Resumen de aritmética de Peano

UDELAR/FING/IMERL

16 de febrero de 2017

1. Fundamentos de la Aritmética de Peano.

Axioma 1.1. *Existe un conjunto al que denotamos* $\mathbb{N}$*, un elemento* $0 \in \mathbb{N}$ *y una función* $\mathrm{s} : \mathbb{N} \to \mathbb{N}$ *que satisfacen:*

1. s *es inyectiva.*
2. $0 \notin \mathrm{Im(s)}$.
3. Principio de inducción*: Para todo* $A \subseteq \mathbb{N}$*, si* $0 \in A$ *y* $\forall x \in A \quad \mathrm{s}(x) \in A$*; entonces* $A = \mathbb{N}$.

Un conjunto A tal que $0 \in A$ y $\forall x \in A \quad \mathrm{s}(x) \in A$ diremos que es *inductivo.*

Corolario 1.2. Demostraciones por Inducción Completa: *Sea* $\varphi(x)$ *una propiedad acerca de un natural genérico* x*. Para demostrar* $\forall n \in \mathbb{N} \quad \varphi(n)$ *basta con demostrar* $\varphi(0)$ *y* $\forall n \in \mathbb{N} \quad \varphi(n) \Rightarrow \varphi(n+1)$.

Demostración. Bajo estas hipótesis, si definimos $A = \{x \in \mathbb{N} \mid \varphi(x)\}$, el conjunto A es inductivo. □

Proposición 1.3. $\mathbb{N} = \{0\} \cup \mathrm{Im(s)}$

Demostración. $\{0\} \cup \mathrm{Im(s)}$ es inductivo. □

Corolario 1.4. $\forall x \in \mathbb{N} \quad x \neq 0 \Leftrightarrow (\exists y \quad x = \mathrm{s}(y))$.

Observación 1.5. Principio de recurrencia: *Sea* A *un conjunto (cualquiera),* $c \in A$ *y* $F : A \to A$*. Entonces existe una única función* $f : \mathbb{N} \to A$ *tal que* $f(0) = c$ *y* $\forall x \in \mathbb{N} \quad f(\mathrm{s}(x)) = F(f(x))$.

Las condiciones de f son una receta para calcularla y, por lo tanto, la definen en un sentido computacional: $f(\mathrm{s}(\mathrm{s}(\mathrm{s}\,0))) = F(F(F(c)))$. Intuitivamente, las condiciones de f dicen que el conjunto donde se puede calcular es inductivo y, por lo tanto, es todo $\mathbb{N}$.

Justificar esto requiere definir una n-aproximación de f como una función que satisface lo pedido hasta el natural n y luego probar por inducción que para cada natural n existe una única n-aproximación. Por último, la f pedida es la unión de todas las n-aproximaciones.

Por tratarse de una prueba técnica, aceptaremos el resultados como si fuera parte del axioma, sabiendo que podríamos demostrarlo.

2. Operaciones y orden.

Definición 2.1. *Definiciones recursivas de suma y producto:*

$$\begin{aligned} 0+n &= n \\ \mathrm{s}(m)+n &= \mathrm{s}(m+n) \\ 0\times n &= 0 \\ \mathrm{s}(m)\times n &= (m\times n)+n \end{aligned}$$

Observación: en estas definiciones n es un parámetro. De hecho se define una función suma y una función producto de una variable para cada valor de n de la otra variable.

Proposición 2.2.

1. $\forall x \in \mathbb{N} \quad x+0=0+x=x.$
2. $\forall xyz \in \mathbb{N} \quad (x+y)+z=x+(y+z).$
3. $\forall xy \in \mathbb{N} \quad x+y=y+x.$
4. $\forall xyz \in \mathbb{N} \quad (x+y=x+z \Rightarrow y=z).$

Demostración.
1. y 2. son directos. Para 3., probamos el siguiente

Lema 2.3. $\forall xy \in \mathbb{N} \quad \mathrm{s}(x)+y=x+\mathrm{s}(y).$

Demostración. Por inducción en x. La base inductiva ($x=0$) se verifica directamente: $\mathrm{s}(0)+y=\mathrm{s}(0+y)=\mathrm{s}(y)=0+\mathrm{s}(y)$.

Paso inductivo: $\mathrm{s}(\mathrm{s}(x))+y=\mathrm{s}(\mathrm{s}(x)+y)=\mathrm{s}(x+\mathrm{s}(y))=\mathrm{s}(x)+\mathrm{s}(y)$. La segunda igualdad corresponde a la aplicación de la hipótesis de inducción. □

Luego probamos 3. por inducción en x: Para $x=0$ es consecuencia de 1. Supongamos que $x+y=y+x$. Entonces $\mathrm{s}(x)+y=\mathrm{s}(x+y)=\mathrm{s}(y+x)=\mathrm{s}(y)+x=y+\mathrm{s}(x)$, siendo la última igualdad consecuencia de 2.3.

Para 4. el paso inductivo se deduce de la inyectividad de s. □

Proposición 2.4. *Propiedad distributiva:*

1. $\forall xyz \in \mathbb{N} \quad (x+y)\times z=(x\times z)+(y\times z).$
2. $\forall xyz \in \mathbb{N} \quad x\times(y+z)=(x\times y)+(x\times z).$

Demostración. Las dos identidades de la propiedad distributiva se prueban por inducción en x. □

Observación 2.5. *Denotamos* 1 *a* $\mathrm{s}(0)$. *Observamos que* $\mathrm{s}(x)=\mathrm{s}(x)+0=x+\mathrm{s}(0)=x+1$.

Observación 2.6. *Si* $x,y\in\mathbb{N}$ *y* $x+y=0$, *entonces* $x=y=0$. *En efecto, si* $x\neq 0$, *entonces* $x=\mathrm{s}(h)$ *para algún* h *y substituyendo* $x+y=\mathrm{s}(h)+y=\mathrm{s}(h+y)\neq 0$ *(absurdo). Si* $y\neq 0$, *por la conmutatividad de la suma se llega a la misma contradicción. Entonces* $x=y=0$.

Proposición 2.7.

1. $\forall x \in \mathbb{N} \quad x \times 1 = 1 \times x = x$.
2. $\forall xyz \in \mathbb{N} \quad (x \times y) \times z = x \times (y \times z)$.
3. $\forall xy \in \mathbb{N} \quad x \times y = y \times x$.
4. $\forall xyz \in \mathbb{N} \quad x \neq 0 \Rightarrow (x \times y = x \times z \Rightarrow y = z)$.

Demostración.
1. es directo. 2. se puede probar por inducción en x y usando la propiedad distributiva. Probar 3 es posible mediante el siguiente

Lema 2.8. $\forall xyz \in \mathbb{N} \quad y \times \mathrm{s}(x) = y \times x + y$.

Demostración. $y \times \mathrm{s}(x) = y \times (x + 1) = y \times x + y \times 1 = y \times x + y$. □

Para demostrar 3., lo hacemos por inducción en x. Para $x = 0$ es directo. Supongamos que $x \times y = y \times x$. Entonces $\mathrm{s}(x) \times y = x \times y + y = y \times x + y = y \times \mathrm{s}(x)$, donde la segunda igualdad es consecuencia de la hipótesis de inducción y la tercera del lema 2.8.

Para probar 4., probamos los siguientes

Lema 2.9. $\forall xy \in \mathbb{N} \quad x \times y = 0 \Rightarrow x = 0 \vee y = 0$.

Demostración. Por absurdo: si $x, y \neq 0$, entonces $x \times y = \mathrm{s}(m) \times \mathrm{s}(n)$ para ciertos $m, n \in \mathbb{N}$. Luego $0 = \mathrm{s}(m) \times \mathrm{s}(n) = m \times \mathrm{s}(n) + \mathrm{s}(n) = \mathrm{s}(n) + m \times \mathrm{s}(n) = \mathrm{s}(n + m \times \mathrm{s}(n)) \neq 0$ por el corolario 1.4 (absurdo). Entonces $x = 0$ o $y = 0$. □

Lema 2.10. *Para todo $x, y \in \mathbb{N}$ se cumple una y sólo una de las siguientes: $x = y$, o bien existe $h \neq 0$ tal que $x = y + h$, o bien existe $h \neq 0$ tal que $y = x + h$.*

Demostración. La propiedad cancelativa de la suma permite observar que las tres posibilidades son excluyentes. Para probar la disyunción, hacemos inducción en x (con y fijo). Para $x = 0$ es consecuencia del corolario 1.4. Paso inductivo: Suponemos que el resultado vale para x y lo probamos para $\mathrm{s}(x)$.

- Si $x = y$, entonces $\mathrm{s}(x) = \mathrm{s}(y) = y + \mathrm{s}(0) = y + h$ con $h = 1$.
- Si $x = y + h$, entonces $\mathrm{s}(x) = \mathrm{s}(y + h) = y + \mathrm{s}(h) = y + h'$ con $h' = \mathrm{s}(h)$.
- Si $y = x + h$ con $h \neq 0$, entonces $h = \mathrm{s}(k)$ para algún k.
  - Si $k = 0$, entonces $y = x + \mathrm{s}(0) = \mathrm{s}(x + 0) = \mathrm{s}(x)$.
  - Si $k \neq 0$, entonces $k = \mathrm{s}(\ell)$ para algún ℓ e $y = x + \mathrm{s}(\mathrm{s}(\ell)) = \mathrm{s}(x) + \mathrm{s}(\ell)$. La última igualdad es consecuencia del Lema 2.3.

□

Ahora probamos 4.: Supongamos que $y \neq z$. Por el Lema 2.10, tenemos que $z = y + h$ o bien $y = z + h$ con $h \neq 0$. Supongamos que $z = y + h$. Por hipótesis $x \times y + 0 = x \times y = x \times z = x \times (y + h) = x \times y + x \times h$. Por la cancelativa de la suma, deducimos que $0 = x \times h$ y como $x \neq 0$, entonces $h = 0$, lo cual es absurdo. □

Observación 2.11. *Las definiciones de suma y producto que presentamos hacen recurrencia en el primer argumento. Podríamos haber presentado definiciones por recurrencia en el segundo argumento. Los lemas 2.3 y 2.8 prueban que ambas elecciones conducen a las mismas operaciones. Dicho de otro modo: a los efectos de probar que las operaciones definidas son conmutativas probamos primero que las respectivas definiciones no dependen del argumento que se elige para hacer recursión.*

Definición 2.12. *Dados dos naturales x, y, decimos que $x < y$ si y sólo si existe $h \neq 0$ tal que $y = x + h$.*

Observación 2.13. *Tenemos que $1 = 0 + 1$ y que $1 \neq 0$. Entonces $1 > 0$. Más en general, $\mathrm{s}(x) = x + 1$, de donde $\mathrm{s}(x) > x$.*

Si $x < y$, entonces $y = x + h$ con $h \neq 0$. De ahí $\mathrm{s}(y) = \mathrm{s}(x + h) = x + \mathrm{s}(h)$ por lema 2.3, lo que permite concluir que $\mathrm{s}(y) > \mathrm{s}(x)$. Es decir: la función sucesor es (estrictamente) creciente.

Proposición 2.14.

1. $\forall xyz \in \mathbb{N} \quad x < y < z \Rightarrow x < z$.
2. *Para todo $x, y \in \mathbb{N}$ se cumple una y sólo una de las siguientes: $x = y$, o bien $y > x$, o bien $x > y$.*

Demostración. La transitividad del orden es directa: $z = y + k = x + h + k$ y $h + k$ es diferente de cero porque h es diferentes de cero (es un sucesor que al sumarlo a k se obtiene un sucesor). El lema 2.10 establece 2. (la *tricotomía*). □

Proposición 2.15.

1. $\forall xyz \in \mathbb{N} \quad x < y \Leftrightarrow x + z < y + z$.
2. $\forall xyz \in \mathbb{N} \quad z \neq 0 \Rightarrow (x < y \Leftrightarrow x \times z < y \times z)$.

Demostración.

1. $y = x + h$ con $h \neq 0$ implica que $y + z = x + h + z$; donde $h + z \neq 0$ porque $h \neq 0$. Recíprocamente, si $y + z = x + z + h$ con $h \neq 0$, por la prop cancelativa (y la conmutativa y la asociativa usadas discrecionalmente), se deduce que $y = x + h$.
2. $y = x + h$ con $h \neq 0$ implica que $y \times z = (x + h) \times z = x \times z + h \times z$. Como $h, z \neq 0$, entocens $h \times z \neq 0$. Recíprocamente, supongamos que $x \times z < y \times z$ con $z \neq 0$. Por tricotomía existen tres posibilidades para x e y:

a) $x = y$, en cuyo caso $x \times z = y \times z$ (absurdo).

b) $x > y$, que por el directo implica que $x \times z > y \times z$ (absurdo).

c) $x < y$, que es entonces la que se cumple.

□

3. Buena ordenación e inducción fuerte.

El *Principio de Buena Ordenación* establece lo siguiente:

Proposición 3.1. *Todo conjunto no vacío de naturales tiene mínimo.*

Es más simple para la demostración razonar sobre el contrarrecíproco de este enunciado, es decir:

Proposición 3.2. *Si $A \subseteq \mathbb{N}$ no tiene mínimo, entonces $A = \emptyset$.*

Intuitivamente se puede razonar del siguiente modo: Como A no tiene mínimo, entonces $0 \notin A$, es decir que $0 \in A^c$. Como $0 \in A^c$, si $1 \in A$, entonces 1 sería el mínimo de A. Por lo tanto $0, 1 \in A^c$. Como $0, 1 \in A^c$, si $2 \in A$, entonces 2 sería el mínimo de A y entonces $0, 1, 2 \in A^c$. Siguiendo así sucesivamente con este razonamiento obtenemos que $0, 1, 2, \cdots n \cdots \in A^c$, es decir que $A^c = \mathbb{N}$ y concluimos que $A = \emptyset$.

Para dar un sentido preciso a la expresión *"y así sucesivamente"* contamos con la inducción y con las definiciones recursivas. Pero para que este razonamiento funcione es preciso saber que si $0 \notin A$ y $1 \in A$, entonces 1 es el mínimo de A. Es decir, que no existan naturales menores que 1 y mayores que 0:

Lema 3.3. $\{x \in \mathbb{N} \mid 0 < x < 1\} = \emptyset$.

Demostración. Consideramos $X = \{0\} \cup \{x \in \mathbb{N} \mid 1 \leq x\}$. Este conjunto es inductivo: en efecto, $\mathrm{s}(0) = 1 \in X$ y si $0 \neq x \in X$, entonces $1 \leq x$ y por la observación 2.13 $1 < x < \mathrm{s}(x)$ y concluimos que $\mathrm{s}(x) \in X$.

Como X es inductivo, entonces $X = \mathbb{N}$. Además, para todo $x \in X$ no se satisface que $0 < x < 1$; lo cual termina la demostración. □

Corolario 3.4. $\forall n \in \mathbb{N} \quad \{x \in \mathbb{N} \mid n < x < n + 1\} = \emptyset$.

Demostración. Si $n < x$, entonces $x = n + h$ para algún $h \neq 0$. Si además $x < n + 1$, tenemos que $n = n + 0 < n + h < n + 1$, de donde, por monotonía se deduce que $0 < h < 1$ (absurdo). □

Ahora probaremos el contrarrecíproco del *Principio de Buena Ordenación* (proposición 3.1): *Si A no tiene mínimo, entonces A es vacío.*

Demostración. Definimos $I_n := \{x \in \mathbb{N} \mid x \leq n\}$. Se verifica directamente que $\bigcup_{n \in \mathbb{N}} I_n = \mathbb{N}$. Por el corolario 3.4, tenemos que $I_{n+1} \setminus I_n = \{n + 1\}$, es decir que $I_{n+1} = I_n \cup \{n+1\}$. Concluimos que si $I_n \subseteq A^c$ pero $I_{n+1} \not\subseteq A^c$, entonces $n+1$ sería el mínimo de A (absurdo). Entonces tenemos:

- $I_0 \subseteq A^c$ (porque que A no tiene mínimo implica que $0 \notin A$)
- $\forall n \in \mathbb{N} \quad I_n \subseteq A^c \Rightarrow I_{n+1} \subseteq A^c$

Por inducción concluimos que $\forall n \in \mathbb{N} \quad I_n \subseteq A^c$, de donde $\mathbb{N} = \bigcup_{n\in\mathbb{N}} I_n \subseteq A^c$, $A^c = \mathbb{N}$ y concluimos que $A = \emptyset$. □

No siempre es posible demostrar una propiedad acerca de los naturales por inducción completa: Veamos el caso del *Teorema Fundamental de la Aritmética*.

Definición 3.5. *Dados dos naturales m, n, decimos que m* divide *a n si y sólo si existe $k \in \mathbb{N}$ tal que $n = k \times m$. Decimos que $p \in \mathbb{N}$ es* primo *si y sólo si $p \neq 1$ y sus únicos divisores son $\{1, p\}$. Un número que no es primo se dice* compuesto*.*

Observación 3.6. *Un número natural q es compuesto si y sólo si existen naturales $m, n \geq 2$ tales que $q = m \times n$. Por monotonía del producto, $m \times 1 < m \times n = q$ y $n \times 1 < n \times m = q$, es decir, los dos factores m, n son menores que q.*

Teorema 3.7. *Todo natural $q \geq 2$ se descompone como producto de números primos. Más aún, esta descomposición es única a menos de permutaciones.*

Si intentamos probarlo por inducción, deberíamos probar que si n admite una descomposición en factores primos, entonces $n + 1$ también. Sin embargo, las descomposiciones en factores primos de n y $n + 1$, en principio no tienen relación alguna. Por ejemplo, ¿Cómo probar que 14 se descompone en producto de factores primos sabiendo que 13 es su propia descomposición en factores primos?

Podemos razonar de otra forma: Si q es primo, q es su propia descomposición. Si q es compuesto, entonces existen $m, n \geq 2$ tales que $q = m \times n$. Como m, n son menores que q, si ya tenemos probado que *todos los números menores que q admiten una descomposición en factores primos*, entonces es evidente que q es producto de factores primos. Hacer este razonamiento, en lugar de suponer apenas que $q - 1$ satisface el teorema, da más información para probar que q lo satisface. Veremos que esta forma de paso inductivo, usando una hipótesis más fuerte, permite también probar teoremas para todos los naturales.

Proposición 3.8. Principio de Inducción Fuerte:

$\varphi(x)$ una propiedad aritmética acerca un natural (genérico) x[1]*. Supongamos que:*

1. *$\varphi(0)$ se satisface.*

[1] $\varphi(x)$ es una propiedad que involucra a los símbolos de $0, \mathrm{s}, +, \times$, a la variable x, conectivas booleanas $(\wedge, \vee, \neg \Rightarrow)$ y cuantificadores $\forall$ y $\exists$. Por ejemplo, $\varphi(x) = \exists y \quad x = y + y$ es una propiedad que expresa que x es par. Entonces en los naturales $\varphi(1)$ es falsa, pero $\varphi(2)$ es verdadera. Técnicamente φ es lo que se denomina una *fórmula de primer orden de la aritmética*. En el curso de lógica se verá una definición rigurosa de esta idea.

2. Para todo natural $m \neq 0$, $\Big(\forall n < m \quad \varphi(n)\Big) \Rightarrow \varphi(m)$.

Entonces $\forall n \in \mathbb{N} \quad \varphi(n)$.

Demostración. Sea $A = \{x \in \mathbb{N} \mid \neg\varphi(x)\}$. Debemos probar que $A = \emptyset$. Por absurdo, si $A \neq \emptyset$, entonces existe m mínimo de A. Como $\varphi(0)$ se satisface, entonces $0 \notin A$, de modo que $m \neq 0$. Para todo $n < m$, $n \notin A$, de donde se deduce que $\forall n < m \quad \varphi(n)$. Por la condición 2. sabemos que se satisface $\varphi(m)$ y concluimos que $m \notin A$ (absurdo). □