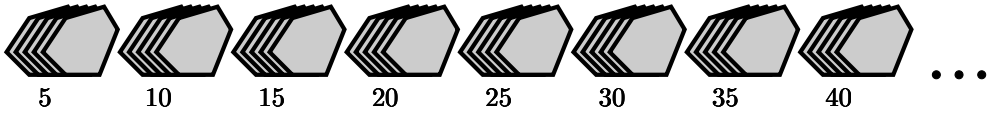


Pudimos haber determinado una cantidad (haber determinado cuándo íbamos a terminar de contar, normalmente debido a que nuestra realidad está limitada a nuestra existencia y capacidad de percepción):



Y pudimos tomar cualquier orden:

Inclusive que nuestro conteo sea implícito y que algunos objetos se perciban de forma yuxtapuesta, de modo tal que algunos objetos estén tapados o no a simple vista:



En cualquier caso, usaremos la siguiente representación cuando nos refiramos al proceso de conteo: Dibujaremos la colección de objetos como círculos y los ordenaremos en una fila (uno a la derecha del anterior, y así sucesivamente), a manera del primero, como se ve en el gráfico:

3.1.2 Formalización

Axioma 3.1.2 (Axiomas de Peano)**.** Definimos un conjunto de números naturales como aquel $\mathbb{N} \neq \phi$ en donde se verifican las siguientes propiedades:

1. (Hay sucesor) $\exists S : \mathbb{N} \to \mathbb{N}$ inyectiva
2. (Existe la unidad) $\exists 1 \in \mathbb{N} : (\forall a \in \mathbb{N}, S(a) \neq 1)$

   Esto es, el conjunto $\mathbb{N}$ es no vacío y hay un elemento sin sucesor.

   Equivalentemente, $\exists 1 \in \mathbb{N} : 1 \notin S(\mathbb{N})$.

   O también: $\mathbb{N} - S(\mathbb{N}) \neq \emptyset$
3. (Propiedad inductiva) Para todo $M \subseteq \mathbb{N}$, si M verifica (a) y (b):

   (a) $1 \in M$

   (b) $S(M) \subseteq M$

   $\Rightarrow M = \mathbb{N}$

Comentario 3.1.3. Este último listado de Axiomas puede darse como axiomas si se quiere evitar el tedio de construir al conjunto de números Naturales. Sin embargo, nosotros demostraremos que en efecto existe a partir del Axioma del Infinito y nuestra teoría de conjuntos. Los axiomas son por lo demás, bastante intuitivos: Podemos contar objetos, hay un número a partir del cual empezamos a contar objetos (cuando distinguimos a un objeto como tal), si yo verifico que el 1 cumple un propiedad y el siguiente cumple la propiedad, entonces todos los que cuento verifican la propiedad (Veremos más adelante que es inducción)

Proposición 3.1.4 ($\exists \mathbb{N}$)**.** *Existe un conjunto de Números Naturales*

Demostración.

- De manera informal:

  Construiremos el conjunto a partir de: ϕ y $S(a) = a \cup \{a\}$
  Tomemos entonces $S(\phi) = \phi \cup \{\phi\} = \{\phi\} \neq \phi$
  Luego $S \circ S(\phi) = S(\{\phi\}) = \{\phi\} \cup \{\{\phi\}\} = \{\phi, \{\phi\}\}$
  Vemos que $S(\phi) \subseteq S \circ S(\phi) \subseteq S \circ S \circ S(\phi) \subseteq ...$

  Esto se corresponde al proceso de conteo, y es fácil ver que nuestra intuición de los números naturales (los de contar) se verifica a partir de el conjunto formado por la reunión de todos estos objetos.

- Formalizando:

  Decimos que un conjunto A es inductivo si verifica :

  1. $\phi \in A$
  2. $x \in A \Rightarrow x \cup \{x\} \in A$

Por Axioma del Infinito, $\exists C$ conjunto inductivo
Por lo tanto, definimos $\mathbb{N} := \bigcap\{B : B \text{ es inductivo}\} - \{\phi\}$
Definamos como antes, $S(x) := x \cup \{x\}$ para todo conjunto x.

1. Notemos que nuestra función sucesor no puede tomar a ϕ en su dominio, pues en este caso tendríamos que hay el 1 es sucesor de algún número. Definamos nuestra función sucesor como $S_{|\mathbb{N}-\{\phi\}}$. En el capítulo anterior probamos que es inyectiva
2. Procedamos por contradicción: $\exists a \in \mathbb{N} : a \cup \{a\} = S(a) = 1 = S(\phi) = \{\phi\}$

   Para tal caso, $\{a\} \subseteq a \cup \{a\} \subseteq \{\phi\} \Rightarrow \{a\} \subseteq \{\phi\} \Rightarrow a = \phi \Rightarrow \phi = a \in \mathbb{N} \Rightarrow \phi \in \mathbb{N}(\Rightarrow\Leftarrow)$
3. Dado $M \subseteq \mathbb{N}$ con la propiedad inductiva, sabemos que $M \cup \{\phi\}$ es un conjunto inductivo, luego $\mathbb{N} \subseteq (M \cup \{\phi\}) - \{\phi\} = M \subseteq \mathbb{N} \Rightarrow M = \mathbb{N}$

□

Comentario 3.1.5. Notemos la motivación detrás del argumento: Recordemos que la intersección de todos los conjuntos cuyos elementos verifican una propiedad resulta en el conjunto mínimo (bajo inclusión) cuyos elementos verifican esa misma propiedad. En este caso, es inmediato ver que el conjunto $\mathbb{N}$ es inductivo, y que cualquier subconjunto con propiedad inductiva va a estar encerrado (con la unión conveniente del elemento conjunto vacío) entre $\mathbb{N}$ y $\mathbb{N}$

Comentario 3.1.6. Durante la crisis del siglo XIX- XX los matemáticos tuvieron que crear una serie de axiomas para poder preservar la mayor cantidad de sistemas matemáticos útiles posibles, evitando redundar o crear sistemas formales muy complejos. Los axiomas de Peano son uno de esos planteamientos para salvar toda la construcción posterior a los naturales. Cabe recalcar que, por motivos didácticos, estamos usando la construcción antigua de los axiomas de Peano. La versión moderna considera el cero como un natural, saltándose un par de pasos en la demostración.

Teorema 3.1.7. $S(\mathbb{N}) \cup \{1\} = \mathbb{N}$

Demostración. $S(\mathbb{N}) \subseteq \mathbb{N}$. Vemos que $S(\mathbb{N}) \cup \{1\}$ cumple propiedad inductiva.
En efecto:

1. $1 \in \{1\} \subseteq S(\mathbb{N}) \cup \{1\}$
2. $x \in S(\mathbb{N}) \cup \{1\} \Rightarrow \exists(a \in \mathbb{N} : x = S(a)) \vee (x = 1) \Rightarrow (S(x) = S(S(a)) \in S(\mathbb{N}) \cup \{1\}) \vee (S(x) = S(1) \in S(\mathbb{N}) \cup \{1\})$.

De donde $S(\mathbb{N}) \cup \{1\} = \mathbb{N}$ □

Corolario 3.1.8 ($\exists!1$)**.** *El 1 es único.*

Demostración. Supongamos que hubiera otra unidad (digamos, a). Se verificaría:

$$\exists a(\neq 1) \in \mathbb{N} : a \notin S(\mathbb{N}) \Rightarrow a \notin S(\mathbb{N}) \cup \{1\}(\Rightarrow\Leftarrow)$$

□

Definición 3.1.9. Definiremos los iterados de un elemento $x \in X$ bajo una función $f : X \to X$ como:

$$f^1(x) := f(x)$$
$$f^{S(n)}(x) := f(f^n(x)), \forall n \in \mathbb{N}$$

Se llaman respectivamente el iterado $n-$ésimo del elemento bajo la función f.

Comentario 3.1.10. El teorema anterior justifica la definición anterior, después de todo, un natural o es sucesor de otro, o es el 1

Proposición 3.1.11. *$f : X \to X$ es inyectiva $\Rightarrow \forall n \in \mathbb{N}, f^n : X \to X$ es inyectiva*

Demostración. Definamos $K := \{m \in \mathbb{N} : F^m \text{ inyectiva}\}$

Por hipótesis del Lema, se tiene que $F = F^1$ es inyectiva, entonces $1 \in K$

Si $j \in K \Rightarrow F^j$ es inyectiva $\Rightarrow F^{j+1}$ inyectiva por Teorema de sección anterior $\Rightarrow j+1 \in \mathbb{N}$ □

Corolario 3.1.12. *Los iterados del sucesor son todos inyectivos*

Proposición 3.1.13. $\forall n \in \mathbb{N}, f^n \circ f = f \circ f^n$

Demostración. En efecto, definamos el conjunto $A := \{a \in \mathbb{N} : f^a \circ f = f \circ f^a\}$

Como $f^1 = f \Rightarrow f^1 \circ f = f \circ f = f \circ f^1 \Rightarrow 1 \in A$

Notamos que si $c \in A \Rightarrow f^c \circ f = f \circ f^c \Rightarrow f^{S(c)} \circ f = f \circ f^c \circ f = f \circ f \circ f^c = f \circ f^{S(c)} \Rightarrow S(c) \in A$

Luego todos los naturales cumplen. □

Proposición 3.1.14. *Podemos escribir al conjunto de naturales como* $\mathbb{N} = \{S^i(1) : i \in \mathbb{N}\} \cup \{1\}$

Demostración. Veamos que tiene la propiedad inductiva (la primera parte es inmediata, el 1 está en $\{S^i(1) : i \in \mathbb{N}\} \cup \{1\}$ por construcción)

Dado un $x \in \{S^i(1) : i \in \mathbb{N}\} \cup \{1\} \Rightarrow (\exists j \in \mathbb{N} : x = S^j(1)) \vee (x = 1) \Rightarrow (S(x) = S(S^j(1)) = S^{j+1}(1)) \vee (S(x) = S(1) = S^1(1))$

En ambos casos, $\Rightarrow \exists r \in \mathbb{N}(r = j + 1 \vee r = 1) : S(x) = S^r(1) \Rightarrow S(x) \in \{S^i(1) : i \in \mathbb{N}\} \Rightarrow S(x) \in \{S^i(1) : i \in \mathbb{N}\} \cup \{1\}$

Por lo tanto, el conjunto tiene la propiedad inductiva y hemos probado el teorema

□

Corolario 3.1.15. *Todo natural distinto de* 1 *se puede escribir como cadena de sucesores de* 1*. Esto es,*

$$\forall n \in \mathbb{N}, S(n) = S^n(1)$$

(Recordemos que un natural o es 1 *o es sucesor de algún otro natural)*

Proof. Definamos $R := \{r \in \mathbb{N} : S(r) = S^r(1)\}$ Veamos que R tiene la propiedad inductiva

1. De forma inmediata $S(1) = S^1(1) \Rightarrow 1 \in R$

2. $n \in R \Rightarrow S(n) = S^n(1) \Rightarrow S(S(n)) = S(S^n(1)) = S^{S(n)}(1) \Rightarrow S(n) \in R$

Por lo tanto $R = \mathbb{N} = S(\mathbb{N}) \cup \{1\}$. Luego se cumple el resultado. □

Comentario 3.1.16. La proposición anterior nos dice que podemos escribir todos los números naturales como un conteo a partir de un número que no es el resultado de contar ningún otro (nuestro primer objeto).

Esto es, podemos "nombrar" a los naturales. La palabra nombre significa identificación, distinción, etiqueta. En esencia, podemos distinguir los números (redundando, podemos etiquetar las etiquetas).

Corolario 3.1.17. *Ningún natural es sucesor de sí mismo*

Demostración. Supongamos que no sea así, es decir: $\exists x \in \mathbb{N} : S(x) = x$. Si $x = 1 \Rightarrow S(1) = 1 \Rightarrow 1 \in S(\mathbb{N})(\Rightarrow\Leftarrow)$ Si $x = S(y) \Rightarrow S(S(y)) = S(y) \Rightarrow S(S^y(1)) = S^y(1) \Rightarrow S^y(S(1)) = S^y(1)$ Por proposición anterior, S^y inyectiva, entonces $S(1) = 1 \Rightarrow 1 \in S(\mathbb{N})(\Rightarrow\Leftarrow)$.

Como la existencia de x es contradictoria, eso quiere decir que no existe tal x. En otras palabras, no hay ningún natural que verifique ser sucesor de sí mismo. □

Notación 3.1.18. Vamos a ponerles un nombre preliminar a algunos números:

- 1 se llamará "uno"
- $2 := S(1)$ se llamará "dos"
- $3 := S(2)$ se llamará "tres"
- $4 := S(3)$ se llamará "cuatro"
- $5 := S(4)$ se llamará "cinco"
- $6 := S(5)$ se llamará "seis"
- $7 := S(6)$ se llamará "siete"
- $8 := S(7)$ se llamará "ocho"
- $9 := S(8)$ se llamará "nueve"
- $a := S(9)$ se llamará "diez"
- $b := S(a)$ se llamará "once"
- $c := S(b)$ se llamará "doce"
- $d := S(c)$ se llamará "trece"
- $e := S(d)$ se llamará "catorce"
- $f := S(e)$ se llamará "quince"

El lector nuevo a los sistemas de numeración debe encontrarse confundido por el uso de letras en vez de los comúmes $10, 11, 12, ...$ para referirse a diez, once, doce, etc. Se espera de este, su paciencia para lograr construir de forma natural dicha representación. En lo sucesivo, indicaremos (si no es evidente por el contexto) cuando una letra se refiere a un número, a una función, a una proposición, etc

Ejemplo 3.1.19. Con nuestra nueva notación, somos capaces de responder la siguiente pregunta:

¿Qué pasa si el sucesor no es inyectivo?

Basta considerar dos $3, 5$ que verifiquen $4 = S(3) = S(5) = 6$ esto quiere decir que $4 = 6 = S(S(4)) = S(S(6)) = 8$.

Esto es, $4 = 6 = 8 = a = c = e = ...$

Podemos hacer un argumento análogo para otra cadena de números: $5 = S(4) = S(6) = 7 = S(S(5)) = S(S(7)) = 9$.

Esto es, $5 = 7 = 9 = b = d = f = ...$

Ejemplo 3.1.20. Otra pregunta natural surge, ¿por qué asumimos que no hay un número antes del uno, siendo que en nuestra construcción (y en la construcción moderna de los axiomas de Peano) usamos el vacío como el "cero"?

Esta pregunta podría responderse simplemente diciendo que, en efecto, es posible empezar con otra "unidad" (en el sentido que no es sucesor de ningún otro número) como el cero, la papa o el azul y que no haría ninguna diferencia (en el caso de nuestra construcción, el vacío es la alternativa más evidente)

Pero esta respuesta es insatisfactoria, pues transladaríamos la pregunta a este nuevo objeto y crearíamos otro objeto que rellene su lugar (y en el caso del vacío, simplemente diríamos que es lo más algebraicamente conveniente).

La respuesta más natural (a nuestro parecer) radica en el hecho de que si $1 \in S(\mathbb{N})$, tenemos que:

$$\exists n \in \mathbb{N} : 1 = S(n) = S^n(1) \Rightarrow 1 = S^n(1) = S^n(S^n(1)) = ...$$

En este caso, los naturales serían descritos de la siguiente forma:

$$\{1, 2, ..., n, S(n) = 1, 2, ...\} = \{1, 2, 3, ...n\}$$

Por sentido común, sabemos que siempre podemos seguir contando. Normalmente usamos un indicador visual, como piedras, nudos, etc, cuando hacemos eso, si suponemos que en algún punto debemos parar por un limitante en nuestra teoría, entonces basta decir, llegado a ese punto, que si añadimos una piedra, nudo, etc más que lo que ya teníamos, hemos superado dicho limitante.

Ejemplo 3.1.21. Por la demostración del Teorema 3.1.3. Si suponemos que un subconjunto propio de los naturales cumple la propiedad inductiva, entonces la razón natural nos sugiere que los naturales pueden dividirse en varias unidades (Elementos que no son sucesores de ningún otro)

Veamos: $\mathbb{A} := \{1, \alpha, \beta\} \cup \{S^i(1) : i \in \mathbb{N}\} \cup \{S^i(\alpha) : i \in \mathbb{N}\} \cup \{S^i(\beta) : i \in \mathbb{N}\}$

Cumple las 3 primeras propiedades. Sin embargo, $\mathbb{N} \subseteq \mathbb{A}$ cumple con la propiedad inductiva, pero sigue siendo subconjunto propio.

3.2 Operaciones en $\mathbb{N}$

Teorema 3.2.1 (Teorema de Recursión)**.** *Sea $G : A \to A$, para $A \neq \phi$ y $a \in A$. Entonces existe una única función $F : \mathbb{N} \to A$) que verifica $F(1) = a$ y $\forall n \in \mathbb{N}$,$F(S(n)) = G(F(n))$. Es decir:*

$$\forall G : A \to A, \forall a \in A, \exists!(F : \mathbb{N} \to A) : \Big(F(1) = a \wedge \forall n \in \mathbb{N}, F(S(n)) = G(F(n))\Big)$$

Proof. □

3.2.1 Suma

Definición 3.2.2 (Operaciones)**.** Una operación algebraica (binaria) f sobre un conjunto se define como una aplicación del producto cartesiano de un conjunto consigo mismo hacia el mismo. Esto es:

$$f : A \times A \to A$$

Comentario 3.2.3. Dada la naturaleza de las aplicaciones, el resultado debe estar definido unívocamente. Hacemos esta aclaración porque puede que la función se contruya a partir de un proceso que involucre sacar información del objeto de salida la cual (como información) no sea un objeto como tal, sino un conjunto de objetos, en este caso el resultado de la operación no debe cambiar si la elegimos esta o aquella representación, sino que el proceso debe determinar de forma única un objeto de llegada a partir de sus objetos de salida.

Definición 3.2.4 (Función suma a Derecha)**.** Definimos la funcion suma a izquierda por a en los naturales, $f_a : \mathbb{N} \to \mathbb{N}$ como sigue:

$$f_a(1) := s(a)$$
$$f_a(S(b)) := S(f_a(b))$$

Recordemos que todo natural es o sucesor de un natural (segundo caso) o es el 1. Entonces hemos definido para todos los naturales el valor de la suma a izquierda.

Definición 3.2.5 (Operación Suma)**.** Definimos la operación suma $+ : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ como sigue:

$$+ (a, b) = f_a(b)$$

Notación 3.2.6. Escribiremos: $a + b := +(a, b)$

Comentario 3.2.7. A partir de ahora, usaremos indistintamente $S(n)$ o $n + 1$

Comentario 3.2.8. Todas las representaciones que hagamos de la suma que respeten sus entradas y salidas verificando propiedades, son útiles. En didáctica, estos son llamados

'métodos', sin embargo, este nombre le queda demasiado grande, pues todos son el mismo proceso, aunque llamados de distinta forma.

Proposición 3.2.9 (Sumar es contar varias veces)**.** $\forall a, b \in \mathbb{N}, a + b = S^b(a)$

Proof. Empezaremos definiendo, como antes hacíamos, un conjunto caracterizado con la propiedad que buscamos probar. Si demostramos que tiene la propiedad inductiva, este conjunto será el propio $\mathbb{N}$, luego todos los naturales verifican la propiedad dada.

Tomemos un natural cualquiera n, y definamos $X_n := \{m \in \mathbb{N}, n + m = S^m(n)\}$

Veamos que tiene la propiedad inductiva:

1. $n + 1 = S(n) = S^1(n) \Rightarrow 1 \in X_n$
2. $m \in X_n \Rightarrow n + m = S^m(n) \Rightarrow n + S(m) = S(n + m) = S(S^m(n)) = S^{S(m)}(n) \Rightarrow S(m) \in X_n$

Luego el conjunto X_n tiene la propiedad inductiva. Por el Axioma 4 de los Axiomas de Peano, $X_n = \mathbb{N}$. Esto quiere decir que todo natural m cumple $n + m = S^m(n)$ para cualquier natural n. Esto último es lo mismo que si yo tomo dos naturales cualesquiera, puedo construir el conjunto X_n a partir del primer natural, y el segundo natural verificará la propiedad, en resúmen: $\forall n, m \in \mathbb{N}, n + m = S^m(n)$ □

Comentario 3.2.10. El proceso de suma como conteo iterado nos permite visualizar la suma como un movimiento en la cadena de iterados definida anteriormente

Definición 3.2.11. Decimos que una operación f es asociativa si verifica:

$$f(f(a, b), c) = f(a, f(b, c))$$

Notación 3.2.12. Cuando no quede claro cual operación está siendo aplicada (pueden haber confusión con respecto al orden), usaremos los paréntesis: "(" y ")", para agrupar de forma más precisa.

Notación 3.2.13. Usaremos una operación $* : X \times X \to X$ sobre X, con la misma notación que la suma, $a * b = *(a, b)$.

En este caso: $(a * b) * c$ quiere decir: aplicamos la operación $*$ al par (a, b) y obtenemos un resultado en X. A este resultado lo adjuntamos con c, formando un par. Ahora a este par le aplicamos $*$.

En resumen: $\Big((a, b) \mapsto *(a * b) =: x \Rightarrow (x, c) \mapsto *(x * c) =: y\Big) \Rightarrow y = (a * b) * c$

Notación 3.2.14. Con la notación anterior, la propiedad asociativa queda como: $(a + b) + c = a + (b + c)$

Proposición 3.2.15. $a + S(b) = S(a + b)$

Proof. Basta ver que $a + S(b) = f_a(S(b)) = S(f_a(b)) = S(a + b)$ □

Teorema 3.2.16. *La suma es asociativa. Esto es:* $(a + b) + c = a + (b + c)$

Demostración. Fijemos un par arbitrario $(a, b) \in \mathbb{N} \times \mathbb{N}$. Definamos el conjunto: $A := \{c \in \mathbb{N} : (a + b) + c = a + (b + c)\}$

Veremos que A tiene propiedad inductiva:

- Por proposición anterior, $1 \in A$
- $x \in A \Rightarrow (a+b)+x = a+(b+x) \Rightarrow (a+b)+S(x) = S((a+b)+x) = S(a+(b+x)) = a+S(b+x) = a+(b+S(x)) \Rightarrow S(x) \in A$

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

Como nuestra elección de pares (a,b) fue arbitraria, nuestro resultado vale para todos los pares de naturales. Es decir: $\forall (a,b,c) \in \mathbb{N}, (a+b)+c = a+(b+c)$

□

Comentario 3.2.17. El Teorema anterior nos indica que si tenemos una larga fila de sumas consecutivas, puedo considerar cualquier orden para empezar a operar. Esto es, los paréntesis en una fila de sumas pueden ignorarse libremente

Lema 3.2.18. $\forall a \in \mathbb{N}, a+1 = 1+a$

Demostración. Sea $B := \{n \in \mathbb{N} : n+1 = 1+n\}$

Veamos que B tiene la propiedad inductiva:

1. $1+1 = 1+1 \Rightarrow 1 \in B$
2. $x \in B \Rightarrow x+1 = 1+x \Rightarrow S(x)+1 = (x+1)+1 = (1+x)+1 = 1+(x+1) = 1+S(x) \Rightarrow S(x) \in B$

De donde $B = \mathbb{N}$, con lo que se sigue el resultado □

Definición 3.2.19. Decimos que una operación f es commutativa si verifica:

$$f(a,b) = f(b,a)$$

Comentario 3.2.20. En otras palabras, una operación es commutativa si no importa el orden de los elementos a operar

Teorema 3.2.21. *La suma es commutativa*

Demostración. Tomemos un $x \in \mathbb{N}$ arbitrario. Sea $C := \{m \in \mathbb{N} : x+m = m+x\}$.

Afirmamos que C tiene la propiedad inductiva:

- Por Lema anterior, $1 \in C$
- $t \in C \Rightarrow x+t = t+x \Rightarrow x+S(t) = S(x+t) = s(t+x) = t+S(x) = t+(x+1) = t+(1+x) = (t+1)+x = S(t)+x \Rightarrow S(t) \in C$

De donde, y por arbitrareidad de x, tenemos:

$$\forall n, m \in \mathbb{N}, n+m = m+n$$

□

Proposición 3.2.22. *Dado un n natural, no existe un natural p que cumpla $n+p = n$*

Proof. Supongamos que sí, en ese caso: $\exists p \in \mathbb{N} : n + p = n$

Si $n = 1, p = 1 \Rightarrow 1 + 1 = 1$. Pero el 1 no es sucesor de ningún número

Del mismo modo, $n \neq 1, p = 1 \Rightarrow n + 1 = n$. Igualmente, por proposición anterior que ningún natural es sucesor de sí mismo

Si $n = S(m), p \neq 1 \Rightarrow n + p = n \Rightarrow p + n = n + p = n \Rightarrow S^m(S(p)) = S^m(1)$. Por la inyectividad de S^m. Luego $S(p) = 1$ pero 1 no es sucesor de ningún número natural, contradicción ($\Rightarrow\Leftarrow$)

La existencia de ese par lleva a una contradicción, luego no puede existir, y se da el resultado □

Proposición 3.2.23 (Cancelación)**.** $\forall n, m, p \in \mathbb{N}, (n = m \iff n + p = m + p)$

Demostración. La primera parte es inmediata, en efecto, aplicarle una función al mismo objeto resulta en el mismo resultado. Es decir $n = m \Rightarrow n + p = f_p(n) = f_p(m) = m + p$ Usaremos la técnica usada en la demostración anterior. Para comenzar, veamos que si $n + p = m + p \Rightarrow p + n = p + m \Rightarrow S^{A(p)}(n) = S^{A(p)}(m) \Rightarrow n = m$ por la inyectividad de S^p □

Definición 3.2.24 (Cálculo Numérico)**.** Definimos calcular como el proceso de aplicar operaciones algebraicas una o más veces.

Ejemplo 3.2.25. Empecemos dando algunos ejemplos de sumas:

1. Una suma estándar (sin ningún tipo de técnica) tendría esta forma:

   $4+7 = S^7(4) = S(S(S(S(S(S(S(4)))))))) = (((((((4+1)+1)+1)+1)+1)+1)+1 = (((((5+1)+1)+1)+1)+1)+1 = ((((6+$

   Sin embargo, recordemos que podemos usar la commutatividad, en este caso:

   $4+7 = 7+4 = S^4(7) = S(S(S(S(7)))) = (((7+1)+1)+1)+1 = ((8+1)+1)+1 = (9+1)+1 = a+1 = b$

   Recordemos que podemos ignorar los paréntesis (por asociatividad). En este caso podemos reducir nuestro proceso a:

   $$4 + 7 = 7 + 4 = 7 + 1 + 1 + 1 + 1 = 8 + 1 + 1 + 1 = 9 + 1 + 1 = a + 1 = b$$

   Lo cual es mucho más ameno.

2. Podemos sumar de forma ágil términos de acuerdo a lo que se encuentre más fijo en nuestra memoria. Veamos el siguiente problema: Hallar el valor de 3+5+2+8+7+3+2 (Ya hemos ignorado los paréntesis por asociatividad).

   Usando commutatividad podremos posicionar los números que sumen a unos al costado de otros. Indicaremos con signos de agrupación qué números suman a y veremos como se procede:

   Verifiquemos: $3+7 = 5+3+2 = 8+2 = a$. En efecto: $3+7 = 7+3 = 7+1+1+1 = 8+1+1 = 9+1 = a$. Del mismo modo, $8+2 = 8+1+1 = a$. Asímismo, $5+3+2 = 5+1+1+1+2 = 6+1+1+2 = 7+1+2 = 8+2 = a$. Ahora agrupemos:

$[3]+(5)+\{8\}+[7]+(3+2)+\{2\} = [3]+[7]+(5)+(3+2)+\{8\}+\{2\} = [3+7]+(5+3+2) = \{8+2\} = [a]+(a)+\{a$

Luego veremos como estos métodos se combinan con otros de otras operaciones para dar lugar a un cálculo mínimamente ágil

Definición 3.2.26. Decimos que una función $s : \mathbb{N} \to X$ (con X un conjunto cualquiera) es una secuencia

Notación 3.2.27. Una secuencia representa una lista "infinita" de puntos o elementos de X, la cuál está ordenada como el propio $\mathbb{N}$. Es decir, vamos "contando" los objetos en X. Por esto, usaremos la siguiente notación:

$$s_n = s(n), \forall n \in \mathbb{N}$$

Además, usaremos:

$$\{s_n\}_{n\in\mathbb{N}} \subseteq X$$

para referirnos a que la secuencia es "como un conjunto de puntos" en "X", los cuales toman como indices (recordemos del capítulo anterior que son como identificadores) al conjunto de los naturales (es decir, están identificados o nombrados por estos).

Formalmente, si $ran(s) \subseteq X \Rightarrow \{s_n\}_{n\in\mathbb{N}} \subseteq X$

Definición 3.2.28 (Sumatoria)**.** Dado $\{a_n\}_{n\in\mathbb{N}} \subseteq \mathbb{N}$ secuencia de números naturales. Escribiremos:

$$\sum_{i=1}^{1} a_i := a_1$$
$$\sum_{i=1}^{n+1} a_i := \sum_{i=1}^{n} a_i + a_{n+1}$$

Esto es: $\sum_{i=1}^{n} a_i = a_1 + a_2 + a_3 + ... + a_n$

Notación 3.2.29. Cuando nos dan sólo una lista de números, consideramos que todos los demás son 1 o 0 (si usamos los axiomas de Peano en su versión moderna). Además, escribiremos:

$$\sum_{i=1}^{n} a$$

Cuando queramos referirnos a la secuencia $a_n = a, \forall n \in \mathbb{N}$. Es decir, $a : \mathbb{N} \to X$ es la función constante con valor a

3.2.2 Producto

Definición 3.2.30 (Funcion producto a izquierda)**.** Conocida la operación suma, definamos la función producto a izquierda $g_a : \mathbb{N} \to \mathbb{N}$ de la siguiente forma:

$$g_a(1) = a$$
$$g_a(S(b)) = g_a(b) + a$$

Definición 3.2.31 (Producto)**.** Definimos la operación producto o multiplicación como $\times : \mathbb{N} \to \mathbb{N}$ como:

$$\times(a, b) = g_a(b)$$

Notación 3.2.32. Escribiremos $ab = a.b = a \times b = \times(a, b)$ indistintamente y como nos plazca

Proposición 3.2.33 (Multiplicar es Sumar varias veces)**.** *Se verifica:*

$$\forall a, b \in \mathbb{N}, a.b = \sum_{i=1}^{b} a$$

Demostración. En efecto, definamos: $D := \{d \in \mathbb{N} : a.d = \sum_{i=1}^{d} a\}$

Afirmamos que el conjunto D tiene la propiedad inductiva:

1. $a.1 = g_a(1) = a = \sum_{i=1}^{1} a \Rightarrow 1 \in D$

2. Supongamos que $b \in D \Rightarrow a.b = \sum_{i=1}^{b} a \Rightarrow a.S(b) = g_a(S(b)) = g_a(b) + a = a.b + a = \sum_{i=1}^{b} a + a = \sum_{i=1}^{S(b)} a \Rightarrow S(b) \in D$

Luego $D = \mathbb{N}$, entonces $\forall a, b \in \mathbb{N}, a.b = \sum_{i=1}^{b} a$ □

Comentario 3.2.34. La proposición anterior quiere decir que multiplicar por b a la derecha es lo mismo que sumar b veces el número a

Es por eso que en inglés se usa la expresión : 'b times a' y en español se usa: 'b veces a'.

Ambas quieren decir lo mismo. Estamos sumando (¿cuántas veces?) b veces, el número (¿qué número?) a.

Proposición 3.2.35. *El producto verifica:*

$$a.1 = a$$
$$a.S(b) = a.b + a$$

Proof. $a.1 = g_a(1) = a$

Además $a.(b+1) = g_a(b+1) = g_a(b)+a = a.b+a$. Luego se sigue de forma inmediata. □

Teorema 3.2.36. *El producto verifica lo siguiente:*

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

Decimos de esta propiedad que el producto se distribuye a la izquierda con respecto a la suma

Demostración. Veamos, definamos el conjunto $E := \{y \in \mathbb{N} : a.(b + y) = a.b + a.y\}$
Afirmamos que E cumple propiedad inductiva:

1. $a.(b + 1) = a.(S(b)) = a.b + a = a.b + a.1 \Rightarrow 1 \in E$
2. $y \in E \Rightarrow a.(b + y) = a.b + a.y \Rightarrow a.(b + S(y)) = a.(S(b + y)) = a.(b + y) + a = a.b + a.y + a = a.b + a.(y + 1) = a.b + a.S(y) \Rightarrow S(y) \in E$

Esto quiere decir que $E = \mathbb{N}$, lo que a su vez implica: $\forall a, b, c \in \mathbb{N}, a.(b+c) = a.b+a.c$ □

Teorema 3.2.37. *De forma análoga, el producto verifica:*

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

Decimos de esta propiedad que el producto se distribuye a la derecha con respecto a la suma

Demostración. La prueba es casi idéntica a la anterior: $E' := \{w \in \mathbb{N} : (a+b).w = a.w+b.w\}$
Afirmamos que E' cumple propiedad inductiva:

1. $(a + b).1 = a + b = a.1 + b.1 \Rightarrow 1 \in E'$
2. $w \in E' \Rightarrow (a+b).w = a.w+b.w \Rightarrow (a+b).S(w) = (a+b).w+(a+b) = a.w+b.w+a+b = a.w + a.1 + b.w + b.1 = a.(w + 1) + b.(w + 1) = a.S(w) + b.S(w) \Rightarrow S(w) \in E'$

Esto quiere decir que $E' = \mathbb{N}$, lo que a su vez implica: $\forall a, b, c \in \mathbb{N}, (a+b).c = a.c+b.c$ □

Teorema 3.2.38. *El producto es asociativo*

Demostración. Definamos el conjunto $F := \{c \in \mathbb{N} : (a.b).c = a.(b.c)\}$
Afirmamos que E cumple propiedad inductiva:

1. $(a.b).1 = g_{a.b}(1) = a.b = a.(g_b(1)) = a.(b.1) \Rightarrow 1 \in F$
2. $c \in F \Rightarrow (a.b).c = a.(b.c) \Rightarrow (a.b).S(c) = g_{a.b}(S(c)) = g_{a.b}(c) + a.b = (a.b).c + a.b = a.(b.c) + a.b = a.(b.c + b) = a.(g_b(S(c))) = a.(b.S(c)) \Rightarrow S(c) \in F$

Luego, $\forall a, b, c \in \mathbb{N}, (a.b).c = a.(b.c)$ □

Lema 3.2.39. *a.1 = 1.a*

Demostración. Veamos, definamos el conjunto $G := \{r \in \mathbb{N} : r.1 = 1.r\}$
Afirmamos que G cumple propiedad inductiva:

1. $1.1 = 1.1 \Rightarrow 1 \in G$

2. $r \in G \Rightarrow r.1 = 1.r \Rightarrow S(r).1 = g_{S(r)}(1) = S(r) = r + 1 = r.1 + 1 = 1.r + 1.1 = 1.(r + 1) = 1.(S(r)) \Rightarrow S(r) \in G$

Luego, $\forall a \in \mathbb{N}, a.1 = 1.a$ □

Teorema 3.2.40. *El producto es commutativo*

Demostración. Procedemos como antes, tomando un a natural arbitrario, definamos el conjunto $H := \{h \in \mathbb{N} : a.h = h.a\}$

Afirmamos que H cumple propiedad inductiva:

1. Por Lema anterior: $a.1 = 1.a \Rightarrow 1 \in H$

2. $z \in H \Rightarrow a.z = z.a \Rightarrow a.S(z) = a.z + a = z.a + 1.a = (z + 1).a = S(z).a \Rightarrow S(z) \in H$

Luego, $\forall a, b \in \mathbb{N}, a.b = b.a$ □

Comentario 3.2.41. No se puede dejar de recalcar lo IMPORTANTÍSIMO que es comprender estas propiedades. De hecho, este es el corazón del producto, su esencia. El hecho de que podamos relacionar producto y suma implica que las estructuras algebraicas que surjan de estas operaciones gozan de múltiples propiedades. Un ejemplo de estas aplicaciones (aunque a nivel numérico) la veremos cuando tratemos de optimizar la velocidad de nuestras multiplicaciones, a fin de lograr mayor rapidez y cálculo mental.

3.2.3 Potenciación

Definición 3.2.42 (Función potenciación)**.** Definimos la función $h_a : \mathbb{N} \to \mathbb{N}$ como sigue:

$$h_a(1) = a$$
$$h_a(S(b)) = a.h_a(b)$$

Definición 3.2.43 (Potenciación)**.** Definimos la operación potenciación $\hat{} : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ como:

$$\hat{}(a, b) := h_a(b)$$

Notación 3.2.44. Escribiremos $a^b = \hat{}(a, b)$

Definición 3.2.45 (Productoria)**.** Dada una secuencia $\{b_m\}_{m\in\mathbb{N}}$

$$\prod_{j=1}^{1} b_j = b_1$$
$$\prod_{j=1}^{n+1} b_j = b_{n+1}.\prod_{j=1}^{n} b_j$$

Notación 3.2.46. Usamos de manera análoga al caso de la sumatoria:

$$\prod_{i=1}^{n} b$$

para referirnos a la secuencia $b_r = b, \forall r \in \mathbb{N}$

Proposición 3.2.47 (Potenciación es Multiplicar varias veces)**.** *Dados a, b naturales arbitrarios, se cumple:*

$$a^b = \prod_{i=1}^{b} a$$

Demostración. Sea $D' = \{x \in \mathbb{N} : a^x = \prod_{i=1}^{x} a\}$

1. $a^1 = a = \prod_{i=1}^{1} a$
2. $u \in D' \Rightarrow a^u = \prod_{i=1}^{u} a \Rightarrow a^{u+1} = a.a^u = a.\prod_{i=1}^{u} a = \prod_{i=1}^{u+1} a$

El lector ya debe estar familiarizado con este tipo de argumentos y ya debe ser capaz de saber por qué se cumple la proposición. □

Comentario 3.2.48. La proposición anterior muestra que la relación que tiene la potencia y el producto es análoga a la que tienen la suma y el producto. En ese sentido, parece natural querer seguir con este razonamiento y crear tantas operaciones como nos plazca (Potenciamos múltiples veces, a esa operación, la repetimos múltiples veces, a esta última, la repetimos múltiples veces, a esta última...). Recordemos que nuestro anterior comentario hizo hincapié en lo útiles que eran las propiedades algebraicas que relacionaban a la suma y al producto. Verificamos que la potencia no cumple casi ninguna

Recordemos la definición de contraejemplo:

Definición 3.2.49 (Contraejemplo)**.** Un contraejemplo es una técnica de demostración que consiste en presentar un objeto con una propiedad no deseada (Si la propiedad es muy específica y poco intuitiva, llamaremos al contraejemplo patológico, cual si fuera una enfermedad en nuestra teoría), de este modo probaremos que la propieda no se cumple para todos los objetos

Proposición 3.2.50. *La potenciación no es asociativa, ni commutativa, ni distributiva con respecto a la suma (en ningún lado), ni tampoco es distributiva a izquierda con respecto a producto.*

Demostración. Veamos dos contraejemplos:

1. Calculemos $(2^2)^3$ y $2^{(2^3)}$: $(2^2)^3 = (2^2).(2^2).(2^2) = (2.2).(2.2).(2.2) = 4.4.4$ y $2^{(2^3)} = 2^{(2.2.2)} = 2^8 = 2.2.2.2.2.2.2.2 = 4.4.4.4 =$. Ahora bien, escribamos $m = 4.4.4$. Si fuera asociativa, se cumpliría: $(a^b)^c = a^{(b^c)}$ para todos a, b, c naturales. Con nuestro caso particular: $(2^2)^3 = 2^{(2^3)} \Rightarrow m = m.4 = m.3 + m = S^{m.3}(m)$ Lo cual es imposible. Es decir, hemos llegado a una contradicción $(\Rightarrow\Leftarrow)$

2. Calculemos 2^3 y 3^2: $2^3 = 2.2.2 = 8$, $3^2 = 3.3 = 9$. Si la potenciación fuera commutativa, se cumpliría: $a^b = b^a$, en cuyo caso: $8 = 2^3 = 3^2 = 9 = S(8)(\Rightarrow\Leftarrow)$.

3. $(1+1)^2 = 2^2 = 4 \neq 2 = 1^2 + 1^2$. Luego no es distributiva a derecha con respecto a la suma

4. $2^{(1+2)} = 2^3 = 8 \neq 5 = 2 + 4 = 2^1 + 2^2$. Luego no es distributiva a izquierda con respecto a la suma

5. $2^{(1.2)} = 2^2 = 4 \neq 8 = 2.4 = 2^1.2^2$. Luego no es distributiva a izquierda con respecto al producto

□

Proposición 3.2.51 (Distributiva a derecha)**.** *La potenciación es distributiva a derecha con respecto al producto. Esto es:*

$$\forall a, b, c \in \mathbb{N}, (a.b)^c = a^c.b^c$$

Demostración. Tomemos el conjunto $L = \{l \in \mathbb{N} : (a.b)^l = a^l.b^l\}$

$(a.b)^1 = a.b = a^1.b^1$

Si $v \in L \Rightarrow (a.b)^v = a^v.b^v \Rightarrow (a.b)^{v+1} = (a.b).(a.b)^v = (a.b).a^v.b^v = a.a^v.b.b^v = a^{v+1}.b^{v+1} \Rightarrow v + 1 \in L$

Luego la propiedad se cumple □

3.3 Orden

3.3.1 Orden en $\mathbb{N}$

Recordemos las definiciones de relación de orden parcial y total del capítulo anterior:

Definición 3.3.1 (Orden Parcial)**.** Decimos de una relación binaria R en un conjunto X, que es un orden parcial o preorden si verifica:

1. (Reflexiva) $(x, x) \in R$
2. (Antisimétrica) $\Big((x, y) \in R\Big) \wedge \Big((y, x) \in R\Big) \Rightarrow x = y$
3. (Transitiva) $\Big((x, y) \in R\Big) \wedge \Big((y, z)\Big) \in R \Rightarrow (x, z) \in R$

Comentario 3.3.2. Recordemos que podemos escribir de forma análoga:

1. (Reflexiva) xRx
2. (Antisimétrica) $xRy \wedge yRx \Rightarrow x = y$
3. (Transitiva) $xRy \wedge yRz \Rightarrow xRz$

Además si R es un conjunto parcial, entonces (X, R) se llama un conjunto parcialmente ordenado o (alternativamente) poset

Definición 3.3.3 (Orden Total)**.** Decimos que un orden parcial R sobre un conjunto X es un orden total si además, verifica

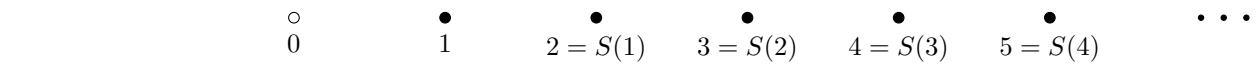
$$\text{(Dicotomía) } \forall x, y \in X, (xRy) \vee (yRx)$$

Visualización 3.3.4. Veamos cómo se graficaría, intuitivamente, el conjunto de los números naturales.

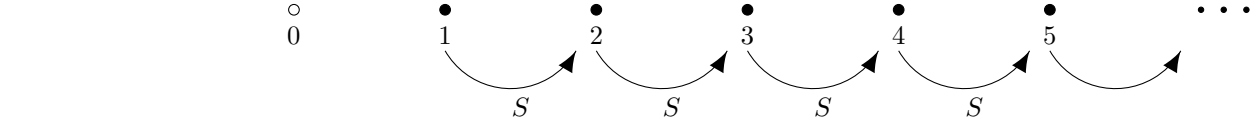
Empezamos con el 0 que está dado por hecho en la construcción (Aunque no forma parte de los naturales y por tanto no está "activo"):

Agreguemos el 1 que tenemos dado por Axiomas de Peano:

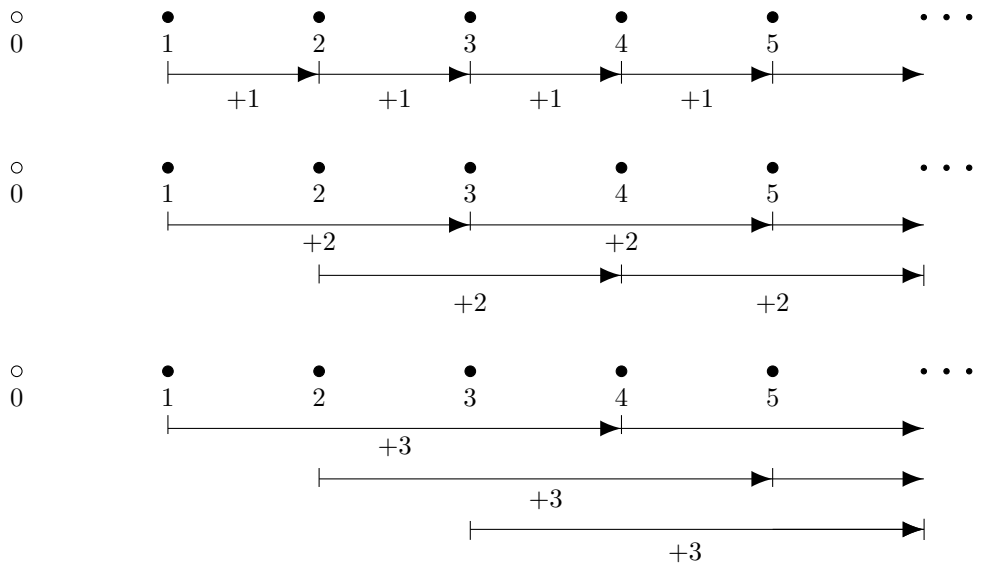
Agreguemos los sucesores uno a la derecha del otro:



Notamos que al ser graficado de esta forma, podemos ver cierta noción de cómo funcionan las operaciones. En efecto, el sucesor consiste en avanzar al siguiente punto de la cadena:



Observamos que la suma se puede interpretar como una translación (o movimiento), en una misma dirección. Es decir, podemos imaginar sumar a la derecha como movernos de acuerdo a la flecha a partir de un número dado. El lector puede verificar que el siguiente diagrama coincide con nuestros resultados usuales sobre la suma.



Comentario 3.3.5. El lector debe advertir de nuestra visualización anterior, que un número x está más a la derecha de otro y si puedo encontrar una flecha $+p$ que me translade de x hacia y (esto es, existe un número natural p que verifica: $x + p = y$). Equivalentemente, puedo ver que un número está a la derecha de otro si en la cadena de flechas que conducen hasta y desde el 1, en algún momento encontramos a x. El lector es libre de verificar que ambos métodos son equivalentes. En vista de eso, formularemos la próxima definición.

Definición 3.3.6 (Orden en $\mathbb{N}$)**.** Definimos la siguiente relación en $\mathbb{N}$:

$$x < y \iff \exists p \in \mathbb{N} : x + p = y \iff \exists q \in \mathbb{N} : S^q(x) = y \iff y \in \{S^i(x) : i \in \mathbb{N}\}$$

Es decir, tendremos que $x < y$, "x es menor que y" si x forma parte de la cadena de sucesores de 1 que construyen a y .

Notación 3.3.7. Diremos de foma análoga que "y es mayor que x" si $y > x$ y lo escribiremos como $y > x$.

Lema 3.3.8. $\forall n(\neq 1) \in \mathbb{N}, 1 < n$

Demostración. Sabemos por proposición anterior que $\mathbb{N} = \{S^i(1) : i \in \mathbb{N}\} \cup \{1\}$
Si $n \in \mathbb{N} - \{1\} \Rightarrow n \in \{S^i(1) : i \in \mathbb{N}\} \Rightarrow \exists i \in \mathbb{N} : n = S^i(1) \Rightarrow 1 < n$ □

Notación 3.3.9. Denotaremos por $x \leq y$ cuando queramos decir que $(x < y) \vee (x = y)$ Análogamente, denotaremos por Denotaremos por $x \geq y$ cuando queramos decir que $(x > y) \vee (x = y)$

Teorema 3.3.10 (Tricotomía)**.** *Sean $x, y \in \mathbb{N}$, dos naturales cualesquiera. Se da uno (y sólo uno) de los siguientes 3 casos:*

1. $x = y$
2. $x < y$
3. $y < x$

(Esto es, si se da el primer caso, no puede darse ni el segundo ni el tercero, si se da el segundo, no puede darse ni el primero ni el tercero, y si se da el tercero, no puede darse ni el primero ni el segundo. Además, debe darse alguno de ellos sí o sí)

Demostración. 1. Veamos la exclusividad:

(a) Supongamos que $x = y$. En este caso, si $x < y \Rightarrow x < x \Rightarrow \exists p \in \mathbb{N} : x + p = x$. Ningún número puede cumplir eso por proposición anterior. Es decir que no puede darse a la vez $x = y$ y $x < y$. Análogamente, no pueden darse al mismo tiempo $x = y$ y $x > y$

(b) Supongamos que $x < y$ y $x > y$. En este caso $\exists p, q \in \mathbb{N} : (x + p = y) \wedge (y + q = x) \Rightarrow (x + p) + q = x \Rightarrow x + (p + q) = x$. Esto es imposible por proposición anterior.

Ahora bien, estos son todos los casos posibles

2. Veamos la necesidad: (Alguno de ellos se debe cumplir)

Definamos la siguiente relación T como sigue: xTy si $(x = y) \vee (x < y) \vee (x > y)$. (Nótese que nunca se afirma que T sea un orden)

Fijemos un x arbitrario y definamos el conjunto $Y_x := \{y \in \mathbb{N} : xTy\}$

Recordemos de la proposición anterior que $x \in \mathbb{N} = \{S^i(1) : i \in \mathbb{N}\} \cup \{1\} \Rightarrow (x = 1) \vee (\exists i \in \mathbb{N} : x = S^q(1)) \Rightarrow (x = y) \vee (x > 1) \Rightarrow xT1 \Rightarrow 1 \in Y_x$

Ahora bien, supongamos $\beta \in Y_x \Rightarrow xT\beta \Rightarrow (x = \beta) \vee (x < \beta) \vee (x > \beta) \Rightarrow (x = \beta < \beta + 1) \vee (x < \beta < \beta + 1) \vee (x > \beta)$

En los dos primeros casos $x < \beta + 1$.

Para el último caso $(x > \beta)$: $\exists t \in \mathbb{N} : x = S^t(\beta)$.

Si $t = 1 \Rightarrow x = S(\beta)$.

Si $t \neq 1 \Rightarrow \exists \alpha \in \mathbb{N} : t = \alpha + 1 \Rightarrow x = S^\alpha(S(\beta)) \Rightarrow x > \beta + 1$

En todos los casos $xT\beta$

Quiere decir que $Y_x = \mathbb{N}$. Por arbitrareidad de x se sigue el resultado

□

Proposición 3.3.11. $\leq$ *es un orden total*

Demostración. 1. (Reflexiva) $x = x \Rightarrow x \leq x$

2. (Transitiva) $(x \leq y) \wedge (y \leq z) \Rightarrow (x < z) \vee x = z$. Con el primero resultando de la aparición de $<$ en alguna de las dos hipótesis, mientras que el segundo sucede si no aparece

3. (Antisimétrica) $(x \leq y) \wedge (y \leq x)$. Si se diera (en el primer caso) $x < y$, tendríamos que todas las posibilidades del otro (del segundo caso) son imposibles por tricotomía. Luego $x = y$ es la única posibilidad

□

Afirmación 3.3.12 (Propiedades del Orden en $\mathbb{N}$)**.** *Se cumplen las siguientes propiedades:*

1. $\forall n \in \mathbb{N}, n < n + 1$
2. $\forall n, m \in \mathbb{N}, n < n + m$
3. *(Regla del Sandwich)* $\forall n, m \in \mathbb{N}\Big((n \leq m) \wedge (m \leq n) \Rightarrow n = m\Big)$
4. $\forall n \in \mathbb{N}, \forall m \in \mathbb{N} - \{1\}, n < nm$
5. $\forall a, b, c \in \mathbb{N}, (a < b \iff a + c < b + c)$
6. $\forall a, b, c \in \mathbb{N}, (a < b \iff a.c < b.c)$
7. *Sean a, b, c, d naturales.* $(a < b) \wedge (c < d) \Rightarrow a.c < b.d$

Demostración. 1. Por definición, $1 \in \mathbb{N}$ cumple el resultado

2. Por definición, $m \in \mathbb{N}$ cumple el resultado
3. Si se cumplen las dos hipótesis, y no se da la igualdad, debe darse la desigualdad estricta en doble sentido, contradicción
4. $n.m = n.(A(m) + 1) = n.A(m) + n = n + n.A(m) \Rightarrow n < n + n.A(m) = n.m$
5. $(\Rightarrow) a < b \Rightarrow \exists q \in \mathbb{N} : a+q = b \Rightarrow b+c = a+q+c \Rightarrow q \in \mathbb{N}$ cumple $(a+c)+q = (b+c)$. Es decir: $a + c < b + c$

   $(\Leftarrow)$ Veamos para el caso de $c \neq 1$:

   $a + c < b + c \Rightarrow \exists q \in \mathbb{N} : (a + c) + q = (b + c) \Rightarrow S^{A(c)}(a + q) = S^{A(c)}(b)$. Por inyectividad de $S^{A(c)}$, $a + q = b$. Luego q verifica en la definición que $a < b$
6. $\forall a, b, c \in \mathbb{N}, (a < b \iff a.c < b.c)$
7. Sean a, b, c, d naturales. $(a < b) \wedge (c < d) \Rightarrow a.c < b.d$

□

3.3.2 Ordinales y Cardinalidad

Definición 3.3.13 (Relación de orden estricta)**.**

Definición 3.3.14 (Conjunto Transitivo)**.**

Definición 3.3.15 (Ordinal)**.**

Proposición 3.3.16 (Propiedades de ordinales)**.**

Definición 3.3.17 (Definición alternativa de $\mathbb{N}$)**.**

Definición 3.3.18 (Axiomas de Peano (versión Moderna))**.**

Teorema 3.3.19 (Forma Normal de Cantor)**.**

Corolario 3.3.20 (Orden en $\mathbb{N}$ usando definición alternativa)**.**

Definición 3.3.21 (Cardinalidad)**.**

Corolario 3.3.22. *Todo conjunto tiene como cardinal al menos a sí mismo.*

Definición 3.3.23 (Conjunto finito)**.**

Definición 3.3.24 (Conjunto Infinito)**.**

Definición 3.3.25 (Secuencias)**.** Una secuencia es una función cuyo dominio son los naturales

Teorema 3.3.26. *El conjunto de los números naturales es infinito*

Teorema 3.3.27. *El conjunto potencia de un conjunto finito tiene como cardinal al resultado de multiplicar el cardinal del conjunto veces el 2. Esto es:*

Notación 3.3.28. Definiremos la cardinalidad de cualquier ordinal como:

Teorema 3.3.29. *No existe biyección entre conjunto de todas las secuencias de números naturales y los naturales*

Proof. □

Proposición 3.3.30. *El conjunto de todas las secuencoas de naturales tiene cardinalidad :* $2^{\aleph_0}$

Comentario 3.3.31. El lector más atento se habrá dado cuenta de lo que lo anterior significa: Hemos encontrado infinitos más grandes que otros.

3.4 Escritura

En esta sección, usaremos la anterior definición de números naturales (La que incluye al 0 como número natural)

Proposición 3.4.1 (División en $\mathbb{N}$)**.** *Dado dos números naturales n, m arbitrarios, con $m \leq n$. Existe un único par de números naturales q, r que verifican $n = mq + r$ con $0 \leq r < m$*

Demostración. En efecto, basta tomar el conjunto $\{n - mp : p \in \mathbb{N}\} \subseteq \mathbb{N}$. Recordemos que $n - m.1 \in \mathbb{N} \Rightarrow 1 \in \{n - mp : p \in \mathbb{N}\}$, luego $\{n - mp : p \in \mathbb{N}\} \neq \phi$. Ahora bien, sabemos que tiene mínimo por el buen orden de $\mathbb{N}$, luego $\exists! r := min\{n - mp : p \in \mathbb{N}\}$. Sabemos que $r \in \{n - mp : p \in \mathbb{N}\} \Rightarrow \exists p_0 \in \mathbb{N} : r = n - mp_0 \Rightarrow r + mp_0 = n$. Si suponemos que $r \geq m \Rightarrow (r - m) = n - mp_0 - m = n - m(p_0 + 1) \in \{n - mp : p \in \mathbb{N}\}$, pero sabemos que $r - m < r$ el cual es el mínimo, es decir, contradicción $(\Rightarrow\Leftarrow)$ □

Teorema 3.4.2 (Bases de numeración)**.** *Sea $S(m)$ un número natural distinto de 1 arbitrario, fijo. $\forall n \in \mathbb{N}, \exists! k \in \mathbb{N}$:*

$$\exists!\{a_i : i \in I_k\} \subseteq I_m : n = \sum_{i=1}^{k} a_i.(S(m))^i$$

El lector no debe confundirse por la notación, lo que estamos afirmando es que para todo natural, hay una lista de algunos números naturales, indexados por algún I_k que verifica que n puede escribirse (o determinarse) enteramente a partir de los números $1, 2, ..., m$.

Definición 3.4.3. Sea $S(m)$ un número natural distinto de 1 arbitrario, fijo. Definimos la función $B_m : \mathbb{N} \to \mathbb{N}^{\mathbb{N}}$ representación base m, como sigue:

$$B(n) = \{a_i : i \in \mathbb{N}\}$$

Donde: Si $i \leq k \Rightarrow a_i$ son del teorema anterior. Si $i > k \Rightarrow a_i = 0$

Proposición 3.4.4. *B_m es inyectiva*

Corolario 3.4.5. *$B_m : \mathbb{N} \to B_m(\mathbb{N})$ tiene inversa*

Notación 3.4.6. Como la función $B_m : \mathbb{N} \to B_m(\mathbb{N})$ tiene inversa, podemos escribir todo número natural de la siguiente forma:

$$n = a_1 a_2 a_3 .... a_k$$

De hecho, toda secuencia descrita como en el lado derecho representará un único número natural. De ser así, decimos que cada a_i es un dígito de la representación base m. Además, decimos que el número está escrito en base m.

Comentario 3.4.7. cuando tomemos $m = S(9)$, obtenemos la representación común de siempre.

Teorema 3.4.8 (Cambio de Base a 10)**.** *Podemos efectuar un cambio de base arbitraria a base 10*

Teorema 3.4.9 (Cambio de Base 10 a cualquiera)**.** *Podemos efectuar un cambio de base de la base 10 a una base arbitraria*

Corolario 3.4.10 (Cambio de Base arbitrario)**.** *Podemos cambiar de base de forma arbitraria*

Ejemplo 3.4.11 (Productos de 2 dígitos Veloces)**.** Usamos distributiva, presentas noción de producto notable:

Definición 3.4.12 (Base Binaria)**.** La base 2 es llamada base Binaria y los números escritos en dicha base se llaman números binarios

Comentario 3.4.13. Todo artefacto electrónico sólo es capaz de interpretar 2 procesos: El flujo de la corriente y la ausencia de este. En este sentido, crear una lógica lo suficientemente robusta para darle instrucciones a un computador consiste en simplemente verificar que un componente este prendido y otro este apagado.

Con todo lo anterior hemos cubierto la lógica, pero el axioma del infinito no parece leerse de forma sencilla en términos de 0 y 1, con lo que nuestra construcción de los naturales no parece llegar más lejos.

Con esto en mente, el cambio de base a base binaria (o base 2) es perfecto, pues permite representar números de todo tipo en térmimos de 0 y 1.

Otras propiedades es que algunas operaciones aritméticas reducen su complejidad debido a que pueden expresarse de forma más sencilla