MONOGRAFÍAS MATEMÁTICAS

LA DERIVADA ARITMÉTICA

FERNANDO REVILLA JIMÉNEZ

RESUMEN. Definimos el concepto de derivada aritmética en los números naturales, estudiamos sus propiedades y la relacionamos con las conjeturas de Goldbach, de la infinitud de los primos gemelos y de Sophie Germain. Generalizamos el concepto a los enteros, racionales, a los dominios de factorización única y a sus cuerpos de fracciones. Demostramos que no es posible en general definir una derivada en dominios que no son de factorización única tomando como contraejemplo $\mathbb{Z}[\sqrt{5}i]$.

ÍNDICE

1. Derivada aritmética natural

Definición 1.1. La función *derivada aritmética* es una función $n' : \mathbb{N} \to \mathbb{N}$ definida recursivamente por $p' = 1$ para todo p primo y que satisface $(ab)' = a'b + ab'$ para todo $a, b \in \mathbb{N}$ (regla de Leibniz).

EJEMPLO 1.1. Se verifica $1' = 0$ y $0' = 0$. En efecto, $1' = (1\cdot 1)' = 1'\cdot 1 + 1\cdot 1' = 2 \cdot 1' \Rightarrow 1' = 0$.. Por otra parte, $0' = (2 \cdot 0)' = 2' \cdot 0 + 2 \cdot 0' = 1 \cdot 0 + 2 \cdot 0' = 2 \cdot 0' \Rightarrow 0' = 0$.

Key words and phrases. Derivada aritmética.

EJEMPLO 1.2. Tenemos $6' = (2 \cdot 3)' = 2' \cdot 3 + 2 \cdot 3' = 1 \cdot 3 + 2 \cdot 1 = 5$, y $9'' = (9')' = 6' = 5$.

EJEMPLO 1.3. Fácilmente podemos verificar las derivadas de los primeros 11 números naturales:

n	0	1	2	3	4	5	6	7	8	9	10
n'	0	0	1	1	4	1	5	1	12	6	7

Todavía no hemos demostrado que la derivada aritmética es una función bien definida. A continuación demostramos que existe y es única, dando una fórmula en términos de la factorización de un número en producto de primos.

Teorema 1.1. Si existe la función derivada aritmética, es única.

Demostración. Si existe la derivada aritmética vimos que necesariamente $0' = 1' = 0$ y por definición, $p' = 1$ para todo p primo. Sea $n \geq 2$ y $n = \prod_{i=1}^{m} p_i$ la descomposición de n en factores primos (repetidos o no). Procedamos por inducción sobre m. Para $m = 1$ tenemos $n' = (p_1)' = 1$. Supongamos determinada unívocamente la derivada aritmética para todos los naturales de la forma $\prod_{i=1}^{m} p_i$, Entonces,

$$\left(\prod_{i=1}^{m+1} p_i\right)' = \left(\left(\prod_{i=1}^{m} p_i\right) \cdot p_{m+1}\right)' = \left(\prod_{i=1}^{m} p_i\right)' \cdot p_{m+1} + \left(\prod_{i=1}^{m} p_i\right),$$

y al estar determinado $(\prod_{i=1}^{m} p_i)'$, lo está $\left(\prod_{i=1}^{m+1} p_i\right)'$. □

Teorema 1.2. La función derivada aritmética existe y es $n' = 0$ si $n = 0$ o $n = 1$ y $n' = n \sum_{i=1}^{m} \frac{n_i}{p_i}$ si $n = \prod_{i=1}^{m} p_i^{n_i} \geq 2$ es la factorización de n en producto de factores primos.

Demostración. Es claro que para $n \geq 2$ la fórmula dada es válida incluso si alguno de los exponente n_i es nulo, por tanto si a, b son dos números mayores o iguales que 2 se pueden expresar en la forma $a = \prod_{i=1}^{k} p_i^{\alpha_i}$, $b = \prod_{i=1}^{k} p_i^{\beta_i}$. Entonces,

$$(ab)' = \left(\prod_{i=1}^{k} p_i^{\alpha_i+\beta_i}\right)' = ab \sum_{i=1}^{k} \frac{\alpha_i + \beta_i}{p_i}$$

$$= \left(a \sum_{i=1}^{k} \frac{\alpha_i}{p_i}\right) b + a \left(b \sum_{i=1}^{k} \frac{\beta_i}{p_i}\right) = a'b + ab'.$$

Si alguno de los a, b es 0 o 1, la comprobación de la regla de Leibniz es inmediata. □

EJEMPLO 1.4. Tenemos $120' = \left(2^3 \cdot 3 \cdot 5\right)' = 120\left(\frac{3}{2} + \frac{1}{3} + \frac{1}{5}\right) = 244$.

2. Propiedades de la derivada aritmética natural

El siguiente teorema recuerda la fórmula de la derivación potencial de funciones $\frac{d}{dx}\left(f(x)^k\right) = kf(x)^{k-1}\frac{d}{dx}f(x)$.

Teorema 2.1. Para k, n enteros positivos se verifica $(n^k)' = kn^{k-1}n'$.

Demostración. Para $k = 1$, $(n^1)' = n' = 1n^{1-1}n'$ y la fórmula se verifica. Para $k = 2$, $(n^2)' = (n \cdot n)' = n'n + nn' = 2nn'$, y también se cumple. Si se cumple para k, $\left(n^{k+1}\right)' = \left(n^k n\right)' = \left(n^k\right)' n + n^k n' = kn^{k-1}n'n + n^k n' = (k+1)n^k n'$, y la fórmula es cierta para $k+1$. □

A continuación demostramos la fórmula de Leibniz para la derivada k-ésima del producto de dos números naturales. Usamos el convenio usual $m^{(0)} = m$.

Teorema 2.2. Para todo a, b números naturales se verifica

$$(ab)^{(k)} = \sum_{i=0}^{k} \binom{k}{i} a^{(k-i)} b^{(i)}.$$

Demostración. La fórmula es cierta para $k = 1$, en efecto $(ab)^{(1)} = (ab)' = a'b + ab'$ $\binom{1}{0}a^{(1)}b^{(0)} + \binom{1}{1}a^{(0)}b^{(1)} = \sum_{i=0}^{1}\binom{1}{i}a^{(1-i)}b^{(i)}$. Supongamos que la fórmula es cierta para k. Entonces,

$$(ab)^{(k+1)} = \left(\sum_{i=0}^{k} \binom{k}{i} a^{(k-i)} b^{(i)}\right)' = \sum_{i=0}^{k} \left(\binom{k}{i} a^{(k-i)} b^{(i)}\right)'$$

$$= \sum_{i=0}^{k} \binom{k}{i} \left(a^{(k-i+1)} b^{(i)} + a^{(k-i)} b^{(i+1)}\right)$$

$$= \sum_{i=0}^{k} \binom{k}{i} a^{(k-i+1)} b^{(i)} + \sum_{i=0}^{k} \binom{k}{i} a^{(k-i)} b^{(i+1)}.$$

Haciendo un cambio de índices y usando las conocidas fórmulas combinatorias $\binom{k}{i} + \binom{k}{i-1} = \binom{k+1}{i}$, $\binom{k}{0} = 1 = \binom{k+1}{0}$, $\binom{k}{k} = 1 = \binom{k+1}{k+1}$ podemos escribir

$$(ab)^{(k+1)} = \sum_{i=0}^{k} \binom{k}{i} a^{(k-i+1)} b^{(i)} + \sum_{i=1}^{k+1} \binom{k}{i-1} a^{(k-i+1)} b^{(i)}$$

$$= \binom{k}{0} a^{(k+1)} b^{(0)} + \sum_{i=1}^{k} \binom{k}{i} a^{(k-i+1)} b^{(i)}$$

$$+ \sum_{i=1}^{k} \binom{k}{i-1} a^{(k-i+1)} b^{(i)} + \binom{k}{k} a^{(0)} b^{(k+1)}$$

$$= \binom{k+1}{0} a^{(k+1)} b^{(0)} + \sum_{i=1}^{k} \binom{k+1}{i} a^{(k+1-i)} b^{(i)} + \binom{k+1}{k+1} a^{(0)} b^{(k+1)}$$

$$= \sum_{i=0}^{k+1} \binom{k+1}{i} a^{(k+1-i)} b^{(i)},$$

lo cual implica que la fórmula es cierta para $k+1$. □

EJEMPLO 2.1. La aditividad de la derivada se verifica en algunos casos y en otros no. Por ejemplo, $(1+2)' = 3' = 1 = 0+1 = 1'+2'$, sin embargo $(3+5)' = 8' = 12,\ 3'+5' = 1+1 = 2 \Rightarrow (3+5)' \neq 3'+5'$.

El siguiente teorema permite generar pares de enteros a partir de dos que cumplen la aditividad de la derivada o desigualdades relacionadas con ella.

Teorema 2.3. Se verifica
(1) $(a+b)' = a'+b' \Rightarrow (ka+kb)' = (ka)' + (kb)' \quad \forall k \in \mathbb{N}$.
(2) $(a+b)' \geq a'+b' \Rightarrow (ka+kb)' \geq (ka)' + (kb)' \quad \forall k \in \mathbb{N}$.
(3) $(a+b)' \leq a'+b' \Rightarrow (ka+kb)' \leq (ka)' + (kb)' \quad \forall k \in \mathbb{N}$.

Demostración. Tenemos
(1) $(ka+kb)' = (k(a+b))' = k'(a+b) + k(a+b)' = k'a + k'b + k(a'+b')$
$= (k'a + ka') + (k'b + kb') = (ka)' + (kb)'$.
(2) $(ka+kb)' = (k(a+b))' = k'(a+b) + k(a+b)' \geq k'a + k'b + k(a'+b')$
$= (k'a + ka') + (k'b + kb') = (ka)' + (kb)'$.
(3) Análogo razonamiento. □

Teorema 2.4. Para todo $k > 1$ número natural se verifica $n' \geq n \geq 1 \Rightarrow (kn)' > kn$ para todo $n \geq 1$.

Demostración. Si $k > 1$ entonces $k' \geq 1$ con lo cual $k'n \geq 1$. Entonces, $(kn)' = k'n + kn' > kn' \geq kn$. □

3. Cotas para la derivada aritmética natural

Teorema 3.1. Para todo entero positivo n se verifica $n' \leq \dfrac{n \log_2 n}{2}$ y si $n = 2^k$ la cota es exacta.

Demostración. Si $n = 1$ se verifica la desigualdad trivialmente. Si $n \geq 2$, sea $n = \prod_{i=1}^{k} p_i^{n_i}$ su descomposición en factores primos. Entonces,

$$n \geq \prod_{i=1}^{k} 2^{n_i} \Rightarrow \log_2 n \geq \log_2 \prod_{i=1}^{k} 2^{n_i} = \sum_{i=1}^{k} n_i.$$

$$\Rightarrow n' = n \sum_{i=1}^{k} \frac{n_i}{p_i} \leq n \sum_{i=1}^{k} \frac{n_i}{2} = \frac{n}{2} \sum_{i=1}^{k} n_i \leq \frac{n \log_2 n}{2}.$$

Si $n = 2^k$, $n' = n \cdot \dfrac{k}{2} = \dfrac{n \log_2 2^k}{2} = \dfrac{n \log_2 n}{2}$. □

Teorema 3.2. Si n es el producto de k factores, cada uno de ellos mayor que 1, se verifica $n' \geq kn^{\frac{k-1}{k}}$ y si $n = 2^k$ la cota es exacta.

Demostración. Sea $n = n_1 n_2 n_3 \cdots n_k$ con $n_i \geq 2$ para todo $i = 1, \ldots, k$. Aplicando la regla de Leibniz y que $n_i' \geq 1$ para todo i,

$$\begin{aligned} n' &= n_1' n_2 n_3 \cdots n_k + n_1 n_2' n_3 \cdots n_k + \ldots + n_1 n_2 n_3 \cdots n_k' \\ &\geq n_2 n_3 \cdots n_k + n_1 n_3 \cdots n_k + \ldots + n_1 n_2 n_3 \cdots n_{k-1} \\ &= n\left(\frac{1}{n_1} + \frac{1}{n_2} + \ldots + \frac{1}{n_k}\right). \end{aligned}$$

Usando que la media aritmética es mayor o igual que la geométrica,

$$n' \geq nk\left(\frac{1}{n_1} \cdot \frac{1}{n_2} \cdot \ldots \cdot \frac{1}{n_k}\right)^{1/k} = knn^{-1/k} = kn^{\frac{k-1}{k}}.$$

Si $n = 2^k$, $n' = 2^k \dfrac{k}{2} = k2^{k-1} = k\left(2^k\right)^{\frac{k-1}{k}} = kn^{\frac{k-1}{k}}$. □

Teorema 3.3. Si $n > 1$ no es primo, entonces $n' \geq 2\sqrt{n}$.

Demostración. Si $n > 1$ no es primo, es el producto de $k \geq 2$ factores mayores que 1, por tanto $n' \geq kn^{\frac{k-1}{k}} \geq 2n^{\frac{2-1}{2}} = 2\sqrt{n}$. □

4. Ecuaciones diferenciales aritméticas

Es natural plantear el problema de encontrar todos los números naturales que satisfacen a la ecuación diferencial aritmética

$$a_k n^{(k)} + a_{k-1} n^{(k-1)} + \cdots + a_2 n'' + a_1 n' + a_0 n = b$$

con los a_i y b, números naturales. Vemos ahora algunos ejemplos sencillos.

Teorema 4.1. El único entero positivo que satisface $n' = 0$ es $n = 1$.

Demostración. Sabemos que $1' = 0$ y si $n \geq 2$, entonces n contiene algún factor primo con lo cual $n' > 0$. □

Teorema 4.2. Los únicos números naturales n que verifican $n' = 1$ son los primos.

Demostración. Si n es primo, entonces $n' = 1$ y si $n \geq 2$ no es primo, contiene al menos un par de primos p_1, p_2 en su factorización, es decir $n = p_1 p_2 \ldots$ y $n' = n\left(\frac{1}{p_1} + \frac{1}{p_2} + \ldots\right) > 1$. □

Teorema 4.3. Si $a - 2$ es primo, la ecuación $n' = a$ tiene al menos la solución $n = 2(a-2)$.

Demostración. En efecto, $(2(a-2))' = 2'(a-2) + 2(a-2)' = a - 2 + 2 = a$. □

Teorema 4.4. $n = p^p$ con p primo es solución de la ecuación $n' = n$

Demostración. Tenemos $(p^p)' = pp^{p-1}p' = p^p$¡ □

5. Conjetura de Goldbach

La conjetura de Goldbach, no resuelta a día de hoy se enuncia como *todo número par mayor que dos es la suma de dos primos*. Proporcionamos una condición necesaria para que la conjetura sea cierta en términos de una ecuación diferencial aritmética.

Teorema 5.1. Si la conjetura de Goldbach es cierta, entonces la ecuación diferencial aritmética $n' = 2a$ tiene solución para todo $a \geq 2$.

Demostración. Si la conjetura de Goldbach es cierta, entonces para todo $a \geq 2$ existen primos p_1, p_2 con $2a = p_1 + p_2$. Si $n = p_1 p_2$, tenemos $n' = (p_1 p_2)' = p_1' p_2 + p_1 p_2' = p_2 + p_1 = 2a$, por tanto $n = p_1 p_2$ es solución de $n' = 2a$. □

6. Conjetura de los primos gemelos

La conjetura de los primos gemelos, no resuelta a día de hoy se enuncia como *existen infinitos pares de números gemelos*, es decir infinitos pares $(p, p+2)$ con p y $p+2$ primos. Proporcionamos una condición necesaria para que la conjetura sea cierta en términos de una ecuación diferencial aritmética.

Teorema 6.1. Si la conjetura de la infinitud de los primos gemelos es cierta, entonces la ecuación diferencial aritmética $n'' = 1$ tiene infinitas soluciones.

Demostración. Si la conjetura de los primos gemelos es cierta, entonces existen infinitos pares de primos de la forma $p, p+2$. Si $n = 2p$, tenemos $n' = (2p)' = 2'p + 2p' = p + 2$. Pero al ser $p+2$ primo, $n'' = (p+2)' = 1$. □

7. Conjetura de Sophie Germain

Un número primo p se dice que es un primo de Sophie Germain si $2p+1$ es también primo. Por ejemplo, 2 es primo de Sophie Germain, y 7 no lo es. Se ha conjeturado que existen infinitos primos de Sophie Germain, pero a día de hoy, esta conjetura ni se ha demostrado. Proporcionamos una equivalencia de la conjetura de Sophie Germain en términos de una ecuación diferencial aritmética.

Teorema 7.1. Si p es primo, entonces $(2^4 p)' = 2^4(2p+1)$.

Demostración. Tenemos $(2^4 p)' = (2^4)'p + 2^4 p' = 4 \cdot 2^3 \cdot 2' \cdot p + 2^4 \cdot 1 = 2^4(2p+1)$. □

Teorema 7.2. Para todo entero positivo m se verifica la desigualdad $(2^4 m)'' \geq 2^4(4m+3)$, con igualdad si y sólo si m es un primo de Sophie Germain.

Demostración. Analicemos los casos m primo y no primo. Si m no es primo,

$$\left(2^4 m\right)' = 4 \cdot 2^3 m + 2^4 m' = 2^4(2m + m'),$$

$$\left(2^4 m\right)'' = \left(2^4(2m+m')\right)' = 4 \cdot 2^3(2m+m') + 2^4(2m+m')'$$

$$= 2^4\left(4m + 2m' + (2m + m')'\right) > 2^4(4m + 3).$$

Si m es primo,

$$\left(2^4 m\right)' = 4 \cdot 2^3 m + 2^4 m' = 2^4(2m + m') = 2^4(2m + 1),$$

$$\left(2^4 m\right)'' = \left(2^4(2m + 1)\right)' = 4 \cdot 2^3(2m + 1) + 2^4(2m + 1)'$$

$$= 2^4\left(4m + 2 + (2m + 1)'\right) \geq 2^4(4m + 3),$$

verificándose la igualdad si y sólo si $2m + 1$ es también primo, es decir si y sólo si m es un primo de Sophie Germain. □

Teorema 7.3. La conjetura de Sophie Germain es cierta si y sólo si la ecuación diferencial aritmética $n'' = 4n + 48$ tiene infinitas soluciones de la forma $n = 2^4 p$ con p primo.

Demostración. Si la conjetura de Sophie Germain es cierta, según el apartado anterior existen infinitos primos p tales que $(2^4 p)' = 2^4(4p + 3)$ y llamando $n = 2^4 p$ queda la ecuación $n'' = 4n + 48$. Recíprocamente, si la ecuación $n'' = 4n + 48$ tiene infinitas soluciones de la forma $n = 2^4 p$, entonces $(2^4 p)' = 2^4(4p + 3)$ y según el apartado anterior, p es primo de Sophie Germain. □

8. La ecuación diferencial $n' = n$

Teorema 8.1. Si $n = p^p m$ con p primo y $m > 1$ natural, entonces $n' = p^p(m + m')$ y $\lim_{k\to\infty} n^{(k)} = \infty$.

Demostración. Tenemos $n' = (p^p m)' = (p^p)' m + p^p m' = p^p \cdot \frac{p}{p} \cdot m + p^p m' = p^p(m + m')$. Dado que $(p^p)^{(i)} = p^p$ para todo $i \geq 0$ y usando la fórmula de la derivada k-ésima del producto,

$$(p^p m)^{(k)} = \sum_{i=0}^{k} \binom{k}{i} (p^p)^{(k-i)} m^{(i)} = p^p\left(m + km' + \cdots\right)$$

$$\geq p^p m + k p^p m' \geq p^p m + k = n + k \Rightarrow \lim_{k\to\infty} n^{(k)} = \infty.$$

□

Teorema 8.2. Sea n número natural y p^k la mayor potencia del primo p tal que $p^k \mid n$. Si $0 < k < p$, entonces p^{k-1} es la mayor potencia de p tal que $p^{k-1} \mid n'$ y todas las derivadas n', n'', $\ldots$, $n^{(k)}$ son distintas.

Demostración. Como $p^k \mid n$, podemos escribir $n = p^k m$. Derivando, $n' = kp^{k-1}m + p^k m' = p^{k-1}(km + pm')$, es decir $p^{k-1} \mid n'$. No puede ocurrir $p^k \mid n'$ pues si así fuera,

$$p^k \mid n' \Rightarrow p^k \mid p^{k-1}(km + pm') \Rightarrow p \mid km + pm',$$

lo cual es absurdo pues $k < p$ y m no contiene el factor p. Deducimos además que n'' sólo puede ser divisible por p^{k-2}, etc. Esto asegura que las derivadas n', n'', $\ldots$, $n^{(k)}$ son distintas. □

Teorema 8.3. Si $n = p^{pk}m$ para algún primo p y enteros $k, m > 1$, entonces $n' = p^{pk}(km + m')$.

Demostración. Tenemos $(p^{pk}m)' = pkp^{pk-1}m + p^{pk}m' = p^{pk}(km + m')$. □

Teorema 8.4. Sea $n \geq 2$ entero. Entonces, n está libre de cuadrados $\Leftrightarrow$ $(n, n') = 1$.

Demostración. $\Rightarrow$) Si $(n, n') \neq 1$, existe primo p tal que $p \mid n$ y $p \mid n'$ y según el teorema 8.2, $p^2 \mid n$ (absurdo).
$\Leftarrow$) Si existe primo p tal que $p^2|n$, por el teorema 8.2 $p \mid n'$ con lo cual $(n, n') \neq 1$ (absurdo). □

Teorema 8.5. Todas las soluciones de la ecuación $n' = n$ son $n = 0$ y $n = p^p$ con p primo.

Demostración. Se verifica $0' = 0$ y $(p^p)' = pp^{p-1}p' = p^p$, luego 0 y p^p son soluciones de la ecuación.

Sea $n \neq 0$ y $n' = n$, con lo cual ha de ser $n \geq 2$. Sea p alguno de los factores primos que aparecen en la factorización de n. Entonces, $p \mid n$ y veamos que al menos $p^p \mid n$. En efecto si p^k con $0 < k < p$ fuera la mayor potencia que divide a n, entonces y según el teorema 8.2, p^{k-1} sería la mayor potencia que divide a $n' = n$ lo cual es absurdo.

Pero si $p^p \mid n$ tenemos $n = p^p m$ con $m \geq 1$. Si fuera $m > 1$ y por el teorema 8.1 $n' = p^p\,(m + m') = p^p m$ implica $m' = 0$ y por tanto $m = 1$, lo cual es es una contradicción. Ha de ser pues $m = 1$ con lo cual necesariamente $n = p^p$. □

9. Derivada aritmética entera

Definición 9.1. Se llama función *derivada aritmética* en los enteros $\mathbb{Z}$ a la función $n' : \mathbb{Z} \to \mathbb{Z}$ dada por
(i) $0' = 1' = (-1)' =: 0$.
(ii) Si $n = up_1p_2 \cdots p_k$ con $u = \pm 1$ y los p_i son primos (alguno de ellos puede estar repetido), entonces $n' := u \sum_{i=1}^{k} p_1 \cdots p_{i-1}p_{i+1} \cdots p_k$.

Nótese que si p es primo, entonces $k = 1$ y el producto anterior es vacío, por tanto $p' = 1$.

Teorema 9.1. La definición anterior generaliza la derivada aritmética definida en $\mathbb{N}$.

Demostración. En efecto, para $n = 0$ y $n = 1$ coinciden y para $n \geq 2$ con descomposición $n = \prod_{i=1}^{m} P_i^{n_i} = 1p_1p_2 \cdots p_k$ tenemos

$$n' = n \sum_{i=1}^{m} \frac{n_i}{P_i} = p_1p_2 \cdots p_k \left(\frac{1}{p_1} + \frac{1}{p_2} + \cdots + \frac{1}{p_k} \right)$$

$$= p_2p_3 \cdots p_k + p_1p_3 \cdots p_k + \ldots + p_1p_2 \cdots p_{k-1} = 1 \sum_{i=1}^{k} p_1 \cdots p_{i-1}p_{i+1} \cdots p_k.$$

□

Es inmediato demostrar $(-n)' = -n'$ para todo $n \in \mathbb{Z}$ y que se verifica la regla de Leibniz.

EJEMPLO 9.1. $(-60)' = -(60)' = -\left(2^2 \cdot 3 \cdot 5\right)' = -60\left(\frac{2}{2} + \frac{1}{3} + \frac{1}{5}\right) = -92.$

10. Derivada aritmética racional

La derivada entera se puede extender a $\mathbb{Q}$ usando como símil la conocida regla de la derivada de un cociente de funciones $\left(\frac{u}{v}\right)' = \frac{u'v - v'u}{v^2}$.

Definición 10.1. Se define la función $(a/b)' : \mathbb{Q} \to \mathbb{Q}$, como

$$\left(\frac{a}{b}\right)' := \frac{a'b - b'a}{b^2}.$$

Teorema 10.1. La función $(a/b)'$ es una extensión de la derivada aritmética en $\mathbb{Z}$, cumple la regla de Leibniz y es la única extensión que la cumple.

Demostración. Veamos que $(a/b)'$ está bien definida, es decir que no depende del representante de cada número racional. En efecto, si $0 \neq k \in \mathbb{Z}$,

$$\left(\frac{ka}{kb}\right)' = \frac{(ka)'(kb) - (kb)'(ka)}{(kb)^2} = \frac{(k'a + ka')(kb) - (k'b + kb')(ka)}{(kb)^2}$$
$$= \frac{k^2(a'b - b'a)}{k^2b^2} = \frac{a'b - b'a}{b^2} = \left(\frac{a}{b}\right)'.$$

Es una extensión de la derivada aritmética en los enteros pues

$$\left(\frac{a}{1}\right)' = \frac{a'1 - 1'a}{1^2} = a'.$$

Cumple la regla de Leibniz:

$$\left(\frac{a}{b}\right)'\left(\frac{c}{d}\right) + \left(\frac{a}{b}\right)\left(\frac{c}{d}\right)' = \frac{a'b - b'a}{b^2} \cdot \frac{c}{d} + \frac{a}{b} \cdot \frac{c'd - d'c}{b^2}$$
$$= \frac{(a'c + ac')(bd) - (ac)(b'd + bd')}{b^2d^2} = \frac{(ac)'(bd) - (bd)'(ac)}{(bc)^2}$$
$$= \left(\frac{ac}{bd}\right)' = \left(\frac{a}{b} \cdot \frac{c}{d}\right)'.$$

No existe otra función de $\mathbb{Q}$ en $\mathbb{Q}$ que extienda a la derivada aritmética en $\mathbb{Z}$ y que cumpla la regla de Leibniz. En efecto, tal derivada ha de cumplir $1' = 0$ y se cumplen las equivalencias

$$1' = 0 \Leftrightarrow \left(n \cdot \frac{1}{n}\right)' = 0 \Leftrightarrow n' \cdot \frac{1}{n} + n \cdot \left(\frac{1}{n}\right)' = 0 \Leftrightarrow \left(\frac{1}{n}\right)' = -\frac{n'}{n^2}.$$

Es decir, necesariamente ha de ser $(1/n)' = -n'/n^2$ y de aquí se deduce que

$$\left(\frac{a}{b}\right)' = \left(a \cdot \frac{1}{b}\right)' = a' \cdot \frac{1}{b} + a \cdot \left(\frac{1}{b}\right)' = \frac{a'}{b} + a \cdot \frac{-b'}{b^2} = \frac{a'b - b'a}{b^2}.$$

□

EJEMPLO 10.1. Fácilmente verificamos:

a	1	2	4	5	6	7	9
b	3	3	5	5	7	8	10
$(a/b)'$	$-\frac{1}{9}$	$\frac{1}{9}$	$\frac{16}{25}$	0	$\frac{29}{49}$	$-\frac{19}{16}$	$-\frac{1}{10}$

11. Derivada aritmética en dominios de factorización única

Sea D un dominio de factorización única y elijamos en D los elementos irreducibles que son "positivos", es decir elijamos un conjunto $\mathcal{P}$ de elementos irreducibles tales que cada elemento irreducible de D está asociado a uno y sólo un elemento de $\mathcal{P}$. Llamemos a $\mathcal{P}$ el conjunto de los *átomos positivos* y sea $\mathcal{U}$ el conjunto de las unidades de D.

Definición 11.1. Para todo $a \in D$ (dominio de factorización única), definimos la derivada a' de a como sigue:
(i) Si $a = 0$ o $a \in \mathcal{U}$ entonces $a' = 0$.
(ii) En otro caso, existen $u \in \mathcal{U}$, $p_1, \ldots, p_k \in \mathcal{P}$ (únicos salvo el orden y tal vez alguno repetido) tales que $a = up_1 \cdots p_k$. Entonces

$$a' := u \sum_{i=1}^{k} p_1 \cdots p_{i-1} p_{i+1} \cdots p_k.$$

Si $a = p \in \mathcal{P}$ entonces $k = 1$ y tenemos un producto vacío, con lo cual $a' = 1$. La función a' depende por supuesto de la elección de $\mathcal{P}$, en consecuencia se debería escribir $a'_{\mathcal{P}}$. No obstante y por simplicidad de notación, escribiremos a' cuando el conjunto de átomos positivos se sobreentienda.

Teorema 11.1. La derivada $a'_{\mathcal{P}}$ definida en un dominio de factorización única D, satisface la regla de Leibniz.

Demostración. Denotemos a $a'_{\mathcal{P}}$ simplemente por a'. Tenemos que demostrar que para todo $a, b \in D$ se verifica $(ab)' = a'b + ab'$. Supongamos que tanto a como b no son nulos ni unidades, caso contrario el resultado es evidente. Sean $a = up_1 \cdots p_k$ y $b = vp_{k+1} \cdots p_m$ con u, v unidades y los $p_i \in \mathcal{P}$, entonces

$$\begin{aligned} a'b + ab' &= \left(u \sum_{i=1}^{k} p_1 \cdots p_{i-1} p_{i+1} \cdots p_k \right) (vp_{k+1} \cdots p_m) \\ &\quad + (up_1 \cdots p_k) \left(v \sum_{i=k+1}^{m} p_{k+1} \cdots p_{i-1} p_{i+1} \cdots p_m \right) \\ &= uv \sum_{i=1}^{k} p_1 \cdots p_{i-1} p_{i+1} \cdots p_k p_{k+1} \cdots p_m \\ &\quad + uv \sum_{i=k+1}^{m} p_1 \cdots p_k p_{k+1} \cdots p_{i-1} p_{i+1} \cdots p_m \end{aligned}$$

$$= (uv)\sum_{i=1}^{m} p_1 \cdots p_{i-1}p_{i+1} \cdots p_m = (ab)'.$$

□

EJEMPLO 11.1. En $D = \mathbb{Z}$, se consideran los conjuntos de átomos positivos dados por $\mathcal{P}_1 = \{2, 3, 5, 7, \ldots\}$ y $\mathcal{P}_2 = \{2, -3, 5, -7, \ldots\}$. El conjunto de la unidades es $\mathcal{U} = \{1, -1\}$. Entonces, $(6)'_{\mathcal{P}_1} = (1 \cdot 2 \cdot 3)' = 1(3 + 2) = 5$ y $(6)'_{\mathcal{P}_2} = ((-1) \cdot 2 \cdot (-3))' = (-1)(-3 + 2) = 1$.

Nótese que la derivada en $\mathbb{Z}$ que ya se definió es la que corresponde a $\mathcal{P}_1$.

EJEMPLO 11.2. Si $D = \mathbb{R}[x]$, el conjunto de la unidades es $\mathcal{U} = \mathbb{R} \setminus \{0\}$. Elijamos como conjunto $\mathcal{P}$ de átomos positivos, el conjunto de los polinomios mónicos de primer grado unión el de los mónicos de segundo grado con discriminante menor que 0 y sea $f(x) = -x^4+2x^3-3x^2$. La descomposición de $f(x)$ en producto de irreducibles es $(-1) \cdot x \cdot x \cdot (x^2 - 2x + 3)$ y por tanto $(f(x))'_{\mathcal{P}} = (-1)\left[x \cdot (x^2 - 2x + 3) + x \cdot (x^2 - 2x + 3) + x \cdot x\right] = -2x^3+3x^2-6x$.

Para todo dominio de factorización única D que no es un cuerpo y con la derivada aritmética $a'_{\mathcal{P}}$, se puede definir una derivada aritmética en su cuerpo de fracciones K que es extensión de $a'_{\mathcal{P}}$, de la misma manera que se hizo en $\mathbb{Q}$:

$$\left(\frac{a}{b}\right)'_{\mathcal{P}} = \frac{a'_{\mathcal{P}}b - b'_{\mathcal{P}}a}{b^2},$$

y la demostración es análoga.

EJEMPLO 11.3. En $\mathbb{R}[x]$ con los átomos positivos del problema anterior calculemos $\left(\frac{(x-1)^2}{x^2+1}\right)'$ en el cuerpo de fracciones de $\mathbb{R}[x]$. Tenemos

$$\left((x-1)^2\right)' = x - 1 + x - 1 = 2x - 2, \quad (x^2 + 1)' = 1$$

$$\Rightarrow \left(\frac{(x-1)^2}{x^2+1}\right)' = \frac{(2x-2)(x^2+1) - 1 \cdot (x-1)^2}{(x^2+1)^2} = \frac{2x^3 - 3x^2 + 4x - 3}{(x^2+1)^2}.$$

12. Derivada aritmética y factorización no única. Anillo $\mathbb{Z}[\sqrt{5}i]$

En general no es posible definir una derivada aritmética en dominios que no son de factorización única. Verificamos esto con el anillo $\mathbb{Z}[\sqrt{5}i]$.

Los tres siguientes teoremas prueban que $\mathbb{Z}[\sqrt{5}i]$ no es dominio de factorización única.

Teorema 12.1. $\mathbb{Z}[\sqrt{5}i] = \{a + b\sqrt{5}i : a, b \in \mathbb{Z}\}$ es dominio de integridad con las operaciones habituales suma y producto de complejos.

Demostración. Como $\mathbb{Z}[\sqrt{5}i] \subset \mathbb{C}$ bastará demostrar que $\mathbb{Z}[\sqrt{5}i]$ es subanillo de $\mathbb{C}$. Usamos el conocido teorema de caracterización de subanillos. Claramente, $\mathbb{Z}[\sqrt{5}i] \neq \emptyset$. Para cada par de elementos $a + b\sqrt{5}i$ y $c + d\sqrt{5}i$ de $\mathbb{Z}[\sqrt{5}i]$, $(a + b\sqrt{5}i) - (c + d\sqrt{5}i) = (a - c) + (b - d)\sqrt{5}i \in \mathbb{Z}[\sqrt{5}i]$ y $(a + b\sqrt{5}i)(c + d\sqrt{5}i) = (ac - 5bd) + (ad + bc)\sqrt{5}i \in \mathbb{Z}[\sqrt{5}i]$. Hemos demostrado pues que $\mathbb{Z}[\sqrt{5}i]$ es anillo. Dado que $\mathbb{C}$ es conmutativo, también lo es $\mathbb{Z}[\sqrt{5}i]$. Por otra parte $1 = 1 + 0i \in \mathbb{Z}[\sqrt{5}i]$, luego es unitario. Al ser $(\mathbb{C}, +, \cdot)$ es dominio de integridad, también lo es $\mathbb{Z}[\sqrt{5}i]$ □

Teorema 12.2. El conjunto de las unidades de $\mathbb{Z}[\sqrt{5}i]$ es $\mathcal{U} = \{1, -1\}$.

Demostración. Un elemento $a + b\sqrt{5}i \in \mathbb{Z}[\sqrt{5}i]$ no nulo es unidad si y sólo si existe un $a' + b'\sqrt{5}i \in \mathbb{Z}[\sqrt{5}i]$ no nulo tal que $(a + b\sqrt{5}i)(a' + b'\sqrt{5}i) = 1$. Tomando módulos al cuadrado, obtenemos $(a^2 + 5b^2)(a'^2 + 5b'^2) = 1$. Como los dos factores anteriores son enteros positivos, ha de ser necesariamente $a^2 + 5b^2 = 1$ o equivalentemente $a = \pm 1 \ \wedge \ b = 0$. Es decir, las únicas posibles unidades de $\mathbb{Z}[\sqrt{5}i]$ son $1, -1$. Pero estos elementos son efectivamente unidades al cumplirse $1 \cdot 1 = 1$, $(-1) \cdot (-1) = 1$. Concluimos que $\mathcal{U} = \{1, -1\}$. □

Teorema 12.3. El elemento $6 \in \mathbb{Z}[\sqrt{5}i]$ puede descomponerse en dos formas esencialmente distintas en producto de factores irreducibles.
Nota. Esto prueba que $\mathbb{Z}[\sqrt{5}i]$ no es un dominio de factorización única.

Demostración. Expresemos $6 = (a + b\sqrt{5}i)(c + d\sqrt{5}i)$ como producto de dos factores no nulos. Esto equivale a

$$\begin{cases} ac - 5bd = 6 \\ bc + ad = 0 \end{cases}$$

Resolviendo en las incógnitas c, d obtenemos

$$c = \frac{\begin{vmatrix} 6 & -5b \\ 0 & a \end{vmatrix}}{\begin{vmatrix} a & -5b \\ b & a \end{vmatrix}} = \frac{6a}{a^2 + 5b^2}\ ,\ d = \frac{\begin{vmatrix} a & 6 \\ b & 0 \end{vmatrix}}{\begin{vmatrix} a & -5b \\ b & a \end{vmatrix}} = \frac{-6b}{a^2 + 5b^2}.$$

Dando los valores $a = 1, b = 1$ obtenemos $c = 1, d = -1$ y por tanto

$$6 = (1 + \sqrt{5}i)(1 - \sqrt{5}i). \quad (1)$$

Por otra parte tenemos la factorización

$$6 = 2 \cdot 3 = (2 + 0\sqrt{5}i)(3 + 0\sqrt{5}i). \quad (2)$$

Veamos que los elementos $1 + \sqrt{5}i, 1 - \sqrt{5}i, 2, 3$ son irreducibles. En efecto, si $x + y\sqrt{5}i \in \mathbb{Z}[\sqrt{5}i]$ divide a $1 + \sqrt{5}i$, existe $u + v\sqrt{5}i \in \mathbb{Z}[\sqrt{5}i]$ tal que $1 + \sqrt{5}i = (x + y\sqrt{5}i)(u + v\sqrt{5}i)$. Tomando módulos al cuadrado queda $6 = (x^2 + 5y^2)(u + 5v^2)$ lo cual implica que $x^2 + 5y^2$ ha de dividir a 6. Esto ocurre en los casos $x = \pm 1, y = 0$ o $x = \pm 1, y = \pm 1$ es decir, los posibles divisores de $1 + \sqrt{5}i$ son ± 1, $\pm(1 + \sqrt{5}i)$, $\pm(1 - \sqrt{5}i)$. Los elementos ± 1 y

$\pm(1+\sqrt{5}i)$ claramente dividen a $1+\sqrt{5}i$ pero los primeros son unidades y los segundos sus asociados. Por otra parte, $\pm(1-\sqrt{5}i)$ no dividen a $1+\sqrt{5}i$ pues

$$\frac{1+\sqrt{5}i}{\pm(1-\sqrt{5}i)} = \pm\frac{(1+\sqrt{5}i)(1+\sqrt{5}i)}{(1-\sqrt{5}i)(1+\sqrt{5}i)} = \pm\left(-\frac{2}{3}+\frac{\sqrt{5}}{3}i\right) \notin \mathbb{Z}[\sqrt{5}i].$$

Hemos demostrado que $1+\sqrt{5}i$ es irreducible. De manera análoga podemos demostrar que $1-\sqrt{5}i, 2, 3$ también lo son. Debido a las factorizaciones (1) y (2), concluimos que $\mathbb{Z}[\sqrt{5}i]$ no es dominio de factorización única. □

Teorema 12.4. No se puede construir una derivada aritmética en $\mathbb{Z}[\sqrt{5}i]$.

Demostración. Veamos que para cualquier elección $\mathcal{P}$ de los átomos positivos, no se puede construir una derivada aritmética en $\mathbb{Z}[\sqrt{5}i]$.
Caso 1. Elijamos un conjunto $\mathcal{P}$ de átomos positivos que contiene a los elementos irreducibles $2, 3, 1+\sqrt{5}i, 1-\sqrt{5}i$. Entonces,

$$6 = 2\cdot 3 \Rightarrow 6' = 2+3 = 5,$$
$$6 = (1+\sqrt{5}i)(1-\sqrt{5}i) \Rightarrow 6' = (1+\sqrt{5}i)+(1-\sqrt{5}i) = 2.$$

Caso 2. Si $\mathcal{P}$ contiene a los elementos irreducibles $-2, 3, 1+\sqrt{5}i, 1-\sqrt{5}i$,

$$6 = (-1)\cdot(-2)\cdot 3 \Rightarrow 6' = (-1)\left((-2)+3\right) = -1,$$
$$6 = (1+\sqrt{5}i)(1-\sqrt{5}i) \Rightarrow 6' = (1+\sqrt{5}i)+(1-\sqrt{5}i) = 2.$$

Caso 3. Si $\mathcal{P}$ contiene a los elementos irreducibles $2, -3, 1+\sqrt{5}i, 1-\sqrt{5}i$,

$$6 = (-1)\cdot 2\cdot(-3) \Rightarrow 6' = (-1)\left(2+(-3)\right) = 1,$$
$$6 = (1+\sqrt{5}i)(1-\sqrt{5}i) \Rightarrow 6' = (1+\sqrt{5}i)+(1-\sqrt{5}i) = 2.$$

Caso 4. Si $\mathcal{P}$ contiene a los elementos irreducibles $-2, -3, 1+\sqrt{5}i, 1-\sqrt{5}i$,

$$6 = (-2)\cdot(-3) \Rightarrow 6' = (-2)+(-3) = -5,$$
$$6 = (1+\sqrt{5}i)(1-\sqrt{5}i) \Rightarrow 6' = (1+\sqrt{5}i)+(1-\sqrt{5}i) = 2.$$

Caso 5. Si $\mathcal{P}$ contiene a los elementos irreducibles $-2, -3, 1+\sqrt{5}i, -1+\sqrt{5}i$,

$$6 = 2\cdot 3 \Rightarrow 6' = 2+3 = 5,$$
$$6 = (-1)\cdot(1+\sqrt{5}i)(-1+\sqrt{5}i) \Rightarrow$$
$$6' = (-1)\left((1+\sqrt{5}i)+(-1+\sqrt{5}i)\right) = -2\sqrt{5}i.$$

En todos los casos anteriores la derivada no está bien definida, y de manera análoga podemos verificar los restantes casos. □

Documentación

[1] Ahlander, Bo and Ufnarovski, Victor. *How to differentiate a Number*, Journal of Integer Sequences. Vol. 6 (2003).
[2] Barbeau E. J., *Remark on an arithmetic derivative*, Canad. Math. Bull. 4 (1961), 117– 122.
[3] Kovič Jurij, *The Arithmetic Derivative and Antiderivative*, Journal of Integer Sequences, Vol. 15 (2012), Article 12.3.8

Más material en http://www.fernandorevilla.es

Fernando Revilla Jiménez. Jefe del Departamento de Matemáticas del IES Santa Teresa de Jesús de la Comunidad de Madrid y Profesor de Métodos Matemáticos de la Universidad Alfonso X El Sabio de Villanueva de la Cañada, Madrid (Hasta el curso académico 2008-2009).
E-mail address: frej0002@ficus.pntic.mec.es