Miscelánea Matemática **74** (2022) 25-38 SMM

DOI: https://doi.org/10.47234/mm.7404

La paridad de los números naturales

Josefina Álvarez
Departamento de Matemáticas
New Mexico State University
jalvarez@nmsu.edu
y
Larry Hughes
Departamento de Matemáticas
New Mexico State University
lorenz.hughes@gmail.com

1. Introducción

Si preguntamos «¿es 655 par o impar?», la respuesta «obvia» debería de ser «es impar». Esto ocurre porque nuestro cerebro está acostumbrado a trabajar en el sistema decimal, en el cual 655 representa al número

$$6 \times 10^2 + 5 \times 10^1 + 5 \times 10^0. \tag{1}$$

Cada dígito, $6, 5, 5$, tiene el valor indicado por la potencia de 10. El dígito 5 se usa dos veces, cada vez con un valor diferente. Por esto el sistema decimal es lo que se llama un sistema de notación posicional.

Aunque estamos muy acostumbrados al sistema decimal, en realidad no tiene nada de especial. Los números naturales se pueden representar usando cualquier número natural $b > 1$ como base, siendo los dígitos $0, 1, 2, \ldots, b-1$. Por ejemplo, en base 9, con dígitos $0, 1, 2, 3, 4, 5, 6, 7, 8$, el símbolo 655 representa al número

$$6 \times 9^2 + 5 \times 9^1 + 5 \times 9^0, \tag{2}$$

el cual, a su vez, tiene la representación 536 en base 10. Es decir, ¡655 en realidad representa, en base 9, a un número par!

Motivados por estas observaciones, el propósito de nuestro artículo es el formular un criterio que nos permita decidir la paridad de un número simplemente examinando su representación en cualquier base. Pero antes de emprender esto, necesitaremos responder a varias preguntas que ya están insinuadas en esta introducción. Por ejemplo, habiendo usado

Palabras clave: números naturales, axiomas, propiedades, teorema de la división, representación de números naturales, función módulo, paridad.

las palabras número, número natural y representación de un número natural, tenemos que explicar lo que ellas significan. Además, necesitamos probar que la representación de un número natural en una base dada siempre existe y es única y, finalmente, que la paridad de un número natural es una característica intrínseca del número, independiente de su representación.

Digamos que una vez que hayamos establecido nuestro sistema numérico, es decir los números naturales, todos los resultados serán enunciados y probados dentro de este sistema, sin hacer referencia a ningún otro.

Entonces, pongámonos a trabajar.

2. Números y numerales

En una colección de artículos publicado en 1888 con el título *Was sind und was sollendie Zahlen?* (Los números, ¿qué son y qué deberían de ser?), Richard Dedekind responde a la pregunta del título con gran lucidez. Por ejemplo dice [2, p. 14] «En la ciencia, nada que pueda ser probado debe ser aceptado sin demostración. Aunque esta condición parecería ser muy razonable no puedo decir que haya sido satisfecha en los métodos, aún los más recientes, usados en la fundamentación de la ciencia más simple, aquella parte de la lógica que se dedica a la teoría de números. Cuando hablo de la aritmética como parte de la lógica quiero implicar que considero al concepto de número completamente independiente de las nociones o intuiciones de espacio y tiempo, que lo considero una consecuencia inmediata de las leyes del pensamiento. Mi respuesta a los problemas sugeridos en el título de este artículo es, sucintamente, que los números son creaciones de la mente humana, que sirven para concebir con más claridad las diferencias entre diversas cosas. Desde que nacemos, continuamente y de manera creciente, somos llevados a relacionar unas cosas con otras y, por lo tanto, a usar la facultad de la mente de la que depende la creación de los números... Así adquirimos una reserva de verdades aritméticas a las cuales nuestros primeros maestros aluden como algo simple, obvio, guardado en nuestra consciencia interna. De esta manera ocurre que muchas nociones muy complejas (por ejemplo la noción de cantidad) son consideradas, incorrectamente, muy simples.»

Dedekind también dice [2, p. 2], «Considero a la totalidad de la aritmética como una consecuencia necesaria, o al menos natural, de la acción aritmética más sencilla, el contar, que no es nada más que la creación sucesiva de la serie infinita de los números positivos en la cual cada individuo se define usando el que lo precede inmediatamente;

la acción más simple es el pasar de un individuo ya formado al nuevo individuo por formar... Sumar es combinar en una acción única repeticiones arbitrarias de la acción más simple que acabamos de mencionar; de la acción de sumar surge la multiplicación en una manera similar.»

Puesto que, específicamente, estamos interesados en los números llamados naturales, su introducción formal nos lleva a considerar la obra de Guiseppe Peano.

Inspirado en el trabajo de Dedekind, Peano incluyó nueve axiomas en su libro *Arithmetices principia, nova methodo exposita* (Los principios de la aritmética presentados de una nueva manera) [3] publicado en 1889. El primer axioma establece la existencia de por lo menos un número natural, representado por el símbolo 1, que más tarde es reemplazado con 0. Los siguientes cuatro axiomas introducen la noción de igualdad como una relación reflexiva, simétrica y transitiva, y declaran que los números natural son un conjunto cerrado con respecto a la igualdad. Estos cuatro axiomas dejaron de ser incluídos cuando fueron reconocidos como parte de la lógica en general en lugar de ser específicos de los números naturales. Los siguientes tres axiomas corresponden a una operación S, llamada operación sucesora, que crea números naturales. El último axioma, el principio de inducción, asegura que todos los números naturales son creados de esa manera. Dedekind ya había afirmado [2, p. 14] que uno de sus propósitos era el probar que «la forma de argumentar llamada inducción completa (o la inferencia de $n+1$ a partir de n) es realmente concluyente y que, por lo tanto, la definición por inducción (o recursión) está determinada y es consistente.»

A continuación incluímos una formulación moderna de la axiomática de Peano, donde $\mathbb{N}$ indica los números naturales.

1. $0 \in \mathbb{N}$.
2. Existe una operación sucesora S tal que
   $1 \stackrel{def}{=} S(0), 2 \stackrel{def}{=} S(S(0)), 3 \stackrel{def}{=} S(S(S(0))), \ldots$
3. La operación sucesora es inyectiva. Esto es, ningún número natural puede ser el sucesor de dos números naturales.
4. No existe un número natural A tal que $S(A) = 0$. Es decir, 0 no es el sucesor de ningún número natural.
5. (Principio de inducción) Sea $\mathbb{K}$ un subconjunto de $\mathbb{N}$ con las siguientes propiedades:
   (a) $0 \in \mathbb{K}$.
   (b) $A \in \mathbb{K}$ implica $S(A) \in \mathbb{K}$.
   Entonces, $\mathbb{K} = \mathbb{N}$.

Observemos que la elección de los símbolos $0, 1, 2, 3, \ldots$ se debe a nuestra familiaridad con los numerales indoarábigos. En realidad,

los números naturales son $*, S(*), S(S(*)), S(S(S(*))), \ldots$ donde se puede reemplazar $*$ con absolutamente cualquier símbolo.

A partir de los axiomas 1) a 5) la suma y la multiplicación se definen recursivamente de la siguiente manera:

S1: $A + 0 = A$,
S2: $A + S(B) = S(A + B)$,
M1: $A \cdot 0 = 0$,
M2: $A \cdot S(B) = A + (A \cdot B)$.

Por ejemplo, si queremos calcular $4 + 3$, usamos S1) y S2) de la siguiente manera:

$$\begin{aligned} 4 + 3 &= S(S(S(S(0)))) + S(S(S(0))) = S(S(S(S(S(0))))) + S(S(0))) \\ &= S(S(S(S(S(S(0))))) + S(0))) = S(S(S(S(S(S(0)))) + 0))) \\ &= S(S(S(S(S(S(S(0))))))) = 7. \end{aligned}$$

Una vez más, los símbolos 4, 3 y 7 son simplemente elecciones convenientes.

Similarmente, usando M1) y M2),

$$\begin{aligned} 4 \cdot 3 &= 4 \cdot S(2) = 4 + (4 \cdot 2) = 4 + 4 + (4 \cdot 1) \\ &= 4 + 4 + 4 + (4 \cdot 0) = 4 + 4 + 4 + 0 \\ &= 4 + 4 + 4, \end{aligned}$$

donde la suma se calcula usando S1) y S2).

Por lo tanto, la expresión (2) tiene un significado preciso en términos de la operación sucesora, una vez que definimos $9^2 \stackrel{def}{=} 9 \cdot 9$, $9^1 \stackrel{def}{=} 9$ y $9^0 \stackrel{def}{=} 1$. Sin embargo el escribir

$$6 \cdot 9^2 + 5 \cdot 9^1 + 5 \cdot 9^0 = 536$$

constituye un abuso de notación porque realmente no es una igualdad. En cambio debe leerse como «536 representa $6 \cdot 9^2 + 5 \cdot 9^1 + 5 \cdot 9^0$ en base 9».

Se puede probar que la suma y la multiplicación, definidas de la manera indicada, son operaciones conmutativas y asociativas, que $S(0)$ es la identidad multiplicativa y que la multiplicación distribuye sobre la suma.

Se define un orden total $\leq$ en $\mathbb{N}$ de la manera siguiente:

Definición 2.1. Si $A, B \in \mathbb{N}$, $A \leq B$ significa que existe $C \in \mathbb{N}$ tal que $A + C = B$. Similarmente, $A \geq B$ indica $B \leq A$. Asociado al orden $\leq$ hay un orden estricto $<$, donde $A < B$ significa $A \leq B$ y $A \neq B$. De la misma manera, $A > B$ significa $B < A$.

Dados $A, B \in \mathbb{N}$ una, y solo una, de $A = B$ o $A < B$ o $A > B$ es posible. Además, $A < B$ si, y solo si, existe $C > 0$ tal que $A + C = B$.

A partir de la definición y la conmutatividad de la multiplicación, se tiene $0 \cdot B = A \cdot 0 = 0$ para todo $A, B \in \mathbb{N}$. El resultado que sigue muestra que el recíproco también es cierto.

Proposición 2.2. *(Propiedad del producto igual a cero) Dados $A, B \in \mathbb{N}$, si $A \cdot B = 0$ entonces $A = 0$ o $B = 0$.*

Demostración. Vamos a probar la contraposición. Es decir, $A > 0$ y $B > 0$ implica $A \cdot B > 0$.

En efecto, $B > 0$ significa $B = 1 + C$ con $C \in \mathbb{N}$. Entonces

$$A \cdot B = A \cdot (1 + C) = A + A \cdot C \geq A > 0$$

y la proposición está probada. □

El orden total $\leq$ es estable con respecto a la suma, y también con respecto a la multiplicación por números diferentes de cero. O sea,

Proposición 2.3. *Dados $A, B, C \in \mathbb{N}$,*

1. *$A \leq B$ si, y solo si, $A + C \leq B + C$,*
2. *$A \leq B$ implica $A \cdot C \leq B \cdot C$,*
3. *$A \cdot C \leq B \cdot C$ y $C > 0$ implica $A \leq B$.*

Demostración. Para probar 1) comenzamos suponiendo $A \leq B$, por lo que hay $m \in \mathbb{N}$ tal que $A + m = B$. Entonces

$$(A + C) + m = (A + m) + C = B + C$$

y en consecuencia $A + C \leq B + C$.

Recíprocamente, si $A + C \leq B + C$ existe $m \in \mathbb{N}$ tal que $A + C + m = B + C$. Como $A \leq B$ o $A > B$, si $A > B$ existe $m' \in \mathbb{N}$ positivo tal que $A = B + m'$. Es decir

$$B + m' + C = B + C$$

o $B + C < B + C$, lo cual no es posible. Entonces $A \leq B$ y 1) está probado.

Si $A \leq B$ existe $m \in \mathbb{N}$ tal que $A + m = B$. O sea,

$$B \cdot C = (A + m) \cdot C = A \cdot C + m \cdot C$$

o $A \cdot C \leq B \cdot C$, lo cual prueba 2).

Finalmente, supongamos $A \cdot C \leq B \cdot C$ y $C > 0$. Debe ser $A \leq B$ o $A > B$. Si $A > B$ existe $m \in \mathbb{N}$ tal que $A = B + m$. Es decir,

$$A \cdot C = (B + m) \cdot C = B \cdot C + m \cdot C$$

o $A \cdot C > B \cdot C$, lo cual contradice nuestra suposición $A \cdot C \leq B \cdot C$ y $C > 0$. Entonces $A \leq B$ lo que prueba 3) y completa la demostración de la proposición. □

El siguiente resultado es una consecuencia inmediata de la proposición 2.3.

Corolario 2.4. *Dados* $A, B, C \in \mathbb{N}$,

a): $A = B$ *si, y solo si,* $A + C = B + C$.
b): $A < B$ *si, y solo si,* $A + C < B + C$.
c): $A = B$ *implica* $A \cdot C = B \cdot C$.
d): $A \cdot C = B \cdot C$ *y* $C > 0$ *implica* $A = B$.
e): $A < B$ *y* $C > 0$ *implica* $A \cdot C < B \cdot C$.
f): $A \cdot C < B \cdot C$ *y* $C > 0$ *implica* $A < B$.

De la parte a) del corolario 2.4 resulta que el número C en la definición 2.1 es único. Lo escribimos como $B - A$, lo cual es más que nada una notación puesto que la resta no está completamente definida en $\mathbb{N}$.

El orden $\leq$ es una buena ordenación de los números naturales. Esto es, todo subconjunto no vacío de $\mathbb{N}$ tiene un elemento que es el primero, o el menor, en el orden. En consecuencia, $0 < 1 < 2 < \ldots < A < A + 1 < \ldots$ para todo $A \in \mathbb{N}$.

La buena ordenación de los números naturales es equivalente al principio de inducción (la demostración se puede ver, por ejemplo, en [1]).

Mencionemos que los resultados de Dedekind, así como los de Peano están basados en resultados anteriores debidos a Hermann Grassmann y Charles Sander Peirce. Grassmann ya había indicado, en 1861, que muchos resultados de la aritmética podían ser obtenidos a partir de la operación sucesora, y Peirce había formulado, en 1881, una axiomatización de la aritmética de los números naturales, que fue refinada y simplificada en la obra de Dedekind y, especialmente, en la de Peano. Estos logros notables lo son más aún si se recuerda el estado rudimentario en que se encontraba la lógica en esos años. Bertrand Russell menciona en su autobiografía [5, p. 148], que la obra de Peano le causó tanta impresión que decidió aislarse en el campo «para estudiar en paz todos los trabajos producidos por Peano y sus discípulos». Russell presenta en su libro introductorio [4] una discussion muy bien escrita del concepto de número, sin tecnicismos.

Nos toca ahora hablar sobre la representación de los números, de la que podemos dar muchos ejemplos: Muescas en huesos o estacas, jeroglíficos, incisiones en arcilla y numerales tales como los chinos o los romanos. Por supuesto, el conjunto formado por Álvarez, Hughes y su perrita Lily puede interpretarse como una representación del número $3 \stackrel{\text{def}}{=} S(S(S(0)))$. Cualquier sistema posicional es una manera excelente de representar números. Aunque comúnmente los dígitos y la base se escriben usando símbolos indoarábigos, este no es siempre el caso. En el sistema hexadecimal, o de base 16, los dígitos son

$$0, 1, 2, 3, 4, 5, 6, 7, 8, 9, A, B, C, D, F.$$

Es decir, que mientras la palabra número tiene un significado muy preciso y bastante abstracto, podemos representar a los números de muchas formas muy concretas. En este artículo nos limitaremos a los sistemas posicionales usando dígitos indoarábigos.

3. Existencia y unicidad de la representación de los números naturales en base b

Comenzamos con la siguiente definición.

Definición 3.1. Dado un número natural $b > 1$, el conjunto

$$\mathbb{D} = \{0, 1, 2, \ldots, b-1\}$$

es el conjunto de los dígitos asociados a la base b,

Un numeral distinto de cero es $(a_k, a_{k-1}, \ldots, a_1, a_0)_b$ donde $a_j \in \mathbb{D}$ para $0 \leq j \leq k$ y $a_k > 0$. Decimos que $A \in \mathbb{N}$, diferente de cero, está representado por el numeral distinto de cero $(a_k, a_{k-1}, \ldots, a_1, a_0)_b$ si

$$A = \sum_{j=0}^{k} a_j b^j.$$

Tal representación se indicará

$$A \to (a_k, a_{k-1}, \ldots, a_1, a_0)_b .$$

En lo que sigue indicamos algunas notaciones.

Con $(0)_b$ denotamos el numeral cero y escribimos $0 \to (0)_b$. El conjunto de los números naturales diferentes de cero será indicado $\mathbb{N}^+$. La multiplicación $A \cdot B$ será generalmente denotada AB.

Teorema 3.2. *Si $A \in \mathbb{N}^+$, existen $a_k, a_{k-1}, \ldots, a_1, a_0 \in \mathbb{D}$, $a_k \neq 0$, únicos tales que*

$$A \to (a_k, a_{k-1}, \ldots, a_1, a_0)_b .$$

La demostración de este teorema usa el teorema de la división para los números naturales, que enunciamos y demostramos a continuación.

Teorema 3.3. *Fijemos $A, B \in \mathbb{N}$, con $B > 0$. Existen números naturales d y r únicos tales que $0 \leq r < B$ y*

$$A = dB + r. \tag{3}$$

Demostración. Probemos primero la existencia.

Si $A = B$, escribimos $A = A + 0$. Es decir, tenemos (3) con $d = 1$ y $0 = r < B$. Si $0 \leq A < B$, escribimos $A = 0B + A$, con lo cual obtenemos (3) con $d = 0$ and $0 \leq r = A < B$.

Nos queda por considerar el caso $B < A$.

Sea

$$\mathbb{S} = \{t \in \mathbb{N} : 0 \leq tB \leq A\}.$$

El conjunto $\mathbb{S}$ no es vacío porque $0 \in \mathbb{S}$. Además es finito porque el ser B positivo implica que $tB > A$ cuando $t > A$. Para ver esto recordemos que $B > 0$ implica $B \geq 1$, de donde $B = 1 + m$ para cierto $m \in \mathbb{N}$. Entonces,

$$tB = t + tm \overset{(i)}{>} A + tm \geq A$$

donde hemos usado en (i) la parte b) del corolario 2.4. Si $tB = A$ tendríamos una igualdad en (i) lo cual no es posible. Por lo tanto $tB > A$ de donde resulta que $\mathbb{S}$ tiene un último o mayor elemento, t_0.

Que $t_0 B \leq A$ significa que hay $r \in \mathbb{N}$ tal que $A = t_0 B + r$. Como $t_0 + 1 \notin \mathbb{S}$,

$$A < (t_0 + 1)\, B = t_0 B + B$$

o

$$t_0 B + r < t_0 B + B$$

lo cual implica $0 \leq r < B$ usando a) en el corolario 2.4. Es decir, obtenemos (3) con $d = t_0$ y r.

En cuanto a la unicidad, supongamos

$$A = dB + r = d'B + r'$$

con $0 \leq r, r' < B$.

Si $d \leq d'$, existe $C \in \mathbb{N}$ tal que $d' = d + C$ o

$$d'B + r' = dB + CB + r' = dB + r.$$

Usando la parte a) en el corolario 2.4,

$$r = CB + r'.$$

Como $0 \leq r < B$, debe ser $C = 0$. Si no lo fuera, $C = 1 + m$ para cierto $m \in \mathbb{N}$. O sea

$$r = (1 + m)\, B + r' = B + Bm + r' \geq B$$

lo cual contradice la hipótesis $0 \leq r < B$. Siendo $C = 0$ resulta $r = r'$ usando a) en el corolario 2.4. Entonces $dB = d'B$ y por lo tanto $d = d'$, usando d) en el corolario 2.4.

Esto prueba la unicidad y completa la demostración del teorema. □

En (3), A, B, d, r se llaman dividendo, divisor, cociente y resto, respectivamente.

A partir de ahora nos referiremos al teorema 3.3 como el teorema de la división.

Y ahora sí estamos listos para probar el teorema 3.2.

Demostración. Ambas, la existencia y la unicidad, resultan del teorema de la división, usando el principio de inducción.

Sea

$$\mathbb{K} = \left\{ k \in \mathbb{N} : A \in \mathbb{N} \text{ y } A < b^{k+1} \text{ implica } A \text{ tiene una única representación en base } b \right\}.$$

Afirmamos que $0 \in \mathbb{K}$. En efecto, dado $0 \leq A < b$, el teorema de la división garantiza que $(A)_b$ es la representación de A.

Suponiendo que $k \in \mathbb{K}$ tenemos que mostrar que $k+1 \in \mathbb{K}$.

Sea $A \in \mathbb{N}$ con $A < b^{k+2}$. De acuerdo al teorema de la división, existen $d, r \in \mathbb{N}$ únicos con $0 \leq r < b$, tal que $A = db + r$. Puesto que

$$db \leq db + r = A < b^{k+2},$$

la parte d) del corolario 2.4 implica $d < b^{k+1}$.

Cuando $d = 0$, tenemos $A = r$ y $A \to (A)_b$. Si $d \geq 1$, la hipótesis inductiva nos dice que d tiene una única representación en base b,

$$d \to (d_l, d_{l-1}, \ldots, d_1, d_0)_b$$

donde $d_j \in \mathbb{D}$ para $j = 0, \ldots, l$, $d_l > 0$ y $d = \sum_{j=0}^{l} d_j b^j$, como dijimos en la definición 3.1.

Por lo tanto,

$$A = db + r = \sum_{j=0}^{l} d_j b^{j+1} + r.$$

Llamando $a_j = d_{j-1}$ para $j = 1, \ldots, l+1$ y $a_0 = r$, tenemos

$$A \to (a_l, a_{l-1}, \ldots, a_1, a_0)_b$$

con unicidad. En efecto, si también

$$A \to \left(a'_m, a'_{m-1}, \ldots, a'_1, a'_0\right)_b$$

tendríamos

$$A = \left(\sum_{j=1}^{l} a_j b^{j-1} \right) b + a_0 = \left(\sum_{j=1}^{m} a'_j b^{j-1} \right) b + a'_0.$$

Debido a la unicidad en el teorema de la división, $a_0 = a'_0$ y

$$d = \sum_{j=1}^{l} a_j b^{j-1} = \sum_{j=1}^{m} a'_j b^{j-1},$$

lo cual, usando la hipótesis inductiva, implica $l = m$ y $a_j = a'_j$ para $j = 0, \ldots, l$.

Por lo tanto, $\mathbb{K} = \mathbb{N}$ y la prueba del teorema está completa. □

En la sección que sigue definimos y estudiamos una función que jugará un papel esencial en la caracterización de la paridad.

4. La función módulo

Recordemos que dado $A \in \mathbb{N}$ y $l \in \mathbb{N}^+$, el teorema de la división nos dice que hay $d, r \in \mathbb{N}$ únicos tales que

$$A = dl + r$$

con $0 \leq r < l$.

De acuerdo con esto, formulamos la siguiente definición.

Definición 4.1. La función módulo l de $\mathbb{N}$ en $\mathbb{N}$, que se denota mod_l, se define como

$$\mathrm{mod}_l(A) = r.$$

Proposición 4.2. *La función mod_l tiene las siguiente propiedades:*

1. *Si $A < l$,*
$$\mathrm{mod}_l(A) = A.$$
2. *La función mod_l es idempotente. Esto es,*
$$\mathrm{mod}_l[\mathrm{mod}_l(A)] = \mathrm{mod}_l(A)$$
para todo $A \in \mathbb{N}$.
3. *Si A es un múltiplo de l,*
$$\mathrm{mod}_l(A) = 0.$$
4. $$\mathrm{mod}_l\left(\sum_{j=1}^{J} A_j\right) = \mathrm{mod}_l\left[\sum_{j=1}^{J} \mathrm{mod}_l(A_j)\right]$$
para todo $A_1, \ldots, A_J \in \mathbb{N}$.
5. $$\mathrm{mod}_l\left(\prod_{j=1}^{J} A_j\right) = \mathrm{mod}_l\left[\prod_{j=1}^{J} \mathrm{mod}_l(A_j)\right]$$
para todo $A_1, \ldots, A_J \in \mathbb{N}$.

Demostración. Si $A < l$ escribimos $A = 0 \cdot l + A$ lo cual muestra, por definición, $\mathrm{mod}_l(A) = A$. Así, 1) está probado. Otra vez por definición, $\mathrm{mod}_l(A) < l$, por lo cual 2) es una consecuencia de 1).

Que A es un múltiplo de l significa que existe $d \in \mathbb{N}$ tal que $A = dl$ o $A = dl + 0$. Es decir, $\mathrm{mod}_l(A) = 0$, lo cual nos da 3).

Para probar 4) usamos el teorema de la división para escribir A_j, para cada $j = 1, \ldots, J$, como $A_j = d_j l + r_j$ donde $d_j, r_j \in \mathbb{N}$ y $0 \leq r_j < l$. O sea,

$$\sum_{j=1}^{J} A_j = \left(\sum_{j=1}^{J} d_j\right) l + \sum_{j=1}^{J} r_j.$$

Además,

$$\sum_{j=1}^{J} r_j = dl + r$$

con $d, r \in \mathbb{N}$ y $0 \leq r < l$. Por lo tanto,

$$\sum_{j=1}^{J} A_j = \left[\left(\sum_{j=1}^{J} d_j \right) + d \right] l + r$$

y

$$\mathrm{mod}_l \left(\sum_{j=1}^{J} A_j \right) = r,$$

mientras que

$$\mathrm{mod}_l \left[\sum_{j=1}^{J} \mathrm{mod}_l \left(A_j \right) \right] = \mathrm{mod}_l \left(\sum_{j=1}^{J} r_j \right) = r,$$

lo cual prueba 4). Observemos que $\sum_{j=1}^{J} r_j < l$ implica $r = \sum_{j=1}^{J} r_j$.

Finalmente, para probar 5) usamos otra vez el teorema de la división para cada $j = 1, \ldots, J$, escribiendo $A_j = d_j l + r_j$ donde $d_j, r_j \in \mathbb{N}$ y $0 \leq r_j < l$. En consecuencia,

$$\prod_{j=1}^{J} A_j = \mathcal{E}\left(l, D, R\right) \cdot l + \prod_{j=1}^{J} r_j$$

donde $\mathcal{E}\left(l, D, R\right)$ es una expresión que depende de l, $D = (d_1, \ldots, d_J)$, y $R = (r_1, \ldots, r_J)$.

O sea,

$$\begin{aligned} \mathrm{mod}_l \left(\prod_{j=1}^{J} A_j \right) &= \mathrm{mod}_l \left\{ \mathrm{mod}_l \left[\mathcal{E}\left(l, D, R\right) \cdot l \right] + \mathrm{mod}_l \left(\prod_{j=1}^{J} r_j \right) \right\} \\ &= \mathrm{mod}_l \left(\prod_{j=1}^{J} r_j \right), \end{aligned}$$

de acuerdo con 3).

Además,

$$\prod_{j=1}^{J} r_j = dl + r$$

con $d, r \in \mathbb{N}$ y $0 \leq r < l$. Es decir

$$\mathrm{mod}_l \left(\prod_{j=1}^{J} r_j \right) = r,$$

en tanto que

$$\mathrm{mod}_l \left[\prod_{j=1}^{J} \mathrm{mod}_l \left(A_j \right) \right] = \mathrm{mod}_l \left[\prod_{j=1}^{J} r_j \right] = r,$$

lo cual prueba 5) y completa la prueba de la proposición □

Es más común el considerar a la función $A \to \mathrm{mod}_l (A)$, introducida en la definición 4.1, como una operación binaria que se indica $A \mathrm{mod} l$.

5. Caracterización de la paridad

Recordemos otra vez que dado $A \in \mathbb{N}$, el teorema de la división nos permite escribir $A = 2d + r$, donde $d, r \in \mathbb{N}$ y $0 \leq r < 2$.

Definición 5.1. Decimos que A es par si es un múltiplo de 2 o, equivalentemente, si $r = 0$. Cuando $r = 1$, decimos que A es impar.

Puesto que $0 = 0 \cdot 2 + 0$, es natural que 0 sea clasificado como par.

Lemma 5.2. *El número A es par si, y solo si,* $\mathrm{mod}_2 (A) = 0$. *Es impar si, y solo si,* $\mathrm{mod}_2 (A) = 1$.

Demostración. Resulta inmediatamente del teorema de la división y la definición de la función mod_2. □

La definición 5.1 y el lema 5.2 describen la paridad de un número natural como una propiedad intrínsica del número, independiente de cualquier representación.

Dados $A, b \in \mathbb{N}^+$ con $b > 1$, en relación a la representación $A \to (a_k, a_{k-1}, \ldots, a_1, a_0)_b$ con $a_k \neq 0$ tenemos el siguiente resultado:

Teorema 5.3. *La paridad de un número natural se puede caracterizar de la siguiente manera:*

1. *Si b es par, A es par (resp. impar) si, y solo si, a_0 es par (resp. impar).*
2. *If b es impar, A es par (resp. impar) si, y solo si, $\sum_{j=0}^{k} a_j$ es par (resp. impar).*

Demostración. Para probar 1) nos basta mostrar que

$$\mathrm{mod}_2 (A) = \mathrm{mod}_2 (a_0) .$$

Puesto que b es par, escribimos $b = 2d$ con $d > 0$. Por lo tanto, usando la proposición 4.2,

$$\begin{aligned}\mathrm{mod}_2(A) &= \mathrm{mod}_2\left(2\sum\nolimits_{-j=1}^{k} a_j 2^{j-1} d^j + a_0\right)\\ &= \mathrm{mod}_2\left[\mathrm{mod}_2\left(2\sum\nolimits_{-j=1}^{k} a_j 2^{j-1} d^j\right) + \mathrm{mod}_2(a_0)\right]\\ &= \mathrm{mod}_2\left[0 + \mathrm{mod}_2(a_0)\right] = \mathrm{mod}_2(a_0),\end{aligned}$$

lo cual prueba 1).

En cuanto a 2), usando otra vez la proposición 4.2,

$$\begin{aligned}\mathrm{mod}_2(A) &= \mathrm{mod}_2\left(\sum_{j=0}^{k} a_j b^j\right) = \mathrm{mod}_2\left[\sum_{j=0}^{k} \mathrm{mod}_2\left(a_j b^j\right)\right]\\ &= \mathrm{mod}_2\left\{\sum_{j=0}^{k} \mathrm{mod}_2\left[\mathrm{mod}_2(a_j)\,\mathrm{mod}_2\left(b^j\right)\right]\right\}\\ &= \mathrm{mod}_2\left\{\mathrm{mod}_2(a_0)\right.\\ &\quad \left. + \sum_{j=1}^{k} \mathrm{mod}_2\left[\mathrm{mod}_2(a_j)\,\mathrm{mod}_2\left(\prod_{j=1}^{k} \mathrm{mod}_2(b)\right)\right]\right\}.\end{aligned}$$

Puesto que b es impar,

$$\mathrm{mod}_2\left(\prod_{j=1}^{k} \mathrm{mod}_2(b)\right) = \mathrm{mod}_2(1) = 1.$$

Por lo tanto

$$\mathrm{mod}_2(A) = \mathrm{mod}_2\left[\mathrm{mod}_2(a_0) + \sum_{j=1}^{k} \mathrm{mod}_2(a_j)\right] = \mathrm{mod}_2\left(\sum_{j=0}^{k} a_j\right),$$

lo cual prueba 2).

Así, la prueba del teorema está completa. □

En vista del teorema 5.3, debería de estar claro por qué nuestro ejemplo introductorio

$$6 \times 9^2 + 5 \times 9^1 + 5 \times 9^0 \to (6, 5, 5)_9$$

es par. La suma de los dígitos, $6 + 5 + 5$, es par.

Para concluir, mencionemos que, aunque hemos caracterizado la paridad de A para cualquier base b, par o impar, las caracterizaciones son bastante diferentes. Cuando b es par, la paridad de A está determinada por un dígito, a_0. Es decir, aún si la representación de A tuviera millones de dígitos, el criterio se reduce a examinar el último dígito. Cuando b es impar, la caracterización, en principio, requiere que se examine la

suma de todos los dígitos, lo cual, si la representación de A tuviera millones de dígitos, necesitaría más que una simple inspección visual. Sin embargo, aún podemos decir un poco más en este caso en que la base es impar. Recordemos que la suma de dos números pares o de dos números impares es par, mientras que la suma de un número par y de uno impar es impar. Entonces, dado un número A, si el número de dígitos impares en base b es par, el número A será par, en tanto que si el número de dígitos impares es impar, A será impar. Este criterio es más sencillo, aunque si el número de dígitos en la representación de A es muy grande, todavía necesita una cierta implementación computacional.

Bibliografía

[1] Brilliant, «The well-ordering principle», http://brilliant.org/wiki/the-well-ordering-principle.

[2] R. Dedekind, *Was sind und was sollendie Zahlen?*, 1888, Traducción al inglés hecha por Wooster Woodruff Beman, publicada in 1901 por The Open Court Publishing Company, Chicago, con el título *Essays on the Theory of Numbers, I: Continuity and Irrational Numbers, II: The Nature and Meaning of Numbers*, https://www.gutenberg.org/files/21016/21016-pdf.pdf.

[3] G. Peano, *Arithmetices principia, nova methodo expositia*, 1889, Traducción al inglés en *From Frege to Gödel: A Source Book in Mathematical Logic, 1879-1931* (Editor: Jean van Heijenoort), Harvard University Press, 1977, reimpreso con correcciones. Primera edición, 1967.

[4] B. Russell, *Introduction to mathematical philosophy*, London: George Allen & Unwin Ltd. / New York: The MacMillan Co. Primera edición mayo 1919. Segunda edición abril 1920, https://people.umass.edu/klement/imp/imp-ebk.pdf.

[5] ———, *Autobiography*, Routledge, London, New York, 1998.