

Artículo de conferencia

IX CONGRESO INTERNACIONAL SOBRE ENSEÑANZA DE LAS MATEMÁTICAS
(IX CIEM-IREM PUCP, Huancavelica)

El algoritmo de la división en la enseñanza de la aritmética elemental

The algorithm of division in the teaching of elementary arithmetic

Teodulo Isaias Verástegui Chuquillanqui

Pontificia Universidad Católica del Perú, Perú
ORCID: <https://orcid.org/0000-0002-3194-6793>

tverast@pucp.edu.pe

Información

Recibido: 07/04/2018.

Aceptado: 04/07/2018.

Palabras clave:

Máximo común divisor,
algoritmo de división,
números naturales

Resumen

El algoritmo de la división, como herramienta de trabajo y recurso didáctico hacia el logro de aprendizajes significativos y relevantes en los estudiantes y en el proceso del desarrollo de conocimientos, tiene aplicaciones en la estructuración y enseñanza de la aritmética elemental: La representación polinomial de los números naturales, el cálculo del máximo común divisor de números enteros, la representación decimal de números fraccionarios, etc. Por ello, el docente de matemáticas para los niveles iniciales de la educación básica debe conocer, con amplitud y profundidad, el proceso de su estructuración y de su utilidad o aplicaciones, iniciado en el desarrollo de la división como caso particular de la sustracción y con aplicaciones de actividades heurísticas, orientadas al proceso del redescubrimiento con aplicaciones de conceptos y propiedades previas. Teniendo el conjunto \mathbb{N} , en el contexto de la teoría de conjuntos y con representación de sus elementos por numerales, siguen las operaciones básicas y el planteamiento y solución de ecuaciones en \mathbb{N} con aplicaciones de propiedades, llegando a la división con residuo como formalización de procesos de repartir objetos en cantidades iguales, que conduce a la formulación del Algoritmo de la División y se completa con aplicaciones a los cálculos del mayor divisor común y menor múltiplo común de dos números y a la expresión decimal de una fracción de números en \mathbb{N} , presentando propiedades claves con ilustraciones de casos particulares.

Information

Keywords:

Highest common
divisor, division
algorithm, natural
numbers

Abstract

The algorithm of division, as a work tool and didactic resource towards the achievement of significant and relevant learning in students and in the process of knowledge development, has applications in the structuring and teaching of elementary arithmetic: The polynomial representation of the Natural numbers, the calculation of the greatest common divisor of whole numbers, the decimal representation of fractional numbers, etc. Therefore, the mathematics teacher for the initial levels of basic education must know, with breadth and depth, the process of its structuring and its usefulness or applications, initiated in the development of the division as a particular case of subtraction and with applications of heuristic activities, oriented to the process of rediscovery with applications of previous concepts and properties. Taking the set \mathbb{N} , in the context of the set theory and with representation of its elements by numerals, follow the basic operations and the approach and solution of equations in \mathbb{N} with applications of properties, reaching the division with remainder as formalization of processes of distributing objects in equal quantities, which leads to the formulation of the Division Algorithm and is completed with applications to the calculations of the greatest common divisor and least common multiple of two numbers and the decimal expression of a fraction of numbers in \mathbb{N} , presenting properties keys with illustrations of particular cases.

INTRODUCCIÓN

El proceso heurístico:

El algoritmo de la división, como herramienta de trabajo y como recurso didáctico, tiene aplicaciones diversas en la enseñanza de la aritmética elemental. De este algoritmo resultan la representación polinomial de los números naturales en distintas bases, la división como caso particular de la sustracción, los criterios de divisibilidad, el cálculo del máximo divisor común de números enteros, la representación decimal de números fraccionarios, etc.

Lo anterior motiva que el docente de matemáticas tenga suficiente formación en temas que incluya el estudio del algoritmo de la división y sus diversas aplicaciones, para disponer de un recurso didáctico infalible: Conocer bien lo que tiene que enseñar para el logro de aprendizajes significativos (y relevantes) en sus estudiantes.

En la enseñanza y aprendizaje de la matemática, deben realizarse actividades mentales y prácticas: Resolver problemas, analizar y demostrar teoremas, realizar construcciones geométricas, etc. en forma planificada y adecuada respecto al esfuerzo y al tiempo disponible, usando medios auxiliares o siguiendo el proceso heurístico del pensamiento lógico-matemático.

La heurística o eurística, con la realización de ciertas actividades orientadas al proceso de redescubrimiento, al estudiante le facilita hallar, descubrir, inventar y aplicar conceptos y propiedades, con suficientes informaciones previas, para resolver problemas por analogía o semejanza, por reducción, por generalización, por modelación, por inducción, etc. considerando los procesos o método progresivo-regresivo.

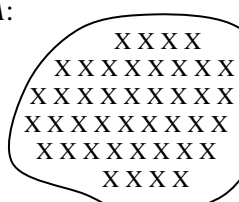
2. Los números naturales y su representación por numerales:

El desarrollo de la matemática en los primeros grados está centrado en el estudio de los números naturales (aritmética) y en el uso de figuras (geometría), adquiriendo destrezas en los cálculos numéricos, comparando y operando con números en formas escrita u oral, realizando mediciones con aproximaciones, indagando formas de solución y verificando resultados. Su punto de partida es el conjunto de los números naturales \mathbb{N} , que se inicia antes de la escuela, continuando con los conjuntos de los números racionales no negativos \mathbb{Q}_0^+ y los números enteros \mathbb{Z} , para completar con los conjuntos de los números reales y complejos, según el desarrollo histórico.

El concepto de número resulta de la cantidad de elementos o cardinal de conjuntos finitos, por la relación de equipotencia, partiendo de conjuntos unitarios y del conjunto vacío, que definen 1 y 0, respectivamente, y se define el sucesor s de un número n es el cardinal de un conjunto que resulta de adicionar un elemento al conjunto que define n y se denota $s(n)$, es una función inyectiva, donde $s(0) = 1, s(1) = 2, s(2) = 3$, etc.

Luego, definidas las operaciones de adición y multiplicación y el orden en \mathbb{N} con sus propiedades básicas, resulta $s(n) = n + 1, n < s(n)$ y $0 \leq n, \forall n \in \mathbb{N}$. Se completa que el conjunto \mathbb{N} es bien ordenado.

Dado un conjunto finito A , ¿qué significa decir que A tiene n elementos o que A define el número que se denota o representa por n o cuyo numeral es n ? o simplemente y si no hay confusión, ¿qué es el número n ?

| | |
|---|---|
| <p>Así, si A es el conjunto del diagrama, ¿cuántos elementos hay?</p> <p>Para esto, agrupando o contando de 10 en 10, resulta 4 grupos de 10 elementos cada uno y quedan 2 elementos sin agrupar; es decir, en base 10 hay $4 \times 10 + 2 = 40 + 2 = 42$ elementos.</p> <p>¿Cómo se representa el cardinal de A agrupando de 5 en 5?</p> | <p>A:</p>  |
|---|---|

En el desarrollo, se consideraron la descomposición polinomial de los números, las propiedades asociativa y conmutativa de la adición, las propiedades distributiva de la multiplicación respecto a la adición y la propiedad de neutralidad de 1 para la multiplicación, entre otras, dentro del proceso de reestructuración del conjunto \mathbb{N} .

3. La división en \mathbb{N} y el algoritmo de la división:

La división como una operación, cuyo resultado depende de la multiplicación, se trata también por la sustracción con el cálculo de diferencias, que responde a la acción de dividir, repartir, agrupar una cantidad de objetos en partes con igual cantidad de elementos, sobrando o no una cantidad de objetos que no es posible repartir entre todas las partes, es decir, hay o no un resto o residuo.

- a) Al repartir 96 juguetes entre un grupo de 12 niños, correspondiendo a cada uno la misma cantidad de juguetes, ¿cuántos juguetes recibirá cada niño?

Se trata de dividir o repartir 96 entre 12, y se obtiene el cociente denotado por q y cumple $12 \times q = 96$. De la multiplicación se sabe que $12 \times 8 = 96$ y se tiene $96 \div 12 = 8$ o $\frac{96}{12} = 8$, que responde a la acción de entregar a cada niño $q = 8$ juguetes.

Otra forma de repartir, más empírica y natural, es entregar a cada uno un juguete, quedando $96 - 12 = 84$ para repetir el proceso, quedando $84 - 12 = 72$ para otra vuelta, y se continúa: $72 - 12 = 60$, $60 - 12 = 48$, $48 - 12 = 36$, $36 - 12 = 24$, $24 - 12 = 12$ y $12 - 12 = 0$ y nada sobra. De esto, en 8 vueltas o en 8 diferencias se termina la repartición, por lo que a cada niño le corresponde 8 juguetes: $96 \div 12 = 8$.

- b) ¿Cómo expresar 60 días calendarios en semanas?

Una semana tiene 7 días y, de los 60 días, al considerar la semana 1 quedan $60 - 7 = 53$ días, considerada la semana 2 quedan $53 - 7 = 46$ días, continuando las diferencias $46 - 7 = 39$, $39 - 7 = 32$, $32 - 7 = 25$, $25 - 7 = 18$, $18 - 7 = 11$, $11 - 7 = 4$ y $4 - 7$ no existe en \mathbb{N} . De esto, la cantidad de diferencias efectuadas indican la cantidad de semanas que hay en 60 días. En este caso son 8 semanas y, como la última diferencia es 4, sobran 4 días; es decir, en 60 días hay 8 semanas y 4 días.

Propiedad 1: El *Algoritmo de la división* en \mathbb{N} , establece que:

Para a y b en \mathbb{N} , con $b \neq 0$, existen únicos números q y r en \mathbb{N} tales que $a = b \times q + r$, donde $0 \leq r < b$; que también se expresa $\frac{a}{b} = q + \frac{r}{b}$, donde $0 \leq r < b$; y se dice que “ q es el cociente y r es el residuo de dividir a entre b ”.

Cuando $r = 0$, es decir, $a = b \times q$ o $\frac{a}{b} = q$, se dice que la división es exacta.

Para esto, como $b \neq 0$, se tiene $b \geq 1$; y, si $0 \leq a < b$ entonces $a = b \times 0 + a$, $q = 0$ y $r = a$.

Si $b \leq a$, existe $t \geq 1$ en \mathbb{N} tal que $b \times t \leq a$ y $t \leq a$; pues, si $t = 1$ se tiene $b \times 1 = b \leq a$, y si para algún t es $t > a$ se tiene $a \geq b \times t > a \times b$ y $a \times b \geq a \times 1 = a$, es decir, $a > a$, lo cual es falsa o contradictoria como resultado de asumir que $t > a$. Por otro lado, como entre 0 y a hay un número finito de estos t , sea q el mayor de tales t , esto es $b \times q \leq a$, y sea $r = a - b \times q$. Entonces $a = b \times q + r$, con $0 \leq r$ y $r < b$; pues, si $r \geq b$ o $a - b \times q \geq b$, resulta $a \geq b \times (q + 1)$, contrario a que q es el elemento mayor que cumple $a \geq b \times q$, siendo $q + 1 > q$ y $a \geq b \times (q + 1)$. Luego, $a = b \times q + r$, con $0 \leq r < b$.

Aplicando la propiedad, para a en \mathbb{N} y $b = 2$, se tiene: $a = 2 \times q + r$, con $0 \leq r < 2$; es decir, $r = 0$ y $a = 2 \times q$ o $r = 1$ y $a = 2 \times q + 1$, llamándose a un **número par** o a un **número impar**, respectivamente, que permite definir una partición de \mathbb{N} en dos partes: Conjunto de los números pares y conjunto de los números impares de \mathbb{N} .

4. Múltiplo y divisor

Dados los números a y b en \mathbb{N} , con $b \neq 0$, se tienen las expresiones equivalentes:

“ b es un **divisor** de a ”, “ b **divide** a ”, “ b es un **submúltiplo** de a ”, “ b es un **factor** de a ”, “ a es un **múltiplo** de b ” o “ a es **divisible** por b ”, significan:

Existe un número q en \mathbb{N} tal que cumple $a = b \times q$; es decir, al dividir a entre b , el resultado es el cociente q , y se denota: $a \div b = q$ o $\frac{a}{b} = q$.

De lo anterior:

- a) Para a, b y q en \mathbb{N} , $a \div b = q \Leftrightarrow a = b \times q$; en donde, si $q \neq 0$, también q es un divisor de a o a es un múltiplo de q ; esto es, $a \div b = q \Leftrightarrow a \div q = b \Leftrightarrow a = b \times q$.
- b) De las propiedades de 1 para la multiplicación y de 0 para la adición:
- Para todo b en \mathbb{N} , se cumple $b \times 1 = 1 \times b = b$; de donde 1 es divisor de b o b es múltiplo de 1, y para $b \neq 0$, b es divisor de b o b es múltiplo de b .
 - Para todo b en \mathbb{N} , se cumple $b \times 0 = 0 \times b = 0$; de donde, para $b \neq 0$, b es divisor de 0 o 0 es múltiplo de b .
- c) En \mathbb{N} , si $b \neq 0$ es un divisor de a , existe q tal que $a = b \times q$, y para $c \neq 0$, se cumple $a \times c = (b \times q) \times c = b \times (q \times c) = (b \times c) \times q$; es decir, $b \times c$ es un divisor de $a \times c$.

Lo anterior, en términos de división, se expresa: Si $\frac{a}{b} = q$, entonces $\frac{a \times c}{b \times c} = q$, esto es, para $c \neq 0$, se cumple $\frac{a}{b} = \frac{a \times c}{b \times c}$ o, equivalentemente, $\frac{a \times c}{b} = q \times c$. ¿Cómo se leen?.

- d) En el contexto de las relaciones binarias en \mathbb{N} , las relaciones “ser múltiplo” y “ser divisor”, son relaciones binarias inversas:

a es múltiplo de $b \Leftrightarrow b$ es un factor de a , o

a es divisible por $b \Leftrightarrow b$ es un divisor de a .

Además, dichas relaciones definen una **relación de orden** en \mathbb{N} , pues son:

- Reflexivas: $\forall b$ en \mathbb{N} , b es múltiplo de b o b es divisor de b , para $b \neq 0$.
 - Anti simétricas: Para a y b en \mathbb{N} , si a es múltiplo de b y b es múltiplo de a , entonces $a = b$.
 - Transitivas: Para a, b y c en \mathbb{N} , si a es múltiplo de b y b es múltiplo de c , entonces a es múltiplo de c .
- e) Para a y b en $\mathbb{N} - \{0\}$, si “ b es un divisor de a ”, entonces se cumple $0 < b \leq a$.

Para esto: b es un divisor de $a \Leftrightarrow$ Existe q en \mathbb{N} tal que $a = b \times q$; y como $a \neq 0$, también $q \neq 0$ y $q \geq 1$. Luego, $b \times q \geq b \times 1 = b$, de donde $a \geq b$ o $b \leq a$.

En resumen:

- Todo número $a \neq 0$ en \mathbb{N} , tiene como divisores a 1 o al mismo número a .
- Los divisores de a forman el “conjunto de los divisores de a ”, que se denota $D(a)$ y se tiene $D(a) = \{b / b \in \mathbb{N}, b \neq 0, b \text{ es divisor de } a \text{ y } 0 < b \leq a\} \neq \emptyset$, no vacío. Además, $1 \in D(a)$ y $a \in D(a)$.
- $D(a) \subset \{1, 2, 3, \dots, a-1, a\}$ y es un conjunto finito; es decir, a tiene un número finito de divisores.
- Todo número $a \neq 0$ en \mathbb{N} , tiene como múltiplos a 0 y al mismo número a .
- Los múltiplos de a forman el “conjunto de los múltiplos de a ”, se denota por $M(a)$ y se tiene $M(a) = \{ac / c \in \mathbb{N}\} \neq \emptyset$ y es un conjunto infinito; es decir, $a \neq 0$ tiene infinitud de múltiplos. Además, $0 \in M(a)$ y $a \in M(a)$.
- En particular, para $a > 1$, si $D(a) = \{1, a\}$, se dice que a es un **número primo**; y, en otro caso, se dice que a es un **número compuesto**.

5. Máximo común divisor y mínimo común múltiplo:

Para a y b en $\mathbb{N} - \{0\}$, ¿Qué es el MCD de a y b ? y ¿Qué es el MCM de a y b ?

- Sean $D(a)$ y $D(b)$ los conjuntos divisores de a y de b , que son conjuntos finitos.

Se tiene $D(a) \cap D(b) = D(a, b)$, el conjunto de divisores comunes de a y b , es un conjunto finito, pues $D(a, b) \subset D(a)$, y $D(a, b) \subset D(b)$.

Luego, sea d el mayor o máximo de los elementos de $D(a, b)$, llamado el **Máximo Común Divisor** de a y b ; y se denota $d = \text{MCD}(a, b)$.

- Sean $M(a)$ y $M(b)$ los conjuntos múltiplos de a y de b , que son conjuntos infinitos.

Se tiene $M(a) \cap M(b) = M(a, b)$, el conjunto de los múltiplos comunes de a y b , es un conjunto infinito.

Luego, sea $m \neq 0$ el menor de los elementos de $M(a, b)$, llamado el MCM de a y b ; y se denota $m = \text{MCM}(a, b)$.

Por ejemplo: Para 6 y 8, $D(6) = \{1, 2, 3, 6\}$, $D(8) = \{1, 2, 4, 8\}$ y $D(8, 6) = \{1, 2\}$, de donde $\text{MCD}(8, 6) = 2$.

También, $M(6) = \{0, 6, 12, 18, 24, 30, 36, 42, 48, 54, 60, 66, 72, 78, \dots\}$,

$M(8) = \{0, 8, 16, 24, 32, 40, 48, 56, 64, 72, 80, \dots\}$ y

$M(8, 6) = \{0, 24, 48, 72, \dots\}$, de donde $\text{MCM}(6, 8) = 24$.

En el contexto anterior, si $\text{MCD}(a, b) = 1$, se dice que a y b son **primos relativos** o son **primos entre sí**.

6. Aplicaciones del algoritmo de la división:

6.1. Escritura de números naturales en base $b > 1$.

Cuando un conjunto A tiene 39 elementos, donde $39 = 30 + 9 = 3 \times 10 + 9$ en el sistema decimal, significa que al agrupar dichos elementos de 10 en 10, hay 3 subconjuntos de 10 elementos cada uno y quedan 9 elementos; es decir, hay 3 decenas y 9 unidades.

¿Cómo se representa la cantidad de elementos de A , si la agrupación se hace de 5 en 5 o de 2 en 2 o de 16 en 16?; es decir, ¿en sistemas de numeración de bases 5, 2 y 16?

En general, para la base $b > 1$, a cada elemento de un conjunto A se llama **unidad simple**, a un grupo de b elementos o unidades simples se llama **unidad de primer orden**, a un grupo de b unidades de primer orden se llama **unidad de segundo orden**, a un grupo de b unidades de segundo orden se llama **unidad de tercer orden** etc.

Según esto, en A con 39 elementos en base 10, para $b = 5$, se forman 7 unidades de primer orden, y quedan 4 unidades simples; luego, con las unidades de primer orden se forman una unidad de segundo orden y quedan 2 unidades de primer orden: La cantidad de elementos de A es 124, en base 5.

Para la base 2, los elementos de A agrupando de 2 en 2, finalmente se tiene: 100111. ¿Qué propiedad sustenta estos procesos?.

Propiedad 2: Para a y b en \mathbb{N} , con $b > 1$, existen únicos $a_0, a_1, a_2, \dots, a_{n-1}, a_n$ en \mathbb{N} , tales que $0 \leq a_i < b, \forall i = 1, 2, \dots, n, a_n > 0$ y $a = a_n b^n + a_{n-1} b^{n-1} + \dots + a_2 b^2 + a_1 b^1 + a_0 b^0 = a_n b^n + a_{n-1} b^{n-1} + \dots + a_2 b^2 + a_1 b + a_0$, es la **representación polinomial** de a en la base b , y se escribe $a = a_n a_{n-1} \dots a_2 a_1 a_0$, donde a_0 es la cifra de unidad simple, a_1 es la cifra de unidad de primer orden, a_2 es la cifra de unidad de segundo orden, \dots, a_n es la cifra de unidad de orden n , en la base b .

En efecto; Para a y b en \mathbb{N} , con $b > 1$, por el algoritmo de la división, existen únicos q_0 y a_0 en \mathbb{N} , que cumple $a = q_0 b + a_0$, con $0 \leq a_0 < b$.

Como $q_0 \in \mathbb{N}$, si $q_0 = 0$ se tiene $a = a_0$; si $q_0 \neq 0$ o sea $q_0 > 0$, para q_0 y b , por el algoritmo de la división, existen únicos q_1 y a_1 en \mathbb{N} , que cumplen $q_0 = q_1b + a_1$, con $0 \leq a_0 < b$, $0 \leq q_1 < q_0$ y $a = (q_1b + a_1)b + a_0 = q_1b^2 + a_1b + a_0$.

Si $q_1 = 0$ se tiene $q_0 = a_1$ y $a = a_1b + a_0 = a_1a_0$; en otro caso, $q_1 \neq 0$ o sea $q_1 > 0$, para q_1 y b , por algoritmo de la división, existen q_2 y a_2 en \mathbb{N} , tal que $q_1 = q_2b + a_2$, con $0 \leq a_2 < b$, $0 \leq q_2 < q_1 < q_0$ y $a = (q_2b + a_2)b^2 + a_0 = q_2b^3 + a_2b^2 + a_1b + a_0$.

Si $q_2 = 0$ se tiene $q_1 = a_1$ y $a = a_2b^2 + a_1b + a_0 = a_2a_1a_0$; y si $q_2 \neq 0$ o sea $q_2 > 0$, para q_2 y b , por algoritmo de la división, existen q_3 y a_3 en \mathbb{N} , tales que $q_2 = q_3b + a_3$, con $0 \leq a_3 < b$, $0 \leq q_3 < q_2 < q_1 < q_0$ y $a = (q_3b + a_3)b^3 + a_2b^2 + a_1b + a_0$

$$= q_3b^4 + a_3b^3 + a_2b^2 + a_1b + a_0.$$

Continuando el proceso, si $q_{n-1} \neq 0$ o sea $q_{n-1} > 0$, para q_{n-1} y b , por algoritmo de la división, existen únicos q_n y a_n en \mathbb{N} , tales que $q_{n-1} = q_nb + a_n$, con $0 \leq a_n < b$, $0 \leq q_n < q_{n-1} < \dots < q_2 < q_1 < q_0$ y $a = q_{n-1}b^n + a_{n-1}b^{n-1} + \dots + a_2b^2 + a_1b + a_0$.

Entre 0 y q_0 hay un número finito de elementos q_i y resulta que $q_n = 0$, $q_{n-1} = a_{n-1}$ y $a = a_nb^n + a_{n-1}b^{n-1} + \dots + a_2b^2 + a_1b + a_0 = a_na_{n-1}\dots a_2a_1a_0$.

Así, para $a = 39$, en base 10, se tiene $a = 39 = 3 \times 10^1 + 9$; en base 5, se tiene $a = 124 = 1 \times 5^2 + 2 \times 5^1 + 4 = 1 \times 5^2 + 2 \times 5 + 4$; en base 2, $a = 100111 = 1 \times 2^5 + 0 \times 2^4 + 0 \times 2^3 + 1 \times 2^2 + 1 \times 2^1 + 1$; y en bases 16, $a = 27 = 2 \times 16 + 7$, etc.

6.2. Cálculo del MCD y MCM de dos números:

Sean a y b dos números en \mathbb{N} , con $0 < b < a$. Se trata de hallar el $\text{MCD}(a, b)$ usando el algoritmo de la división en \mathbb{N} :

1) Para $0 < b < a$ en \mathbb{N} , por el algoritmo de la división, existen únicos números q y r en \mathbb{N} tal que $a = b \times q + r$, con $0 \leq r < b$.

Si $r = 0$, entonces $a = b \times q$; es decir, b es un divisor de a . Luego, si d es un divisor de b , también d es un divisor de a (propiedad transitiva de la relación “.. es divisor de”). De esto, $D(b) \subset D(a)$, $D(b) \cap D(a) = D(b)$ y el mayor elemento en $D(b)$ es b . Por tanto, $\text{MCD}(a, b) = b$.

Si $0 < r < b$, aplicando el algoritmo de la división a b y r , existen únicos q_1 y r_1 en \mathbb{N} tal que $b = r \times q_1 + r_1$, con $0 \leq r_1 < r$.

Propiedad 3: El conjunto de divisores comunes de b y r es igual al conjunto de divisores comunes de a y b ; es decir, $D(b, r) = D(a, b)$.

En efecto, si $d \in D(b, r)$, entonces existen t y r en \mathbb{N} tales que $b = d \times t$ y $r = d \times s$. Como $a = b \times q + r$ se tiene $a = (d \times t) \times q + (d \times s) = d \times (t \times q + s) = d \times h$, para $h = t \times q + s$ en \mathbb{N} ; es decir, d es un divisor de a y $d \in D(a, b)$.

Luego, $D(b, r) \subset D(a, b)$.

Recíprocamente, si $d \in D(a, b)$, existen u y v en \mathbb{N} tales que $a = d \times u$ y $b = d \times v$. Como $a = b \times q + r$ se tiene $d \times u = (d \times v) \times q + r$; de donde $r = d \times u - (d \times v) \times q = d \times (u - v \times q) = d \times k$, para $k = u - v \times q$ en \mathbb{N} ; es decir, d es un divisor de r y $d \in D(b, r)$. Luego, $D(a, b) \subset D(b, r)$.

Por tanto, $D(b, r) = D(a, b)$; y resulta: $\text{MCD}(b, r) = \text{MCD}(a, b)$.

2) En la expresión $b = r \times q_1 + r_1$, con $0 \leq r_1 < r < b$;

Si $r_1 = 0$, entonces $b = r \times q_1$, r es un divisor de b y $D(b, r) = D(r)$. Por lo tanto, se tiene $\text{MCD}(b, r) = \text{MCD}(a, b) = r$.

Si $0 < r_1 < r < b$, aplicando el algoritmo de la división a r y r_1 , existen q_2 y r_2 en \mathbb{N} tal que $r = r_1 \times q_2 + r_2$, con $0 \leq r_2 < r_1 < r < b$. Luego, $D(r, r_1) = D(a, b)$, por la propiedad dada, y $\text{MCD}(r, r_1) = \text{MCD}(a, b)$.

Si $r_2 = 0$, entonces $r = r_1 \times q_2$; es decir, r_1 es un divisor de r , $D(r, r_1) = D(r_1)$ y, se tiene $\text{MCD}(r, r_1) = \text{MCD}(b, r) = \text{MCD}(a, b) = r_1$.

Si $0 < r_2 < r_1 < r < b$, aplicando el algoritmo de la división a r_1 y r_2 , existen q_3 y r_3 en \mathbb{N} tal que $r_1 = r_2 \times q_3 + r_3$, con $0 \leq r_3 < r_2 < r_1 < r < b$. Luego, $D(r_1, r_2) = D(a, b)$, por la propiedad dada, y $\text{MCD}(r_1, r_2) = \text{MCD}(a, b)$.

Si $r_3 = 0$, entonces $r_1 = r_2 \times q_3$; es decir, r_2 es un divisor de r_1 , $D(r_1, r_2) = D(r_2)$ y, se tiene $\text{MCD}(r_1, r_2) = \text{MCD}(r, r_1) = \text{MCD}(b, r) = \text{MCD}(a, b) = r_2$.

Si $0 < r_3 < r_2 < r_1 < r < b$, se aplica el algoritmo de la división a r_2 y r_3 .

Continuando los procesos anteriores:

Se tiene r_{n-2} en \mathbb{N} tal que $0 < r_{n-2} < \dots < r_2 < r_1 < r < b$; y del algoritmo de la división para r_{n-3} y r_{n-2} , existen q_{n-1} y r_{n-1} en \mathbb{N} tal que $r_{n-3} = r_{n-2} \times q_{n-1} + r_{n-1}$, con $0 < r_{n-1} < r_{n-2} < \dots < r_2 < r_1 < r < b$. Luego, $D(r_{n-3}, r_{n-2}) = D(a, b)$.

Si $r_{n-1} = 0$, entonces $r_{n-3} = r_{n-2} \times q_{n-1}$; es decir, r_{n-2} es un divisor de r_{n-3} , $D(r_{n-2}, r_{n-3}) = D(r_{n-2})$ y $\text{MCD}(r_{n-2}, r_{n-3}) = \text{MCD}(b, r) = \text{MCD}(a, b) = r_{n-2}$.

Si $0 < r_{n-1} < r_{n-2} < \dots < r_2 < r_1 < r < b$, del algoritmo de la división para r_{n-2} y r_{n-1} , existen q_n y r_n en \mathbb{N} tal que $r_{n-2} = r_{n-1} \times q_n + r_n$, con $0 < r_n < r_{n-1} < \dots < r_2 < r_1 < r < b$. Luego, $D(r_{n-2}, r_{n-1}) = D(a, b)$.

Como entre 0 y b hay una cantidad finita de números c en \mathbb{N} tal que $0 < c < b$, los procesos anteriores termina al aplicar el algoritmo de la división a r_{n-1} y r_n , por el cual existen q_{n+1} y r_{n+1} en \mathbb{N} tal que $r_{n-1} = r_n \times q_{n+1} + r_{n+1}$, con $0 = r_{n+1} < r_n < r_{n-1} < \dots < r_2 < r_1 < r < b$; de donde $r_{n-1} = r_n \times q_{n+1} + r_{n+1}$ y r_n es un divisor de r_{n-1} . Luego, $D(r_{n-1}, r_n) = D(r_n)$ y $\text{MCD}(r_{n-1}, r_n) = r_n$.

$$\begin{aligned} \text{Por tanto, } \text{MCD}(r_{n-1}, r_n) &= \text{MCD}(r_{n-2}, r_{n-1}) = \dots = \text{MCD}(b, r) \\ &= \text{MCD}(a, b) = r_n. \end{aligned}$$

En los procesos realizados, de $r_{n-2} = r_{n-1} \times q_n + r_n$ y se tiene $r_n = r_{n-2} - r_{n-1} \times q_n$; y en el paso anterior se tiene $r_{n-3} = r_{n-2} \times q_{n-1} + r_{n-1}$ o $r_{n-1} = r_{n-3} - r_{n-2} \times q_{n-1}$, que al remplazar en r_n se tiene

$$\begin{aligned} r_n &= r_{n-2} - (r_{n-3} - r_{n-2} \times q_{n-1}) \times q_n \\ &= r_{n-2} \times (1 + q_{n-1} \times q_n) - r_{n-3} \times q_n. \end{aligned}$$

En otro paso anterior, $r_{n-4} = r_{n-3} \times q_{n-2} + r_{n-2}$ o $r_{n-2} = r_{n-4} - r_{n-3} \times q_{n-2}$, que al remplazar en r_n , resulta $r_n = (r_{n-4} - r_{n-3} \times q_{n-2}) \times (1 + q_{n-1} \times q_n) - r_{n-3} \times q_n$

$$= (1 + q_{n-1} \times q_n) \times r_{n-4} - (q_{n-2} + q_{n-2} \times q_{n-1} \times q_n + q_n) \times r_{n-3}.$$

Llegando a los primeros pasos, se tienen $b = r \times q_1 + r_1$ o $r_1 = r \times q_1 - b$ y $a = b \times q + r$ o $r = b \times q - a$, que al remplazarlos en r_n , resulta: $r_n = p \times a - q \times b$, para p y q en \mathbb{N} . Pero $r_n = \text{MCD}(a, b)$ y denotando por $d = \text{MCD}(a, b)$, se tiene $d = p \times a - q \times b$, para p y q en \mathbb{N} .

Para hallar el $\text{MCM}(a, b)$, conociendo o hallando el $\text{MCD}(a, b)$, se tiene la siguiente:

Propiedad 4: Para $a \neq 0$ y $b \neq 0$ en \mathbb{N} , $\text{MCD}(a, b) \times \text{MCM}(a, b) = a \times b$.

En efecto, sean $d = \text{MCD}(a, b)$ y $m = \text{MCM}(a, b)$, entonces d es un divisor de a , de b y de $a \times b$, y se tienen $a = d \times k$, $b = d \times h$ y $a \times b = (d \times k) \times (d \times h) = d \times (k \times d \times h)$, para k y h en \mathbb{N} ; de esto $k \times d \times h = (k \times d) \times h = a \times h$ y $k \times d \times h = k \times (d \times h) = k \times b$, es decir, $k \times d \times h$ es múltiplo común de a y de b . Siendo m el menor múltiplo común de a y de b , se tiene $k \times d \times h$ es múltiplo de m o $k \times d \times h = t \times m$, para t en \mathbb{N} , y $a \times b = d \times (k \times d \times h) = d \times (t \times m) = (d \times m) \times t$. De esto, $d \times m$ es un divisor de $a \times b$.

Por otro lado, siendo $d = \text{MCD}(a, b)$, se tiene $d = p \times a - q \times b$, para p y q en \mathbb{N} , y $m = \text{MCM}(a, b)$, se tiene $m = a \times u = b \times v$, para u y v en \mathbb{N} .

$$\begin{aligned} \text{Luego, se tiene } d \times m &= (p \times a - q \times b) \times m = p \times a \times m - q \times b \times m = p \times a \times (b \times v) - q \times b \times (a \times u) = (a \times b) \times (p \times v) - \\ &= (a \times b) \times (q \times u) = (a \times b) \times (p \times v - q \times u). \end{aligned}$$

De lo anterior, $a \times b$ es un divisor de $d \times m$.

Por lo tanto, por la propiedad anti simétrica de la relación "... es divisor de ...", se tiene

$$a \times b = d \times m = \text{MCD}(a, b) \times \text{MCM}(a, b).$$

De esta propiedad, conocidos o calculados $\text{MCD}(a, b)$ y $a \times b$, se halla $\text{MCM}(a, b)$.

Además, si b es un divisor de a , entonces $\text{MCD}(a, b) = b$ y $\text{MCM}(a, b) = a$.

Por ejemplo, hallar: **i)** $\text{MCD}(24, 18)$ y **ii)** $\text{MCD}(825, 315)$.

i) Para $T = \text{MCD}(24, 18)$, se tiene: $24 = 18 \times 1 + 6$ y $18 = 6 \times 3 + 0$. Luego, $T = 6$ y $T = 6 = 1 \times 24 - 1 \times 18$.

ii) Para $U = \text{MCD}(825, 315)$, se tiene $825 = 315 \times 2 + 195$, $315 = 195 \times 1 + 120$, $195 = 120 \times 1 + 75$, $120 = 75 \times 1 + 45$, $120 = 45 \times 2 + 30$, $45 = 30 \times 1 + 15$ y $30 = 15 \times 2 + 0$. Luego, $U = 15$.

Además, hallar p y q en \mathbb{N} tal que $U = 15 = p \times 825 - q \times 315$.

6.3. Expresión decimal de un número fraccionario:

En las fracciones o números racionales, hay que diferenciar las fracciones decimales, cuyos denominadores son 10 o potencias de 10, tales como $\frac{3}{10}$, $\frac{27}{100}$, $\frac{56}{1000}$, etc, que se representan por expresiones decimales 0,3, 0,27, 0,056, etc. y se leen “3 décimos”, “27 centésimos”, “56 milésimos”, etc.

Dada una fracción o número racional $\frac{a}{b}$, con a y b en \mathbb{N} y $b > 0$, por el algoritmo de la división, existen q y r en \mathbb{N} tal que $\frac{a}{b} = q + \frac{r}{b}$, con $0 \leq r < b$. Si $r = 0$, $\frac{a}{b} = q \in \mathbb{N}$; y si $0 < r < b$, entonces $0 < \frac{r}{b} < 1$ y $\frac{r}{b} = \frac{1}{10} \times \frac{10 \times r}{b}$, donde $0 < \frac{10 \times r}{b} < 10$ y, del algoritmo de la división aplicado a $\frac{10 \times r}{b}$ se tiene $\frac{10 \times r}{b} = q_1 + \frac{10 \times r_1}{b}$, con $0 \leq r_1 < b$ y $0 \leq q_1 < 10$.

Luego, $\frac{a}{b} = q + \frac{r}{b} = q + \frac{1}{10} \times \frac{10 \times r}{b} = q + \frac{1}{10} (q_1 + \frac{r_1}{b}) = q + \frac{q_1}{10} + \frac{1}{10} \times (\frac{r_1}{b})$, donde, si $r_1 = 0$, $\frac{a}{b} = q + \frac{r}{b} = q + \frac{q_1}{10} = q + 0$, $q_1 = q$, q_1 es la expresión decimal de $\frac{a}{b}$ y se lee “ q enteros y q_1 décimos” o q es la parte entera y q_1 es la parte decimal o cifra de las décimas de $\frac{a}{b}$.

Si $0 < r_1 < b$, por el algoritmo de la división, $\frac{10 \times r_1}{b} = q_2 + \frac{r_2}{b}$, con $0 \leq r_2 < b$, $0 \leq q_2 < 10$ y $\frac{a}{b} = q + \frac{q_1}{10} + \frac{1}{100} \times (q_2 + \frac{r_2}{b}) = q + \frac{q_1}{10} + \frac{q_2}{100} + \frac{1}{100} \times (\frac{r_2}{b})$.

Si $r_2 = 0$, entonces $\frac{a}{b} = q + \frac{q_1}{10} + \frac{q_2}{100} = q + 0,0q_2 = q, q_1q_2$, expresión decimal de $\frac{a}{b}$, siendo q su parte entera y q_1q_2 su parte decimal, con q_1 la cifra de las décimas y q_2 la cifra de las centésimas, y se lee “ q enteros y q_1q_2 centésimos”.

Si $0 < r_2 < b$, por el algoritmo de la división $\frac{10 \times r_2}{b} = q_3 + \frac{r_3}{b}$, con $0 \leq r_3 < b$, $0 \leq q_3 < 10$ y $\frac{a}{b} = q + \frac{q_1}{10} + \frac{q_2}{100} + \frac{1}{1000} \times (\frac{10 \times r_2}{b}) = q + \frac{q_1}{10} + \frac{q_2}{100} + \frac{1}{1000} \times (q_3 + \frac{r_3}{b})$

$$= q + \frac{q_1}{10} + \frac{q_2}{100} + \frac{q_3}{1000} + \frac{1}{1000} \times \left(\frac{r_3}{b} \right).$$

Si $r_3 = 0$, entonces $\frac{a}{b} = q + \frac{q_1}{10} + \frac{q_2}{100} + \frac{q_3}{1000} = q + 0,q_1+0,0q_2+ 0,00q_3 = q, q_1q_2q_3$, es la expresión decimal de $\frac{a}{b}$, siendo q su parte entera y $q_1q_2q_3$ su parte decimal, con q_1 la cifra de las décimas, q_2 la cifra de las centésimas y q_3 la cifra de las milésimas, y se lee “ q enteros y $q_1q_2q_3$ milésimos”.

Si $0 < r_3 < b$, se repite el proceso anterior con $\frac{10 \times r_3}{b}$, $\frac{10 \times r_4}{b}$, etc. y la expresión decimal de $\frac{a}{b}$ es $\frac{a}{b} = q, q_1q_2q_3q_4\dots\dots$, una expresión periódica.

Por ejemplo, se tiene:

$$\frac{17}{5} = 3 + \frac{2}{5} = 3 + \frac{1}{10} \times \left(\frac{20}{5} \right) = 3 + \frac{1}{10} \times (4) = 3 + \frac{4}{10} = 3 + 0,4 = 3,4;$$

$$\begin{aligned} \frac{13}{18} &= 0 + \frac{13}{18} = 0 + \frac{1}{10} \times \left(\frac{130}{18} \right) = 0 + \frac{1}{10} \times \left(7 + \frac{4}{18} \right) = 0 + \frac{7}{10} + \frac{1}{10} \left(\frac{2}{9} \right) = 0 + \frac{7}{10} + \frac{1}{100} \left(\frac{20}{9} \right) \\ &= 0 + \frac{7}{10} + \frac{1}{100} \left(2 + \frac{2}{9} \right) = 0 + \frac{7}{10} + \frac{2}{100} + \frac{1}{100} \left(\frac{2}{9} \right) = 0 + \frac{7}{10} + \frac{2}{100} + \frac{1}{1000} \left(\frac{20}{9} \right) \\ &= 0 + \frac{7}{10} + \frac{2}{100} + \frac{1}{1000} \left(2 + \frac{2}{9} \right) = 0 + 0,7 + 0,02 + 0,002 + \dots = 0,72222\dots \end{aligned}$$

REFERENCIAS

- Verástegui, T. (1996). *Introducción a la teoría de números*. Edit. Moshera.
- Vinogradov I. M. (1971). *Fundamentos de la teoría de números*. Edit. MIR.
- Serre, J. P. (1973). *A course in arithmetic*. Springer–Verlag.
- Samuel, P. (1972). *Teoría algebraica de números*. Ediciones Omega.
- Andrews, G. E. (1971). *Number theory*. W. B. Saunders Co.
- Pollard, H. H. (1965). *The theory of algebraic numbers*. The mathematicss assoc. of America.