CONFORMACIÓN DE LOS SISTEMAS NUMÉRICOS

Oscar Fernando Soto Ágreda
Segundo Javier Caicedo Zambrano

Editorial
Universidad de Nariño

Editorial
Universidad de Nariño

CONFORMACIÓN DE LOS SITEMAS NUMÉRICOS

CONFORMACIÓN DE LOS SITEMAS NUMÉRICOS

Oscar Fernando Soto Ágreda
Segundo Javier Caicedo Zambrano

Editorial
Universidad de Nariño

Soto Ágreda, Oscar Fernando
Conformación de los sistemas numéricos / Oscar Fernando Soto Ágreda, Segundo Javier Caicedo Zambrano. -- San Juan de Pasto : Editorial Universidad de Nariño, 2023
196 p. : il., tablas

Incluye bibliografía p. 164-165 y datos de los autores p. 3
ISBN: 978-628-7509-77-1 Digital

1. Sistemas numéricos 2. Matemáticas--Enseñanza--Teoría de los números 3. Números reales 4. Números complejos 5. Números enteros 6. Números naturales 7. Didáctica de las matemáticas
I. Caicedo Zambrano, Segundo Javier

Sección de Biblioteca
"Alberto Quijano Guerrero"

CONFORMACIÓN DE LOS SISTEMAS NUMÉRICOS

ISBN: 978-628-7509-77-1
Primera Edición

Revisión de Estilo: Germán Chávez Jurado
Diseño y Diagramación: Manuel Alejandro Insandara Arteaga

Fecha de publicación: Mayo del 2023
San Juan de Pasto-Nariño-Colombia

TABLA DE CONTENIDO

INTRODUCCIÓN

La historia verifica, cómo el hombre tardó miles de años en pasar del manejo de las cantidades al concepto de número; este concepto que subyace en el mundo incorruptible de las ideas y que hoy aparece tan sencillo, trivial y evidente, es el producto de un largo trabajo de abstracción. Seguramente el mediador elemental para conseguir este resultado, se encuentra en la diferencia entre lo singular y lo plural, mirando en cada objeto la existencia de la unidad y escindiendo, en la pluralidad, las diferencias particulares. Y es que el número convive en el límite entre lo parecido y lo diferente, ya que las cosas que se enumeran, son aparentemente parecidas y justamente se rotulan con cifras distintas, porque a la vez son diferentes. Las marcas y el emparejamiento, son los primeros vestigios de la conservación de los números y su consecuente propiedad operativa y para su memorización, recurrieron al cuerpo y muy especialmente a los dedos y las articulaciones.

Algunas civilizaciones pudieron encontrar números grandes a través del Cálculo Digital; por ejemplo, en la China, en el siglo XVI superaron los mil millones recurriendo a procedimientos de representación en los que utilizaban las dos manos.

El siguiente paso fue convertir el conocimiento numérico forjado en la práctica de una simbología primaria y de la necesidad de operar con las cantidades en un sistema de representación de los mismos que hoy se denomina numeración. La numeración actual que, nos parece rutinaria, se caracteriza por varios aspectos mágicos que se ponen de relieve al analizar su sencillez e importancia; en principio, alcanza formas de representación visual, oral y escrita, lo que se traduce en la posibilidad de su captura óptica, su expresión verbal o nombre y su representación simbólica a través de la escritura. Debe recordarse que, la aparición de la escritura es el paso gigantesco que parte en dos la historia de la humanidad y permitió el paso a lo que se llama civilización.

Una buena representación posibilita la actividad de calcular y, en realidad, la pobreza de las numeraciones se rompe con la invención del sistema de numeración posicional hindú que data desde el siglo V de nuestra era. Este sistema de numeración decimal permite hacer mucho con poco. Con los símbolos $0, 1, 2, 3, 4, 5, 6, 7, 8$ y $\mathbf{9}$ se puede representar cualquier cantidad por grande o pequeña que sea y cada representación escrita, desde el

momento de terminar su escritura ya tiene su representación oral; es decir, ya posee un nombre y, al contrario, en la medida en que se va pronunciado su nombre se logra su representación escrita. Y lo posicional indica que, el uno del mil vale mucho más que cualquiera de los nueves del novecientos noventa y nueve. El aspecto más sorprendente que logra el sistema hindú de posición, en cualquier base y, en particular en la base decimal, es que se hace fácil la práctica tardía de efectuar directamente las operaciones de sumar, restar, multiplicar y dividir. Para reconocer la facilidad que tiene la utilización de este sistema al calcular, y con el objetivo de que el lector determine sus diferencias, se presentan a continuación los algoritmos de multiplicación y división utilizados por los egipcios.

Cuando el sistema numérico con el cual se trabaja es pobre, se reduce la posibilidad de pasar de la Aritmética al Álgebra. Los egipcios basaban su aritmética en una suplantación de símbolos, pero no es un sistema posicional. Su sistema, por tanto, es muy similar a la escritura romana y por ello la adición y sustracción se reduce a un "trueque" de símbolos o a una supresión de los mismos. El algoritmo de multiplicación egipcio se fundamenta en la base 2, particularmente en la duplicación sucesiva de uno de los factores hasta completar el otro. Por ejemplo, el producto 19×71 se puede conseguir como se aprecia en Tabla 1.

***Tabla 1**. Ejemplo egipcio de multiplicación:* 19×71

٧	1	71
٧	2	142
	4	284
	8	568
٧	16	1136
Totales	19	1349

٧	1	19
٧	2	38
٧	4	76
	8	152
	16	304
	32	608
٧	64	1216
Totales	71	1349

Se evidencia que, la práctica subyace en las veces que debe tenerse en cuenta uno de los factores; tales veces, en número se equiparan con el otro factor.

El algoritmo de la división, contiene un proceso similar y se logra por la multiplicación del divisor hasta obtener el dividendo. Tal multiplicación es susceptible de ejecutarse por factores fraccionarios. Por ejemplo, para obtener el cociente de la división $35 \div 8$ se efectúan sucesivas duplicaciones del divisor, deteniéndose en el momento en que no excedan

al dividendo. Además, si se hace necesario, se deben efectuar sucesivas divisiones por 2. Se suman aquellos múltiplos y submúltiplos que suman el dividendo. La suma de las correspondientes potencias de 2 se igualan con el cociente. La Tabla 2 presenta los cocientes $35 \div 8$ y $74 \div 16$.

***Tabla 2**. Ejemplo egipcio de división:* $35 \div 8$ *y* $74 \div 16$

1	8	
2	16	
4	32	٧
$\frac{1}{2}$	4	
$\frac{1}{4}$	2	٧
$\frac{1}{8}$	1	٧
$4+\frac{1}{4}+\frac{1}{8}$	35	

1	16	
2	32	
4	64	٧
$\frac{1}{2}$	8	٧
$\frac{1}{8}$	2	٧
$4+\frac{1}{2}+\frac{1}{8}$	74	

Se evidencia que, el sistema de numeración de base 2 juega un papel muy importante, pero los procesos de cálculo se vuelven excesivamente truculentos y tan solo llaman la atención por rodearse de un atractivo didáctico.

Desde este punto de vista y dado que el sistema decimal de numeración que utilizamos contiene la fantasía de su sencillez, no solo puede asegurarse que se puede hacer mucho con poco, sino que se tiene la posibilidad de hacerlo todo, y tan solo este hecho por sí mismo explica la forma sugestiva en que el árabe Muhammad ibn Musa al_Juwarizmi escribiera el *Libro de la adición y la sustracción según el cálculo de los indios*, obra escrita en los dos primeros decenios del siglo IX y que a partir del siglo XII se tradujo al latín varias veces.

Desde allí, desde las obras en latín, lengua de obligatorio uso en los textos científicos en el medioevo y de la época moderna, es fácil predecir la expansión de su uso y la constitución firme de los sistemas de numeración, cada uno de los cuales se aúna en un cuerpo teórico perfectamente definible e importante.

Este libro, evidencia la construcción de algunas estructuras que inicia con los naturales; los enteros, dan tránsito a los racionales, los irracionales y, con ello, a los reales; y termina en el campo de los complejos. Todo esto,

utilizando la lógica aristotélica con sus tres principios fundamentales, a saber, el de identidad, el de no contradicción y el principio del tercero excluido.

Este texto adopta una breve revisión histórica como inicio y motivación al estudio de los sistemas de numeración; percibe una luz en la milenaria construcción que alumbra los procesos didácticos modernos y un afán por revisar más a fondo las circunstancias que permitieron el establecimiento de los mismos. Es fácil intuir que la riqueza de los pueblos se mide en la riqueza que subyace en la palabra escrita que heredan y con la cual trasciende todo pensamiento, pero también, con la vigencia y evidencia de un sistema de numeración que complete el mundo de las ideas y de los conceptos. La palabra y el número, son factores fundamentales en la explicación de cualquier teoría.

La obra se centra en el andamiaje constructivo de los diversos sistemas numéricos y se aparta de los misterios que ellos reúnen. Por ejemplo, la sucesión infinita de los números naturales contiene sorprendentes regularidades, curiosas distribuciones, sobrecogedores resultados; el hecho de que el conjunto de números primos sea infinito, de que todo par superior a 2 se pueda escribir como la suma de una pareja de primos (Conjetura de Goldbach), de que algunas progresiones aritméticas contengan infinidad de números primos (Teorema de Dirichlet); de que la suma de tres naturales consecutivos sea múltiplo de tres y su producto divisible por seis, entre otros, han permitido la constitución de la aritmética de los números naturales que, en el decir de Carl Friedrich Gauss, constituye la “reina de las Matemáticas”.

El libro deja de lado la sutileza de la creación de George Cantor, que incluye toda una constelación de infinitos; la suspicacia pitagórica de Pierre de Fermat, en el que pretende hacer una extensión al famoso teorema geométrico, con el llamado último teorema de Fermat; los resultados de Euler y de Ramanujan y de tantos gigantes, pues, su propósito inicia con el modelo deductivo del italiano Giuseppe Peano, la revisión de sus conclusiones y propiedades operativas entre números naturales y va trasegando por la construcción de los enteros, los racionales, los irracionales, los reales y los complejos. Esta es la ruta trazada en el espacio curricular que ha diseñado el programa de Licenciatura en Matemáticas de la Universidad de Nariño y que el presente libro recorre al acercarse a la componente histórica, a la componente computacional y al rigor lógico de la demostración de los resultados.

El texto reivindica el trabajo axiomático presentado por el lógico americano Charles Sanders Peirce, una década antes de ser legado por Peano. Una investigación histórica debe terminar por restituir el valor de Peirce y determinar el por qué la gran similitud de su propuesta versus la presentada por Peano.

El texto incluye ejemplos sobre procedimientos computacionales implementados con el asistente matemático Derive.

El libro consta de seis (6) capítulos, nombrados de la siguiente manera: Capítulo 1: Generalidades de los sistemas numéricos; Capítulo 2: Los números naturales; Capítulo 3: Los números enteros; Capítulo 4: Los números racionales; Capítulo 5: Los números reales; y Capítulo 6: Los números complejos. En cada caso se revisan las propiedades que cumple cada conjunto en relación con los conceptos de grupo, anillo, cuerpo y relaciones de orden.

Para efectos de producción de la obra, los coautores realizaron sus aportes individuales por capítulos y otros fueron escritos de manera conjunta, así: los capítulos 2 y 4, son de autoría del profesor Oscar Fernando Soto Ágreda; los capítulos 3 y 5 del profesor Segundo Javier Caicedo Zambrano; y los capítulos 1 y 6, con aporte de los dos autores del libro.

CAPÍTULO 1.
GENERALIDADES DE LOS SISTEMAS NUMÉRICOS

Coautores:
Oscar Fernando Soto Ágreda[1]
Segundo Javier Caicedo Zambrano[2]

1.1 Aspectos históricos

Hacia 1850, todos los miembros del sistema numérico ya eran conocidos: naturales, enteros, racionales, irracionales, complejos e hipercomplejos (Cuaternios de Hamilton). Sin embargo, su introducción y manejo creaba muchas resistencias, sobre todo, por los resultados sorpresivos que conllevaba su manejo: el profundo misterio de los naturales donde subyacen resultados y conjeturas asombrosas, el producto de dos reales negativos es uno positivo, la suma y el producto de irracionales puede ser un racional, una sucesión de racionales puede converger a un irracional, la suma y el producto de complejos puede ser un real, las potencias de complejos pueden ser reales, en los complejos no existe el orden, en los hipercomplejos desaparece la conmutatividad y si fuese más adelante, en los octiones no existe la asociatividad (Soto et. al, 2021). De otro lado, el mundo académico carecía del espíritu liberal de nuestros días; eran normales las oposiciones hacia los nuevos objetos matemáticos. Por ejemplo, el matemático inglés Francis Maseres, quien ostentaba el nobiliario título de barón, miembro del Clare College de Cambridge y de las Royal Society, publicó en 1759 su *Dissertation on the Use of the Negative Signs in Algebra*, en la que indica, cómo evitar los números negativos, excepto cuando se trata de restar una cantidad menor de una mayor y, en particular, hace una diatriba en contra de las raíces negativas, mediante la cuidadosa segregación de tipos de ecuaciones cuadráticas de forma que las que poseen raíces negativas son consideradas como una clase aparte, de forma tal que, las raíces negativas deben ser separadas. Sobre las raíces negativas expresa lo siguiente:

> *"... sirven únicamente, en lo que yo puedo juzgar, para confundir toda la doctrina de ecuaciones y para volver en cosas oscuras y misteriosas las que son en su propia naturaleza excesivamente simples y ordinarias... Se debería desear, por lo tanto, que las raíces negativas nunca hubieran sido admitidas dentro del álgebra o que fueran, de nuevo, descartadas de ella, ya que, si esto fuera hecho, hay razón de sobra para imaginar que las objeciones que muchos hombres cultos e ingeniosos ahora hacen de los cómputos algebraicos, como*

[1] Profesor Adscrito al Departamento de Matemáticas y Estadística, Universidad de Nariño.
[2] Profesor Adscrito al Departamento de Matemáticas y Estadística, Universidad de Nariño.

> *ser oscurecidos y confundidos con nociones casi inintelegibles, serían por consiguiente suprimidas; siendo inevitable que el álgebra o la aritmética universales, por su propia naturaleza, una ciencia no menos simple, clara y capaz de demostración que la geometría."*

Los números negativos no fueron bien comprendidos hasta esta época contemporánea; es así como el gran Leonhard Euler (1707, 1783), en la última mitad del siglo XVIII, creía que los números negativos eran mayores que el infinito (Soto et. al, 2021). Carnot, geómetra francés, pensó que los números negativos conducían a conclusiones erróneas. En 1831, Augustus De Morgan (1805-...), profesor de matemáticas del University College de Londres, decía que:

> *"...la expresión matemática raíz cuadrada de menos uno y la expresión negativa menos b tienen este parecido: que cualquiera de ellas, cuando aparece como solución de un problema, indica alguna inconsistencia o absurdo. En cuanto se refiere al significado real, ambas son igualmente imaginarias, ya que −a es tan inconcebible como su raíz cuadrada."*

Esta y muchas otras dificultades no son regaladas; la humanidad tardó miles y miles de años en pasar de la simple percepción de la cantidad al concepto de número. Número es una idea que ahora parece evidente pero que se ha forjado a través de un arduo trabajo de abstracción del pensamiento. Un número se hace teniendo en cuenta la existencia singular de la cantidad como cualidad de las cosas y rechazando todas las otras diferencias particulares; esto determina el carácter abstracto de la Matemática.

Unido al desarrollo del concepto de número y en un proceso igualmente largo, se aviene la dificultad de representar tales números; así, aparecen variados sistemas de representación como el romano y el mal llamado arábigo (en realidad Indio). Este modo de representación posicional es tan potente como los mismos números, es capaz de acompañar a cualquier número que surja, por muy lejos que vaya. Apenas aparece ya le tiene un nombre. Es un sistema propicio para nombrar a lo inédito, es un sistema en el que el 1 del 1000 vale mucho más que cualquiera de los 9 del 999; un sistema en el que se privilegia la posición; dos 1 en la representación de cualquier número expresan ideas diferentes, a pesar de ser el mismo símbolo.

La frase "el 1 del 1000 vale mucho más que cualquiera de los 9 del 999", del párrafo anterior, se expresa en un adagio popular: "Un asno en el peldaño más alto vale más que un león en el más bajo". Para el hombre contemporáneo, esto es una evidencia; escribe con facilidad lo referente a

un cálculo, una suma, una diferencia, un producto, un cociente, una raíz cuadrada, un cambio de base; directamente sobre los números efectúa lo referente a una operatoria en particular; pero esto se revela como una práctica tardía y excepcional en la historia de la humanidad y constituye un hito dentro de la matemática, un paso trascendental, el último escalón hacia la dignificación creativa. Antes de esto, las tareas de llevar cuentas eran arduas, complicadas y sólo unos pocos hombres adiestrados podían realizarlas. De este modo, se permitía un poco guardar el secreto de las contabilidades de los pueblos, y las tareas de auditoría sobre las mismas eran casi prohibitivas.

El cálculo escrito pudo llevarse gracias a la numeración india, sistema posicional provisto de un cero, que apareció hacia el siglo V de nuestra era. ¡Grandioso! ¡Bastan *diez figuras para representar todos los números del mundo!* Aparte de la numeración india, existen vestigios de otros sistemas posicionales que aparecen de modo independiente: en Babilonia, a comienzos del segundo milenio de nuestra era; en China durante el siglo V y en el imperio Maya entre los siglos V y IX. Los Mayas, parece que utilizaban la base 20, pero en lugar de dotarse de 20 símbolos sólo presentaban tres; el uno, el cinco y el cero. La numeración sumeria, de base 60, en lugar de dotarse de 60 símbolos, también presenta sólo dos: el uno y el diez. Estas formas de representación, complicaban su uso y hacían del sistema un método infértil y débil.

Se tiene la referencia de un sistema posicional que ahora se frecuenta, debido a la novísima ciencia de la computación; el sistema binario, que sólo utiliza los símbolos cero y uno. Este sistema es el más arcaico y se utiliza hasta hoy entre los habitantes del estrecho de Torres entre Australia y Nueva Guinea, quienes utilizan la numeración llamada *urapun-okosa* y que viene acompañada de la alternancia de unos y doses:

$1: urapun$
$2: okosa$
$3: okosa - urapun$
$4: okosa - okosa$
$5: okosa - okosa - urapun$
$6: okosa - okosa - okosa \cdots$

La utilización del sistema binario en los computadores ha hecho de estas máquinas unos instrumentos portentosos de cálculo y de manejo de la información. En 1703, el matemático y filósofo alemán Gottfried Wilhelm von Leibniz (1646-1716) escribió:

> "*En vez de la progresión de diez en diez, he empleado desde hace varios años, la progresión más simple de todas, que va de dos en dos, advirtiendo que pertenece correctamente a la ciencia de los números. Así, pues, sólo empleo los caracteres* 0 *y* 1*, y luego al llegar a* 2 *vuelvo a empezar. Por eso se escribe aquí dos como* 1 0 *y dos veces dos o cuatro por* 1 0 0 *y dos veces cuatro u ocho por* 1 0 0 0*, etc*."

Incluso, el mismo Leibniz había diseñado el proyecto de una medalla para celebrar la numeración binaria:

> "*He representado* - dice - *luz y tinieblas o, según la idea que de ello se hacen los hombres, el espíritu de Dios planeando sobre las aguas... Y eso es cierto: los vacíos abismos y el taciturno desierto pertenecen al Cero; en cambio el espíritu de Dios y su luz pertenecen a Uno omnipotente.*"

Para cambiar cualquier número a base 2, simplemente se efectúa una división por dos, y por defecto sucesiva. Frente a cada cociente par se pone un cero y frente a cada mitad impar, un uno. El número en base dos se lee de abajo hacia arriba. Por ejemplo, para escribir el 77 en base 2 se procede así:

77	1
36	0
18	0
9	1
4	0
2	0
1	1

Por lo tanto $77_{(2)}$ =1001001.

La sucesión 1, 2, 3, ... manifiesta una gran realidad y por ello se denominan los números naturales. Es una inagotable sucesión de números enteros que es familiar a todos los pueblos civilizados y a quienes han asistido a ese conocimiento que se produce en las escuelas. Esa serie es muy familiar, sin embargo, oculta sorprendentes e inesperadas regularidades, pero a la vez, pasmosas e inexplicables distribuciones. Estudiar al conjunto de los números naturales a profundidad ha constituido una rama aparte que, a decir de Carl Friedrich Gauss, el príncipe de los Matemáticos, es la reina de las matemáticas, y es un cuerpo perfectamente definido, denominado *Teoría de Números*.

Al genio Euclides, uno de los más grandes matemáticos del siglo III a. C. se le atribuyen muchos resultados de aritmética, el primero de ellos es la

técnica de división euclidiana o la división con resto, en la que, por ejemplo 23, dividido entre 5 es igual a 4 y deja resto 3. Este hecho se escribe así: $23=5\times 4\ +\ 3$.

El estudio de los divisores es el primer recurso de clasificación de los números naturales; los números divisibles por 2 se dicen *pares* y los que al dividirse por 2 dejan residuo 1 se llaman *impares.* Los pares se escriben como $2n$ y los impares como $2n+1$. Y respecto de las operaciones se afirma que la adición no respeta la paridad mientras que la multiplicación sí lo hace.

Ejemplo:

La conjetura de Collatz, resulta ser un excelente juego para aplicar esta primera clasificación. Löthar Collatz la formuló en 1937 y de allí en adelante ha recibido varios bautizos: se la conoce como el problema $3n+1$, Cartografía $3x+1$, Algoritmo de Hasse, Problema de Kikutami, Algoritmo de Syracuse, Conjetura de Thwaites o Problema de Ulam. Esta conjetura se establece a partir de una función tal que si n es par lo aplica en su mitad y si es impar lo multiplica por 3 y luego a este producto le suma 1. La conjetura asegura que aplicando a cualquier número y en forma reiterada esta función, la sucesión de resultados queda atrapada en la órbita $\{4,2,1\}$. A continuación, se presenta un ejemplo a partir de la raíz 33.

$$\{33, 100, 50, 25, 76, 38, 19, 58, 29, 88, 44, 22, 11, 34, 17, 52, 26, 13, 40, 20, 10, 5, 16, 8, 4, 2, 1\}$$

La conjetura de Collatz se evidencia de manera rápida en el sistema de Cálculo Simbólico Derive, al definir las dos siguientes funciones:

$$F(n) := If(Mod(n,2)=0, \frac{n}{2}, 3n+1)$$
$$Collatz(a,m) := Iterates(F(i), i, a, m)$$

La función $Collatz\ (a,m)$ ejecuta m iteraciones de la función condicional F a partir de la raíz a; por ejemplo, la simplificación de la expresión Collatz (19,20) es el siguiente vector:

$$[19, 58, 29, 88, 44, 22, 11, 34, 17, 52, 26, 13, 40, 20, 10, 5, 16, 8, 4, 2, 1].$$

Una segunda clasificación en el establecimiento de una tipología para los números, la constituyen aquellos que no son divisibles en absoluto, excepto por el 1 y por ellos mismos. A este tipo de números se les llama *primos*. La secuencia de números de esta clase inicia así:

$$2, 3, 5, 7, 11, 13, 17, 19, 23, \ldots$$

Euclides demostró que la secuencia de números primos es infinita y uno de los problemas clásicos en el aprendizaje de la Aritmética lo constituye la descomposición de un número en sus factores primos. Un resultado sorprendente es que todo número es susceptible de descomponerse de manera única como el producto de factores primos, resultado denominado Teorema Fundamental de la Aritmética.

Los números primos tienen un comportamiento extraño y fascinante, su estudio ha entretenido a matemáticos profesionales y aficionados en todos los tiempos, y el hallazgo de primos gigantescos tiene grandes aplicaciones en Criptografía. En la revista de Investigación y Ciencia, de noviembre de 1979, página 182, se da como último primo descubierto al número de Mersenne $2^{44497} - 1$. En este orden, se presenta el siguiente flash informativo:

> "8 de septiembre de 1985, 7: 30 p.m. Houston, Tejas. Se acaba de descubrir el mayor número primo hasta la fecha. Bienvenido el $2^{216091} - 1$ un número de 65050 cifras".

Entre los números primos, los de Martin Mersenne (1588- 1648), de la forma $M^n = 2^n - 1$ (siendo n un entero) son muy apreciados. Su búsqueda es un deporte popular. Hasta 1963 se conocían veintidós. Para saludar el descubrimiento del 23avo en 1963, $2^{11213} - 1$, se creó una estampilla postal. El mayor número de Mersenne conocido hasta 1997 era el 34avo y se corresponde con $2^{1257287} - 1$, número que tiene algo más de 378 632 dígitos. Cabe resaltar que estos descubrimientos son fruto de la cooperación de eficaces buscadores y de computadores cada vez más sofisticados. El primo de Mersenne $2^{756839} - 1$ se descubrió en 1992 utilizando una computadora Cray - 2.

Una tercera manera de clasificar los números naturales y estudiada inicialmente por los griegos es la de medir la divisibilidad de los números considerando la suma de sus divisores sin contarse él mismo. La suma de sus divisores puede ser menor que tal número o igual o mayor. El 8 es mayor que la suma de sus divisores por eso corresponde a los llamados *escasos o deficientes;* en cambio el 12 es menor que la suma de sus divisores, corresponde a los números *abundantes;* el 6 en cambio es igual a la suma de sus divisores, estos números son los llamados *perfectos.*

El siguiente número perfecto es el 28 que es la suma 1 + 2 + 4 + 7 + 14. El siguiente número perfecto se encuentra

después de un gran salto; es el 496 y para el siguiente hay que dar un salto todavía mayor, es el 8128. Nicómano, en el siglo I de nuestra era, conocía los primeros cuatro números perfectos: 6, 28, 496 y 8128. Los siguientes números perfectos son el 33550336 y el 8589869056. Resulta claro que se vuelven demasiado grandes; el noveno número perfecto contiene 37 dígitos.

Cierto día le preguntaron a Pitágoras ¿Qué es un amigo? La leyenda cuenta que respondió: "*El que es el otro yo mismo; el que es el otro yo mismo como* 220 *y*284." Y es que estos números tienen un vínculo fuerte desde el punto de vista de la divisibilidad: la suma de los divisores de 220 es 284 y la suma de los divisores de 284 es 220. Estos pares de números corresponden a los números llamados *amistosos o amigos.*

¡Qué maravilla! Se diría al reconocer que no ha nacido el primer gigante capaz de dominar los números. En su estructura aparecen tantas conjeturas como se resuelven. La estructura de los números naturales sigue siendo para los matemáticos una de las mayores incógnitas. Las herramientas del álgebra, el análisis, la topología, la geometría algebraica, etcétera, se emplean para conocer mejor su sistema, pero basta con contemplar su turbadora arquitectura para encontrar en ellos tantas maravillas como se desee.

Los mejores problemas que tiene la matemática se han expresado de la manera más simple. La Aritmética es una cantera de buenos problemas; por ejemplo, ¿Hay una infinitud de primos gemelos? Dos primos gemelos son aquellos pares de primos que se diferencian en 2, tal como el 3 y el 5, o el 5 y el 7, o el 11 y el13. ¿Hay una infinitud de primos amistosos? ¿Hay números impares que son perfectos? ¿Hay infinitos números perfectos? Por increíble que parezca, todas estas preguntas han sido heredadas de los griegos.

Cierto día de 1742, el matemático Christian Goldbach envió una carta a Leonhard Euler, en la que afirmaba sin demostración que "cualquier número par mayor que 2 es la suma de dos números primos". Después de un poco más de 264 años, no se sabe si esto es cierto o no. Respecto de los números impares, lo único que se ha avanzado es demostrar que cualquier impar mayor que $3^{14348907}$ es la suma de tres primos.

Estas pocas consideraciones históricas, sirven de motivación hacia el estudio de los sistemas numéricos, y muy particularmente al estudio del anillo de los números enteros. Es la simiente esencial que cosechará el fruto de resultados abonados por la lógica, pues este es, el propósito del libro.

1.2 Ramas de la matemática

El juego dialéctico de las fuerzas opuestas como la lógica y la intuición; lo general y lo particular; el análisis y la construcción, constituye la vida, la utilidad y el gran valor que posee la Matemática. El desarrollo histórico de diversos conceptos matemáticos ha obedecido a la presión por resolver problemas prácticos, pero una vez conceptuado o definido cada uno de ellos toma impulso y supera las motivaciones que le dieron origen. Es decir, del conocimiento práctico se asciende al conocimiento teórico y a continuación se buscan aplicaciones más sofisticadas e innovadoras que rebasan el simple uso de los cálculos. En algún momento, los sustratos teóricos se desligan de las situaciones prácticas y el conocimiento matemático alcanza un mayor grado de abstracción al ser un derivado del razonamiento puro.

Los babilonios y los egipcios utilizaban resultados de la Aritmética y el Álgebra hacia el año 2000 antes de Cristo; pero como ciencia, la Matemática se consolida con los griegos en los siglos IV y III a. C. al haber aplicado los sistemas axiomáticos y el método deductivo aristotélico; resultado que se deriva y obtiene desde sus contactos con el imperio Persa. Es entonces, cuando los sabios griegos tropiezan con grandes dificultades referidas al concepto del infinito, al movimiento y a la continuidad. De esas discusiones filosóficas surge como resultado la teoría de la *inconmensurabilidad* de Eudoxio (360 a.C.). Esta teoría trata de representar a un irracional como límite de magnitudes racionales; y esto sólo puede compararse con la teoría de los números irracionales, creada veinte siglos más tarde. En tiempos de Eudoxio nace la tendencia axiomático-deductiva que se cristalizó en los *Elementos* de Euclides.

Sin embargo, las aplicaciones reales jugaron un papel decisivo en la construcción de la matemática antigua. El descubrimiento de las cantidades inconmensurables desvió un poco la atención griega en el desarrollo del Cálculo Numérico, pero dio apertura a la geometría axiomática pura, la cual, predominó durante 20 siglos y retrasó el desarrollo de los cálculos numéricos y la consolidación del Álgebra. Los pitagóricos, por ejemplo, que aducían que el mundo se interpretaba tan solo a través de

los números, adoptaron para ellos una metodología más contemplativa que operativa. Esta etapa de tranquilidad y abandono numérico sirvió de preparación y gestación de la Revolución Matemática de los siglos XVII y XVIII, tanto en sus temáticas de estudio, como en el desarrollo de conceptos y la invención y adecuación de una adecuada simbología.

En los siglos XVII y XVIII aparecen ramas de la ciencia matemática como las siguientes:

La Geometría Analítica, que se impele con los trabajos de René Descartes y Pierre de Fermat.

El Cálculo Diferencial e Integral, que inicia con la solución a problemas de índole físico y geométrico presentados por Sir Isaac Newton y Gotfried Wihelm Leibniz. De hecho, el cálculo integral inicia con el método de exhaución presentado por Arquímedes.

En el siglo XIX aparecen:

- Las Geometrías no Euclideanas, que surgen a partir del estudio del postulado de las paralelas y culmina con los estudios de Carl Friedrich Gauss, Janos Bolyai, Nicolás Lobatschewski y Bernard Riemann.
- La teoría de Grupos, cuyo origen se establece en los resultados logrados por Evaristo Galois y Niels Henrick Abel.
- La Aritmetización del Análisis, que realiza David Hilbert.
- La Lógica Matemática, rama en la cual sobresalen George Boole y Kurt Gödel.

Y también, en esta época surgen ramas de la ciencia con trabajos de colectivos académicos o raíces en congresos de matemáticos; algunas de ellas son:

- La Teoría de Conjuntos, que se establece con el grupo de los Bourbaki.
- Las Nuevas Álgebras.
- Las Estructuras Algebraicas.
- Los Sistemas Matemáticos.

Y en el siglo XX:

- La Ciencia de la Computación.
- El Álgebra Computacional.
- La Geometría Diferencial.
- La Geometría Computacional.

En esta época se confía a ciegas en los procesos formales que consolidan demostraciones rigurosas conducidas por la mente humana y que logran conquistar un mundo de infinita riqueza. El advenimiento de la Revolución Francesa en 1789, impulsó la enseñanza superior y con ella, la revisión de los fundamentos de la nueva matemática, en particular, del Cálculo Diferencial e Integral. Como consecuencia se obtuvo una gran solidez interna, una comprensión clara y precisa de los conceptos y una buena simplificación de los contenidos.

Por ahora, se respira un aire de unión entre la ciencia pura y la aplicada, y un equilibrio estable entre lo abstracto y lo concreto. En efecto, la invención constructiva y la intuición directora, son el núcleo de todo resultado matemático, aún en los campos más abstractos. El análisis lógico no representa a toda la matemática, pero ha contribuido a la comprensión profunda de los hechos matemáticos, de su interdependencia y a penetrar en la esencia de sus conceptos. Lo que realmente interesa en el estudio de puntos, rectas y números, es su estructura y sus relaciones; dos puntos determinan una recta, dos números se combinan según cierta regla para producir un nuevo número, tres segmentos de recta pueden o no determinar un triángulo en concordancia con una definición.

1.3 Los sistemas numéricos

Hasta finales del siglo XIX se creía que los números naturales eran los más simples y transparentes para la mente humana, pues fueron creados para contar objetos agrupados de diferentes maneras, sin tener en cuenta la naturaleza del objeto en sí. Por ejemplo, el número 5 es la abstracción de todas las colecciones que contienen cinco objetos, como los dedos de la mano; las vocales del alfabeto indio; los océanos del mundo; la cantidad de letras que componen la palabra PASTO.

Los griegos tomaron como base de su matemática los conceptos de Punto y de Recta. Hoy se admite como principio director que toda la matemática

puede ser reducida, en última instancia, a proposiciones sobre los números naturales 1,2,3,..., así lo asegura Leopoldo Kronecker (Prusia 1823-1895): "*Dios creó los números naturales, lo demás es obra del hombre."* Con estas palabras, Kronecker señaló la base precisa sobre la cual puede construirse toda la matemática.

Para comprender el significado de los números naturales no basta con exponer el conjunto $\mathbb{N} = \{1, 2, 3, \ldots\}$; se hace necesario considerar el orden que llevan sus elementos y algunas características como las que se señalan a continuación.

1. Hay un primer elemento llamado Cero.
2. La sucesión de números no termina ni se ramifica.
3. La sucesión no se cierra sobre sí misma.
4. Ningún elemento tiene dos antecesores.
5. No hay números naturales intercalados "entre" dos cualesquiera y consecutivos de la sucesión. (Es decir, a partir de 0 se obtiene todo $\mathbb{N}$).

Estas consideraciones llevaron a Richard Dedekind (1831-1916) y Giuseppe Peano (1858-1932) en1889 a fundamentar el concepto de número natural en cinco postulados que se estudiarán más adelante y de donde surgen de un modo deductivo todas sus características, operaciones y propiedades, tal y como si en ellos se condensara toda la aritmética. Resulta atractivo considerar la gran similitud con *Los Elementos* de Euclides, donde, de manera análoga, todo el conocimiento geométrico de su modelo, surge desde cinco postulados.

Georg Cantor (1845-1918) y Gottlob Frege (1890-1900) llegaron al mismo resultado al concebir la idea de coordinabilidad entre conjuntos. A la pregunta, ¿Hay aquí tantos escritorios como estudiantes? Se puede responder por dos caminos: contando escritorios y estudiantes o haciendo que los estudiantes se sienten en sendos escritorios. En el segundo caso puede suceder que:

a. Sobran escritorios
b. Faltan escritorios
c. Ni sobran ni faltan escritorios

En el caso c). se dice que el conjunto de escritorios es coordinable con el conjunto de estudiantes ya que tienen el mismo número de elementos. No interesa cuántos estudiantes haya, sino que los dos conjuntos tengan el

mismo número de elementos. Por ello, se dice que el número cardinal de un conjunto C, es la clase de todos los conjuntos coordinables con C.

El criterio de la coordinabilidad de conjuntos se aplica a los conjuntos infinitos bajo idéntico modelo conceptual que se consolida con la configuración de relaciones biyectivas. A manera de ejemplo se considera el conjunto de los números naturales y el conjunto de los números pares positivos. A cada $n \in \mathbb{N}$ le corresponde el número $2n$ que es par.

$$1 \to 2, \quad 2 \to 4, \quad 3 \to 6, \cdots, n \to 2n.$$

Así que, $\mathbb{N}$ tiene el mismo número de elementos que P, considerando a P como el conjunto de los números pares, aunque se argumente que en $\mathbb{N}$, no se han contado los números impares. Se puede probar que la función $f: \mathbb{N} \to P$ tal que $f(n) = 2n$ es biyectiva.

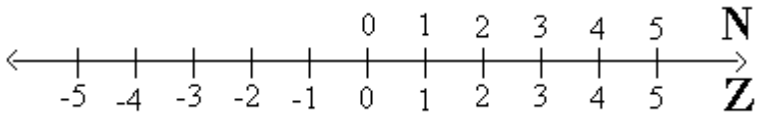

Figura 1. Función biunívoca $f: \mathbb{N} \to P$ tal que $f(n) = 2n$.

La Figura 1 sugiere que existen más enteros que naturales; sin embargo, un examen cuidadoso indica que los números naturales pares se pueden poner en correspondencia biunívoca con los enteros no negativos, mientras los números naturales impares se pone en correspondencia biunívoca con los enteros negativos, lo que prueba que existen tantos números naturales como enteros.

Definición. La cantidad de elementos de un conjunto A se denomina cardinal del conjunto y se denota por $card(A)$ sin importar si el conjunto es finito o infinito. Dos conjuntos que poseen el mismo cardinal se llaman coordinables o equinumerosos.

Galileo Galilei en 1638 encontró la curiosa propiedad del cardinal de los naturales y es que se puede establecer una biyección entre los naturales y algunos subconjuntos propios más pequeños. Por ejemplo, $f(n) = n^3$ establece una función biyectiva entre los naturales y su subconjunto propio formado por los cubos perfectos. De este modo, el axioma de Euclides (Noción común) de que el todo es más grande que la parte, en este caso queda sin piso y se debería cambiar por otra más generosa, por ejemplo, el todo es mayor o igual que la parte.

Nota 1. El cardinal de $\mathbb{N}$, $\mathbb{Z}$ y $\mathbb{Q}$ es el mismo y se denota por la primera letra del alfabeto hebreo aleph con subíndice cero; esto es, $\aleph_0$.

Se puede establecer una función biyectiva entre $\mathbb{N}$ y $\mathbb{Z}$ para determinar su coordinabilidad; por ejemplo, $f: \mathbb{N} \to \mathbb{Z}$ tal que,

$$f(n) = \begin{cases} -\frac{n}{2} \ si \ n \ es \ par \\ \frac{1+n}{2} \ si \ n \ es \ impar \end{cases}$$

La anterior función es biyectiva, con lo cual, se demuestra que la cardinalidad de $\mathbb{N}$ y $\mathbb{Z}$ son iguales.

El cardinal de $\mathbb{R}$ se llama el continuo numérico y se denota por $\varsigma = 2^{\aleph_0}$.

La equivalencia de conjuntos que se demuestra al definir una función biyectiva entre dos conjuntos es equivalente a decir que los dos conjuntos son coordinables o equinumerosos. Así las cosas, el siguiente ejemplo muestra que dos segmentos tienen el mismo número de puntos.

Ejemplo:

Dos segmentos tienen el mismo número de puntos.

Demostración

En efecto, dados dos segmentos de recta $\overline{AB}$ y $\overline{A'B'}$, es suficiente, para lograr el cometido propuesto, con proyectar un segmento sobre el otro desde un centro adecuado, así $\overline{AB'} \cap \overline{BA'} = O_1$, como en la Figura 2 y $\overline{AA'} \cap \overline{BB'} = O_2$ como en la Figura 3. La imagen de C entre A y B sobre $\overline{A'B'}$ se corresponde con la intersección de CO_2 ó CO_1 con $\overline{A'B'}$.

De manera que todo punto situado entre A y B tiene su correspondiente entre A' y B', tal y como se observa en las Figura 2 y Figura 3, que indican dos formas similares de establecer la relación biunívoca entre los puntos de dos segmentos.

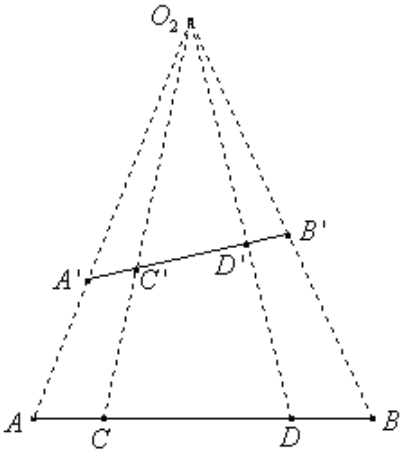

Figura 2. Correspondencia biunívoca de puntos entre dos segmentos

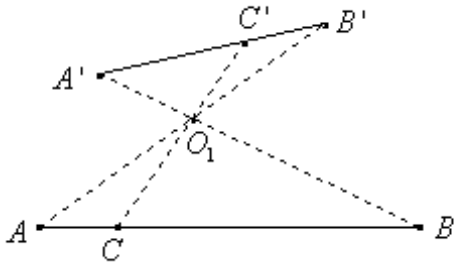

Figura 3. Correspondencia biunívoca de puntos entre dos segmentos

Ejemplo:

El conjunto $\mathbb{N}$ es equivalente o coordinable con $\mathbb{Q}$.

Demostración

Georg Cantor demostró la numerabilidad del conjunto de los racionales siguiendo el método de la diagonal en el que se evidencia una malversación de los naturales al rotular a los racionales positivos, dando la sensación de que existen muchos más números naturales que racionales. La demostración de Cantor inicia disponiendo los racionales positivos en una matriz infinita por dos costados como se muestra en la Tabla 3 y contando cada uno de ellos siguiendo el camino señalado en la Figura 4, lo cual produce la garantía de contar todos los racionales. Más aún, cada número racional positivo queda rotulado infinitas veces con sendos números naturales y la función construida $f: \mathbb{N} \to \mathbb{Q}^+$ es sobreyectiva pero no inyectiva.

***Tabla 3**. Disposición de los racionales en una matriz, según Cantor*

$\frac{1}{1}$	$\frac{1}{2}$	$\frac{1}{3}$	$\frac{1}{4}$	$\frac{1}{5}$	$\frac{1}{6}$	$\frac{1}{7}$	…
$\frac{2}{1}$	$\frac{2}{2}$	$\frac{2}{3}$	$\frac{2}{4}$	$\frac{2}{5}$	$\frac{2}{6}$	$\frac{2}{7}$	…
$\frac{3}{1}$	$\frac{3}{2}$	$\frac{3}{3}$	$\frac{3}{4}$	$\frac{3}{5}$	$\frac{3}{6}$	$\frac{3}{7}$	…
$\frac{4}{1}$	$\frac{4}{2}$	$\frac{4}{3}$	$\frac{4}{4}$	$\frac{4}{5}$	$\frac{4}{6}$	$\frac{4}{7}$	…
$\frac{5}{1}$	$\frac{5}{2}$	$\frac{5}{3}$	$\frac{5}{4}$	$\frac{5}{5}$	$\frac{5}{6}$	$\frac{5}{7}$	…
⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋱

El racional 1 aparece en la diagonal principal infinitas veces e igual ocurre con todos y cada uno de los racionales positivos.

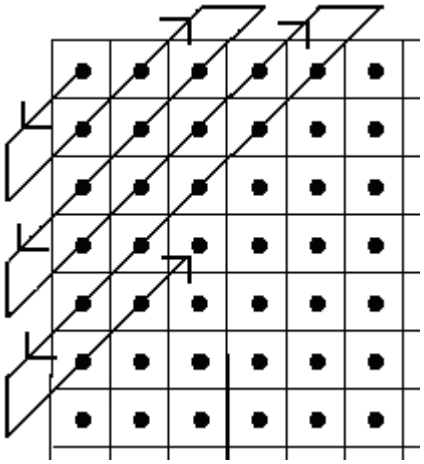

Figura 4. Recorrido de los elementos de la matriz de racionales, según Cantor

El razonamiento elaborado por Cantor con su método de la diagonal es como sigue:

a) Como $\mathbb{N} \subseteq \mathbb{Q}$ es indudable que $card(\mathbb{N}) \leq card(\mathbb{Q})$.

b) El camino diagonal construye la función sobreyectiva $f: \mathbb{N} \to \mathbb{Q}^+$ que demuestra que los racionales quedan cubiertos con los naturales y en consecuencia $card(\mathbb{Q}) \leq card(\mathbb{N})$.

c) La consecuencia de las situaciones a) y b) es que $card(\mathbb{Q}) = card(\mathbb{N})$. Este cardinal se denomina aleph cero $\aleph_0$.

d) Todo conjunto S tal que $\mathbb{N} \subseteq S \subseteq \mathbb{Q}$ tiene el mismo cardinal $\aleph_0$ de $\mathbb{N}$, en particular $card(\mathbb{Z}) = \aleph_0$.

e) Existen conjuntos B contenidos propiamente en $\mathbb{N}$, $\mathbb{Z}$ o en $\mathbb{Q}$ con igual cardinal $\aleph_0$. Por ejemplo, el conjunto de los números primos, el de los cuadrados perfectos, las fracciones de numerador 1, los enteros pares, entre otros.

A través de la función $f: \mathbb{Q} \to \mathbb{N}$ tal que $f\left(\frac{a}{b}\right) = 2^a \cdot 3^b$ que es inyectiva pero no sobreyectiva, se adquiere la misma sensación de abundancia de naturales; pues, una infinitud de ellos deja de ser imagen a través de esta función; es decir, no se emplean para rotular racionales debido a que son

escasos los naturales que poseen la forma $2^a \cdot 3^b$. Exceptuando al 27, ningún otro número terminado en 7 es imagen de f.

Otra forma de demostrar la numerabilidad de los racionales consiste en disponer todas las fracciones en una cuadrícula infinita, tal como se muestra en la Tabla 4.

Y ahora se recorre el camino en espiral que presenta la Figura 5, camino que garantiza que todos los racionales quedan contados. Sin embargo, el procedimiento define una función sobreyectiva de los naturales hacia los racionales debido a que la tabla contiene a cada racional un número infinito de veces. De este modo, queda la sensación de malversar a los naturales puesto que existen infinitos conjuntos infinitos que cuentan a un mismo racional.

***Tabla 4**. Otra forma de disponer las fracciones en una cuadrícula*

⋱	⋮	⋮	⋮	⋮	⋮	⋮	⋰
…	$\frac{2}{-3}$	$\frac{2}{-2}$	$\frac{2}{-1}$	$\frac{2}{1}$	$\frac{2}{2}$	$\frac{2}{3}$	…
…	$\frac{1}{-3}$	$\frac{1}{-2}$	$\frac{1}{-1}$	$\frac{1}{1}$	$\frac{1}{2}$	$\frac{1}{3}$	…
…	$\frac{0}{-3}$	$\frac{0}{-2}$	$\frac{0}{-1}$	$\frac{0}{1}$	$\frac{0}{2}$	$\frac{0}{3}$	…
…	$\frac{-1}{-3}$	$\frac{-1}{-2}$	$\frac{-1}{-1}$	$\frac{-1}{1}$	$\frac{-1}{2}$	$\frac{-1}{3}$	…
…	$\frac{-2}{-3}$	$\frac{-2}{-2}$	$\frac{-2}{-1}$	$\frac{-2}{1}$	$\frac{-2}{2}$	$\frac{-2}{3}$	…
⋰	⋮	⋮	⋮	⋮	⋮	⋮	⋱

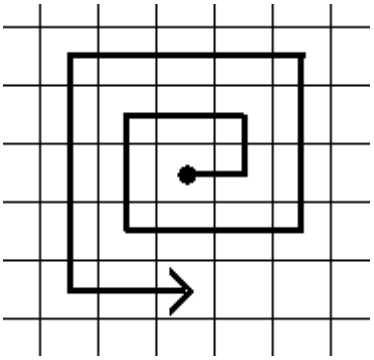

*Figura 5. Recorrido en espiral de la **Tabla 4**.*

Un mecanismo más exitoso para demostrar la numerabilidad de los racionales positivos consiste en seleccionar los conjuntos de aquellos racionales $\frac{a}{b}$ cuya suma de numerador y denominador va tomando los

valores de la secuencia natural $2, 3, 4, 5, 6, \ldots$ ordenarlos de menor a mayor; descartar los que no aparecen simplificados y rotularlos en concordancia con el conjunto de los números naturales. El conjunto de los racionales cuyos numeradores y denominadores suman 2 es el conjunto unitario $\left\{\frac{1}{1}\right\}$ y por ello el racional $\frac{1}{1}$ se rotula con el 1; el conjunto $\left\{\frac{1}{2}, \frac{2}{1}\right\}$ es el de los racionales cuyos numeradores y denominadores suman 3 y por ello, en el proceso de contar al $\frac{1}{2}$ le corresponde el 2 y al $\frac{2}{1}$ el 3; los racionales con suma 4 entre su numerador y denominador configuran el conjunto $\left\{\frac{1}{3}, \frac{2}{2}, \frac{3}{1}\right\}$ pero de allí se descarta el $\frac{2}{2}$ por no aparecer simplificado. Así, en el proceso de contar, al $\frac{1}{3}$ le corresponde el 4 y al $\frac{3}{1}$ el 5. Si la suma entre numerador y denominador es 5 se consigue el conjunto $\left\{\frac{1}{4}, \frac{2}{3}, \frac{3}{2}, \frac{4}{1}\right\}$ y sus elementos se rotulan con los naturales $6, 7, 8$ y 9. Así se prosigue indefinidamente. Este procedimiento construye una función biyectiva entre los racionales y los naturales, pero su tratamiento es costoso, pues en los pasos sucesivos la cantidad de elementos que se descartan, por no aparecer simplificados, van en aumento.

En 1997, siguiendo una conjetura del lógico americano Charles Sanders Peirce (1839-1914) también endilgada a Moritz Stern, matemático alemán y Achille Brocot, relojero francés (1858 -1860) por la construcción del Árbol Stern- Brocot, se construyó una función biyectiva que fue implementada en el sistema de Cálculo Simbólico Maple y con la cual se cuenta de manera efectiva a los racionales positivos. Esta forma divertida de construir los números racionales positivos se presenta de manera sucinta a continuación conjuntamente con los procedimientos que se elaboraron para el sistema Maple y que definen las funciones $ida: \mathbb{N} \to \mathbb{Q}$ y su inversa $vuelta: \mathbb{Q} \to \mathbb{N}$.

Empezando con las fracciones $\frac{0}{1}$ y $\frac{1}{0}$ se suman los numeradores y denominadores separadamente para obtener la fracción $\frac{1}{1}$ que se ubica entre ellos $\frac{0}{1} \quad \frac{1}{1} \quad \frac{1}{0}$.

Se repite esta operación con cada par de fracciones adyacentes situando la nueva fracción entre ellas. En el segundo paso se obtiene:

$$\frac{0}{1} \quad \frac{1}{2} \quad \frac{1}{1} \quad \frac{2}{1} \quad \frac{1}{0}$$

Estas cinco fracciones crecen a nueve por idéntico procedimiento:

$$\frac{0}{1} \quad \frac{1}{3} \quad \frac{1}{2} \quad \frac{2}{3} \quad \frac{1}{1} \quad \frac{3}{2} \quad \frac{2}{1} \quad \frac{3}{1} \quad \frac{1}{0}$$

y así se procede indefinidamente.

La posibilidad de contar a los racionales uno a uno sin repetir, consiste en rotularlos con la sucesión de números naturales en la medida que van haciendo su aparición en la tabla. Las líneas de procedimiento para la función *ida* entre los naturales y racionales, y la función *vuelta* entre los racionales y los naturales, se escriben a continuación dentro del lenguaje de programación establecido por el sistema Maple que es similar a los lenguajes de programación estructurada que se halla en el mercado.

```
ida:= proc(natural)
local potencia, nbits, ai, bi, af, bf,n;
nbits := length(convert(natural,binary));
potencia:= 2**(nbits-1);
ai:= 0;
bi:= 1;
af:= 1;
bf:= 0;
n:= natural;
while nbits   1 do
 nbits := nbits -1;
 if n  = potencia then
     n := n - potencia
 fi;
 potencia := potencia /  2;
 if n < potencia then
   af := ai + af;
   bf := bi + bf;
 else

  ai := ai + af;
  bi := bi + bf;
 fi
od;
 (ai + af) / (bi + bf)
end:
```

```
vuelta:=proc(racional)
local ai,bi,af,bf,ac,bc,n,mcd,a,b;
ai:=0;
bi:=1;
af:=1;
bf:=0;
ac:=1;
bc:=1;
n:=1;
a:=numer(racional);
b:=denom(racional);
while(a< ac) or (b< bc) do
        if (b*ac)<(a*bc) then
                ai:=ac;
                bi:=bc;
                n:=n*2+1;
else
                af:=ac;
                bf:=bc;
                n:=n*2
        fi;
                ac:=ai+af;
                bc:=bi+bf;
        od;
n:
end:
```

Los siguientes resultados se consiguen con el uso de estos procedimientos:

$ida(234567897);$

$$\frac{58276}{31159}$$

$vuelta(786567/896543);$

$$266919870589352577309915285691731007442518015$$

1.4 Operatoria con los números naturales

Es factible encontrar nuevos números naturales a partir de otros conocidos; algunas de las formas usuales requieren la definición de dos operaciones básicas llamadas adición y multiplicación, de manera que sus resultados queden unívocamente determinados. Para ello es necesario concebir un proceso general y abstracto que abarque todos los casos particulares.

Sea $+: \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ tal que $(a,\ b) \mapsto a + b$ y sea $\bullet: \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ tal que $(a,\ b) \mapsto a\,.\,b$ tomando a y b arbitrarios en $\mathbb{N}$.

Así pues, $3 + 4 = 7$ y $3 \times 4 = 4 + 4 + 4 = 12$; además $4 + 3 = 7$ y $4 \times 3 = 3 + 3 + 3 + 3 = 12$, producto que se puede encontrar, como todos los productos de dos enteros, mediante distribuciones rectangulares tal y como se indica en la Figura 6.

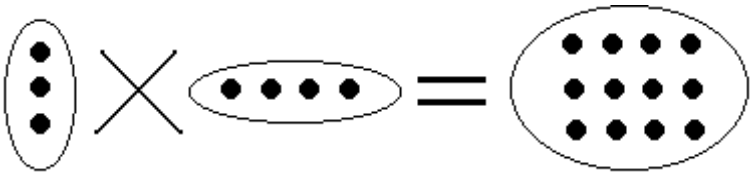

Figura 6. Multiplicación de dos números naturales

La adición y multiplicación de naturales tienen, entre otras, las propiedades indicadas en la Tabla 5. Algunas propiedades de la adición y multiplicación de naturales:

***Tabla 5**. Algunas propiedades de la adición y multiplicación de naturales*

1) Asociativa $(a + b) + c = a + (b + c)$	$(a \times b) \times c = a \times (b \times c)$
2) Conmutativa $a + b = b + a$	$a \times b = b \times a$
3) Distributiva de " × " respecto a " + " $a \times (b + c) = (a \times b) + (a \times c)$	

Ejemplo:

$$3 \times (2 + 4) = (3 \times 2) + (3 \times 4) \Leftrightarrow 3 \times 6 = 6 + 12 \Leftrightarrow 18 = 18.$$

1.5 El concepto de divisor

Sean $a, d \in \mathbb{N}$. Si $a = d \times c,\ \exists\ c \in \mathbb{N}$, se dice que d es un Divisor de a (Factor de a).

Ejemplo:

$36 = 9 \times 4 = 2 \times 18 = 3 \times 12$, entonces, 2 es un factor de 36; 9 también es un factor o divisor de 36; sin embargo, 8 no es un factor de 36, por lo tanto, tampoco es divisor de 36.

Cuando $a \in \mathbb{N}$ y sólo tiene como factores o divisores el 1 y el mismo a, se dice que a es un número primo o irreducible. Así, pues, los números $2,\ 3,\ 5,\ 7,\ 13,\ 17,\ 19,\ 23, \ldots$ son *números primos* en $\mathbb{N}$.

Las tres propiedades mencionadas en la Tabla 5 se pueden extender a los números enteros, racionales, reales y complejos. Sin embargo, ellas sólo son válidas en estos sistemas numéricos. Al cambiar de conjunto o de situación natural, es posible que no se cumplan. Por ejemplo, en Química $H_2SO_4 + H_2O$ (diluye), no es equivalente con la mezcla $H_2O + H_2SO_4$ (explota), lo que indica que en muchas circunstancias no es factible la conmutatividad.

1.6 Números enteros

La operación inversa de la adición se llama sustracción y no siempre está bien definida en $\mathbb{N}$.

Por ejemplo $7 - 3 = 4$ ya que $7 = 4 + 3$. Además $5 - 5 = 0$ y se ha tomado $0 \in \mathbb{N}$; pero $3 - 7$ no es posible en $\mathbb{N}$.

Esta consideración obliga a extender el conjunto $\mathbb{N}$ de manera que la *sustracción* pueda efectuarse sin restricciones en un nuevo conjunto y en el que se satisfaga la equivalencia:

$$a - b = c \Leftrightarrow a = c + b.$$

El nuevo conjunto se llama conjunto de los *números enteros* y se denota por $\mathbb{Z}$, así:

$$\mathbb{Z} = \{0,\ \pm 1,\ \pm 2,\ \pm 3, \dots\}.$$

En $\mathbb{Z}$ las operaciones de adición y multiplicación son igualmente válidas; pero es necesario tener cuidado con sus elementos negativos (Figura 7); en particular, conservar la siguiente regla:

$$a + (-a) = (-a) + a = 0, \forall\ a \in \mathbb{Z}.$$

Los números enteros se representan como puntos equidistantes en una recta orientada, eligiendo de manera arbitraria un punto que sirva de origen y estableciendo a cada lado dos sentidos contrarios. La unidad o patrón de medida que separa a cada par de puntos es igualmente escogida al azar o por conveniencia.

Mediante una regla y un triángulo cualquiera es factible construir la escala métrica para $\mathbb{Z}$ empleando los conceptos de *incidencia* y *paralelismo.* Se traza la recta l y se hace coincidir un lado de triángulo con ella (Figura 7).

Por deslizamiento del triángulo sobre la recta se describen rectas paralelas $r_1 \parallel r_2$ o bien $t_1 \parallel t_2$. Si se desea trazar una recta paralela a r_1 y que pase por un punto P, basta deslizar el triángulo sobre l hasta que un borde coincida con P. La Figura 7 y Figura 8, contienen dos representaciones gráficas de números enteros.

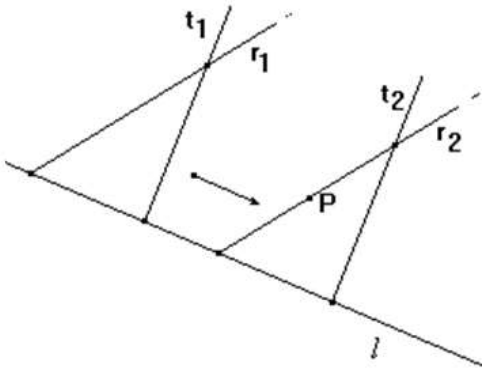

Figura 7. Representación de un número entero

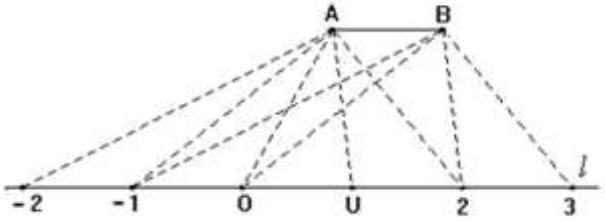

Figura 8. Representación de un número entero

Sean O y U puntos ("enteros") sobre una recta. Se traza $\overline{OA} \parallel \overline{UB}$ por deslizamiento del triángulo. Entonces $\overline{AB} \cong \overline{OU}$. Es decir $OUBA$ es un paralelogramo. Para ubicar el entero 2 sobre la recta, basta construir el paralelogramo $UAB(2)$; igual para localizar el entero -1, para lo cual es suficiente construir el paralelogramo $OAB(-1)$ (Figura 8).

La escala métrica para el conjunto de los números enteros $\mathbb{Z}$ facilita el cálculo de sumas algebraicas como $2 - 5 + 6$. Partiendo del origen se salta a 2 por la derecha y de aquí 5 unidades a la izquierda y por último 6 unidades a la derecha para llegar finalmente al punto rotulado con el 3, como se muestra en la Figura 9.

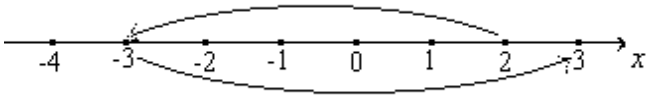

Figura 9

Luego $2 - 5 + 6 = 3$ puesto que $2 - 5 = -3$ y $-3 + 6 = 3$.

1.7 Operaciones enteras

La adición y multiplicación definidas en $\mathbb{N}$ tienen plena validez en $\mathbb{Z}$, pero es necesario tener en cuenta varias propiedades, incluidas las leyes de los signos.

Por ejemplo, si se gastan \$20 diarios durante los 5 días siguientes, ¿cuánto se gasta en total? $5 \times (\$(-20)) = \$(-100)$.

Si se gastan $\$12$ durante los últimos cuatro días, ¿cuánto se tenía entonces? $(4) \times (\$12) = \$48$.

Para no recurrir a ejemplos cada vez, es necesario abstraer y demostrar cada resultado de una manera general. Al tomar dos rectas con sus escalas correspondientes configuradas con enteros y que se cortan en el punto común O que se rotula para los dos ejes con el número cero y siendo que los enteros aparecen distribuidos en los dos ejes no necesariamente perpendiculares, es factible multiplicar números enteros geométricamente utilizando una regla, el concepto de triángulo y la noción de paralelismo.

Ejemplo:

Como se observa en la Figura 10, para hallar el producto 2×3 basta unir mediante un segmento el punto rotulado con 1 del eje y con el punto rotulado con 3 del eje horizontal y a continuación por el punto rotulado con 2 en el eje y se traza una paralela al primer segmento, tal paralela corta al eje x en un punto que equivale al producto 6.

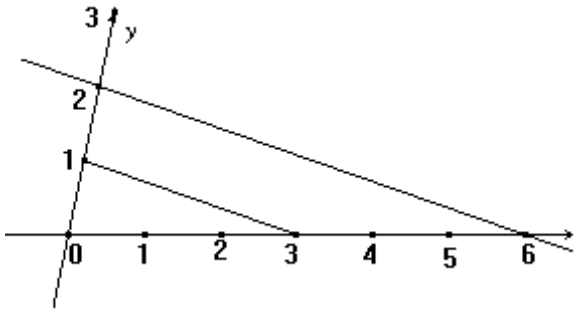

Figura 10. Representación del producto 2×3

Ejemplo:

En la Figura 11, se muestra el cálculo de los productos $(-2) \times 3$ y $(-2) \times (-3)$.

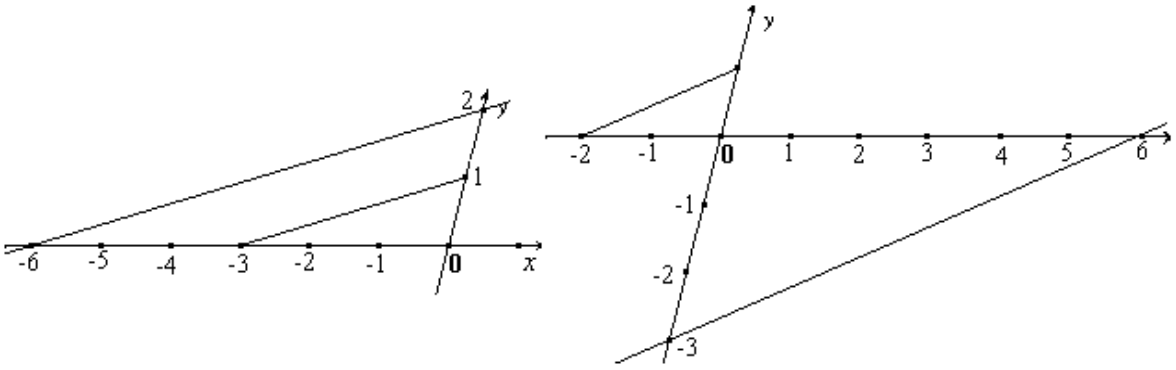

Figura 11. cálculo de los productos $(-2) \times 3$ *y* $(-2) \times (-3)$

Las operaciones de adición, sustracción y multiplicación, en este caso, se llaman operaciones enteras y se pueden realizar con regla y triángulo, como se ha evidenciado en los ejemplos anteriores.

Las operaciones de adición y multiplicación en $\mathbb{Z}$ satisfacen las siguientes propiedades:

Propiedades de la adición:

a) $(a + b) + c = a + (b + c), \forall a, b, c \in \mathbb{Z}$. $(\forall a, \forall b, \forall c \; en \; \mathbb{Z} \equiv \forall a, b, c \in \mathbb{Z})$.

b) $\exists \; 0 \in \mathbb{Z}$ tal que $a + 0 = 0 + a = a, \; \forall a \in \mathbb{Z}$, 0 es el neutro aditivo.

c) $\forall a \in \mathbb{Z}, \; \exists (-a) \in \mathbb{Z}$ tal que $a + (-a) = (-a) + a = 0, \; (-a)$ es inverso aditivo de a.

d) $a + b = b + a, \forall a, b \in \mathbb{Z}$.

Propiedades de la multiplicación:

a) $(a \times b) \times c = a \times (b \times c), \forall a, b, c \in \mathbb{Z}$.

b) $a \times 1 = 1 \times a = a, \forall a \in \mathbb{Z}; 1 \neq 0$.

c) $a \times b = b \times a, \; \forall a, b \in \mathbb{Z}$.

Propiedad distributiva:

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

1.9 Números racionales y densidad

En algunas actividades de la vida diaria para muchas personas no es suficiente saber contar ya que se requiere medir longitudes, calcular áreas, tomar tiempos, encontrar pesos, hacer conversiones de divisas, calcular husos horarios, fraccionar cantidades monetarias, hallar cifras equivalentes en diferentes sistemas de medida. Algunas magnitudes son susceptibles de subdivisiones tan pequeñas o tan grandes como se quiera: kilómetro, hectómetro, decámetro, metro, decímetro, centímetro, milímetro, micra; tonelada, kilogramo, libra, onza, gramo, miligramo; milenio, siglo, década, lustro, año, mes, día, hora, minuto, segundo. Estos ejemplos muestran cómo la unidad inicial se ha dividido en otras partes más pequeñas, ose ha multiplicado en otras más grandes, pero de manera convencional.

Es decir, si la unidad se divide en n partes, cada una mide $\frac{1}{n}$ y si se toma $m$de ellas, se encuentra $\frac{m}{n}$. Este símbolo se llama una fracción o una razón. Con el paso de los siglos, el símbolo $\frac{m}{n}$ fue desposeído de referencias concretas (medidas) y se consideró como un número cuando m y n son números enteros, con $n \neq 0$. El símbolo $\frac{m}{n}$ se llama número racional.

La *división* de enteros se toma como la operación inversa de la multiplicación y consiste en encontrar un número que multiplicado por el divisor reproduzca el dividendo:

$$a \div d = c \ \Leftrightarrow a = d \times c.$$

Por ejemplo: $12 \div 3 = 4 \ \Leftrightarrow \ 12 = 3 \times 4.$

Sin embargo, el cociente no siempre es entero; como se puede observar en los siguientes ejemplos: $2 \div 5,\ 3 \div 7,\ 4 \div 9, \ldots$

La división no siempre es posible en $\mathbb{Z}$ y es necesario extender el conjunto $\mathbb{Z}$ mediante la introducción de los inversos multiplicativos para elementos no nulos.

$$a \times a^{-1} = a^{-1} \times a = 1, \quad \forall a \neq 0 \in \mathbb{Z}.$$

Ejemplo:

$$2 \div 5 = 2 \times 5^{-1} = 2 \times \frac{1}{5} = \frac{2}{5}.$$

En efecto:

$$\frac{2}{5} \times 5 = 2 \times \left(\frac{5}{5}\right) = 2 \times (1) = 2.$$

Análogamente,

$$3 \div (-7) = 3 \times \left(-\frac{1}{7}\right) = -\frac{3}{7}.$$

De esta manera se construye el conjunto de los números racionales:

$$\mathbb{Q} = \left\{\frac{a}{b} / a, b \in \mathbb{Z},\ b \neq 0\right\}.$$

Hecho esto, es factible ampliar la escala métrica que se construyó para $\mathbb{Z}$ con el objeto de posibilitar la representación de cualquier número racional en un sistema coordenado. Como antes, se utiliza la regla, el triángulo y el concepto de paralelismo.

Ejemplo:

En la Figura 12, se ilustra el uso de la regla y el triángulo con la representación del racional $\frac{3}{5}$; en el eje E_1 se representa la unidad de medida y en el eje E_2 se representan las partes en las que se divide la unidad con un patrón de medida uniforme (en este caso cinco partes).

Se traza el segmento determinado por los puntos rotulados por E y 1, y por el punto C se traza una paralela que corta al eje E_1 en F y que corresponde al racional $\frac{3}{5}$.

Por su parte, en la Figura 13, el punto D representa al racional $\frac{2}{3}$ y se ha ubicado con los conceptos y procedimientos geométricos indicados.

Las operaciones de adición, sustracción, multiplicación y división exceptuando el cero, toman el nombre de operaciones racionales, puesto que son cerradas en el conjunto $\mathbb{Q}$.

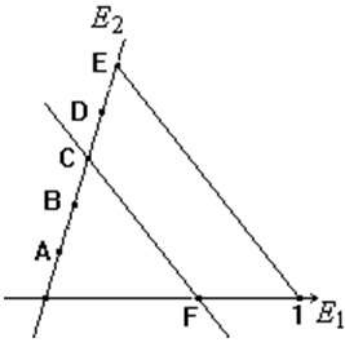

Figura 12. Representación del racional $\frac{3}{5}$ mediante uso de regla y triángulo

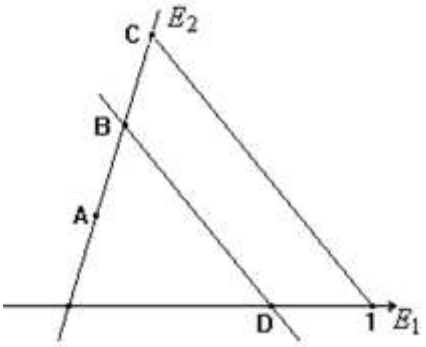

Figura 13. Representación del racional $\frac{2}{3}$ mediante uso de regla y triángulo

Propiedades de los racionales

$a)\ \frac{a}{b} = \frac{c}{d} \Leftrightarrow ad = bc$

$b)\ \frac{a}{b} \pm \frac{c}{d} = \frac{ad \pm bc}{bd}$; entonces $\frac{a}{b} + \frac{c}{b} = \frac{a+c}{b}$

$c)\ \frac{a}{b} \times \frac{c}{d} = \frac{ac}{bd}$

$d)\ \frac{a}{b} \div \frac{c}{d} = \frac{a}{b} \times \left(\frac{c}{d}\right)^{-1} = \frac{a}{b} \times \frac{d}{c} = \frac{ad}{bc}$

Bajo las condiciones indicadas, las operaciones de adición y multiplicación cubren el caso de los números enteros. Por tanto $(\mathbb{Q}, +,)$ forma un *anillo conmutativo con unidad*. Además, cada elemento no nulo, tiene inverso multiplicativo, con lo cual, $(\mathbb{Q}, +,)$ es un cuerpo. Cabe anotar que los términos *número racional* y *fracción racional*, son sinónimos y por tanto se pueden intercambiar. La palabra fracción indica cualquier expresión que tenga numerador y denominador, como $\frac{\sqrt{3}}{5}, \frac{5}{\sqrt{3}}, \frac{\sqrt{3}}{\sqrt{5}}$.

En consecuencia, una fracción no necesariamente representa a un número racional. Sin embargo, en algunos casos, es válido y posible transformar cualquier fracción a una fracción racional, en la cual, numerador y denominador sean enteros, con la condición que el denominador no sea nulo.

Ejemplos:

$$a)\ \frac{\sqrt{12}}{\sqrt{3}} = \frac{\sqrt{4\times 3}}{\sqrt{3}} = \frac{\sqrt{4}\times\sqrt{3}}{\sqrt{3}} = \frac{2}{1} \in \mathbb{Q}$$

$$b)\ \frac{\sqrt{15}}{\sqrt{3}} = \frac{\sqrt{5}\cdot\sqrt{3}}{\sqrt{3}} = \frac{\sqrt{5}}{1} \notin \mathbb{Q}$$

Las operaciones racionales también se pueden efectuar geométricamente, utilizando la regla y el triángulo, como una aplicación del Teorema de Tales (625 -546 a.C.). A manera de ejemplo se presenta el cálculo del cociente $\frac{2}{3} \div \frac{4}{5}$.

Para ello, se procede en concordancia con los pasos que se detallan en la Figura 14:

1. Se localiza $\frac{2}{3}$ sobre E_1 y $\frac{4}{5}$ en el eje E_2.
2. Se traza el segmento que une los puntos rotulados con los racionales anteriores.
3. Por el punto que representa a la unidad en E_2 se traza una paralela al segmento anterior.
4. La recta anterior corta al eje E_1 en el cociente $\frac{5}{6}$.

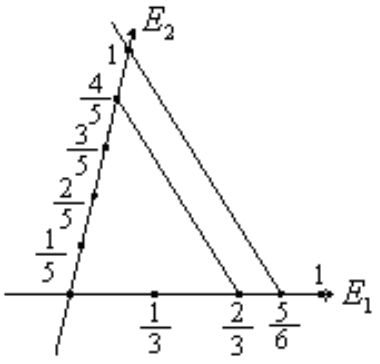

Figura 14. Aplicación del Teoema de Thalespara obtener el cociente $\frac{2}{3} \div \frac{4}{5}$

En efecto,

$$\frac{2}{3} \div \frac{4}{5} = \frac{2}{3} \times \left(\frac{4}{5}\right)^{-1} = \frac{2}{3} \times \frac{5}{4} = \frac{2}{3} \times \frac{5}{2 \times 2} = \frac{5}{6}.$$

1.9.1 Densidad

Dados dos números racionales a y b tales que $a < b$, siempre se encuentra otro número racional r tal que $a < r < b$. Entonces se dice que "r está entre a y b." Para esto, basta tomar su semisuma o promedio $a < \frac{a+b}{2} < b$ que, además es el punto medio de los puntos que representan a los racionales a y b.

Ahora, entre a y r está su semisuma $a < \frac{a+r}{2} < r$ y entre r y b también está su semisuma $r < \frac{b+r}{2} < b$, entre a y $\frac{a+r}{2}$ vuelve a quedar su semisuma $a < \frac{3a+r}{4} < \frac{a+r}{2}$ y también se encuentra que $\frac{b+r}{2} < \frac{3b+r}{4} < b$ y así sucesivamente.

Se hace evidente que, entre dos números racionales por cercanos o distantes que se encuentren, hay una infinidad de números racionales. Esto equivale a decir que el *conjunto de los números racionales es denso* con respecto a la relación "*menor que*" Dicho de otra manera, los puntos racionales se acumulan en todas partes de la recta, por tanto, toda magnitud medible se puede expresar mediante números racionales con cualquier grado de aproximación (densidad), sin importar el instrumento de medida que se utilice.

Esta característica de densidad, burla a los principiantes y a los neófitos respecto de la numerabilidad del conjunto, pues a simple vista parece que tuviese muchísimos más elementos que el conjunto de los naturales, sin sospechar siquiera que, por el contrario, estos dos conjuntos son coordinables, es decir, tienen la misma cantidad de elementos.

1.10 Números irracionales

A pesar de que la recta racional es densa, los números racionales no bastan para cubrir toda la línea recta. Para verificarlo, se puede realizar la división de m por n en el sistema decimal, encontrando inicialmente que, la expansión decimal de todo racional es periódica y que el periodo puede tener cualquier longitud. Pueden ocurrir dos casos:

a) Expansión decimal finita (residuo cero)

Por ejemplo:

$\frac{1}{2} = 0.5; \frac{3}{4} = 0.75; \frac{3}{8} = 0.375; \frac{5}{16} = 0.325.$

En este caso se dice que el período tiene longitud cero y está conformado por una cola infinita de ceros.

b) Expansión decimal infinita

Por ejemplo:

$\frac{5}{3} = 1.666\ldots = 1.\overline{6}; \frac{3}{11} = 0.2727\ldots = 0.\overline{27}.$
$\frac{31}{27} = 1.148148\ldots = 1.\overline{148}; \frac{23}{41} = 0.\overline{56097}.$
$\frac{12}{23} = 0.\overline{521739130434782608695 6}.$

La *periodicidad* en la expansión decimal infinita es exclusiva de los números racionales y puede contener cualquier longitud, lo cual es natural puesto que el racional $\frac{m}{n}$ indica la división de m por n, y de acuerdo con el algoritmo de la división, en cada paso existen n posibles residuos y por ello, a lo sumo, al cabo de n divisiones se encuentra un ciclo repetitivo. Al tener en la periodicidad un sello exclusivo de los números racionales, entonces, si se presenta un número cuya expansión decimal no sea periódica, es decir que sea aperiódica, este pertenece al conjunto de los números irracionales; su nombre se debe a que no son la razón entre dos enteros $\frac{m}{n}$.

Por ejemplo:

$\sqrt{2} = 1.414213562 \ldots$
$\sqrt{3} = 1.732050808 \ldots$
$\pi = 3.141592654 \ldots$
$\Phi = \frac{1+\sqrt{5}}{2} = 1.61803398875 \ldots$

Por ejemplo, $\pi = \frac{C}{D}$ es la razón entre la longitud de una circunferencia y su diámetro, donde C no puede ser un número entero, aunque D si lo sea. El conjunto de los números irracionales completa la representación de la recta numérica, y por increíble que parezca, en cantidad son muchísimos más

que el conjunto de los naturales y de los racionales. Sin embargo, y como se estudiará más adelante, algunos números irracionales expresados como fracciones continuas simples poseen período, cualidad que permite hacer un trabajo de ida y vuelta en este tipo de representación; es decir, dado un irracional se puede hallar la fracción continua simple y periódica que le corresponde y viceversa.

A continuación, se demuestra que $\sqrt{2}$ es irracional; este número fue el primer irracional que se descubrió y su aparición originó una crisis en la matemática de la antigua Grecia. La demostración de su irracionalidad sigue la técnica clásica de las demostraciones indirectas, en este caso por reducción al absurdo.

Sea OABun triángulo rectángulo isósceles de cateto 1, como se indica en la Figura 14.

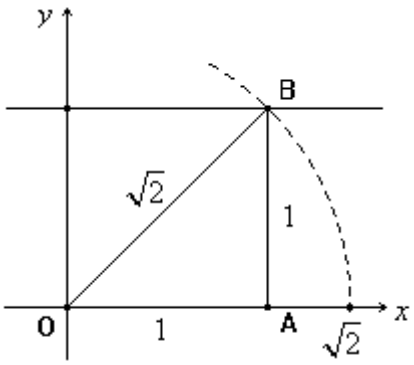

Figura 15. Representación del irracional $\sqrt{2}$

Por el Teorema de Pitágoras se tiene que:

$\overline{OA}^2 + \overline{AB}^2 = \overline{OB}^2$, así $\overline{OB}^2 = 1 + 1 = 2 \Rightarrow \overline{OB} = \sqrt{2}$

Como $1^2 = 1 < 2$ y $2^2 = 4 > 2 \Rightarrow \sqrt{2}$ está entre 1 y 2 y en consecuencia $\sqrt{2} \notin \mathbb{Z}$, quedando dos opciones, que $\sqrt{2} \in \mathbb{Q}$ o bien $\sqrt{2} \notin \mathbb{Q}$.

Al suponer que $\sqrt{2} \in \mathbb{Q}$; o sea $\sqrt{2} = \frac{a}{b}$ donde

Por el Teorema de Pitágoras se tiene que:

$$\overline{OA}^2 + \overline{AB}^2 = \overline{OB}^2$$
$$\overline{OB}^2 = 1 + 1 = 2 \Rightarrow \overline{OB} = \sqrt{2}$$

Como $1^2 = 1 < 2$ y $2^2 = 4 > 2 \Rightarrow \sqrt{2}$ está entre 1 y 2 y en consecuencia $\sqrt{2} \notin \mathbb{Z}$ quedando dos opciones, que $\sqrt{2} \in \mathbb{Q}$ o bien $\sqrt{2} \notin \mathbb{Q}$.

Supongamos que $\sqrt{2} \in \mathbb{Q}$; o sea $\sqrt{2} = \frac{a}{b}$ donde a, b están en $\mathbb{Z}$, $b \neq 1$, donde a y b no tienen factores en común, es decir, son primos relativos o primos entre sí, con lo cual, se conforma una fracción irreducible.

Al elevar al cuadrado se obtiene: $2 = \frac{a^2}{b^2} \Rightarrow a^2 = 2b^2 \quad (1)$

Esto significa que 2 es un divisor de a^2 y como 2 es un número primo, entonces, si $2|a^2 \Rightarrow 2|a \times a \Rightarrow 2|a$ y por lo tanto a es un número par, esto es $\exists k \in \mathbb{Z}$ tal que $a = 2k$. De aquí se sigue que $a^2 = 4k^2$ y al remplazar en la expresión (1) se obtiene que:

$4k^2 = 2b^2 \Rightarrow 2k^2 = b^2 \Rightarrow 2|b^2$, y siendo 2 un número primo, se tiene que:

$$2|b \times b \Rightarrow 2|b \text{ y por ello, } \exists t \in \mathbb{Z} \,/\, b = 2t.$$

Esto asegura que tanto a como b son múltiplos de 2, lo que contradice la condición inicial de que son irreducibles. Por lo tanto, el supuesto $\sqrt{2} = \frac{a}{b}$ es falso; es decir, $\sqrt{2}$ es irracional.

Por la misma vía (reducción al absurdo) se demuestra que $\sqrt{3}$ es irracional, al igual que la irracionalidad de muchos otros números.

Siendo $\sqrt{2}$ un número irracional se puede demostrar que son irracionales todos los términos de la siguiente secuencia:

$$\frac{\sqrt{2}}{2}, \frac{\sqrt{2}}{3}, \frac{\sqrt{2}}{4}, \frac{\sqrt{2}}{5}, \ldots \frac{\sqrt{2}}{n}, \ldots$$

Todos los números de la forma $\sqrt{n}$ con $n \in \mathbb{N}$, son construíbles con regla y compás, construcción que se fundamenta en un método auténticamente inductivo, ya que para tal efecto se debe tener construido el número $\sqrt{n-1}$, de modo que es suficiente construir un triángulo rectángulo con catetos de dimensión $\sqrt{n-1}$ y 1; la hipotenusa de este triángulo, en concordancia con el Teorema de Pitágoras, mide:

$$\sqrt{\left(\sqrt{n-1}\right)^2 + 1} = \sqrt{(n-1)+1} = \sqrt{n}.$$

Como consecuencia inmediata de este hecho; si $m \in \mathbb{N}$, todos los números de la forma $\frac{\sqrt{n}}{m}$ también son construibles; igual ocurre con otras formas diversas, como las siguientes:

$$m\sqrt{n}, \sqrt{m}+\sqrt{n}, \sqrt{m}-\sqrt{n}, \frac{\sqrt{n}}{\sqrt{m}}, \ldots$$

Si α es un número irracional y r es racional distinto de cero, las siguientes combinaciones y expresiones producen números irracionales:

$$\alpha + r;\ \alpha - r; r - \alpha; r \cdot \alpha;\ \frac{\alpha}{r};\ \frac{r}{\alpha}; -\alpha;\ \alpha^{-1}.$$

La demostración de este hecho se puede realizar por el método indirecto de reducción al absurdo.

Ejemplos:

a) Al suponer que $\alpha + r = r_1$ con $r_1 \in \mathbb{Q}$ se seguiría que $\alpha = r_1 - r$ y como $(r_1 - r) \in \mathbb{Q}$ se deduciría que α es racional, lo cual es contrario a la hipótesis de ser irracional. Como $\alpha \in \mathbb{Q}$ es imposible, se concluye que $\alpha + r$ es irracional.

b) Al suponer que $r \times \alpha$ sea racional, se tendría que $r \cdot \alpha = r_1, r_1 \in \mathbb{Q}$ y por tanto $\alpha = \frac{r_1}{r}$ con $r \neq 0$ y como $\frac{r_1}{r} \in \mathbb{Q} \Rightarrow \alpha \in \mathbb{Q}$ lo que es imposible; por ello el número $r \times \alpha$ es irracional.

c) Al suponer que $\frac{r}{\alpha} = r_1$ sea un racional, y siendo $r \neq 0$ y $\alpha \neq 0$, se tiene que $r_1 \neq 0$ y por ello $\alpha = \frac{r}{r_1} \in \mathbb{Q}$, lo que contraría a la hipótesis. Luego $\frac{r}{\alpha}$ es irracional.

1.11 Segmentos inconmensurables

Al científico griego Eudoxio, que vivió en el siglo IV a.C., se le atribuye la constitución de una teoría de intervalos inconmensurables que son cocientes entre magnitudes especiales como las longitudes de los segmentos, y que no se pueden representar por medio de la razón de dos enteros.

Esta teoría se expresa en el Libro V de los elementos de Euclides, que estudia la teoría de las magnitudes y de sus razones, y por ello la teoría de la inconmensurabilidad, siempre bajo forma geométrica; pues los griegos no habían concebido los números irracionales ni tenían un símbolo para expresar de manera adecuada al número $\sqrt{2}$. Estas razones fueron las que permitieron que toda la aritmética griega se desarrollara a través de la geometría; incluso, descubrieron métodos geométricos para resolver algunas clases de ecuaciones cuadráticas como las establecidas en el Libro

II de los Elementos de Euclides y que se recrean en el Apéndice 4 de este libro.

Dos segmentos a y b se llaman *conmensurables* cuando la longitud de uno es múltiplo de la longitud del otro. Así pues, si $b = \overline{AB}$ y $a = \overline{PQ}$, en la Figura 16 se evidencia que $b = 4a$ y en consecuencia a y b son conmensurables.

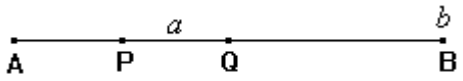

Figura 16. Segmentos conmensurables

En el caso en el que a no cupiese exactamente un determinado número de veces en b, se puede requerir de refinar la unidad de medida $\frac{a}{n} = u$. Si en b caben m de estas unidades, entonces $b = mu = \frac{m}{n}a$. En este caso a y b tienen una medida común. Cada punto de la división representa un número racional. En caso de que a y b no tengan la medida común, se dice que los dos *segmentos son inconmensurables*. Esto es lo que sucede, de manera particular, con la diagonal y el lado de cualquier cuadrado.

Es factible construir con regla y compás una infinitud de números irracionales como los de la secuencia $(\sqrt{n}) = \{\sqrt{1},\ \sqrt{2},\ \sqrt{3},\ \sqrt{4},\ \sqrt{5}, \ldots\}$ y los números de la lista $3\sqrt{2},\ 2\sqrt{3},\ \sqrt{2}+\sqrt{3},\ \frac{\sqrt{2}}{\sqrt{3}}, \ldots$ Pero también, otra infinitud de irracionales deja de ser construible, como es el caso de los trascendentes e y π, y en consecuencia, cualquier múltiplo de ellos ne o $n\pi$ o cualquier parte de la forma $\frac{e}{n}$ o $\frac{\pi}{n}$ donde n es un número natural.

Por tanto, es fácil construir tantos pares de segmentos inconmensurables tomando de manera arbitraria cualquier medida como unidad patrón.

El descubrimiento de los inconmensurables por los griegos (Eudoxio 408-335 a.C.) fue un acontecimiento de gran trascendencia científica que dejó profunda huella, tanto en la Matemática como en la Filosofía, pero que solo fue apreciada en toda su magnitud después de la segunda mitad del siglo XIX, cuando Dedekind, Frege, Cantor y Weirestrass construyeron una teoría rigurosa del número real.

Debido a la densidad de $\mathbb{Q}$, todo número irracional se puede aproximar mediante números racionales, con el grado de precisión que se quiera. Por ejemplo, en seguida se muestran aproximaciones por defecto y por exceso

del racional 2 y en consecuencia, al extraer raíz cuadrada a las partes, se obtiene una aproximación por exceso y por defecto del irracional $\sqrt{2}$.

$$1 = 1^2 < 2 < 2^2 = 4$$
$$1.96 = (1.4)^2 < 2 < (1.5)^2 = 2.25$$
$$1.9881 = (1.41)^2 < 2 < (1.42)^2 = 2.0164$$
$$1.999396 = (1.414)^2 < 2 < (1.415)^2 = 2.00225$$
$$1.99996164 = (1.4142)^2 < 2 < (1.4143)^2 = 2.00024449$$

Estas aproximaciones se consiguen por defecto y o por exceso en la parte entera, decimal, centesimal, milesimal, diezmilesimal, etc.

El sistema de los números racionales e irracionales se conoce con el nombre de *continuo numérico*.

1.12 Aproximaciones decimales

La notación decimal adoptada como un sistema formal de representación es fundamental y trascendente en el desarrollo de la historia de la matemática y en su tratamiento y, por ello, en su aprendizaje. La notación decimal y posicional hindú permitió la simplificación de procesos contables y el ejercicio de la actividad científica, como también la comparación entre los mismos números. En consecuencia, con algunos recursos técnicos es posible ordenar cualquier conjunto de números de menor a mayor o viceversa, siempre que estén expresados como decimales.

Todo número decimal infinito n, se puede expresar como una sucesión de números decimales finitos: $n_0,\ n_1,\ n_2,\ n_3,\ldots$ que representan sus aproximaciones decimales al entero, al décimo, al centésimo, ..., de manera que, si n tiene k dígitos antes del punto decimal, los primeros $k + h$ dígitos de las aproximaciones $n_h, n_{h+1}, n_{h+2},\ldots$ son los mismos.

Ejemplo:

Sea $n = 4\pi = 12.56637061$ entonces,

$n_0 = 12$
$n_1 = 12.5$
$n_2 = 12.56$
$n_3 = 12.566$
$n_4 = 12.5663$ ...

Los primeros $2 + 4$ dígitos de las demás aproximaciones $n_5,\ n_6,\ n_7,\ldots$ son los mismos del decimal finito 12.5663.

Para un decimal infinito como $0.9999\ldots = 0.\overline{9}$, donde todos sus dígitos a partir del segundo son iguales a 9, la sucesión de aproximaciones decimales queda de la forma $0, 0.9, 0.99, 0.999, 0.9999, \ldots$.

Por conveniencia, todo decimal infinito cuyos dígitos sean 9, a partir de uno se representa por un decimal finito redondeado. Por ejemplo:

$$0.\overline{9} = 1;\ 3.6\overline{9} = 3.7; -4.5\overline{9} = -4.6; 2.8\overline{9} = 2.99.$$

Con estas consideraciones, se dice que todo decimal infinito es un número real.

Ejemplo:

La siguiente lista presenta números reales, de los cuales, tres son racionales y los demás irracionales.

$$\frac{3}{4} = 0.75;\ \frac{7}{11} = 0.\overline{63};\ \frac{5}{6} = 0.8\overline{3};\ \sqrt{6} = 2.449489743;\ \frac{\sqrt{2}}{3} = 0.4714045207;$$
$$5.101001000100001\ldots$$

1.15 Números algebraicos y trascendentes

Hasta aquí se ha considerado a los números reales como la unión de los racionales con los irracionales y a los complejos, como pares ordenados de números reales. Una clasificación más reciente separa a los números reales en dos categorías: Algebraicos y Trascendentes.

Un número real x cualquiera, se llama *algebraico* si satisface una ecuación algebraica con coeficientes enteros o racionales, de la forma:

$$a_0 + a_1x + a_2x^2 + \ldots + a_nx^n = 0;\ n \geq 1,\ a_i \in \mathbb{Z},\ a_n \neq 0.$$

Si el número x no satisface una ecuación polinómica con coeficientes racionales, se llama trascendente (más allá de...). Entre estos números se encuentran los famosos irracionales π y e de los cuales se presentan sendos ensayos en el capítulo 5.

Como se observa, el concepto de número algebraico es la generalización del concepto de número racional para el caso en que el grado del polinomio sea 1 $(n = 1)$; $\sqrt{2}$ es algebraico porque satisface la ecuación $x^2 - 2 = 0$; $\sqrt[3]{3}$ es algebraico porque satisface la ecuación $x^3 - 3 = 0$.

Vale la pena advertir que, mientras todo número irracional algebraico x (con expansión decimal infinita periódica) se puede aproximar mediante una

sucesión de números racionales, como la que se indica enseguida, cuyos denominadores son crecientes, es imposible hacer lo mismo con los números trascendentes, debido a que, para ellos, en algún paso se encuentra que $\left|x-\frac{a}{b}\right| > \frac{1}{b^{n+1}}$ desde algún n en adelante.

$$x: \frac{a_0}{b_0}, \frac{a_1}{b_1}, \frac{a_2}{b_2}, \frac{a_3}{b_3}, \ldots, \frac{a_k}{b_k}, \ldots$$

1.13 Sucesiones convergentes

Se ha dicho que todo número decimal infinito puede aproximarse con cualquier grado de precisión, mediante una sucesión de números racionales. Por ejemplo, al tomar un intervalo de longitud 1, dividirlo en dos partes iguales y de ellas tomar la parte de la izquierda; la segunda mitad se vuelve a dividir en dos partes iguales y de ella, nuevamente se toma la mitad izquierda, y proceder reiteradamente de esta manera hasta obtener una subdivisión de longitud $\frac{1}{2^n}$, con n lo suficientemente grande ($n = 100$, $n = 1000, \ldots$), como lo sugiere la Figura 17, y sumar la longitud de los intervalos, se genera la serie:

$$S_n = \frac{1}{2} + \frac{1}{4} + \frac{1}{8} + \frac{1}{16} + \ldots + \frac{1}{2^n} \qquad (1)$$

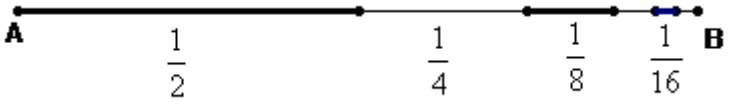

Figura 17

S_n difiere de 1 en $\frac{1}{2^n}$, diferencia que puede hacerse tan pequeña como se quiera con tan solo hacer crecer n de forma progresiva o indefinidamente. Pero esta diferencia jamás es cero. Es decir, la suma tiende a 1 cuando n tiende a infinito; por lo cual, no es erróneo escribir que:

$$1 = \frac{1}{2} + \frac{1}{2^2} + \frac{1}{2^3} + \frac{1}{2^4} + \frac{1}{2^5} + \cdots$$

Utilizando simbología matemática, se escribe de manera sintética que $S_n \to 1$ cuando $n \to \infty$, o lo que es lo mismo: $\lim_{n\to\infty} S_n = 1$. En este caso, se dice que la sucesión S_n converge a 1.

Ejemplo:

Sea $-1 < a < 1$ y las potencias sucesivas de a:

$$a,\ a^2,\ a^3,\ a^4, \ldots,\ a^n, \ldots$$

Cuando n crece sin límite, $\{a_n\}$ tiende a cero. Si $a < 0$, el signo de a^n cambia alternadamente de negativo a positivo, de manera tal que a^n se acerca a cero por izquierda y por derecha. Por ejemplo, se puede examinar el caso particular de $a = -\frac{1}{2}$, obteniendo los siguientes valores con sus potencias:

$$a^2 = \left(-\frac{1}{2}\right)^2 = \frac{1}{4}; a^3 = \left(-\frac{1}{2}\right)^3 = -\frac{1}{8}; a^4 = \left(-\frac{1}{2}\right)^4 = \frac{1}{16}; a^5 = \left(-\frac{1}{2}\right)^5 = -\frac{1}{32}; \ldots$$

En este caso se escribe que, $\lim_{n\to\infty}\left(-\frac{1}{2}\right)^n = 0$.

Observe que, si $|a| > 1$, los valores de la sucesión $\{a^n\}$ crecen indefinidamente.

Ejemplo:

Sea la progresión geométrica:

$$S_n = 1 + r + r^2 + r^3 + \cdots + r^n.$$

Para expresarla en forma más compacta, cada término de la igualdad se multiplica por la razón $r \neq 0$:

$$rS_n = r + r^2 + r^3 + r^4 + \cdots + r^{n+1}$$

Se obtiene que $S_n - rS_n = 1 - r^{n+1}$ y de aquí, $S_n = \frac{1-r^{n+1}}{1-r} = \frac{1}{1-r} - \frac{r^{n+1}}{1-r}$ de manera que,

$$\lim_{n\to\infty} S_n = \frac{1}{1-r}; -1 < r < 1.$$

En este caso, se puede escribir $1 + r + r^2 + r^3 + r^4 + \cdots = \frac{1}{1-r}$, resultado al que se llega por división algebraica.

Como un ejemplo del resultado anterior, se puede tomar $r = \frac{1}{2}$, con lo cual se obtiene:

$$1 + \frac{1}{2} + \frac{1}{2^2} + \frac{1}{2^3} + \frac{1}{2^4} + \cdots = \frac{1}{1 - \frac{1}{2}} = 2.$$

En el caso en que $r = \frac{1}{10}$ se tiene que:

$$1 + \frac{1}{10} + \frac{1}{10^2} + \frac{1}{10^3} + \frac{1}{10^4} + \cdots = \frac{1}{1 - \frac{1}{10}} = \frac{10}{9}.$$

Por lo tanto,

$$\frac{9}{10} + \frac{9}{10^2} + \frac{9}{10^3} + \frac{9}{10^4} + \cdots = 0.99999 \ldots = 1.$$

Con base en la definición de número real y en la de sucesión convergente, se puede definir las operaciones fundamentales en $\mathbb{R}$. Para realizar esta tarea se procede como se detalla en seguida.

Sean a y b dos números reales, escritos como sigue:

$$a = a_0, a_1, a_2, a_3, \ldots$$
$$b = b_0, b_1, b_2, b_3, \ldots$$

Entonces, las siguientes sucesiones de números reales son convergentes y se llaman suma, diferencia y producto, respectivamente:

$$a + b = a_0 + b_0, a_1 + b_1, a_2 + b_2 \ldots$$
$$a - b = a_0 - b_0, a_1 - b_1, a_2 - b_2, \ldots$$
$$a \times b = a_0 \times b_0, a_1 \times b_1, a_2 \times b_2, \ldots$$

Para la división, el divisor en cada caso, debe ser un número real distinto de cero; es decir, sus aproximaciones decimales son no nulas a partir de una de ellas.

Por ejemplo: si $b = 0.007$ se tiene que:

$$b_0 = 0;\ b_1 = 0.0;\ b_2 = 0.00; b_3 = 0.007 = b_4 = b_5 = \ldots = b_n = \cdots$$

entonces $b_n \neq 0, \forall n \geq 3$.

Es decir, en la sucesión $b: b_0, b_1, b_2, b_3, \ldots$ se puede suprimir un número finito de términos y la sucesión sigue siendo convergente al mismo límite b. Llamando tal sucesión $b: b'_0, b'_1, b'_2, b'_3, \ldots$ y por eso la sucesión de cocientes que sigue, es una sucesión convergente y se llama cociente de a entre b (a y $b$en $\mathbb{R}$, con $b \neq 0$):

$$\frac{a}{b}: \frac{a_0}{b'_0}, \frac{a_1}{b'_1}, \frac{a_2}{b'_2}, \frac{a_3}{b'_3}, \ldots$$

1.14 Números complejos

El álgebra elemental se ocupa de establecer de manera general la operatividad con los números y de resolver ecuaciones. El matemático francés François Viéte ((1540-1603) fue el primero en utilizar símbolos literales para representar las cantidades dando un salto cualitativo para utilizar este recurso en la solución y planteamiento de problemas; en este sentido, el álgebra se traduce como el lenguaje de la Matemática. El desarrollo del conocimiento algebraico inició en el antiguo Egipto y Babilonia, donde por el siglo VII a. C. fueron capaces de resolver ecuaciones lineales y cuadráticas, y calcular triadas pitagóricas; para ello utilizaban los métodos que se aplican actualmente.

Los matemáticos árabes del siglo X d. C. ampliaron el sistema indio de posiciones decimales en aritmética de números enteros, extendiéndolo a las fracciones decimales; fueron los gestores de la divulgación del sistema posicional que se utiliza hoy en día. En el siglo XII, el matemático persa Omar Jayyam generalizó los métodos indios de extracción de raíces cuadradas y cúbicas para calcular raíces cuartas, quintas y de grado superior. El matemático árabe Al-Jwārizmī, de cuyo nombre procede la palabra algoritmo, desarrolló el álgebra de los polinomios en su libro *Al-jabrwa'l Muqabalah*, de donde surge la palabra álgebra y por ello se considera el matemático más sobresaliente de Arabia en la época dorada de ese país (Acevedo & Falk, 1997).

La expresión Al-jabrwa'l Muqabalah significa restauración y equilibrio; entrega la idea básica de los procedimientos algebraicos puesto que para resolver una ecuación no solo se equilibran las partes, sino que al realizar una operación en uno de los lados de la igualdad, se restaura el equilibrio realizando la misma operación en el otro lado.

Se puede realizar un recorrido sucinto por cada uno de los conjuntos de números utilizando el legado de las ecuaciones propuesto por Al-Jwārizmī. Y de hecho, la ecuación $3x - 7 = 8$, utilizando el método de la restauración y el equilibrio, determina que $x = 5$; y se supondría que para solucionar cualquier ecuación de coeficientes naturales de la forma $ax + b = c$, es suficiente disponer del conjunto de los números naturales; lo cual es erróneo, puesto que la ecuación $3x + 14 = 2$ se traduce en una igualdad sólo si $x = -4$, con lo cual se requiere la utilización de los enteros negativos.

Con más prevención y al estudiar una ecuación como $3x + 1 = 9$ se admite que ni siquiera el conjunto de los enteros basta para resolver una ecuación lineal, y se amplía el conjunto de posibilidades al de los racionales. En el ejemplo, el número que soluciona la ecuación es $\frac{8}{3}$. Sin embargo, en general, las ecuaciones con las que se trabaja no sólo son lineales; el menor y más típico caso es el estudio de las ecuaciones cuadráticas de la forma $x^2 - n = 0$, donde n es un número natural. Una de las soluciones de este prototipo de ecuaciones es $x = \sqrt{n}$ y salvo pocas pero infinitas excepciones, los números de esta forma no son racionales. El primer número de esta forma, con el que se toparon los griegos, es $\sqrt{2}$ y causó estupor y extrañeza. La unión de todos los números racionales con los irracionales constituye el conjunto de los números reales.

Esta amplia colección de números aparenta ser suficiente para resolver cualquier ecuación lineal o cuadrática; sin embargo, al intentar encontrar la raíz de una ecuación cuadrática tan simple como $x^2 + 1 = 0$, se detecta que el conjunto de números reales no es suficiente y es imperativo construir el conjunto de los números complejos. En este nuevo conjunto la solución $\sqrt{-1}$ de la ecuación $x^2 + 1 = 0$ se denota por i y se llama la unidad imaginaria.

Este primer capítulo que presenta una revisión general de los diversos conjuntos de números, sigue este derrotero: utilizar la resolución de ecuaciones de primer y segundo grado como una estrategia que genera la ampliación de un conjunto de números en otro.

Se ha visto cómo, para poder restar, se ha pasado de $\mathbb{N}$ a $\mathbb{Z}$ y de $\mathbb{Z}$ se pasa a $\mathbb{Q}$, para que sea posible dividir y de este último conjunto se pasa a $\mathbb{R}$ para que sea factible resolver la ecuación de segundo grado $ax^2 + bx + c = 0$, con $a \neq 0$.

Las soluciones de esta ecuación se determinan con los siguientes pasos:

De $x^2+\frac{b}{a}x=-\frac{c}{a}$, se completa el cuadrado; $x^2+\frac{b}{a}x+\left(\frac{b}{2a}\right)^2=-\frac{c}{a}+\left(\frac{b}{2a}\right)^2=\frac{b^2-4ac}{4a^2}$ que se escribe como $\left(x+\frac{b}{2a}\right)^2=\frac{b^2-4ac}{4a^2}$ y al extraer raíz cuadrada a ambas partes se tiene $x+\frac{b}{2a}=\pm\sqrt{\frac{b^2-4ac}{4a^2}}$ de donde $x=\frac{-b\pm\sqrt{b^2-4ac}}{2a}$.

De la última expresión se sigue que $x\in\mathbb{R}\Leftrightarrow b^2-4ac\geq 0$, pero si ocurre que $b^2-4ac<0$, la solución no pertenece al conjunto de los números reales. De modo que, al intentar solucionar una ecuación de segundo grado: $ax^2+bx+c=0$ en la que $b^2-4ac<0$, (discriminante) se tiene dos alternativas:

a) Dejar la ecuación sin resolver.

b) Ampliar nuevamente el campo numérico.

Desde el punto de vista teórico es preferible la segunda opción, para lo cual se define la unidad imaginaria i de manera que $i^2=-1$. Esta unidad carece de sentido en $\mathbb{R}$, puesto que el cuadrado de cualquier número real jamás es negativo; en este sentido, no es válida la siguiente argumentación:

Si $i=\sqrt{-1}\Rightarrow i^2=\sqrt{-1}\times\sqrt{-1}=\sqrt{(-1)(-1)}=\sqrt{1}=1$ es decir $i^2=1$. Unido a esto hay que aseverar que expresiones como $\sqrt{-9},\sqrt{-27},log(-5)$ no existen en el conjunto de los números reales.

$$\sqrt{-9}=\sqrt{9(-1)}=\sqrt{9}\times\sqrt{-1}=\pm 3i.$$
$$\sqrt{-27}=\sqrt{9\times 3\times(-1)}=\sqrt{9}\times\sqrt{3}\times\sqrt{-1}=\pm 3\sqrt{3}\ i.$$

Los números de la forma $a+bi$ donde a y b son números reales e i es la unidad imaginaria, se llaman *números complejos* y determinan el siguiente conjunto:

$$\mathbb{C}=\{a+b\ i: a,b\ en\ \mathbb{R};\ i^2=-1\}.$$

Las operaciones de adición y multiplicación se desarrollan considerando los números complejos como binomios algebraicos comunes, y se definen así:

1) $a+bi=c+di\Leftrightarrow a=c, b=d$
2) $(a+bi)+(c+di)=(a+c)+(b+d)i$
3) $(a+bi)\times(c+di)=a(c+di)+bi(c+di)=ac+adi+bci+bdi^2$
$=(ac-bd)+(ad+bc)i$

Ejemplo:

Al resolver la ecuación $x^2 - 2x + 2 = 0$ se encuentra $x = \frac{2 \pm \sqrt{-4}}{2}$, de donde las raíces son $x_1 = 1 + i, x_2 = 1 - i$.

Se propone al lector que determine las raíces cúbicas de la unidad.

Para hallar el cociente de dos números complejos, basta multiplicar numerador y denominador por el conjugado del denominador, así:

$$\frac{a + bi}{c + di} = \frac{(a + bi)(c - di)}{(c + di)(c - di)} = \frac{ac + bd}{c^2 + d^2} + \frac{bc - ad}{c^2 + d^2} i$$

Bajo las definiciones de adición y multiplicación (junto con la división), la estructura $(\mathbb{C}, +, \times)$ es un cuerpo o campo y contiene como casos particulares a los cuerpos $(\mathbb{R}, +, \times)$ y $(\mathbb{Q}, +, \times)$. Sin embargo, los cuerpos $(\mathbb{R}, +, \times)$ y $(\mathbb{Q}, +, \times)$ son de mayor utilidad operatoria que $(\mathbb{C}, +, \times)$, debido a las propiedades operatorias que tienen. Por ejemplo, el cuerpo de los reales es ordenado, completo y satisface la propiedad arquimediana.

Desde el punto de vista geométrico, $\mathbb{C} = \mathbb{R} \times \mathbb{R}$ y se puede representar por todos los puntos del plano con referencia a dos escalas o ejes concurrentes. En este caso, se toman ejes perpendiculares, donde E_1 (eje x) es el eje de partes reales (a) y E_2 (eje y), es el eje de las partes imaginarias (b).

Con esta suposición, un número complejo $a + bi$ se interpreta como un par ordenado $(a,\ b)$ o como el vector anclado en el origen de coordenadas y con extremo final en el punto de componentes $(a,\ b)$.

Ejemplo:

Sean los siguientes números complejos:

$$P(2,3) \equiv 2 + 3i \equiv \overrightarrow{OP};\ Q(-3,2) \equiv -3 + 2i \equiv \overrightarrow{OQ}$$

Para sumar geométricamente los números complejos $a + bi$ con $c + di$, se aplica la suma de pares ordenadas o la ley del paralelogramo, tal como se indica en la Figura 18.

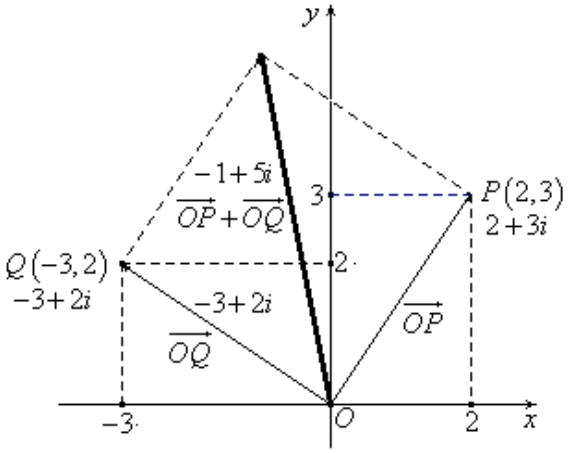

Figura 18. Suma de $2 + 3i$ *con* $-3 + 2i$

1.8 Estructuras de grupo, anillo y cuerpo

En el conjunto de los números enteros aparecen tres propiedades adicionales ligadas a las operaciones definidas anteriormente.

a. $a \times 0 = 0 \times a = 0, \forall a \in \mathbb{Z}$; propiedad llamada absorción del cero.

   En efecto, $a \times a = a \times a + 0 = a \times (a + 0) = a \times a + a \times 0$.

   Dado que $a \times a + 0 = a \times a + a \times 0$,entonces, $a \times 0 = 0$.

b. $a \times (-b) = (-a) \times b = -(a \times b), \forall a, b \in \mathbb{Z}$

c. $(-a) \times (-b) = a \times b, \forall a, b \in \mathbb{Z}$.

En efecto:

$$0 = 0 \times (-b) = [a + (-a)] \times (-b) = a(-b) + (-a)(-b) = -ab + (-a)(-b)$$
$$= -ab + ab.$$

En consecuencia, por igualación de términos se tiene que: $(-a)(-b) = a \times b$.

Si $a = d \times c$ en $\mathbb{Z}$, donde $a, d, c \in \mathbb{Z}$, entonces d es un divisor o factor de a.

Por ejemplo, $-18 = 2 \times (-9) = 3 \times (-6) = 6 \times (-3, \dots)$, entonces, $2, -3, 6, -9, \dots$ son factores o divisores de -18.

Si $p \in \mathbb{Z}$ tiene únicamente los siguientes cuatro divisores: $1,\ -1,\ p$ y $-p$, se tiene que p es primo en $\mathbb{Z}$ o que es un irreducible. Por esta razón, la lista conformada por $-3,\ 5,\ -7,\ 11,\ -13,\ -17,\ldots$ muestra algunos números primos de $\mathbb{Z}$.

Los números enteros, igual que los naturales, se pueden dividir en pares e impares:

$$2\mathbb{Z} = (2) = \{x \in \mathbb{Z}: x = 2k,\ \forall k \in \mathbb{Z}\} = \{0,\ \pm 2,\ \pm 4,\ \pm 6,\ldots\}.$$
$$I = \{x \in \mathbb{Z}: x = 2k + 1, \forall k \in \mathbb{Z}\} = \{\pm 1,\ \pm 3,\ \pm 5,\ \pm 7,\ldots\}.$$

El conjunto de los enteros pares es cerrado para las operaciones de adición y multiplicación.

En efecto: si a y b están en (2); $a = 2k_1$ y $b = 2k_2$ para algunos k_1 y k_2 en $\mathbb{Z}$; entonces,

$a + b = 2 \times (k_1 + k_2)$; por su parte, $a \times b = 2 \times (2 \times k_1 \times k_2)$.

El conjunto de los enteros impares es cerrado para la multiplicación pero no para la adición.

Si a y b son impares, entonces $a = 2k_1 + 1$ y $b = 2k_2 + 1$ para algunos k_1 y k_2 en $\mathbb{Z}$; entonces, $a + b = 2 \cdot (k_1 + k_2 + 1)$ que es un número par.

Por su parte, $a \times b = 2 \times (2k_1 \cdot k_2 + k_1 + k_2) + 1$ es impar.

De otra parte, el producto de un entero par y un impar es par, siendo la paridad una característica absorbente en la multiplicación.

CAPÍTULO 2.
LOS NÚMEROS NATURALES

Autor:
Oscar Fernando Soto Ágreda[3]

La matemática actual se desarrolla con base en los sistemas axiomáticos, los cuales, por su carácter abstracto, hacen que las consideraciones particulares se enmarquen dentro de las demostraciones generales y universales que utilizan los modos de argumentación aristotélicos. El conocimiento científico se alcanza cuando las proposiciones se estructuran de manera sistemática, dejando en claro sus relaciones. Algunas proposiciones se consideran como conceptos primitivos de naturaleza arbitraria y aceptadas sin demostración ni definición, pero susceptibles de poseer alguna interpretación. En el caso del modelo euclidiano de la Geometría, los términos línea y punto son primitivos y suelen asociarse al significado de club y socio cuando requieren de interpretación. Otras, se deducen a partir de los conceptos primitivos sometidos a determinadas condiciones (axiomas, postulados). Por tanto, un sistema deductivo empieza con términos primitivos (que se aceptan sin discusión, como el lenguaje) y unas suposiciones acerca de ellas que determinan las relaciones básicas del sistema y que suelen llamarse términos derivados y luego el sistema, tomando como mediador y motor de inferencia a la lógica, demuestra proposiciones o deriva conclusiones a las que llama teoremas. Es posible que dentro del sistema, por la vía de la intuición o la inducción natural establezca premonitoriamente hechos que de no ser demostrados alcanzan la estatura de conjeturas. Ese todo compacto y carente de contradicciones es lo que se llama teoría del sistema (conjuntos, números, relaciones, funciones, ecuaciones, polinomios, matrices, límites, derivadas, integrales, ...).

Cuando se remplazan los términos primitivos por variables concretas, se tiene la interpretación real del sistema y según el caso que se considere, resultan diferentes Modelos Matemáticos que, en el mejor de los casos, se pueden aplicar en otras ciencias o ramas del conocimiento como la Física, la Biología, las Ciencias Sociales, la Economía, entre otras.

[3] Profesor Adscrito al Departamento de Matemáticas y Estadística, Universidad de Nariño.

2.1 Los axiomas

Desde Euclides hasta el siglo XIX, se consideró al Axioma como una verdad evidente en sí misma y con este concepto se construyó cualquier teoría deductiva. Al decir que es evidente en sí misma se manifiesta que el Axioma no se ha establecido empíricamente, sino como una propiedad del pensamiento mismo. Cuando Euclides organizó la Geometría como sistema deductivo enunció unos axiomas como fundamento del sistema que aparecen como diez nociones comunes que son relativamente válidas en cualquier ciencia y cinco postulados que se refieren a la Geometría en particular; con ellos y con el apoyo de la lógica aristotélica, construyó su tratado de Geometría y Aritmética al que llamó Elementos. Aparte de ello dispuso veintitrés definiciones para delimitar los objetos sobre los que iba a determinar sus conclusiones.

Con el objeto de establecer diferencias con el conjunto axiomático que se presentará para la Aritmética, se presenta este conjunto básico y también el euclidiano para la Geometría.

Del Libro I de los Elementos de Euclides, se tiene:

Definiciones (Términos Primitivos y Derivados)

Este libro introduce 23 términos técnicos entre fundamentales y derivados, a saber:

I. Punto, es aquello que no tiene partes.

II. Línea, es longitud sin ancho.

III. Las extremidades de una línea son puntos.

IV. Línea recta, es una línea que se halla igualmente dispuesta con respecto a todos sus puntos.

V. Superficie, es lo que posee longitud y ancho.

VI. Las extremidades de una superficie son líneas.

VII. Superficie plana, es una superficie que se halla igualmente dispuesta con respecto a todas sus líneas rectas.

VIII. Ángulo plano, es la inclinación mutua de dos líneas planas que se cruzan y no se hallan sobre una misma línea recta.

IX. Cuando las líneas que determinan el ángulo son rectas, el ángulo se dice rectilíneo.

X. Cuando la línea recta que cruza otra línea recta forma ángulos contiguos (adyacentes) iguales, cada ángulo se dice recto y las líneas rectas que se cruzan se dicen perpendiculares.

XI. Un ángulo obtuso, es un ángulo mayor que un ángulo recto.

XII. Un ángulo agudo, es un ángulo menor que un ángulo recto.

XIII. Confín, es lo que es extremidad de una cosa.

XIV. Figura es todo lo que tiene confín.

XV. Círculo, es una figura plana delimitada por una línea tal que todos los segmentos que salen de ella hasta un mismo punto interno al círculo resultan iguales.

XVI. Y el punto, se llama centro del círculo.

XVII. Diámetro del círculo, es cualquier segmento que pasa por el centro y termina en ambos sentidos sobre la frontera (circunferencia) del círculo y divide por mitad al círculo.

XVIII. Semicírculo, es una figura delimitada por un diámetro y una circunferencia cortada por el diámetro.

XIX. Figuras rectilíneas (polígonos), son figuras delimitadas por segmentos, siendo las figuras trilaterales delimitadas por tres segmentos, cuadrilaterales las delimitadas por cuatro segmentos y las multilaterales, delimitadas por más de cuatro segmentos.

XX. De las figuras trilaterales, un triángulo equilátero es el que tiene los tres lados iguales, un triángulo isósceles es que tiene dos lados iguales y un triángulo escaleno el que tiene los tres lados desiguales.

XXI. De las figuras trilaterales, un triángulo rectángulo es el que tiene un ángulo recto, un triángulo obtusángulo el que tiene un ángulo obtuso y un triángulo acutángulo el que tiene los tres ángulos agudos.

XXII. De las figuras cuadrilaterales, un cuadrado es el que tiene los lados iguales y los ángulos rectos; un oblongo (rectángulo), el que tiene los ángulos rectos pero los lados no iguales; un rombo, el que tiene los lados iguales pero los ángulos no rectos; y un romboide (paralelogramo), el que tiene los lados y los ángulos opuestos iguales entre sí pero no todos los lados iguales y los ángulos rectos. Y las demás figuras cuadrilaterales se llaman trapezoides.

XXIII. Se dicen paralelas las líneas rectas que perteneciendo al mismo plano, si prolongadas en ambos sentidos, nunca se cruzan.

Postulados

Euclides postula que es posible:

I. Poder trazar una línea recta de un punto a otro punto.

II. Y que cada línea recta se pueda prolongar indefinidamente por derecho.

III. Y que se pueda trazar una circunferencia con centro en todo punto y con distancia todo segmento.

IV. Y que todos los ángulos rectos son iguales entre sí.

V. Y si dos líneas rectas forman con una transversal ángulos internos que de una misma parte suman menos de dos rectos, entonces las rectas, si son suficientemente prolongadas, se cruzan de aquella parte.

Algunas nociones comunes o Axiomas

I. Cosas iguales a una misma cosa son iguales entre sí.

II. Y si a cosas iguales se agregan cosas iguales, se consiguen cosas iguales.

III. Y si de cosas iguales se quitan cosas iguales, se consiguen cosas iguales.

IV. Y si a cosas desiguales se agregan cosas iguales, se consiguen cosas desiguales.

V. Y dobles de una misma cosa son iguales.

VI. Y mitades de una misma cosa son iguales.

VII. Y cosas que pueden sobreponerse con coincidencia una a otra son iguales.

VIII. Y el todo es más grande que la parte.

El postulado V o de las paralelas dio lugar a mucha controversia y discusión, debido a que no era tan evidente como los demás. Algunos pensaron que se podía demostrar como un teorema y trataron de reemplazarlo por otro enunciado. Para sorpresa de todos, lo único que se alcanzó fue a reafirmar la concepción de Euclides y la creación de las nuevas Geometrías (Elíptica e Hiperbólica) consistentes internamente, pero inconsistente cada una con respecto de la otra. La conclusión obtenida de toda esta discusión es que los axiomas del sistema son independientes y pueden sustituirse o modificarse para obtener nuevos sistemas axiomáticos. El origen de los nuevos modelos geométricos y que se llaman no euclidianos, parte de las formas de negación que admite el quinto postulado; esto es, que por un punto exterior a una recta no se pueda trazar paralela alguna o que, de otra forma, sea posible trazar más de una paralela.

Desde los sistemas numéricos estudiados $\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}$ y $\mathbb{C}$, se inició la construcción de nuevas estructuras algebraicas, según las propiedades (axiomas) que cumplan las respectivas operaciones. Se obtuvo las estructuras de Grupo, Anillo, Dominio de Integridad, Cuerpo. El método axiomático que inicialmente se desarrolló en la Geometría se introdujo en el Álgebra, haciendo que todas las estructuras matemáticas tengan carácter axiomático y posteriormente abarcando otras ramas del saber.

Pero, ¿cómo se distingue una estructura algebraica de una geométrica dentro de los sistemas matemáticos abstractos? La estructura algebraica se caracteriza por una o más operaciones que cumplen determinadas condiciones (Axiomas); por su parte, la estructura geométrica se caracteriza por una clase particular de subconjuntos que cumplen determinadas

condiciones (Axiomas). Actualmente, existen sistemas matemáticos provistos de estructura algebraica y geométrica (Álgebra Topológica, Geometría Algebraica) y por tanto hay una mezcla de métodos para su estudio.

2.2 El Sistema axiomático de Peano

El matemático italiano Giuseppe Peano (1858-1932), nació en Cuneo, fue profesor en la Academia Militar de Turín; construyó un sistema descriptivo que permitía enunciar cualquier proposición de lógica o de matemáticas sin recurrir al lenguaje. Fue fundador de dos publicaciones de matemáticas y, justamente en una de ellas, *Arithmetices Principia Nova Exposita* publicada en 1889, y desconociendo los resultados propuestos por Dedekind en una época proclive a la axiomatización de las teorías matemáticas, hizo una exposición axiomática y deductiva de la aritmética de los números naturales, la cual se estudia en este capítulo (Saldarriaga, 2013).

En este mismo capítulo se revisa el aporte de gran afinidad elaborado por el lógico americano Charles Sanders Peirce una década antes del presentado por Peano. Quizás, el del americano no trascendió, pues la mayoría de su obra se publicó de manera póstuma, tal vez por el carácter caprichoso, rebelde y desconfiado que siempre le acompañó.

Giuseppe Peano consideró el conjunto de los números naturales $\mathbb{N}$, formado por la sucesión de elementos $0, 1, 2, 3, 4, \ldots$ y los conceptos primitivos o términos no definidos de conjunto, número natural, sucesor y la relación *pertenecer a*.

En tal sentido, Peano definió:

1. Los elementos de $\mathbb{N}$ se llaman Números Naturales.
2. El elemento 0 de $\mathbb{N}$, se llama Cero.
3. La relación "Ser Sucesor de", establece que $a\,R\,b$ en $\mathbb{N}$ es equivalente a decir que "b es sucesor de a", y se denota por $b = suc(a) = a^*$.

Los conceptos primitivos se relacionan entre sí mediante los siguientes enunciados, llamados Axiomas de Peano:

P1. El elemento $0 \in \mathbb{N}$ (Establece que el conjunto de los naturales tiene al menos un elemento).

P2. $\forall a \in \mathbb{N}, \exists!\ a^* \in \mathbb{N}$ tal que $a^* = suc(a)$ (Cada número natural tiene sucesor único).

P3. $\forall a \in \mathbb{N}, a^* \neq 0$ (Cero es el primer elemento, o mejor, cero no tiene antecesor, o bien, cero no es el sucesor de ningún número).

P4. Si $a^* = b^*$ se implica que $a = b$, $\forall a,\ \forall b$ en $\mathbb{N}$ (Un número natural no puede ser sucesor de dos números diferentes).

P5. Si $A \subseteq \mathbb{N}$ y se cumple que:

a) $0 \in A$

b) Y si de $a \in A$ se sigue que $a^* \in A$, entonces $A = \mathbb{N}$ (A partir de un primer elemento se obtiene todo el conjunto de los números naturales; este axioma se llama de Recurrencia).

Este quinto Axioma, asevera que si $0 \in A$, siendo A un conjunto arbitrario, y si cada que un natural pertenece a A, se tiene que su sucesor pertenece a A, entonces todos los números naturales pertenecen a A.

Para elaborar las deducciones que parecen condensadas en estos cinco axiomas, Peano también adoptó como instrumento de deducción la relación de equivalencia denominada *igualdad* y que goza de las propiedades de reflexividad, es decir $a = a$; simetría, si $a = b$ se sigue que $b = a$; y transitividad, si $a = b$ y a la vez $b = c$, entonces $a = c$.

El último Axioma puede entenderse de la siguiente manera: un conjunto de números naturales al que pertenece el primer elemento y el sucesor de cada uno de sus elementos, es la totalidad de ellos, lo cual deriva en el método de inducción que es un método de razonamiento constructivo, y consiste en definir el enunciado p para $n = 0$ y luego generalizar el procedimiento para construir $p(n + 1)$ a partir de $p(n)$.

2.3 Método de inducción completa

El Axioma P_5, llamado *Axioma de Recurrencia* o *de Inducción Completa*, se utiliza como método de definición y de demostración. En realidad, es una de las herramientas más poderosas de la matemática, comparable por

analogía con una cadena infinita de fichas de dominó tal que, con solo empujar la primera de ellas caen todas las fichas, pero si no se empuja la primera no cae ninguna, o si falta alguna, a partir de ella no cae ninguna más.

A continuación, se enuncian y demuestran dos teoremas que sintetizan el método demostrativo de inducción completa.

Teorema 1

Sea p una proposición que depende de un número natural n, $p(n)$.

Si se cumple que:

i. $p(0)$ es verdadera; y

ii. de $p(k)$ se sigue $p(k+1)$, $\forall\, k \in \mathbb{N}$, entonces, la proposición p es válida $\forall n \in \mathbb{N}$.

Demostración

Basta aplicar el Axioma P_5 al conjunto:

$$A = \{k \in \mathbb{N}: p(k)\ es\ verdadera\}$$

Según las hipótesis $i)$ y $ii)$, $A \neq \emptyset$ ya que $0 \in A$ y $A \subseteq \mathbb{N}$. Por tanto A cumple las condiciones del quinto Axioma de Peano. Así que, $A = \mathbb{N}$. Luego p es verdadera $\forall n \in \mathbb{N}$. Es decir, vale $p(n)$ para cualquier valor de n en $\mathbb{N}$.

Teorema 2

Sea p una proposición que depende de un número natural $n: p(n)$. Si para un determinado número natural n_0, se cumple que:

i. $p(n_0)$ es verdadera; y

ii. $p(k) \Rightarrow p(k+1), \forall\, k \geq n_0, k \in \mathbb{N}$, entonces, $p(n)$ es válida, $\forall\, n \geq n_0, n \in \mathbb{N}$.

Demostración

Se define una proposición q tal que,

$$q(k) = \begin{cases} k\ si\ k < n_0, \forall\, k \in \mathbb{N} \\ p(k)\ si\ k \geq n_0 \end{cases}$$

Es decir, $q(k)$ es la función identidad $\forall k < n_0$ y $q(k)$ coincide con $p(k)$, $\forall\, k \geq n_0$. Según el Teorema 1, $q(k)$ es verdadera $\forall k \in \mathbb{N}$; por tanto, $p(k)$ es verdadera $\forall k \geq n_0$.

El teorema 2 aparece por la necesidad de restringir el dominio de veracidad de varias proposiciones a subconjuntos de números naturales.

Ejemplo 1

Demostrar que $2^n > n, \forall\, n \in \mathbb{N}$.

Solución

Sea p: $2^n > n$, entonces p depende de n.

i. $p(0)$ es verdadera porque $2^0 = 1$ y $1 > 0$.

ii. Sea $n_0 = 1 \Rightarrow p(n_0) = p(1)$ y es evidente que $2^1 > 1$.

iii. $\forall k > 1$, suponga que $2^k > k$. Multiplicando las dos partes de la desigualdad por 2, se encuentra que, $2 \times 2^k > 2k = k + k$ y como $k + k > k + 1, \forall\, k > 1$, entonces $2^{k+1} > k + 1$, $\forall\, k \geq 1$ y en consecuencia $2^n > n, \forall\, n \in \mathbb{N}$ en concordancia con el Teorema 2.

Ejemplo 2. La Torre De Hanoi

La Torre de Hanoi es un rompecabezas de origen antiguo divulgado por el matemático francés Édouard Lucas, el cual consiste de un tablero horizontal con tres clavos verticales. En uno de los clavos hay una serie de discos de diferentes tamaños, con radios cada vez más pequeños si se dirige la vista de abajo hacia arriba. El problema consiste en pasar todos los discos del clavo I al clavo III de la Figura 19, de tal manera que la disposición final sea igual a la del clavo I, procediendo según las dos reglas siguientes:

1. *Sólo se puede mover un disco cada vez.*
2. *Ningún disco puede quedar, en un movimiento, encima de otro que sea más pequeño que él.*

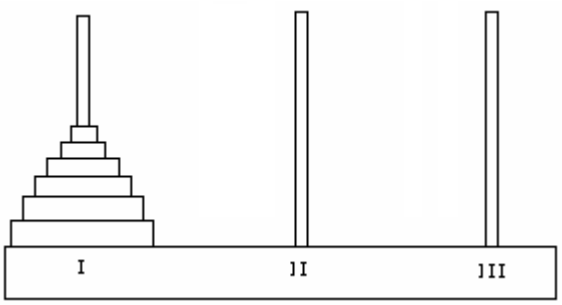

Figura 19. Torres de Hanoi

¿Cuál es el número mínimo de pasos que se requiere para resolver el acertijo si existe un número determinado *n* de discos en el clavo I? ¿Puede demostrar su conjetura?

W.W.R. Ball en su obra, *Mathematical Recreations and Essays,* páginas 285 y 286, describe el origen del juego de la siguiente manera:

> *"En el gran templo de Benares, bajo la cúpula que señala el centro del mundo, hay una bandeja de bronce con tres agujas de diamante, cada una de un codo de alta y del grosor del cuerpo de una abeja. En la creación, colocó Dios sesenta y cuatro discos de oro puro, el mayor de ellos inmediatamente encima de la bandeja de bronce y los demás, cada vez más pequeños, hacia arriba. Esta es la torre de Brahama. Día y noche, incesantemente, cambian los sacerdotes los discos de una a otra aguja de diamante de acuerdo con las leyes inmutables de Brahama, que especifican que el sacerdote en turno no ha de mover más que un disco a la vez, y que ha de colocarlo en otra de las agujas, de tal manera que no quede debajo de él ningún disco más pequeño. Cuando los sesenta y cuatro discos hayan sido transferidos desde la aguja en que los colocó Dios en la Creación, a otra de las agujas, se desharán en añicos la torre, el templo y los Brahamanes, y en medio de un trueno, el mundo dejará de existir."*

Para el caso de los sesenta y cuatro discos, se puede demostrar que el menor número de pasos requeridos es 18.446.744.073.709.551.615, es decir, algo más de diez y ocho trillones. Si los sacerdotes fueran capaces de abocar cada paso en un solo segundo, tal número sería equivalente a la cantidad de tiempo empleada en resolver el acertijo. Al dividir este número por sesenta, se obtiene el mismo tiempo en minutos; o sea 307.445.734.561.825.860 minutos. Al volver a dividir por 60 se tienen 5.124.095.576.030.431 horas. Al dividir por 24 se tienen

213.503.982.334.601 días. Al dividir por 365 se halla 533.759.955.836, que es el tiempo en años.

Los historiadores aseguran que la vigencia del hombre sobre la tierra data de hace quince mil millones de años. Al quitar esta cantidad de 533.759.955.836 se obtiene 518.759´.955.836 años, que con la fantástica velocidad de un paso por segundo se concluye que estos sacerdotes terminarán su trabajo dentro de 5.187´.599.558 siglos. ¡Cerca de cinco mil millones de siglos!

Después de algunos ensayos con diversa cantidad de discos, la intuición asegura que para n discos, el número mínimo de pasos para resolver el rompecabezas es $2^n - 1$ y en efecto, este hecho se demuestra por inducción completa, como sigue.

i. Se escribe $q(0) = 0$ y $q(n) = p(n)$, $\forall n \geq 1$; de este modo $q(0)$ es verdadera.

ii. Sea $n_0 = 1 \Rightarrow q(n_0) = q(1) = p(1)$, esto es $p(1) = 2^1 - 1 = 1$ y en efecto, se requiere de un solo paso para pasar un disco de la peonza I a la III.

iii. Al suponer que para k discos se requieren $2^k - 1$ pasos; esto es, que $q(k) = p(k)$ es cierta, basta demostrar que $q(k+1) = p(k+1) = 2^{k+1} - 1$ también es cierta; entonces, para $k+1$ discos se procede como sigue. Se pasan los k primeros discos de la peonza I a la II, lo cual, por suposición se realiza en $2^k - 1$ pasos; el disco más grande se pasa del clavo I al III en 1 paso (Parte ii) y los k discos que han permanecido en el clavo II se los traslada al III en otros $2^k - 1$ pasos; por ello, en total se han requerido de $2 \cdot (2^k - 1) + 1 = 2^{k+1} - 1$ pasos. Por lo tanto, $q(k+1)$ es verdadera y en consecuencia $p(n)$ es verdadera
$\forall n \in \mathbb{N}, n \geq 1$.

Ejemplo:

En lugar de definir la potencia n, $n \in \mathbb{N}$, de un real $a > 0$, como el producto de n factores, todos iguales con a, se utiliza recurrencia, así:

$$\begin{cases} a^0 = 1 \\ a^{n+1} = a^n \times a \end{cases}$$

De esta definición, por inducción se demuestra que:

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

Solución

i) Para $n = 0$, en virtud de la definición anterior se tiene:

$(a \times b)^0 = 1 = 1 \times 1 = a^0 \times b^0$

ii) La suposición de que la proposición es válida para $n = k$ conduce a asegurar como verdadero que $(a \cdot b)^k = a^k \cdot b^k$. Multiplicando por $a \cdot b$ los dos miembros de esta igualdad y aplicando las propiedades conmutativas y asociativas de la multiplicación se tiene:

$$(a \times b)^{k+1} = (a \times b)^k \times (a \times b) == (a^k \times b^k) \times (a \times b)$$

$$= (a^k \times a) \times (b^k \times b) = a^{k+1} \times b^{k+1}$$

Esto significa que $(a \times b)^n = a^n \times b^n$ es verdadera $\forall\, n \in \mathbb{N}$.

Ejemplo:

Demostrar que para todo número real $h > -1$ y todo número natural n se cumple que $(1 + h)^n \geq 1 + n \times h$.

Solución

i) Para $n = 0$ se cumple la proposición ya que ambos miembros son iguales a 1 y por lo tanto $1 \geq 1$.

ii) Al suponer que la proposición es cierta para $n = k$, es decir, que:

$(1 + h)^k \geq 1 + k \times h$ se debe probar que es verdadera para $n = k + 1$. Para ello se multiplica ambos miembros de la inecuación del supuesto, por el factor $1 + h$, obteniendo:

$$(1 + h)^k \times (1 + h) = (1 + h)^{k+1} \geq (1 + k \cdot h) \cdot (1 + h)$$
$$= 1 + kh + h + kh^2$$

y como $kh^2 \geq 0$, resulta que,

$(1 + h)^{k+1} \geq 1 + k \cdot h + h = 1 + (k + 1) \times h.$

En consecuencia, $(1+h)^n \geq 1+n\times h$ es verdadera $\forall n \in \mathbb{N}$.

2.4 Primeras consecuencias de los Axiomas de Peano

A partir de los cinco axiomas de Giuseppe Peano presentados en 1889, se pueden deducir todas las propiedades que satisfacen los números naturales y sus operaciones.

Teorema 3

Si $a \neq b$ en $\mathbb{N}$ entonces $a^* \neq b^*$, o lo que es lo mismo, $suc(a) \neq suc(b)$ o aún mejor, $a+1 \neq b+1$.

Demostración

Según la lógica matemática $p \Rightarrow q$ es equivalente con la proposición $\sim q \Rightarrow \sim p$. Así que $a^* = b^* \Rightarrow a = b, \forall a, \forall b \in \mathbb{N}$. Pero esto asegura el cumplimiento del axioma P_4. de Peano; luego $a \neq b$ en $\mathbb{N}$ implica que $a^* \neq b^*$.

Teorema 4

$a^* \neq a, \forall a \in \mathbb{N}$. Esto es, el sucesor de un número natural es distinto de él o mejor un número natural y su sucesor, jamás coinciden.

Demostración

Sea $A = \{k \in \mathbb{N}: k^* \neq k\}$; entonces,

$0 \in A$, porque $0 \in \mathbb{N}$ ($Axioma\ P_1$.) y $0^* \neq 0$ (Axioma P_3).

Si $k \in A \Rightarrow k \in \mathbb{N}$ y $k^* \neq k$.

Aplicando la parte ii del Teorema 1, se puede inferir que $(k^*)^* \neq k^*$ y por lo tanto,
$k^* \in A$. Por el axioma P_5, se tiene que $A = \mathbb{N}$.

En resumen, $a^* \neq a, \forall a \in \mathbb{N}$. I

Teorema 5

Si $a \neq 0$ en $\mathbb{N}$, entonces $\exists b \in \mathbb{N} \ni a = b^*$.

Demostración

Sea $A = \{0\} \cup \{k \in \mathbb{N}: k \neq 0\}$, entonces $A \subseteq \mathbb{N}$; y por ello,

i) $0 \in A$, por construcción de A.

ii) Sea $k \in A$ tal que $k \neq 0$. Como $k^* = k^*$, entonces k^* satisface el teorema con solo escribir $b = k$. Por tanto $k^* \in A$ y de acuerdo con el axioma P_5, se cumple que $A = \mathbb{N}$.

El elemento $b \in \mathbb{N}$ tal que $a = b^*$ es único, según el axioma P_4. Por tanto, la función $*: \mathbb{N} \to \mathbb{N} - \{0\}$ tal que $a \mapsto a^*$ es una función biyectiva. Si $a = b^*$, se afirma que b es el antecesor (predecesor) de a en $\mathbb{N}$.

Ahora ya se puede definir por recurrencia las dos operaciones de adición y multiplicación en $\mathbb{N}$ y estudiar sus propiedades.

2.5 Adición de números naturales

Si a un niño se le pide que sume 4 con 3, lo que hace es: $4 + 3 = \big((4 + 1) + 1\big) + 1$, es decir $4 + 3 = (5 + 1) + 1 = 6 + 1 = 7$. Se habla de un niño muy pequeño, que intuitivamente determina el sucesor de un número natural n, como $n^* = n + 1$, de manera que $n + 2 = (n + 1)^* = (n^*)^* = (n + 1) + 1$; de este modo, también es el caso que, $n + 3 = (n + 2)^* = \big((n + 1) + 1\big)^* = \big((n + 1) + 1\big) + 1$.

Con base en estas experiencias se define una función unívoca, llamada adición.

Definición:

Sobre el conjunto de los números naturales se define la ley de composición interna:

$$+: \mathbb{N} \times \mathbb{N} \to \mathbb{N} \;/\; (a, b) \mapsto a + b.$$

Ese único número natural $a + b$ se llama la suma de a y b, donde:

$(a, 0) \mapsto a + 0 = a.$

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

Cabe anotar que,

$$b^* + a = (b + a)^* = (a + b)^* = a + b^*.$$

i) $a = 0 \Rightarrow b^* + 0 = b^* = (0 + b)^* = 0 + b^*.$

ii) Al suponer que $b^* + k = (b + k)^* = (k + b)^* = k + b^*$ se encuentra que:

$b^* + k^* = b^* + (k + 1) = (b^* + k) + 1 = (k + b^*) + 1 = (k + 1) + b^* = k^* + b^*$ y en consecuencia, $a + b^* = (a + b)^* = b^* + a, \forall a, \ \forall b \in \mathbb{N}$.

Es decir, $a + b$ es el resultado de sumar b veces el número 1 al número natural a.

En adelante, las demostraciones por inducción completa se harán en tres pasos como se ha hecho en ejemplos anteriores.

2.6 El aporte de Charles Sanders Peirce

Charles Sanders Peirce (1839-1914), nació en Cambridge (Massachusetts), hijo del matemático Benjamin Peirce, profesor de la Universidad de Harvard. Desarrolló clases de Lógica y Filosofía en las universidades de Harvard y Johns Hopkins, entre 1864 y 1884. Desarrolló muchos trabajos y conjeturas, los cuales, en su mayoría se publicaron de manera póstuma. Entre los trabajos están 9 volúmenes de sus Collected Papers (Escritos reunidos, 1931-1938), donde se recogen más de 100.000 páginas de reseñas y ensayos editados en revistas. Desde 1867 se interesó por el sistema de lógica creado por George Boole y trabajó para la ampliación y transformación del Álgebra de Boole hasta 1885 (Los Sofistas, 2009).

En el estudio de la matemática, se atribuye a Giuseppe Peano el aporte de la axiomatización de los números naturales mediante su trabajo *Arithmetices Principia Nova Método Exposita*, publicado en 1889. Por su parte, Charles Sanders Peirce, también realizó un trabajo de axiomatización de la aritmética, anterior al de Peano. En este sentido, se conoce su trabajo *On de logic of Number* que se publicó en el *American Journal of Mathematics* en 1881 y fue reimpreso en *Collected Papers of Charles Sanders Peirce,* volumen 3.

Un poco en honor a este pensador majestuoso y gigante, en este texto se reescriben sus demostraciones, que corresponden a las propiedades que satisfacen la adición y la multiplicación respetando cada uno de sus pasos y argumentaciones.

Por $n + m$ se entiende, para el caso en que $n = 1$, que se trata del sucesor inmediato de m y, en los otros casos, el sucesor inmediato del número $n^* + m$, donde n es el antecesor inmediato n^*.

Las siguientes seis demostraciones fueron realizadas por Peirce:

1) Propiedad asociativa de la adición

Demostrar que, $(n + m) + p = n + (m + p)$, para cualquier terna n, m, p en $\mathbb{N}$.

Demostración

Primero, esto es verdadero para $n = 1$, porque $(1 + m) + p = 1 + (m + p)$, por la definición de adición en su literal ii.

Ahora debe probarse que si es cierto para $n = k$, también lo es para $n = k + 1$. Esto es: si $(k + m) + p = k + (m + p)$, entonces $\big((1 + k) + m\big) + p = (1 + k) + (m + p)$, pues:

$\big((1 + k) + m\big) + p$	
$= \big(1 + (k + m)\big) + p$	Por la definición de adición.
$= 1 + \big((k + m) + p\big)$	Por la definición de adición.
$= 1 + \big(k + (m + p)\big)$	Por hipótesis.
$= (1 + k) + (m + p)$	Por la definición de adición.

Por tanto $(n + m) + p = n + (m + p)$, $\forall n, \forall m, \forall p$ en $\mathbb{N}$.

2) Propiedad conmutativa de la adición

Demostrar que, $n + m = m + n, \forall n, \forall m$ en $\mathbb{N}$.

Demostración

Primero, esto es cierto para $n = 1$ y $m = 1$, siendo en este caso una identidad explícita. Segundo, si esto es verdadero para $n = k$ y $m = 1$,

entonces es verdadero para $n = 1 + k$ y $m = 1$; esto es, si $k + 1 = 1 + k$, entonces también es cierto que $(1 + k) + 1 = 1 + (1 + k)$, porque:

$(1 + k) + 1 = 1 + (k + 1)$	Por propiedad asociativa.
$=1 + (1 + k)$	Por hipótesis.

Así se ha probado que para todo natural n, $n + 1 = 1 + n$, o que $n + m = m + n$ para $m = 1$. Ahora se debe demostrar que, si esto es cierto para $m = k$, también es verdadero para $m = k + 1$; esto es, si $n + k = k + n$, entonces $n + (1 + k) = (1 + k) + n$. Ahora bien:

$n + (1 + k)$	
$= (n + 1) + k$	Por propiedad asociativa.
$= (1 + n) + k$	Como se acaba de probar.
$= 1 + (n + k)$	Por definición de adición.
$= 1 + (k + n)$	Por hipótesis.
$= (1 + k) + n$	Por definición de adición.

Con lo anterior se completa la prueba.

En la definición de multiplicación, y como se verá más adelante, se entiende por $n \times m$, en el caso $n = 1$, el número m; y en los otros casos, $m + n^* m$, donde n es el antecesor inmediato de n^*.

3) Propiedad distributiva de la multiplicación respecto a la adición

Demostrar que,

a) $(n + m)p = np + mp$.

b) $n(m + p) = nm + np$

Demostración

Caso a)

Primero, la igualdad es cierta para $n = 1$, pues,

$(1 + m)p$	
$= p + mp$	Por definición de multiplicación.
$= 1p + mp$	Por definición de multiplicación.

Segundo, si es cierto para $n = k$, es cierta para $n = 1 + k$; esto es, si se cumple que $(k + m)p = kp + mp$, también se cumple $\big((1 + k) + m\big)p = (1 + k)p + mp$, porque:

$\big((1 + k) + m\big)p$	
$= \big(1 + (k + m)\big)p$	Por definición de adición.
$= p + (k + m)p$	Por definición de multiplicación.
$= p + (kp + mp)$	Por hipótesis.
$= (p + kp) + mp$	Por propiedad asociativa de la adición.
$= (1 + k)p + mp$	Por definición de multiplicación. I

Caso b)

Se prueba que, $n(m + p) = nm + np$.

Demostración

Primero, la igualdad es verdadera para $n = 1$; porque,

$1(m + p)$	
$(m + p)$	Por definición de multiplicación.
$1m + 1p$	Por definición de multiplicación.

Segundo, si es verdadero para $n = k$, es verdadero para $n = 1 + k$; esto es; si $k(m + p) = km + kp$, entonces $(1 + k)(m + p) = (1 + k)m + (1 + k)p$, pues,

$(1 + k)(m + p)$	
$= (m + p) + k(m + p)$	Por definición de multiplicación.
$= (m + p) + (km + kp)$	Por hipótesis.
$= (m + km) + (p + kp)$	Por propiedades de la adición.
$= (1 + k)m + (1 + k)p$	Por definición de multiplicación. I

4) Propiedad asociativa de la multiplicación

Demostrar que, $(nm)p = n(mp)$ para cualquier tripleta de números naturales n, m, p.

Demostración

Primero, esto es verdadero para $n = 1$, porque,

$(1m)p$	
$= mp$	Por definición de multiplicación.
$= 1 \cdot mp$	Por definición de multiplicación.
$= 1 \cdot (mp)$	

Segundo, si es verdadero para $n = k$, es válido para $n = 1 + k$; esto es, si $(km)p = k(mp)$, entonces $\big((1 + k)m\big)p = (1 + k)(mp)$, porque,

$\big((1 + k)m\big)p$	
$= (m + km)p$	Por definición de multiplicación.
$= mp + (km)p$	Por propiedad distributiva.
$= mp + k(mp)$	Por hipótesis.
$(1 + k)(mp)$	Por definición de multiplicación. l

5) Propiedad conmutativa de la multiplicación

Probar que, $nm = mn$ para cualquier par de números naturales n, m.

Demostración

En primer lugar, se verifica que es verdadera para $m = 1$. Para tal fin, primero se evidencia su veracidad para $m = 1$ y $n = 1$; y enseguida que si es verdadero para $m = 1$ y $n = k$, también es verdadero para $m = 1$ y $n = 1 + k$.

Para $m = 1$ y $n = 1$ se encuentra una identidad explícita. El paso subsiguiente consiste en probar que si $k1 = 1k$, entonces $(1 + k)1 = 1(1 + k)$. Ahora bien,

$(1 + k)1$	
$= 1 + k1$	Por definición de multiplicación.
$= 1 + 1n$	Por hipótesis.
$= 1 + n$	Por definición de multiplicación.
$1(1 + n)$	Por definición de multiplicación.

Habiendo mostrado que la propiedad conmutativa es verdadera para $m = 1$, se procede a probar que, si es verdadera para $m = k$, también es verdadera para $m = k + 1$; esto es, que si $nk = kn$, entonces $n(1 + k) = (1 + k)n$. En efecto,

$(1 + k)n$	
$= n + kn$	Por definición de multiplicación.
$= n + nk$	Por hipótesis.
$= 1n + nk$	Por definición de multiplicación.
$= n1 + nk$	Como ya se probó.
$= n(1 + k)$	Por propiedad distributiva.

Todo lo demostrado hasta ahora se traslada de manera natural al conjunto de los números enteros que son infinitos en ambas direcciones, y donde la extensión del sucesor y del antecesor de un entero permite que, en ocasiones, este sea un número negativo. Para probar en este conjunto que $x + 0 = x$, sea x' el antecesor inmediato de x, entonces,

$x + 0$	
$= (1 + x') + 0$	Por definición de x'.
$= (1 + 0) + x'$	Por propiedades de la adición.
$= 1 + x'$	Por definición de cero.
$= x$	Por definición de x'.

Para demostrar que $x \cdot 0 = 0$, primero, en el caso $x = 1$, la proposición vale por la definición de multiplicación. Además, si es verdadera para $x = k$, también es verdadera para $x = 1 + k$, porque,

$(1 + k)0$	
$= 1 \cdot 0 + k \cdot 0$	Por propiedad distributiva.
$= 1 \cdot 0 + 0$	Por hipótesis.
$= 1 \cdot 0$	Por el último teorema.
$= 0$	Como antes.

Tercero, si la proposición es verdadera para $x = 1 + k$, entonces también es verdadera para $x = k$, porque, cambiando el orden de las transformaciones, se obtiene,

$$1 \cdot 0 + 0 = 1 \cdot 0 = 0 = (1 + k)0 = 1 \cdot 0 + k \cdot 0.$$

Por lo tanto, queda probado que $x \cdot 0 = 0$ para todo entero x.

Con la definición del entero opuesto o negativo de otro entero, y que es tal que, sumado con él, produce cero, se puede probar que $(-x)y = -(xy)$. Para ello se tiene,

$0 = x + (-x)$	Por definición de negativo.
$0 = 0y = \big(x + (-x)\big)y$	Por penúltima proposición.
$0 = xy + (-x)y$	Por propiedad distributiva.
$-(xy) = (-x)y$	Por definición de negativo. l

Hasta aquí, se han presentado algunas de las elaboraciones de Charles Sanders Peirce y que son, sin lugar a dudas, anteriores al tratado que sobre la axiomatización de la Aritmética presenta Giuseppe Peano. El texto retoma la discusión de la propuesta presentada por el ilustre italiano.

2.7 Otras propiedades de los números naturales en el modelo de Peano

La adición se definió como sigue:

$+: \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ tal que $(a, b) \mapsto a + b$.

El único número natural $a + b$ se llama la suma de a y b donde,

$(a, 0) \mapsto a + 0 = a$

$(a, b^*) \mapsto a + b^* = a^* + b = (a + b)^*, \forall a, \forall b \; en \; \mathbb{N}$

Cabe anotar que,

$$b^* + a = (b + a)^* = (a + b)^* = a + b^* = a^* + b = b + a^*.$$

i. Si $a = 0 \Rightarrow b^* + 0 = b^* = (0 + b)^* = 0 + b^*$

ii. Al suponer que $b^* + k = (b + k)^* = (k + b)^* = k + b^*$ se encuentra:

$b^* + k^* = b^* + (k + 1) = (b^* + k) + 1 = (k + b^*) + 1 = (k + 1) + b^* = k^* + b^*$ y en consecuencia, $\forall a, \forall b$ en $\mathbb{N}$ se tiene que $a + b^* = (a + b)^* = b^* + a$.

En concordancia con esto, se demuestran a continuación, las propiedades que satisface la adición.

A1. La Adición es Modulativa. O sea $a + 0 = a = 0 + a, \forall a \in \mathbb{N}$.

Demostración. $a + 0 = a, \forall a \in \mathbb{N}$, por la definición de adición. Falta demostrar que $0 + a = a$ y para ello, se aplica inducción sobre a, así:

i) Si $a = 0$, entonces $0 + 0 = 0$ es un resultado evidentemente verdadero.

ii) Se asume la verdad del enunciado para $a = k, \forall\, k \in \mathbb{N}$; es decir, se asume que $0 + k = k$ y en seguida se prueba que $0 + (k + 1) = k + 1$.

En efecto, al considerar el sucesor de k se tiene:

$0 + k^* = (0 + k)^* = k^*, \quad \forall\, k \in \mathbb{N}$ y como el enunciado (propiedad modulativa) es válido para k^*, entonces es válido $\forall a \in \mathbb{N}$; es decir $a + 0 = a, \quad \forall a \in \mathbb{N}$, como se quería demostrar. I

A2. La Adición es Asociativa. Esto es $(a + b) + c = a + (b + c); \forall\, a, \forall\, b, \forall\, c$ en $\mathbb{N}$.

Demostración. Para demostrar este hecho se aplica inducción sobre c.

i) Si $c = 0$ entonces $(a + b) + 0 = a + b = a + (b + 0)$, de acuerdo con A1.

ii) Se asume la validez del enunciado para cuando $c = k, k \in \mathbb{N}$; entonces
$(a + b) + k = a + (b + k)$ y se prueba que también se cumple cuando $c = k + 1$ al tomar el sucesor k^*. En efecto,

$(a + b) + k^* = [(a + b) + k]^* = [a + (b + k)]^*$ y por definición de adición, esto se puede escribir como $a + (b + k)^* = a + (b + k^*)$; luego el enunciado se cumple para todo $c \in \mathbb{N}$: es decir $(a + b) + c = a + (b + c); \forall\, a, \forall\, b, \forall\, c$ en $\mathbb{N}$.

A3. La Adición es Conmutativa. Es decir, $a + b = b + a, \forall\, a, \forall\, b$ en $\mathbb{N}$.

Demostración. Para demostrar este hecho se aplica inducción sobre b.

i) Si $b = 0 \Rightarrow a + 0 = a = 0 + a$, puesto que 0 es el módulo de la adición.

ii) Se supone la validez de la tesis para cuando $b = k, k \in \mathbb{N}$; es decir que $a + k = k + a, \forall\, a \in \mathbb{N}$ y se demuestra su validez para el sucesor.

En efecto, al tomar el sucesor de k se tiene que $a + k^* = (a + k)^*$ y por el supuesto, es igual a $(k + a)^* = k^* + a$ según la definición de la adición en los naturales.

Por tanto, el enunciado es válido $\forall\, b \in \mathbb{N}$, o sea $a + b = b + a, \forall\, a, \forall\, b$ en $\mathbb{N}$.

A4. Ley cancelativa de la adición. Si $a + c = b + c$, entonces es el caso que $a = b, \forall\, a, \forall\, b, \forall c$ en $\mathbb{N}$.

Demostración. En la demostración se aplica inducción sobre c.

i) Si $c = 0$ entonces, si $a + 0 = b + 0$ por propiedad modulativa se tiene de inmediato que $a = b$.

ii) Para $c = k$ se asume que de $a + k = b + k$ se implica $a = b$ y se demuestra que la cancelación permanece para el sucesor k^*. En efecto:

Si $a + k^* = b + k^*$ entonces $(a + k)^* = (b + k)^*$ por definición de adición.

Entonces $a + k = b + k$ por el axioma P_4, y de aquí, por el supuesto, se sigue que $a = b$.

En consecuencia, por el axioma P_5, el enunciado se cumple, es decir:

si $a + c = b + c$, entonces $a = b, \forall a\,, \forall\, b, \forall\, c$ en $\mathbb{N}$.

2.8 Orden en el conjunto de los números naturales

Definición:

Si a y b están en $\mathbb{N}$; se dice que a es menor o igual que b si $\exists\ t \in \mathbb{N}$ tal que $a + t = b$. Si $a \neq b$, entonces $t \geq 1$, en este caso, se asevera que $a < b$ (a estrictamente menor que b).

A5. Ley de Tricotomía. Si a y b están en $\mathbb{N}$, se cumple una y una sola de las siguientes tres condiciones: $a = b, a < b$ o $a > b$.

Demostración. Si a y b están en $\mathbb{N}$, al compararlos ocurre una de las dos siguientes situaciones: $a = b$ o $a \neq b$. Si ocurre lo primero, queda demostrado que se cumple el primer resultado o condición a demostrar.

Si $a \neq b$ puede darse que $a < b$ o $a > b$. Si $a < b$, $\exists t \in \mathbb{N}$, $t \neq 0$ tal que $a + t = b$. Si $b < a$,$\exists k \in \mathbb{N}$, $k \neq 0$ tal que $b + k = a$.

Consecuencia. Si $a \leq b$ y $b \leq a$ en $\mathbb{N}$, entonces $a = b$. Basta ver que si $a \leq b$ y $b \leq a$ no puede ocurrir que $a \neq b$ porque en este caso o bien $a < b$ o $b < a$, lo que contradice la hipótesis.

A6. La Relación de orden Menor o Igual que ($\leq$) es Transitiva, es decir, si $a \leq b$ y $b \leq c$ entonces $a \leq c$, $\forall\ a$, $\forall\ b$ y $\forall\ c$ en $\mathbb{N}$.

Demostración. Si $(a \leq b) \wedge (b \leq c)$, existen t y k en $\mathbb{N}$ tales que $a + t = b$ y $b + k = c$. Remplazando el valor de b de la primera igualdad en la segunda se tiene: $(a + t) + k = c$ o mejor $a + (t + k) = c$ y como $(t + k) \in \mathbb{N}$, por definición se tiene que $a \leq c$. I

Definición:

Una relación que sea reflexiva, antisimétrica y transitiva se llama una relación de orden; es decir; si,

i) $aRa, \forall\ a \in \mathbb{N}$ (reflexiva).
ii) aRb y bRa entonces $a = b$ (antisimétrica).
iii) aRb y $bRc \Rightarrow aRc$ (transitiva).

Según esta definición, la relación menor o igual que ($\leq$) ya estudiada, es una relación de orden en el conjunto de los números naturales $\mathbb{N}$.

A7. Monotonía de la Adición. Si a los dos lados de una desigualdad de números naturales se adiciona el mismo número natural, la desigualdad se mantiene, esto es $a < b \Leftrightarrow a + c < b + c, \forall\, a, \forall\, b, \forall\, c$ en $\mathbb{N}$.

Demostración. Para demostrar este hecho, se aplica inducción sobre $c \in \mathbb{N}$.

i) Si $c = 0 \Rightarrow a + 0 = a < b = b + 0$ porque 0 es el neutro de la adición en $\mathbb{N}$.

ii) Para $k \in \mathbb{N}$ se supone que $a < b$ implica $a + k < b + k$.

iii) Ahora se estudia lo que ocurre con el sucesor de k.
Como $a < b$ implica $a + k < b + k$ y de acuerdo con el Teorema 3, en el que se prueba que elementos diferentes tienen sucesores diferentes, se tiene que $(a + k)^* < (b + k)^*$ y por la definición de adición aplicada a cada una de las partes de la desigualdad se puede escribir $a + k^* < b + k^*$.

En conclusión, esto prueba que $a < b$ implica que $a + k^* < b + k^*$, $\forall k^*$ en $\mathbb{N}$.
Es decir $a < b \Leftrightarrow a + c < b + c, \forall\, a, \forall\, b, \forall\, c$ en $\mathbb{N}$.

2.9 Multiplicación de números naturales

La multiplicación de números naturales se define en términos de la adición y por la observación recurrente: $1 \cdot a = a, 2 \cdot a = 1 \cdot a + a, 3 \cdot a = 2 \cdot a + a = (a + a) + a, \ldots$ Por tanto, si a cualquier número natural a se le aplica la definición por recurrencia de la adición, es factible definir la multiplicación de naturales como sigue:

Definición:

En conjunto de números naturales se define la ley de composición interna:

$: \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ tal que $(a, b) \mapsto a \cdot b$.

Este único natural $a \cdot b$ se llama el producto de a y b donde,

$(a, 0) \mapsto a \cdot 0 = 0, \forall\, a \in \mathbb{N}$;
$(a, b^*) \mapsto a \cdot b^* = a \cdot b + a$.

Ejemplos de resultados al utilizar la definición 3, son los siguientes:

$$(a, 0^*) \mapsto a \cdot (0+1) = a \cdot 0 + a = 0 + a = a$$
$$(a, 1^*) \mapsto a \cdot (1+1) = a \cdot 1 + a = a + a = 2a$$
$$(a, 2^*) \mapsto a \cdot (2+1) = a \cdot 2 + a = a \cdot 2 + a = a + a + a = 3a, \ldots$$

2.10 Propiedades de la multiplicación

Una vez establecida la definición de la multiplicación de números naturales, se recurre al método de inducción completa establecido en el axioma P_5. para demostrar sus propiedades básicas.

M1. La multiplicación de naturales es Modulativa. Esto es, $a \cdot 1 = 1 \cdot a = a, \forall\, a \in \mathbb{N}$.

Demostración

Para demostrar este hecho se aplica inducción sobre el natural a.

i) Si $a = 0$, entonces $0 \cdot 1 = 0$, por definición de multiplicación.

ii) Se supone que $k \cdot 1 = k = 1 \cdot k$ para un k cualquiera en $\mathbb{N}$, y se considera el sucesor de k, $k^* \cdot 1 = (k+1) \cdot 1 = k \cdot 1 + 1 = k + 1 = k^*$.
Similarmente, $k^* = 1 + k = 1 + 1 \cdot k = 1 \cdot (1 + k) = 1 \cdot k^*, \forall\, k^* \in \mathbb{N}$.

Luego, y por el axioma de recurrencia P_5, el enunciado es válido $\forall\, a \in \mathbb{N}$. Esto es,

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

M2. La Multiplicación de naturales es Asociativa: $(a \cdot b) \cdot c = a \cdot (b \cdot c) \forall a,\ \forall b,\ \forall c \in \mathbb{N}$.

Demostración. Para demostrar este hecho, se aplica inducción sobre c.

i) Si $c = 0, \text{entonces } (a \cdot b) \cdot 0 = 0 = a \cdot 0 = a \cdot (b \cdot 0)$ por definición de multiplicación.

ii) Se parte de la suposición de que $(a \cdot b) \cdot k = a \cdot (b \cdot k)$, $\forall k \in \mathbb{N}$ y se considera lo que ocurre para el sucesor de k, k^*:

$$\begin{aligned}(a \cdot b) \cdot k^* &= (a \cdot b)(k+1) = (a \cdot b) \cdot k + (a \cdot b) \\ &= a \cdot (b \cdot k) + a \cdot b \\ &= a \cdot (b \cdot k + b) \\ &= a \cdot [b \cdot (k+1)] \\ &= a \cdot (b \cdot k^*), \forall k^* \in \mathbb{N}\end{aligned}$$

Por el principio de inducción matemática, se tiene que:

$(a \cdot b) \cdot c = a \cdot (b \cdot c), \forall\, a, \forall\, b, \forall\, c$ en $\mathbb{N}$.

M3. La Multiplicación es Conmutativa. O sea, $a \cdot b = b \cdot a$, $\forall a,\ \forall b$ en $\mathbb{N}$.

Demostración. Para demostrar esto, se aplica inducción matemática sobre b.

i) Si $b = 0 \Rightarrow a \cdot 0 = 0 = 0 \cdot a, \forall\, a \in \mathbb{N}$, por definición de multiplicación.

ii) Se asume la validez del enunciado para un elemento $k \in \mathbb{N}$, entonces se prueba que $a \cdot k = k \cdot a$ implica $a \cdot k^* = k^* \cdot a$.

iii) En efecto, $a \cdot k^* = a \cdot (k + 1) = a \cdot k + a = k \cdot a + a = (k + 1) \cdot a = k^* \cdot a$.

En consecuencia, $a \cdot b = b \cdot a$, $\forall\, a, \forall\, b$ en $\mathbb{N}$.

M4. La Multiplicación se distribuye con respecto a la adición:

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

Demostración. Para demostrar este hecho, se aplica inducción matemática sobre el primer factor a.

i) $0 \cdot (b + c) = 0$, por definición de multiplicación.
$= 0 + 0$ porque 0 es el módulo de la adición.
$= 0 \cdot a + 0 \cdot b$, $\forall a, \forall b$ en $\mathbb{N}$; por definición de la multiplicación.

ii) Se asume la verdad del enunciado para un elemento $k \in \mathbb{N}$; esto es, $k \cdot (b + c) = (k \cdot b) + (k \cdot c)\ \ \forall a,\ \forall b$ en $\mathbb{N}$.

iii) Ahora, $k^*(b + c) = (k + 1)(b + c)$
$= k(b + c) + (b + c)$ por definición
$(kb + kc) + (b + c)$ por suposición hipotética
$= (kb + b) + (kc + c)$ por asociatividad de la adición
$= (k + 1)b + (k + 1)c$ por definición de la multiplicación
$= k^*b + k^*c, \forall k^* \in \mathbb{N}$.

Luego, por el principio de inducción matemática, el enunciado es válido $\forall a \in \mathbb{N}$; esto es:

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

M5. Ley de absorción del cero. Esto es, $a \cdot 0 = 0 = 0 \cdot a, \forall\, a \in \mathbb{N}$.

Demostración. La primera parte proviene de la definición de multiplicación. Para la segunda parte se requiere utilizar inducción matemática sobre a.

i) Si $a = 0 \Rightarrow 0 \cdot 0 = 0$ por la definición de multiplicación.
ii) Se asume la verdad del enunciado para un elemento $k \in \mathbb{N}$; esto es $0.k = 0$.
iii) Ahora, se toma el sucesor de k en $\mathbb{N}$ y se encuentra que, $0 \cdot k^* = 0 \cdot (k+1) = 0 \cdot k + 0 = 0 + 0 = 0$ por ser el 0 el neutro aditivo y cumpliéndose esto $\forall k^* \in \mathbb{N}$.

En consecuencia, y por el principio de inducción matemática, el enunciado es válido $\forall a \in \mathbb{N}$; esto es,

$$a \cdot 0 = 0 = 0 \cdot a.$$

M6. Ley cancelativa de la multiplicación. Si $a \cdot c = b \cdot c$ y $c \neq 0$, entonces $a = b$.

Demostración. Para la demostración se aplica el Principio de Inducción Completa sobre el primer factor a.

i) Si $a = 0 \Rightarrow 0 \cdot c = 0 = b \cdot c$ y como $c \neq 0$, entonces $b = 0$ ya que si fuera $b \neq 0$, basta tomar $b = 1 \neq 0$ entonces $0 = 1 \cdot c = c$ lo que es absurdo, puesto que $c \neq 0$. En consecuencia $a = b = 0$.
ii) Se asume la verdad del enunciado para un elemento $k \in \mathbb{N}$; en consecuencia, si $k \cdot c = b \cdot c$ y $c \neq 0$, entonces $k = b$.
iii) Se toma el sucesor de k, obteniendo de $k^* \cdot c = (k+1) \cdot c = b \cdot c$ y $c \neq 0$.
iv) Al suponer que $b = 0$, entonces $(k+1) \cdot c = 0 \cdot c = 0, \forall c \neq 0$; así, $k \cdot c + c = 0$ y como si $k \cdot c = b \cdot c$ y $c \neq 0$ se sigue $k = b$; entonces $b \cdot c + c = 0 \cdot c + c = 0 + c = c = 0$, hecho que contradice a la hipótesis. Luego $b \neq 0$. Siendo así, $\exists q \in \mathbb{N}$ tal que $b = q + 1$, entonces $(k+1) \cdot c = (q+1) \cdot c$ y $c \neq 0$ implica que, $k \cdot c + c = q \cdot c + c$ y por la ley cancelativa de la adición, resulta que $k \cdot c = q \cdot c$ donde $c \neq 0$.

Ahora, por hipótesis de inducción $k = q$ y al sumar 1 se consigue $k + 1 = q + 1$ o mejor $k^* = q^*$ y por lo tanto $k^* \cdot c = q^* \cdot c$. Es decir $\forall a \in \mathbb{N}$ se tiene que si $a \cdot c = b \cdot c$ y $c \neq 0$, entonces $a = b$.

2.11 Potenciación

Cuando la multiplicación se repite con el mismo factor, se obtiene una nueva operación llamada Potenciación. Sin embargo, en vez de definir a^n como el producto de n factores, cada uno de ellos igual con a, se definirá por recurrencia, como sigue.

Definición:

Para cada natural $a \notin \{0\}$ y para el natural n, se define:

$$\begin{cases} a^0 = 1 \\ a^{n+1} = a^n \cdot a \end{cases}$$

Es decir, se adopta $a^0 = 1$, $\forall a \in \mathbb{N}$, $a \neq 0$ con el fin de evitar casos de aberración y que son tema de estudio en cursos de Análisis Matemático. Además, en concordancia con la definición, dado a^n, se sigue que $a^{n+1} = a^n \cdot a$.

Como consecuencias inmediatas de esta definición, y que se demuestran aplicando inducción matemática, se tienen los resultados que siguen:

Teorema 6

1. $a^1 = a, \forall\, a \in \mathbb{N}$.
2. $a^m \cdot a^n = a^{m+n}, \forall\, a, \forall\, m, \forall\, n$ en $\mathbb{N}$, con $a \neq 0$ o $m \neq 0$ o $n \neq 0$.
3. $(a \cdot b)^n = a^n \cdot b^n, \forall\, a, \forall\, b, \forall\, n$ en $\mathbb{N}$, con $(a \neq 0$ y $b \neq 0)$ o $n \neq 0$.
4. $(a^m)^n = a^{m \cdot n}, \forall\, a, \forall\, m, \forall\, n$ en $\mathbb{N}$, con $a \neq 0$ o $(m \neq 0$ y $n \neq 0)$.

Demostración

1. Si $a = 0$ entonces $a^1 = 0^1 = 0$ porque el cero se toma una vez como factor.

   Se supone que $k^1 = k$, $\forall k \in \mathbb{N}$ y considera su sucesor k^*; y en efecto se tiene que $(k^*)^1 = (k + 1) = k^*$, luego $a^1 = a, \forall a \in \mathbb{N}$.

2. Inicialmente se fija a y m e n $\mathbb{N}$ y se aplica inducción sobre n.

   Si $n = 0$ entonces $a^m \cdot a^0 = a^m \cdot 1 = a^m = a^{m+0}$, con $a \neq 0$.

   Se supone la veracidad del enunciado para $n = k$; esto es $a^m \cdot a^k = a^{m+k}$, $\forall k \in \mathbb{N}$ y se demuestra que también es cierto para $n = k + 1$.

En efecto, si $n = k + 1$ se implica que $a^m \cdot a^{k^*} = a^m \cdot a^{k+1} = a^m \cdot (a^k \cdot a) = (a^m \cdot a^k) \cdot a$ y desde ahí se escribe $a^m \cdot a^{k^*} = a^{m+k} \cdot a = a^{(m+k)+1} = a^{m+(k+1)}$; luego el enunciado se cumple $\forall n \in \mathbb{N}$; esto es $a^m \cdot a^n = a^{m+n}, \forall\, a, \forall\, m, \forall\, n$ en $\mathbb{N}$.

3. Para $n = 0$ se ve que $(ab)^0 = 1 = 1 \cdot 1 = a^0 \cdot b^0$, con $a \neq 0$ y $b \neq 0$.

   Se parte de suponer $(a \cdot b)^k = a^k \cdot b^k$, $\forall k \in \mathbb{N}$ y de inmediato, se multiplica cada miembro por ab, con lo cual se obtiene:

$$
\begin{aligned}
&(a \cdot b)^k \cdot (ab) = a^k \cdot b^k \cdot (ab) = [(a^k \cdot b^k) \cdot a] \cdot b \\
&= [a^k (b^k \cdot a)] \cdot b \text{ por asociatividad de la multiplicación,} \\
&= [a^k (a \cdot b^k)] \cdot b \text{ por conmutatividad de la multiplicación} \\
&= (a^k a) \cdot (b^k \cdot b) \text{ por asociatividad en la multiplicación} \\
&= a^{k+1} \cdot b^{k+1} \text{ por hipótesis de inducción.}
\end{aligned}
$$

   Por el principio de inducción, queda demostrado que,

   $(a \cdot b)^n = a^n \cdot b^n, \forall\, a, \forall\, b, \forall\, n$ en $\mathbb{N}$ con $(a \neq 0$ y $b \neq 0)$ o $n \neq 0$.

4. Se aplica inducción sobre n. Para $n = 0$ se tiene, $(a^m)^0 = 1 = a^0 = a^{m \times 0}$, $\forall m \in \mathbb{N}$; de igual forma, para $n = 1$ se encuentra que $(a^m)^1 = a^m = a^{m \cdot 1}$, $\forall m \in \mathbb{N}$.

   En seguida, al suponer que es cierto el enunciado $(a^m)^k = a^{m \cdot k}$, $\forall k \in \mathbb{N}$, se determina lo que ocurre para su sucesor $k + 1$, así: $(a^m)^{k+1} = (a^m)^k \cdot (a^m) = a^{m \cdot k} \cdot a^m = a^{mk+m} = a^{m(k+1)}$, $\forall m$, $\forall k \in \mathbb{N}$. Por lo tanto, el enunciado es válido $\forall n \in \mathbb{N}$; esto es, $(a^m)^n = a^{mn}$, con $a \neq 0$ o $(m \neq 0$ y $n \neq 0)$.

Se dispone a continuación, tres ejemplos en los que se utiliza el Principio de Inducción Completa, que constituye un excelente método de demostración. El primer ejemplo se estudió con antelación.

Ejemplo:

1) Demostrar que $\forall \alpha > -1$ y $\forall n \in \mathbb{N}$, se cumple que: $(1 + \alpha)^n \geq 1 + n\alpha$.

Demostración

i) Si $n = 0$ se tiene $(1 + 0)^0 = 1 \geq 1 + 0\alpha$, ya que $1 \geq 1$ es evidente.

ii) Se supone que $(1+\alpha)^k \geq 1+k\alpha$ para $k \in \mathbb{N}$. Si $n = k+1$ se multiplica cada lado de la desigualdad del paso anterior $(1+\alpha)^k \geq 1+k\alpha$, por $(1+\alpha)$; se obtiene: $(1+\alpha)^k \cdot (1+\alpha) = (1+\alpha)^{k+1} \geq (1+k\alpha)\cdot(1+\alpha) = 1+k\alpha+\alpha+k\alpha^2$.
Como $k\alpha^2 \geq 0$ se tiene que $(1+\alpha)^{k+1} \geq 1+k\alpha+\alpha = 1+(k+1)\alpha$. Por esta razón y de acuerdo con el Teorema 1; se sigue que, $(1+\alpha)^n \geq 1+n\alpha$. $\forall\alpha > -1$ y $\forall n \in \mathbb{N}$.

La condición $\forall\alpha > -1$, es de mucha importancia porque, de ocurrir lo contrario, la expresión $(1+\alpha)$ adoptaría valores negativos que hacen que la potencia $(1+\alpha)^n$ tome valores negativos y positivos de manera alternada, mientras $1+n\alpha$ sólo toma valores negativos a partir de un determinado valor de n.

Ejemplos:

1) Si $\alpha = -3$, se tiene:

$$(-2)^0 = 0;$$
$$(-2)^1 = -2 \geq 1+1\cdot(-3);$$
$$(-2)^2 = 4 \geq 1+2\cdot(-3) = -5;$$
$$(-2)^3 = -8 \geq 1+3\cdot(-3) = -8;$$
$$(-2)^4 = 16 \geq 1+4\cdot(-3) = -11;$$
$$(-2)^5 = -32 \leq 1+5\cdot(-3) = -14.$$

A partir de $\boldsymbol{n = 5}$, no se satisface el enunciado.

2) Demostrar que, para todo entero positivo n, se tiene,

$$Sen\left[\theta + \frac{(2n-1)}{2}\pi\right] = (-1)^{n-1}Cos\theta.$$

Demostración

i) Si $n = 1$ se tiene $Sen\left[\theta + \frac{(2n-1)}{2}\pi\right] = Sen\left[\theta + \frac{\pi}{2}\right] = (-1)^0 Cos\theta = Cos\theta$.

ii) Se supone la veracidad del hecho para $n = k$; esto es,

$$Sen\left[\theta + \frac{(2k-1)}{2}\pi\right] = (-1)^{k-1}Cos\theta.$$

iii) Si $n = k + 1$, se encuentra que,

$$Sen\left[\theta + \frac{(2n-1)}{2}\pi\right] = Sen\left[\theta + \frac{(2k+1)}{2}\pi\right] = Sen\left[\left(\theta + \frac{(2k-1)}{2}\pi\right) + \pi\right].$$

Aplicando la fórmula de reducción $Sen(\alpha + \pi) = -Sen\alpha$, a la última expresión, se tiene que,

$$Sen\left[\left(\theta + \frac{(2k-1)}{2}\pi\right) + \pi\right] = -Sen\left[\theta + \frac{(2k-1)}{2}\pi\right]$$
$$= (-1)(-1)^{k-1}Cos\theta = (-1)^{(k+1)-1}Cos\theta.$$

En definitiva, se cumple que,

$$Sen\left[\theta + \frac{(2n-1)}{2}\pi\right] = (-1)^{n-1}Cos\theta, \forall\, n \in \mathbb{N}.$$

3) Produciendo **Unos**, un problema de Knuth.

En el libro *Algoritmos Fundamentales*; *El Arte de Programar Ordenadores*, en la página 36, Donald Knuth, su autor, expone lo siguiente:

El Dr. I. J. Matrix observó una importante sucesión de fórmulas, y a la vez propone dos problemas, como se indica en seguida:

$$9 \times 1 + 2 = 11$$
$$9 \times 12 + 3 = 111$$
$$9 \times 123 + 4 = 1111$$
$$9 \times 1234 + 5 = 11111 \ldots$$

a) Escribir el gran descubrimiento del buen doctor en términos de la notación $\sum$.
b) Su respuesta al apartado a), sin duda, envuelve al número como base del sistema decimal; generalizar dicha fórmula de manera que se obtenga una fórmula apta a cualquier base b.

El problema conduce a la siguiente expresión y nueva formulación: utilizando inducción matemática, demostrar que $\forall n \geq 2$ se tiene que,

$$n + 9\sum_{i=0}^{n-2}(i+1)\cdot 10^{n-2-i} = \sum_{i=0}^{n-1} 10^{n-1-i}.$$

De hecho, en los términos más generales, esto es tomando cualquier base b, se desea demostrar que para todo n mayor o igual que 2, es válida la expresión:

$$n + (b-1)\sum_{i=0}^{n-2}(i+1)\cdot b^{n-2-i} = \sum_{i=0}^{n-1} b^{n-1-i}$$

Lo primero y por familiaridad con la base 10, a continuación se presenta una prueba de este resultado para $b = 10$, dejando como ejercicio para el lector acucioso, la generalidad del mismo en una base cualquiera.

Demostración

i) Para $n = 2$, se tiene:

$$2 + 9\sum_{i=0}^{0}(i+1)\cdot 10^{2-2-i} = 2 + 9\times 1 = \sum_{i=0}^{1} 10^{1-i} = 10 + 1 = 11$$

ii) Se supone la veracidad del resultado para $n = k$, esto es

$$k + 9\sum_{i=0}^{k-2}(i+1)\cdot 10^{k-2-i} = \sum_{i=0}^{k-1} 10^{k-1-i}$$

iii) Se demuestra que el hecho es igualmente cierto para $n = k+1$ y en este caso debe probarse que,

$$(k+1) + 9\sum_{i=0}^{k-1}(i+1)\cdot 10^{k-1-i} = \sum_{i=0}^{k} 10^{k-i}$$

En efecto,

$$\begin{aligned}(k+1) + 9\sum_{i=0}^{k-1}(i+1)\cdot 10^{k-1-i} &= (k+1) + 9\left(k + \sum_{i=0}^{k-2}(i+1)\cdot 10^{k-1-i}\right)\\ &= 1 + 10k + 90\left(\sum_{i=0}^{k-2}(i+1)\cdot 10^{k-2-i}\right)\\ &= 1 + 10\left(k + 9\sum_{i=0}^{k-2}(i+1)\cdot 10^{k-2-i}\right)\end{aligned}$$

$$= 1 + 10\sum_{i=0}^{k-1} 10^{k-1-i}$$
$$= 1 + \sum_{i=0}^{k-1} 10^{k-i} = \sum_{i=0}^{k} 10^{k-i}$$

En consecuencia,

$$n + 9\sum_{i=0}^{n-2}(i+1)\cdot 10^{n-2-i} = \sum_{i=0}^{n-1} 10^{n-1-i}, \forall \in \mathbb{N}, n \geq 2.$$

Con el asistente Derive es fácil evidenciar la veracidad de este resultado, basta con construir las siguientes funciones:

i) U(n):=SUM((i_+1)*b^(n-2-i_),i_,0,n-2)

ii) V(n):=n+(b-1)*U(n)

Su uso inicia con el establecimiento del valor de la constante b. Para ello, y como ejemplo, se puede establecer desde la línea de Autor: $b := 8$ y esto indica que la salida de los resultados se produce en base octal. Este cambio de base se realiza con el comando Opciones/Preferencias de Entrada y Preferencias de Salida del sistema. Derive permite escribir cantidades en las bases binaria, octal, decimal y hexadecimal.

La función $V(n)$ es una fábrica de *Unos*; de hecho, n aparece escrito en base 8; de este modo, si se desea producir un número tal que todos sus dígitos sean 1 y de longitud 20, se introduce la expresión $V(20)$, que en pantalla se vería como $V(24)$ y que al ser simplificada produce 11111111111111111111, que consiste en una cadena de veinte unos.

Al establecer un nuevo valor para b, en concordancia con las posibilidades del sistema es necesario adecuar la base de salida para las simplificaciones y recordar que cada simplificación indica la cantidad de Unos que se desea obtener a partir de la función$V(n)$.

CAPÍTULO 3.
LOS NÚMEROS ENTEROS

Autor:
Segundo Javier Caicedo Zambrano[4]

Conocidas las características y propiedades de los números naturales el paso siguiente es definir y establecer las propiedades de los números enteros. La idea es definir cada entero como un par ordenado (a, b), $a \in \mathbb{N}$ y $b \in \mathbb{N}$, con el significado intuitivo de que (a, b) no es más que la diferencia $a - b$. Por la *Ley de Tricotomía* se puede presentar que $a > b$ en cuyo caso cada pareja (a, b) está definiendo en entero positivo, o si $a = b$ cada par (a, b) define al 0 y cuando se tiene que $a < b$, la pareja (a, b) define a un entero negativo.

3.1 Adición y sustracción de enteros

Al tomar dos números naturales a y b, se puede definir de manera unívoca su suma y su producto, que son otros números naturales. Es decir, la adición y la multiplicación son operaciones cerradas en el conjunto de los números naturales $\mathbb{N}$.

$+: \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ tal que, $(a, b) \mapsto a + b$
$. : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ tal que, $(a, b) \mapsto a\ b$.

El símbolo " $+$ " representa a la adición y el símbolo”.” a la multiplicación.

Con frecuencia se requiere trabajar con números negativos como sucede con las temperaturas bajo cero, las deudas y pérdidas, saldos en rojo en los bancos, gol diferencia en contra.

En la escuela, al requerir efectuar sustracciones y si tan sólo se dispone de números naturales, éstas sólo son posibles cuando el minuendo es mayor o igual que el sustraendo. Esto quiere decir que la sustracción, como operación inversa de la adición, está parcialmente definida en el conjunto de los números naturales $\mathbb{N}$.

La diferencia entre los números naturales a y b, si existe, se define por:

$$a - b = x, si\ a = x + b \qquad (1)$$

[4] Profesor Adscrito al Departamento de Matemáticas y Estadística, Universidad de Nariño.

Así pues, $9-4=5$ porque $9=4+5$; en cambio $5-8$ no está definida en $\mathbb{N}$, porque la ecuación $x+8=5$ carece de solución en $\mathbb{N}$.

Pero si las diferencias $a-b$ y $c-d$ existen en $\mathbb{N}$, se observa que,

$$a-b=c-d, \text{si y sólo si } a+d=b+c \qquad (2)$$

En consecuencia $7-5=12-10$, puesto que $7+10=5+12$ en $\mathbb{N}$.

Ahora; en lugar de $a-b$ se utiliza el par ordenado (a,b) y se dice que (a,b) es equivalente con (c,d) si y sólo si $a+d=b+c$.

Definición:

En el producto cartesiano $\mathbb{N}\times\mathbb{N}$ se define la equivalencia entre pares ordenados, así:

$$(a,b)\sim(c,d) \;\Leftrightarrow\; a+d=b+c \qquad (3)$$

Esta relación es de equivalencia, puesto que satisface las propiedades reflexiva, simétrica y transitiva.

Además, si las diferencias $a-b$ y $c-d$ están definidas en $\mathbb{N}$, entonces,

$$(a-b)+(c-d)=(a+c)-(b+d);$$

$$\begin{aligned}(a-b)\cdot(c-d) &= a\cdot(c-d)-b(c-d)=ac-ad-bc+bd\\ &=(ac+bd)-(ad+bc).\end{aligned}$$

El último resultado se puede escribir como sigue:

$$(a-b)\cdot(c-d)=ac-ad-bc+bd=(ac+bd)-(ad+bc).$$

Esto deriva en la definición de suma y producto de pares ordenados como sigue.

Definición:

En el producto cartesiano $\mathbb{N}\times\mathbb{N}$ se define:

$$(a,b)\oplus(c,d)=(a+c,b+d) \qquad (4)$$

$$(a,b)\odot(c,d)=(ac+bd,ad+bc) \qquad (5)$$

Con estas condiciones, se amplía el conjunto de los números naturales $\mathbb{N}$ y su estructura operatoria, con la inclusión de nuevos números (llamados negativos) y con esto, se ha obtenido el conjunto de los números enteros $\mathbb{Z}$, donde:

1) Se define las operaciones de adición y multiplicación, cuyos resultados coinciden con los obtenidos en $\mathbb{N}$.

2) Se conservan las propiedades de la adición y multiplicación, antes demostradas para los números naturales.

3) Se define la sustracción como una operación cerrada en $\mathbb{Z}$.

Se demuestra enseguida que la relación entre *pares ordenados* definida por (3):

$$(a,b) \sim (c,d) \;\Leftrightarrow\; a+d=b+c \text{ es una relación de equivalencia en } \mathbb{N}$$

i) $(a,b) \sim (a,b)$ puesto que, $a+b=b+a, \forall\, a, \forall\, b$ en $\mathbb{N}$.
ii) Si $(a,b) \sim (c,d)$ entonces $a+d=b+c$; de donde $c+b=d+a$, lo cual implica que $(c,d) \sim (a,b)$.
iii) Si $(a,b) \sim (c,d)$ y $(c,d) \sim (m,n)$, se tiene que $a+d=b+c$ y $c+n=d+m$ y sumando miembro a miembro se halla $a+d+c+n=b+c+d+m$; y aplicando la ley cancelativa en $\mathbb{N}$ se sigue $a+n=b+m$ lo que implica que $(a,b) \sim (m,n)$.

Toda relación de equivalencia induce una partición del conjunto sobre el que se define; cada parte se corresponde con una clase de equivalencia que en general se define, así: $[(a,b)] = \{(x,y) \in \mathbb{N} \times \mathbb{N}: (x,y) \sim (a,b)\}$.

Se simplifica esta notación engorrosa para las clases de equivalencia, escribiendo $[a,b] = \{(x,y) \in \mathbb{N} \times \mathbb{N}:\ x+b=y+a\}$.

Por tanto, $[a,b]=[c,d] \;\Leftrightarrow\; (a,b) \sim (c,d)$, o sea $[a,b]=[c,d] \;\Leftrightarrow\; a+d=b+c$.

Cada clase de equivalencia es la definición de un Número Entero. La representación gráfica de esta partición en clases de equivalencia se indica en la Figura 20.

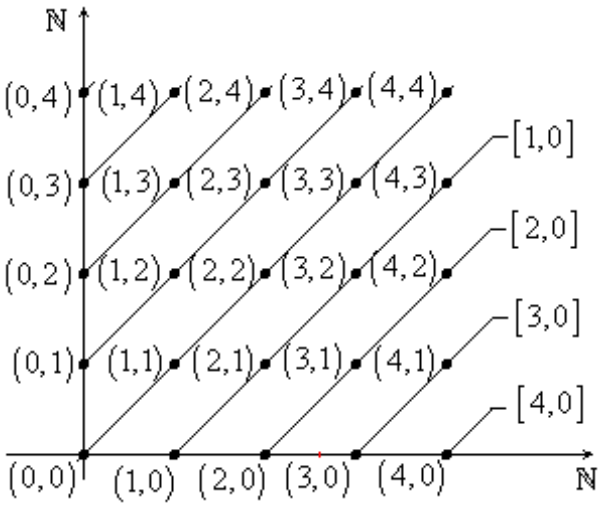

Figura 20. Clases de equivalencia

Los pares ordenados $(a,b) \in \mathbb{N} \times \mathbb{N}$ son los puntos de coordenadas enteras del primer cuadrante y las clases de equivalencia $[a,b]$ son los subconjuntos formados por los puntos del reticulado pertenecientes a las rectas paralelas a la bisectriz del primer cuadrante del plano $\mathbb{N} \times \mathbb{N}$.

Ejemplos:

$(1,0) \sim (2,1)$ porque $1+1=2+0$.
$(2,1) \sim (3,2)$ porque $2+2=3+1$.
$(2,1) \sim (4,3)$ porque $2+3=4+1$.

En consecuencia: $[1,0]=[2,1]=[3,2]=[4,3]=\cdots$

La suma de pares ordenados definida por $(a,b) \oplus (c,d) = (a+c, b+d)$, tiene la propiedad de que al intercambiar un sumando por otro equivalente, el resultado es equivalente.

En lugar de (a,b) se sustituye por su equivalente (a',b') y se calcula la siguiente suma:

$$(a',b') \oplus (c,d) = (a'+c, b', d)$$

Dado que $(a',b') \sim (a,b) \Rightarrow a'+b=b'+a$, se encuentra que,

$$a'+b+c+d=b'+a+c+d.$$

De aquí se obtiene que,

$$(a' + c, b' + d) \sim (a + c, b + d).$$

Esto obliga a definir la suma de números enteros como una suma de clases, a saber:

$$[a, b] \oplus [c, d] = [a + c, b + d].$$

Por ejemplo, $[3,5] \oplus [4,9] = [7,14]$; la cual es equivalente con $[6,8] \oplus [1,6] = [7,14]$.

La diferencia de números enteros corresponde a la diferencia de clases, así:

$$[a, b] - [c, d] = [x, y] \quad \Leftrightarrow \quad [a, b] = [x, y] \oplus [c, d] = [x + c, y + d].$$

Por lo tanto, la *sustracción* es una operación binaria en $\mathbb{Z}$, siempre que la ecuación resultante tenga solución única.

3.2 Multiplicación de enteros

Si $a,\ b,\ c,\ d$ están en $\mathbb{N}$, la definición 3.2 establece que,

$$(a, b) \cdot (c, d) = (ac + bd, ad + bc).$$

De manera que al sustituir uno de los factores por otro equivalente, se obtiene un resultado equivalente; es decir, si $(a', b') \sim (a, b)$, entonces se tiene que,

$$(a', b') \cdot (c, d) = (a'c + b'd, a'd + b'c).$$

Ahora, basta ver que $a'd + bd = b'd + ad$ y $b'c + ac = a'c + bc$, y al sumar a miembros estas dos igualdades, se obtiene $a'd + b'c + ac + bd = a'c + b'd + ad + bc$, lo cual significa que $(ac + bd, ad + bc) \sim (a'c + b'd, a'd + b'c)$, y siendo así, es posible multiplicar números enteros multiplicando las clases respectivas, como sigue:

$$[a, b] \otimes [c, d] = [ac + bd, ad + bc].$$

Por ejemplo, $[5,2] \otimes [7,3] = [35 + 6,15 + 14] = [41,29]$, que escrito de la forma usual representa al producto $3 \times 4 = 12$.

3.3 Propiedades de las operaciones

El paso siguiente, una vez definidas la adición y multiplicación de números enteros, consiste en demostrar las propiedades que ellas cumplen y que básicamente son la asociativa, modulativa, invertiva y la conmutativa.

A1. *La adición es asociativa.*

En efecto,

$$\begin{aligned}([a,b]\oplus[c,d])\oplus[m,n] &= [a+c,b+d]\oplus[m,n]\\ &= [(a+c)+m,(b+d)+n] = [a+(c+m),b+(d+n)]\\ &= [a,b]\oplus([c+m,d+n]) = [a,b]\oplus([c,d]\oplus[m,n]).\end{aligned}$$

Por tanto,

$$([a,b]\oplus[c,d])\oplus[m,n] = [a,b]\oplus([c,d]\oplus[m,n]).$$

A.2 *La adición es modulativa.*

Para determinar el módulo o clase neutra, se parte de suponer que tal clase es $[x,y]$ y por tanto, $[a,b]\oplus[x,y]=[a,b]$ si y sólo si $[a+x,b+y]=[a,b]\Leftrightarrow(a+x,b+y)\sim(a,b)$ que es equivalente con $a+x-b-y=a-b$, de donde se desprende que necesariamente $x-y=0$ o mejor $x=y$.

En consecuencia, el neutro aditivo tiene las dos componentes iguales $[5,5]$, $[12,12]$, $[7,7]$, puesto que en todos los casos la primera componente menos segunda componente es cero.

A3. *La adición es invertible.*

Suponga que el inverso aditivo de $[a,b]$ es $[\alpha,\beta]$; en consecuencia:

$[a,b]\oplus[\alpha,\beta]=[n,n]$, esto es equivalente a decir que $[a+\alpha,b+\beta]=[n,n]$; esto es, $(a+\alpha,b+\beta)\sim(n,n)$, y por tanto, $a+\alpha+n=b+\beta+n$. De aquí se obtiene que $a+\alpha=b+\beta$.

Una solución obvia e inmediata de esta ecuación se consigue al disponer $\alpha=b$ y $\beta=a$. Por tanto, $[\alpha,\beta]$ equivale a $[b,a]$.

En efecto; $[a,b]\oplus[b,a]=[n,n]\Leftrightarrow[a+b,b+a]=[n,n]$.

Así pues, $[5,2] \oplus [2,5] = [7,7]$ lo que implica al traducir las clases a enteros que
$3 + (-3) = 0$.

A4. *La adición es conmutativa.*

En efecto; por definición de la adición de clases, se tiene que:

$$[a,b] \oplus [c,d] = [a+c, b+d] = [c+a, d+b] = [c,d] \oplus [a,b].$$

A5. *La multiplicación es asociativa.*

En efecto,

$$\begin{aligned}([a,b] \otimes [c,d]) \otimes [m,n] &= [ac+bd, ad+bc] \otimes [m,n] \\ &= [(ac+bd)m + (ad+bc)n, (ac+bd)n + (ad+bc)m] \\ &= [acm + bdm + adn + bcn, acn + bdn + adm + bcm] \\ &= \big[a(cm+dn) + b(cn+dm), a\big(cn+dm+b(cm+dn)\big)\big] \\ &= [a,b] \otimes [cm+dn, cn+dm] \\ &= [a,b] \otimes ([c,d] \otimes [m,n]).\end{aligned}$$

Por lo tanto, $([a,b] \otimes [c,d]) \otimes [m,n] = [a,b] \otimes ([c,d] \otimes [m,n])$.

M1. *La multiplicación es modulativa.*

Al suponer aquí, que el módulo es $[x,y]$; como consecuencia se tiene que, $[a,b] \otimes [x,y] = [a,b]$ lo que es equivalente a decir:

$$[ax+by, ay+bx] = [a,b] \Leftrightarrow (ax+by, ay+bx) \sim (a,b).$$

Esto es,

$$ax + by + b = ay + bx + a \;\Leftrightarrow\; ax - bx + by - ay = a - b.$$

Que de inmediato produce,

$$(a-b)x - (a-b)y = a - b \Leftrightarrow\; (a-b)(x-y) = a - b$$

Esto ocurre únicamente cuando $x - y = 1$; por lo tanto, $x = 1 + y$.

El más trivial entre todos los pares (x,y) que satisface esta condición es $(1,0)$ y con todo esto se tiene que $[a,b] \otimes [1,0] = [a,b]$, cualquiera que sea la clase $[a,b]$.

M2. *La multiplicación es conmutativa.*

En este caso debe probarse que, $[a,b] \otimes [c,d] = [c,d] \otimes [a,b]$.

En efecto,

$$[a,b] \otimes [c,d] = [ac + bd, ad + bc] = [ca + db, da + cb]$$
$$= [ca + db, cb + da] = [c,d] \otimes [a,b].$$

Por tanto, $[a,b] \otimes [c,d] = [c,d] \otimes [a,b]$.

M3. *La multiplicación distribuye respecto a la adición.*

En efecto,

$$\begin{aligned}[a,b] \otimes ([c,d] \oplus [m,n]) &= [a,b] \otimes [c+m, d+n] \\ &= [a(c+m) + b(d+n), a(d+n) + b(c+m)] \\ &= [ac + bd + am + bn, ad + bc + an + bm] \\ &= [ac + bd, ad + bc] \oplus [am + bn, an + bm] \\ &= ([a,b] \otimes [c,d]) \oplus ([a,b] \otimes [m,n])\end{aligned}$$

Por tanto,

$$[a,b] \otimes ([c,d] \oplus [m,n]) = ([a,b] \otimes [c,d]) \oplus ([a,b] \otimes [m,n]).$$

Nota. Los números enteros se comportan como los números naturales con respecto a las operaciones de adición y multiplicación, basta tomar como segunda componente de clase el número cero, así:

$$[a,0] \oplus [c,0] = [a + c, 0]$$
$$[a,0] \otimes [c,0] = [a \times c, 0]$$

Esto significa que se tiene la posibilidad de identificar al número entero $[a,0]$ con el número natural a y esto finalmente significa que $\mathbb{N} \subset \mathbb{Z}$.

Reconsiderando la gráfica de las clases de equivalencia, Figura 20, se evidencia que todo número entero se puede representar en una y sólo una de las dos siguientes maneras:

i) $[n,0]\ \forall\ n \in \mathbb{N}$
ii) $[0,n]\ \forall\ n \in \mathbb{N}$ y $n \neq 0$.

El entero $[n, 0]$ se llama no-negativo, y se escribe n; mientras que $[0, n]$, con $n \neq 0$, se llama entero negativo y generalmente se denota por $-n$.

Siendo así,

$$\mathbb{Z} = \{0,\ \pm 1,\ \pm 2,\ \pm 3, \ldots\} = \{\ldots,\ -3,\ -2,\ -1,\ 0,\ 1,\ 2,\ 3, \ldots\}$$

Es conveniente anotar que con esta definición de producto de clases se cumple la ley de los signos, tal como se verifica con los siguientes ejemplos particulares:

$$[3,5] \otimes [7,4] = [41,47] \Leftrightarrow (-2) \times (3) = -6$$
$$[2,5] \otimes [3,7] = [41,29] \Leftrightarrow (-3)(-4) = 12$$

Dicho de otra manera, el conjunto de los números enteros con la adición y multiplicación definidas antes, forma un *Anillo Conmutativo con Unidad*.

En efecto, $(\mathbb{Z}, \oplus)$ es Grupo Abeliano; la multiplicación $\otimes$ es asociativa y distribuye con respecto a la adición $\oplus$; además, la multiplicación $\otimes$ es conmutativa y tiene elemento unidad.

De las propiedades algebraicas de la estructura de anillo, es factible extraer algunas consecuencias inmediatas, como las siguientes:

1. *Ley cancelativa de la adición*

   Si $[a, b] \oplus [c, d] = [a, b] \oplus [m, n]$, entonces $[c, d] = [m, n]$.

   La demostración es como sigue: si $[a, b] \oplus [c, d] = [a, b] \oplus [m, n]$ se tiene que $[a + c, b + d] = [a + m, b + n]$ o lo que es igual, $(a + c, b + d) \sim (a + m, b + n)$, de allí que $a + c + b + n = b + d + a + m$, y aplicando la ley cancelativa de la adición en $\mathbb{N}$, resulta, $c + n = d + m$, de donde $(c, d) \sim (m, n)$ y en consecuencia se tiene que $[c, d] = [m, n]$.

2. *Absorción del cero*

   El elemento cero, en términos generales, tiene sus dos componentes iguales y se puede tomar como $[n, n]$.

   En este sentido, es evidente que $[a, b] \otimes [n, n] = [an + bn, an + bn] = [n, n]$.

3. Leyes de los Signos.

i) $[a,0] \otimes [b,0] = [a \cdot b + a \cdot 0, a \cdot 0 + 0 \cdot b] = [ab, 0]$.
ii) $[a,0] \otimes [0,b] = [a \cdot 0 + 0 \cdot b, a \cdot b + 0 \cdot 0] = [0, ab]$.
iii) $[0,a] \otimes [0,b] = [0 \cdot 0 + a \cdot b, 0 \cdot b + a \cdot 0] = [ab, 0]$.

3.4 Orden en el conjunto de los números enteros

Si a y b están en $\mathbb{N}$ se dice que $a \leq b$ si existe $k \in \mathbb{N}$ tal que $a + k = b$. $a < b$ si $a \neq b$, esto es, si $k \neq 0$.

Ahora, si α y β están en $\mathbb{Z}$, existen $a,\ b,\ c$ y d en $\mathbb{N}$ tales que $\alpha = [a,b]$ y $\beta = [c,d]$; así:

1. $\alpha < \beta$, o mejor $[a,b] < [c,d]$ si y sólo si $a + d < b + c$.
2. $\alpha > \beta$, o mejor $[a,b] > [c,d]$ si y sólo si $a + d > b + c$.

Ley de Tricotomía

Tal como en los números naturales, en los enteros también se cumple la ley de tricotomía.

Si α y β están en $\mathbb{Z}$, se cumple una y sólo una de las tres siguientes condiciones: $\alpha = \beta, \alpha > \beta$ ó $\alpha < \beta$.

En efecto:

Sea $\alpha = [a,b]$ y $\beta = [c,d]$; si $\alpha = \beta$ se infiere que $[a,b] = [c,d]$ y por ello $(a,b) \sim (c,d)$, lo que es equivalente a decir que, $a + d = b + c$.

Si $a + d \neq b + c$, puede suceder que $a + d < b + c$ o bien que $a + d > b + c$ puesto que a, b, c y d son números naturales. Por tanto $\alpha < \beta$ o $\alpha > \beta$.

Además, para $\alpha,\ \beta$ y γ en $\mathbb{Z}$, se cumple que:

1. $\alpha < \beta \Leftrightarrow \alpha + \gamma < \beta + \gamma,\ \forall\, \gamma \in \mathbb{Z}$.
2. $\alpha < \beta \Leftrightarrow \alpha \cdot \gamma < \beta \cdot \gamma,\ \forall\, \gamma \in \mathbb{Z}^+$.
3. $\alpha > \beta \Leftrightarrow \alpha \cdot \gamma < \beta \cdot \gamma,\ \forall\, \gamma \in \mathbb{Z},\ \gamma < 0$.
4. $\alpha = \beta$ si $\alpha \cdot \gamma = \beta \cdot \gamma\ \forall\, \gamma \neq 0$.
5. Si $\alpha \cdot \beta = 0$ entonces $\alpha = 0$ o $\beta = 0$.

Se define:

$$\mathbb{Z}^+ = \{[a,b]: a > b,\ a \in \mathbb{N},\ b \in \mathbb{N}\}.$$
$$\mathbb{Z}^- = \{[a,b]: a < b,\ a \in \mathbb{N},\ b \in \mathbb{N}\}.$$

A continuación, se presentan las demostraciones de algunas de las anteriores afirmaciones. Los enunciados que se demuestran funcionan como equivalencias o dobles implicaciones Aquí se han probado en un sentido; para probar la otra condición, en consecuencia, es suficiente con realizar el proceso contrario.

1. $\alpha < \beta \Leftrightarrow \alpha + \gamma < \beta + \gamma,\ \forall \gamma \in \mathbb{Z}$.
   Sea $\alpha = [a,b]$, $\beta = [c,d]$ y $\gamma = [m,n]$; entonces:
   $\alpha < \beta \ \Leftrightarrow\ [a,b] < [c,d] \ \Leftrightarrow\ a + d < b + c$
   y así:

   $(a + d) + (m + n) < (b + c) + (m + n)$.

   Esto es, $(a + m) + (d + n) < (c + m) + (b + n)$ lo que asegura que se cumple:
   $[a + m, b + n] < [c + m, d + n]$, que se escribe, así:
   $[a,b] \oplus [m,n] < [c,d] \oplus [m,n]$ o en términos más sencillos, $\alpha + \gamma < \beta + \gamma$.

3. Sean $\alpha,\ \beta$ y γ en $\mathbb{Z}$, donde $\gamma > 0$ se tiene que $\alpha \cdot \gamma > \beta \cdot \gamma \Leftrightarrow \alpha > \beta$.
   En efecto, sea $\alpha = [a,b]$, $\beta = [c,d]$ y $\gamma = [m,n]$. Si $\gamma > 0$, entonces $[m,n] > [t,t]$ lo que significa que $m + t > n + t$, o mejor $m > n$; por lo tanto $\exists q \in \mathbb{N},\ q \neq 0$ tal que $m = n + q$.

$$\alpha \cdot \gamma = [a,b] \otimes [m,n] = [am + bn, an + bm]$$
$$\beta \cdot \gamma = [c,d] \otimes [m,n] = [cm + dn, cn + dm]$$

Por ello, $\alpha \cdot \gamma > \beta \cdot \gamma$ es equivalente a $[am + bn, an + bm] > [cm + dn, cn + dm]$ o mejor, $(am + bn) + (cn + dm) > (an + bm) + (cm + dn)$.

Ahora bien, como $m = n + q$ para un $q \in \mathbb{N},\ q \neq 0$ y remplazando en la desigualdad anterior es claro que:

$$a(n + q) + bn + cn + d(n + q) > an + b(n + q) + c(n + q) + dn$$

que es equivalente a tener,

$$an + aq + bn + cn + dn + dq > an + bn + bq + cn + cq + dn$$

Aplicando cancelación, se obtiene $aq + dq > bq + cq$ y esto es equivalente con $(a + d)q > (b + c)q$ y siendo que $q \in \mathbb{N},\ q \neq 0$, se concluye que $a + d > b + c$, esto es, $[a, b] > [c, d] \Leftrightarrow \alpha > \beta$.

4. Con base al orden definido en $\mathbb{Z}$, es factible demostrar también, las leyes de los signos. Por ejemplo, se puede probar que $\forall\alpha,\ \forall\beta$ en $\mathbb{Z}$ se tiene que $(-\alpha) \cdot (-\beta) = \alpha \cdot \beta$. Para ello se toman $\alpha = [a, b]$ y $\beta = [c, d]$. Si $\alpha < 0$ entonces $[a, b] < [t, t]$ o sea que, $a + t < b + t$; por ello $a < b$. Si $\beta < 0$ se sigue que $[c, d] < [q, q]$ o sea $c + q < d + q$ y en consecuencia $c < d$.

Con todo esto se tiene $\alpha \cdot \beta = [a, b] \otimes [c, d] = [ac + bd, ad + bc]$. Pero $\alpha < 0$ y por ello $a < b \ \Rightarrow\ b - a > 0$; así mismo $\beta < 0$, por ello $c < d$, esto es $d - c > 0$; lo que hace que el producto $(b - a)(d - c) > 0$; así $bd - bc - ad + ac > 0$ que se escribe como $ac + bd > bc + ad$, lo que asevera de inmediato que $[ac + bd, bc + ad] > 0$ y por lo tanto $\alpha \cdot \beta > 0$.

5. $\alpha \cdot \beta = 0$ implica que $\alpha = 0$ o $\beta = 0$. En efecto, sea $\alpha = [a, b]$ y $\beta = [c, d]$; en consecuencia, decir que $\alpha \cdot \beta = 0$ es equivalente a escribir que $[a, b] \otimes [c, d] = [t, t]$, o mejor $[ac + bd, ad + bc] = [t, t]$ y por esta razón se puede escribir: $(ac + bd, ad + bc) \sim (t, t)$ y por ello $ac + bd + t = ad + bc + t$, de donde aplicando la ley cancelativa, es claro que $ac + bd = ad + bc$ o si se quiere $a(c - d) = b(c - d)$; de lo que se obtiene $(a - b)(c - d) = 0$. En consecuencia $\alpha = [a, a]$ o $\beta = [c, c]$, lo que asegura como $\alpha = 0$ ó $\beta = 0$.

Se prueba a continuación que si α y β están en $\mathbb{Z}$ entonces $(-\alpha) \cdot \beta = -(\alpha \cdot \beta)$.

En efecto: sea $\alpha = [a, b]$ y $\beta = [c, d]$. Si $\alpha < 0 \Rightarrow [a, b] < [t, t] \Rightarrow a + t < b + t$ y por ello $a < b$. Así se tiene $\alpha \cdot \beta = [a, b] \otimes [c, d] = [ac + bd, ad + bc]$.

Ahora bien, como $a < b$ se tiene que $b - a > 0$. Además $\beta = [c, d] > 0$ implica que $c - d > 0$ y siendo el producto de naturales distintos de cero otro natural se asegura de inmediato que $(b - a)(c - d) > 0$ y entonces $bc - bd - ac + ad > 0$. Esta desigualdad se reescribe como $bc + ad > ac + bd$; o mejor $ac + bd < ad + bc$ y por esta razón la clase $[ac + bd, ad + bc] < 0$. Esto nos dice que $\alpha \cdot \beta < 0$; es decir $(-\alpha) \cdot \beta = -(\alpha \cdot \beta)$.

3.5 La Función valor absoluto

La función valor absoluto es una herramienta que permite calcular distancias entre dos puntos que se encuentran en una recta y se constituye con el uso de otras herramientas matemáticas; en el ejemplo más simple, en la configuración de un espacio métrico.

Definición:

Dado un número entero α, el valor absoluto de α y que se escribe como $|\alpha|$, equivale a su valor numérico, sin tener en cuenta su signo. Es decir,

$$|\alpha| = \begin{cases} \alpha \ \ si\ \alpha \geq 0 \\ -\alpha \ \ si \ \ \alpha < 0 \end{cases}$$

Ejemplo: $|-5| = 5$.

Siendo así, $\forall \alpha \neq 0$, $\alpha \in \mathbb{Z}$ se tiene que $|\alpha| > 0$.

Como consecuencia de la definición, se desprenden las propiedades que siguen.

Teorema 7

Seanα y β números enteros, entonces,

1. $-|\alpha| \leq \alpha \leq |\alpha|$
2. $|\alpha \cdot \beta| = |\alpha| \cdot |\beta|$
3. $|\alpha + \beta| \leq |\alpha| + |\beta|$
4. $|\alpha - \beta| \leq |\alpha| + |\beta|$
5. $|\alpha| - |\beta| \leq |\alpha + \beta|$
6. $|\alpha| - |\beta| \leq |\alpha - \beta|$

Demostraciones

1. Si $\alpha \geq 0$ se tiene $|\alpha| = \alpha$; de donde se deduce que $|\alpha| \geq 0$. Multiplicando por (-1) se obtiene $-|\alpha| \leq 0$ pero a su vez, $0 \leq \alpha$ y $\alpha = |\alpha|$; es decir $\alpha \leq |\alpha|$; por tanto se puede conjuntar todo y escribir $-|\alpha| \leq \alpha \leq |\alpha|$.

   Si $\alpha < 0$, por definición $|\alpha| = -\alpha$; siendo $-\alpha > 0$; en consecuencia $|\alpha| > 0$ y de aquí se sigue $-|\alpha| < 0$, por la propiedad 3 del parágrafo 3.4.1. Luego $-|\alpha| = \alpha < 0 < -\alpha = |\alpha|$ y de nuevo se puede escribir que $-|\alpha| \leq \alpha \leq |\alpha|$.

2. Si $\alpha \geq 0$ y $\beta \geq 0$ se tiene que $\alpha \cdot \beta \geq 0$ y en consecuencia se tiene que $|\alpha| = \alpha$, $|\beta| = \beta$, pero también $|\alpha \cdot \beta| = \alpha \cdot \beta$; sustituyendo los dos primeros valores absolutos en este tercero, se evidencia que $|\alpha \cdot \beta| = \alpha \cdot \beta = |\alpha| \cdot |\beta|$ con lo que se prueba la verdad del enunciado.

   Si $\alpha < 0$ y $\beta < 0$, se encuentra que $\alpha \cdot \beta > 0$ y por lo tanto $|\alpha| = -\alpha$, $|\beta| = -\beta$, pero también $|\alpha \cdot \beta| = \alpha \cdot \beta = (-\alpha)(-\beta) = |\alpha| \cdot |\beta|$; como se consigue con un simple reemplazo.

   Si $\alpha \geq 0$ y $\beta < 0$, se encuentra que $\alpha \cdot \beta \leq 0$ y por lo tanto $|\alpha| = \alpha$, $|\beta| = -\beta$, pero también $|\alpha \cdot \beta| = -(\alpha \cdot \beta) = (\alpha)(-\beta) = |\alpha| \cdot |\beta|$; como se consigue con una simple sustitución. L

3. i) Si $\alpha \geq 0$ y $\beta \geq 0$, se encuentra que $\alpha + \beta \geq 0$ y en razón a estos hechos:
   $|\alpha| = \alpha$, $|\beta| = \beta$, pero a la vez, $|\alpha + \beta| = \alpha + \beta = |\alpha| + |\beta|$; resultado que se consigue con un simple reemplazo.

   ii) Si $\alpha < 0$ y $\beta < 0$, se encuentra que $\alpha + \beta < 0$ y en razón a estos hechos $|\alpha| = -\alpha$, $|\beta| = -\beta$, pero a la vez, $|\alpha + \beta| = -(\alpha + \beta) = (-\alpha) + (-\beta) = |\alpha| + |\beta|$; resultado que se consigue con un simple reemplazo.

   iv) Si $\alpha \geq 0$ y $\beta < 0$, se encuentra que $|\alpha| = \alpha$, $|\beta| = -\beta$, mientras para la suma de estos valores se tiene,

   $$|\alpha + \beta| = \begin{cases} \alpha + \beta \ si \ \alpha + \beta \geq 0 \\ -(\alpha + \beta) \ \ si \ \alpha + \beta < 0 \end{cases}$$

   Pero $\alpha + \beta < \alpha + (-\beta)$ porque $\alpha \geq 0$ y $\beta < 0$; por esta razón se puede escribir $\alpha + \beta < \alpha + (-\beta) = |\alpha| + |\beta|$ o $|\alpha + \beta| \leq |\alpha| + |\beta|$ cuando sea el caso que, $\alpha + \beta \geq 0$.

   Para el otro caso, esto es, cuando $\alpha + \beta < 0$ es suficiente ver que $-(\alpha + \beta)$ se escribe como $= (-\alpha) + (-\beta) \leq \alpha + (-\beta) = |\alpha| + |\beta|$; es decir, que se tiene en definitiva $-(\alpha + \beta) = |\alpha + \beta| \leq |\alpha| + |\beta|$.

4. $|\alpha - \beta| = |\alpha + (-\beta)| \leq |\alpha| + |-\beta| = |\alpha| + |\beta|$; por la propiedad 3; luego:

$|\alpha - \beta| \leq |\alpha| + |\beta|$. Para deducir este resultado se ha utilizad el hecho de que $\forall\ \alpha \in \mathbb{Z}$ se tiene que $|\alpha| = |-\alpha|$.

5. $|\alpha| = |\alpha + \beta - \beta| = |(\alpha + \beta) + (-\beta)| \leq |\alpha + \beta| + |\beta|$ y por ello $|\alpha| - |\beta| \leq |\alpha + \beta|$.

6. $|\alpha| = |\alpha - \beta + \beta| = |(\alpha - \beta) + \beta| \leq |\alpha - \beta| + |\beta|$ y por ello $|\alpha| - |\beta| \leq |\alpha - \beta|$.

3.6 Otras propiedades de los números enteros

1. $a \cdot 0 = 0 = 0 \cdot a,\ \forall a \in \mathbb{Z}$. En efecto; $a + 0 = a = 0 + a$ entonces, $a(a + 0) = a \cdot a \quad \forall a \in \mathbb{Z}$ y por la propiedad distributiva se halla que: $a \cdot a + a \cdot 0 = a \cdot a + 0$ que aplicando la propiedad cancelativa se convierte en $a \cdot 0 = 0$.

2. $a(-b) = (-a)b = -(ab) \quad \forall a,\ \forall b$ en $\mathbb{Z}$ y que se prueba como sigue: $0 = 0 \cdot b = \big(a + (-a)\big)b = ab + (-a)b$ y al sumar a esta igualdad, $0 = ab + (-a)b$ el número $-(ab)$ se consigue que $-(ab) = (-a)b$.

3. $(-a)(-b) = ab, \forall\ a\ \forall\ b$ en $\mathbb{Z}$. Este hecho se demuestra de forma similar a la anterior proposición. $0 = 0 \cdot (-b) = \big(a + (-a)\big)(-b) = a(-b) + (-a)(-b)$; así, $-(ab) + (-a)(-b) = 0$ y sumando ab a los dos miembros produce el hecho $(-a)(-b) = ab$, como se deseaba.

4. $-(-a) = a, \forall a \in \mathbb{Z}$. Esto es evidente ya que si $x = -a$ se tiene por una parte que $x + (-x) = 0$; es decir, se tiene que $(-a) + \big(-(-a)\big) = 0$ y al sumar a a las dos partes se tiene que $a + (-a) + \big(-(-a)\big) = a$ y por asociatividad de la adición en los enteros se tiene $\big(a + (-a)\big) + \big(-(-a)\big) = a$; es decir $0 + \big(-(-a)\big) = a$ que se escribe como $-(-a) = a$.

3.7 Divisibilidad en el conjunto de los números enteros

Un elemento fundamental de la teoría de números y, por ende, de los sistemas numéricos, es el de la divisibilidad de un número por otro. Situaciones relativas a la divisibilidad surgen con frecuencia en el trabajo matemático; por ejemplo, la posibilidad de construir con regla y compás un polígono regular de n lados, depende de la naturaleza de n. Otro caso puntual es el de la resolución de una ecuación lineal de la forma $ax = b$ que no siempre puede resolverse en el conjunto de los números enteros.

Sin embargo, en infinitos casos esto último es posible y, por ello, aparece el concepto de divisibilidad.

Definición:

Sean a y b números enteros y $a \neq 0$. Se afirma que a es un divisor de b, o que a es un factor de b, o que a divide a b, y se denota por $a|b$, si $\exists c \in \mathbb{Z}$ tal que $b = a \cdot c$.

Si ocurre lo anterior, también se dice que b es un múltiplo de a, o bien, b es divisible por a. Si a no divide a b, se escribe $a \nmid b$; así pues, $2|10$; $5|10$; pero $2 \nmid 3$ y $3 \nmid 5$.

Es claro que, si $a \neq 0$, entonces,

$$a|a, a|a^2, a|a^3, a|a^n, \forall\, n \in \mathbb{N}.$$

Además, $\forall a \in \mathbb{Z}$, $1|a$ y $1|(-a)$, $a|(-a)$, $(-a)|a$ y $a|0$. De aquí se concluye, por simple incidencia que, $a||a|$ y, a la vez, $|a||a$. Como consecuencia inmediata se infiere que, todo número entero $a \neq 0$, tiene por lo menos cuatro divisores $\{+1, -1, +a, -a\}$; estos cuatro divisores de cada entero se denominan divisores impropios.

Si existen divisores de a que no son impropios, se llamarán Divisores Propios. Así, pues, 24 es un número que posee divisores propios e impropios; tal lista es, $D(24) = \{\pm 1,\ \pm 2,\ \pm 3,\ \pm 4,\ \pm 6,\ \pm 12,\ \pm 24\}$.

Nota

$\forall a \in \mathbb{N}$ con $a \neq 0$ se tiene que $a|1$ si y sólo si $a = 1$.

3.8 Propiedades de la divisibilidad

1. $1|a$ y $a|a$. En efecto, $1|a$ porque $a = 1 \times a$, y a su vez, $a|a$ porque $a = a \times 1$.

2. Si $a|b$ entonces $a|(-b)$, $(-a)|b$ y $(-a)|(-b)$. En efecto, si $a|b$, entonces existe $k \in \mathbb{Z}$ de modo que $b = a \times k$.

   Si $b > 0$ entonces $a > 0$ y $k > 0$ o bien $a < 0$ y $k < 0$.

Si $b < 0$ entonces $a > 0$ y $k < 0$ o bien $a < 0$ y $k > 0$. Combinando adecuadamente y a la vez cambiando los signos de k, se asegura que $a|(-b)$, $(-a)|b$ y también $(-a)|(-b)$.

3. Si $a|b$ y $b|c$, entonces $a|c$, $\forall\, a, \forall\, b, \forall\, c$ en $\mathbb{Z}$. En efecto, $a|b$ implica la existencia de un entero k tal que $b = a \cdot k$ y $b|c$ induce la existencia de un entero t tal que $c = b \cdot t$. Sustituyendo el valor de b se encuentra $c = (a \cdot k) \cdot t$ y por asociatividad se tiene que $c = a \cdot (k \cdot t)$. Tomo $k \cdot t \in \mathbb{Z}$ se sigue de inmediato que $a|c$.

4. Si $a|b$ y $b \neq 0$ se tiene que $|a| \leq |b|$. En efecto, si $a|b$ entonces $\exists k \in \mathbb{Z}$ tal que $b = a \cdot k$. Como $b \neq 0$ se infiere que $a \neq 0$ y $k \neq 0$. De otra parte se tiene que $|b| = |a \cdot k| = |a| \cdot |k|$ y siendo $k \neq 0$, se sigue que $|k| > 0$.

   Ahora bien, $k \in \mathbb{Z} \Rightarrow |k| = 1$ o $|k| > 1$. Si $|k| = 1$ se tiene que $|b| = |a|$ de donde se obtiene de inmediato que $|a| \leq |b|$. Si $|k| > 1$ y siendo $|b| = |a| \cdot |k|$, se tiene que $|b| > |a|$ y en este caso también se obtiene que $|a| \leq |b|$. En consecuencia, y cualquiera que sea el caso, se concluye que si $a|b$ y $b \neq 0$, se tiene que $|a| \leq |b|$.

5. Si $a|b$ y $b|a$ entonces $a = \pm b$ en $\mathbb{Z}$. En efecto, de $a|b$ se infiere que $b = a \cdot k$ para algún $k \in \mathbb{Z}$; así mismo, de $b|a$ se sigue que existe $t \in \mathbb{Z}$ tal que $a = b \cdot t$. Al sustituir una en otra, de estas dos igualdades se tiene: $a = (a \cdot k) \cdot t = a \cdot (k \cdot t)$ y como $a \neq 0$ lo único que puede ocurrir es que $k \cdot t = 1$; pero para que esto ocurra en el conjunto de los números enteros, lo único que puede pasar es que $k = 1$ y $t = 1$ o que $k = -1$ y $t = -1$. Pero $b = a \cdot k$. Ahora, si $k = 1$ se tiene que $a = b$ y en el caso en que $k = -1$ se sigue que $b = a \cdot (-1) = -a$, de donde $a = -b$. Uniendo estos dos hechos se obtiene que $a = \pm b$.

6. Si $a|b$ y $a|c$ entonces $a|(bx + cy)$, $\forall\, x, \forall\, y$ en $\mathbb{Z}$. Hecho que es absolutamente cierto en virtud a que de $a|b$ y $a|c$ se infiere la existencia de los enteros k y t para los cuales $b = a \cdot k$ y $c = a \cdot t$; de allí que la combinación lineal de enteros $bx + cy = (a \cdot k)x + (a \cdot t)y = a \cdot (k \cdot x) + a \cdot (t \cdot y)$. Esto es, $bx + cy = a \cdot (kx + ty)$, y siendo $(kx + ty) \in \mathbb{Z}$, se concluye que $a|(bx + cy)$. En particular, si $a|b$ y $a|c$ se tiene que $a|(b \pm c)$.

7. Si $a|(b+c)$ y $a|b$ entonces $a|c$. Como$a|(b+c)$, existe $k \in \mathbb{Z}$ que hace que $b+c = a \cdot k$ y también, debido a que $a|b$ se encuentra un valor entero t para el cual $b = a \cdot t$. Remplazando esta igualdad en la anterior se consigue $a \cdot t + c = a \cdot k$ de donde se infiere que $c = a \cdot k - a \cdot t = a \cdot (k-t)$ y siendo $k-t$ un número entero se deduce que $a|c$.

8. Si $a|b \cdot c$ entonces $a|b$ o $a|c$ siempre que a contenga sólo divisores impropios. En efecto; al suponer que $a|(b \cdot c)$ pero $a \nmid b$ se debe encontrar que $a|c$ pues de presentarse que $a \nmid c$ se tendría que $a \nmid (b \cdot c)$ lo que es contrario a lo supuesto. Igual razonamiento se efectúa cuando se supone que $a|(b \cdot c)$ y $a \nmid c$, lo que determina que $a|b$.

   Se debe observar aquí la importancia de que a sólo contenga divisores impropios, pues de no presentarse esto aparecen aberraciones del teorema; por ejemplo, $8 \nmid 12$ y $8 \nmid 20$ y sin embargo $8|240$; es decir $8|12 \times 20$ a pesar de que $8 \nmid 12$ y también $8 \nmid 20$.

9. $a|b \Leftrightarrow a\big||b|$. En efecto:

   ($\Rightarrow$) Si $a|b$ y $b > 0$, se tiene que $b = |b|$ y de inmediato se escribe la hipótesis como $a\big||b|$. Ahora bien, si $b < 0$, entonces $|b| = -b$ y existe $k \in \mathbb{Z}$ para el cual $b = a \cdot k$, igualdad que al multiplicarse por (-1) nos dice que $-b = a \cdot (-k)$ y en consecuencia, nuevamente $a\big||b|$. De esta forma, cualquiera que sea el caso $a\big||b|$. ($\Leftarrow$) Si $a\big||b|$ entonces, es el caso que $a|b$ o $a|(-b)$ según b sea positivo o negativo. Si es el caso que $a|b$, se encuentra un valor $k \in \mathbb{Z}$ para el cual $b = a \cdot k$ y de acuerdo a la definición se tiene que $a|b$. En cambio, si $a|(-b)$, entonces existe $t \in \mathbb{Z}$ para el cual $-b = a \cdot t$, igualdad que se puede escribir como $b = a \cdot (-t)$ y como $-t$ es un número entero, también se consigue que $a|b$; con lo cual, queda demostrada esta condición de suficiencia.

10. $a|b \Leftrightarrow |a||b$. En efecto:

    ($\Rightarrow$) Si $a|b$ entonces $\exists k \in \mathbb{Z}$ tal que $b = a \cdot k$ y como $a \neq 0$, por Ley de Tricotomía se tiene que $a > 0$ o bien $a < 0$. Si $a > 0$ se implica que $b = a \cdot k$ y si $a < 0$ también se sigue que $b = a \cdot (-k)$, o mejor

$b = (-a) \cdot k$, y en consecuencia, se escribe que $\pm a|b$, o lo que es lo mismo, $|a||b$.

($\Leftarrow$) Sea $|a||b$ y como $a \neq 0$ se tiene que $|a| > 0$. Si $a > 0$, se puede escribir que $a|b$, y si $a < 0$ se tiene que $(-a) > 0$ y así $(-a)|b$; o mejor aún, $b = (-a) \cdot t$ para algún entero t. De aquí se infiere que $b = a \cdot (-t)$ y nuevamente $a|b$; con lo que termina la prueba.

Los dos siguientes enunciados, se corresponden con falacias comunes que se debe evitar para no incurrir en errores:

1. Si $a|(b + c)$ no se sigue que $a|b$ o $a|c$. Suficiente con presentar uno de los infinitos contraejemplos como en $3|(5 + 7)$ y sin embargo $3 \nmid 5$ y $3 \nmid 7$.

2. Si $a|b$ y $c|b$ no se sigue que $a \cdot c|b$; basta, como en el caso anterior, con exhibir un contraejemplo: $2|12$ y $4|12$ pero $2 \times 4 = 8 \nmid 12$.

Como ejemplos de la teoría de la divisibilidad, a continuación, utilizando el método de inducción matemática, se comprobarán algunos resultados. El método de inducción cabe a la perfección en la demostración de algunas propiedades de divisibilidad; por ejemplo, se tiene que $a^n - b^n = a^n - ba^{n-1} + ba^{n-1} - b^n = a^{n-1}(a - b) + b(a^{n-1} - b^{n-1})$. Por esta razón $\frac{a^n - b^n}{a-b} = a^{n-1} + b\frac{a^{n-1} - b^{n-1}}{a-b}$; esto significa que la divisibilidad de $a^n - b^n$ por $a - b$ depende de la divisibilidad de $a^{n-1} - b^{n-1}$ por ese mismo número $a - b$. En consecuencia, un proceso inductivo demuestra que $a^n - b^n$ es divisible por $a - b$ para cualquier $n \in \mathbb{N}$, $n \neq 0$.

Una vez demostrado este hecho, aparecen variados resultados adicionales; por ejemplo, se prueba de inmediato que todos los números de la forma $2^{4n} - 1$ son divisibles por 15 ya que $2^{4n} - 1 = (2^4)^n - 1^n = 16^n - 1^n$ y en consecuencia tal número es divisible por $16 - 1 = 15$. De igual manera, todos los números de la forma $3^{2n} - 1$ son divisibles por 8; todos los números de la forma $a^{3n} - 1$, son divisibles por $a^3 - 1$, para a en los naturales; y en general, todos los números de la forma $a^{mn} - 1$ son divisibles por $a^m - 1$, a, m y n en los naturales.

Ejemplo:

Demostrar que $\forall\, n \in \mathbb{N}$ es cierto que $4^n - 1$ es divisible por 3.

Demostración.

i) Si $n = 1$ se tiene que $4^1 - 1 = 3 = 3 \times 1$, y no se tiene nada más que argumentar.

ii) Se asume que $3\big|(4^k - 1)$, $\forall k \in \mathbb{N}$ y se demuestra que esto también es cierto para su sucesor.

iii) De $3\big|(4^k - 1)$ se sigue $4^k - 1 = 3q$ para un $q \in \mathbb{N}$. Se estudia lo que ocurre para $4^{k+1} - 1$.

$$4^{k+1} - 1 = 4^{k+1} - 1 + 4 - 4 = 4^{k+1} - 4 + 3 = (4^{k+1} - 4) + 3$$

y así $= 4 \cdot (4^k - 1) + 3 = 4 \cdot (3q) + 3$ que se puede reescribir como $3 \cdot (4q) + 3 = 3 \cdot (4q + 1)$ y debido a que $(4q + 1) \in \mathbb{Z}$ se demuestra en efecto que $4^n - 1$ es divisible por 3, $\forall n \in \mathbb{N}$.

Este mismo resultado se establece de manera directa como una consecuencia de que todos los enteros de la forma $a^n - 1$ son divisibles por $a - 1$; en el caso particular es suficiente remplazar a por 4.

El apéndice 1 del libro contiene otros ejemplos que contraponen el método de demostración directa con el de inducción matemática.

Ejemplo:

Demostrar que $\forall n \in \mathbb{N}$, $7|(3^{2n+1} + 2^{n+2})$.

Demostración.

i) Si $n = 1$ se encuentra: $3^3 + 2^3 = 27 + 8 = 35 = 7 \times 5$ lo que evidencia el resultado.

ii) Se adopta como verdad que $\forall k \in \mathbb{N}$ se tiene $7\big|(3^{2k+1} + 2^{k+2})$ y se revisa lo que ocurre cuando se toma $n = k + 1$.

iii) Si $n = k + 1$; $3^{2(k+1)+1} + 2^{(k+1)+2} = 3^{2k+3} + 2^{k+3} = 3^{2k+1} \cdot 3^2 + 2^{k+2} \cdot 2$ que se puede descomponer como $3^{2k+1} \cdot 3^2 - 3^{2k+1} \cdot 2 + 3^{2k+1} \cdot 2 + 2^{k+2} \cdot 2$ y esto a su vez es igual a $3^{2k+1} \cdot (3^2 - 2) + 2 \cdot (3^{2k+1} + 2^{k+2})$. Es el momento de aplicar la hipótesis supuesta en el paso ii), de donde resulta que la última expresión es igual a $3^{2k+1} \cdot (7) + 2 \cdot (7q) = 7 \cdot (3^{2k+1} + 2q)$, para determinado q en el conjunto de los números enteros. Esto confirma que, $\forall n \in \mathbb{N}$ se evidencia que $7|(3^{2n+1} + 2^{n+2})$.

3.9 Números primos

Los números primos son simples y fascinantes; en su nicho subyace la Teoría de Números que, al decir de Carl Friedrich Gauss, es la Reina de las Matemáticas. Estas han preocupado a la humanidad desde mucho antes del período de oro Griego. Por ejemplo, Euclides demostró su infinitud y de su estudio aparece de manera majestuosa el Teorema Fundamental de la Aritmética. Antagónico a su tratamiento teórico y a su existencia misteriosa, los números primos poseen aplicaciones en el mundo moderno; son importantes en las tarjetas de crédito, en la confiabilidad de las telecomunicaciones y en la seguridad de las naciones. La idea fundamental de estas aplicaciones radica en que la factorización de un número con factores primos es un problema de alta complejidad. Por ejemplo, factorizar un número de más de 100 dígitos es casi imposible, aún para los computadores más poderosos; y entonces, se puede codificar un mensaje utilizando un módulo que sea el producto de dos primos gigantes (de más de 100 cifras). Descifrar el mensaje requiere de la factorización de tal producto, que es casi imposible develar, a menos que alguien se conozca los dos factores primos.

Definición:

Un número entero $p \neq 0$ y $p \neq \pm 1$ se llama primo si los únicos divisores de p son ± 1 y $\pm p$.

Ejemplo:

$2, 3\ y\ -7$ son números primos debido a que sus divisores determinan los conjuntos $D(2) = \{1,\ -1, 2, -2\}$; $D(3) = \{1, -1, 3, -3\}$; $D(-7) = \{1, -1, 7, -7\}$.

Los números 1 y -1 no se consideran números primos. Todos los números primos tienen cuatro divisores impropios y ocurre que $D(\pm 1) = \{1,\ -1\}$, esto es, 1 y -1 tan solo tienen dos divisores.

Ejemplo:

$-21\ y\ 30$ no son números primos. En efecto, cada uno de los conjuntos de divisores de estos números contiene más de cuatro elementos, como se ve a continuación:

$D(-21) = \{1,\ -1,\ 3,\ -3,\ 7,\ -7,\ 21,\ -21\}$.
$D(30) = \{1,\ -1,\ 2,\ -2,\ 3,\ -3,\ 5,\ -5,\ 6,\ -6,\ 10,\ -10,\ 15,\ -15,\ 30,\ -30\}$.

Nota

p es un número primo si y sólo si $-p$ es número primo. Sin embargo, y para efectos de demostraciones, sólo se utilizan números primos positivos.

Definición:

Un número entero a se llama compuesto si $a = b \cdot c$ donde $|b| > 1$ y $|c| > 1$ siendo además que $b \in \mathbb{Z}$ y $c \in \mathbb{Z}$.

Con todo esto se tiene que $\forall n \in \mathbb{Z} - \{-1,\ 0,\ 1\}$, $(n \neq 0;\ n \neq \pm 1\ )$, n es primo o n es compuesto.

Definición:

Dos números enteros a y b se llaman Coprimos, Primos Relativos o primos entre sí, si $d|a$ y $d|b$ implica que $d = \pm 1$.

Esto significa que dos números coprimos no tienen más divisores comunes que 1 y -1.

Ejemplo:

Sean p y q números primos distintos, entonces p y q son coprimos puesto que $D(p) = \{1,\ -1,\ p,\ -p\}$ y $D(q) = \{1, -1,\ q, -q\}$ de donde, por simple inspección, se tiene que $D(p) \cap D(q) = \{+1, -1\}$.

Ejemplos

Los números 6 y 21 no son coprimos puesto que sus conjuntos de divisores son: $D(6) = \{1, -1,\ 2, -2,\ 3, -3,\ 6, -6\}$, mientras que para el otro entero se tiene: $D(21) = \{1, -1,\ 3, -3,\ 7, -7, 21, -21\}$; en consecuencia, los divisores comunes son $D(6) \cap D(21) = \{1, -1, 3, -3\}$, conjunto muy distinto de $\{-1, 1\}$. Todo esto asegura, que efectivamente los números 6 y 21 no son coprimos o primos relativos pues poseen otros divisores aparte de $+1$ y de -1.

Definición:

Un resultado importante, que no es competencia de este libro, asegura que dos enteros a y b son coprimos si y sólo si es posible encontrar un par de enteros α y β tales que $1 = a\alpha + b\beta$, es decir, la unidad 1 se puede escribir como combinación lineal de a y de b. Con este presupuesto es

relativamente fácil demostrar que dos naturales consecutivos son primos relativos y a la vez, dos impares consecutivos también son primos relativos.

En efecto, para dos naturales consecutivos n y $n+1$ es suficiente escoger los enteros $\alpha = -1$ y $\beta = 1$ para encontrar que $n(-1) + (n+1)(1) = 1$ lo que demuestra que n y $n+1$ son primos relativos.

Para el caso de dos impares consecutivos $2n-1$ y $2n+1$ es suficiente escoger los enteros $\alpha = -(n+1)$ y $\beta = n$ para escribir la combinación lineal $-(n+1)(2n-1) + n(2n+1) = 1$ y con ello probar la verdad de enunciado. Así que, de manera segura y previa, es posible recitar pares de primos relativos, pero dados dos enteros cualesquiera el problema de determinar su primalidad relativa tiene un algoritmo con algún costo.

3.10 Algoritmo de la división

Al dividir un entero a, entre otro $b \neq 0$, el proceso termina al obtener un residuo r tal que $r = 0$ o $r < b$; es decir, el residuo es cero o menor que el divisor. En el primer caso se dice que la división es exacta y en el segundo que es inexacta.

Por ejemplo, para $a = 571$ y $b = 7$, se encuentra el esquema que siguiente.

571	7
11	81
4	

$571 = 7(81) + 4$ y $4 < 7$.
En general se afirma que si a y b son números enteros y $b \neq 0$, existen los enteros q y r tales que,
$a = b \cdot q + r$ siendo $0 \leq r < b$.

Basta observar que cualquier entero a es, bien, múltiplo de b en cuyo caso se ve que $a = bq$ o bien, está comprendido entre dos múltiplos consecutivos de b; es decir, se encuentra un entero q tal que $bq < a < b(q+1)$.

Si $a = bq$ entonces $r = 0$.
Si $bq < a$ entonces $a - bq = r > 0$ (Residuo por defecto.)
Si $a < bq + b$ entonces $a - bq = r < 0$ (Residuo por exceso.)

Por tanto, siempre se encuentra que $0 \leq r < b$.

Como el divisor b puede ser negativo; por ejemplo, $23 = (-7)(-3) + 2$, se encontraría que $0 \leq 2 < -7$, lo que es absurdo y por tanto, en todos estos casos se hace necesario considerar la división entre el valor numérico del

divisor, esto es, entre su valor absoluto $|b|$. Todo esto se sintetiza en el Algoritmo de la División que se demuestra a continuación.

Teorema 8

Dados los números enteros a, b con $b \neq 0$, existen y son únicos los números enteros q y r, que se denomina cociente y residuo (resto), respectivamente, tales que:

$a = bq + r$, donde $0 \leq r < |b|$.

Demostración

I. Existencia de q y de r

Como $b \neq 0$, puede darse que $b > 0$ o $b < 0$.

i) Para $b > 0$, se construye el conjunto:
$M = \{a - bx : x \in \mathbb{Z} \ \wedge \ a - bx \geq 0\}$ entonces $M \neq \emptyset$ porque:

si $a \geq 0$, para $x = 0$; $a - b \cdot 0 = a$. Luego $(a - b \cdot 0) \in M$.

Si $a < 0$ entonces $b \geq 1$, ya que $b > 0$ y $b \in \mathbb{Z}$, por ello $ab \leq a$.

Así, $a - ab \geq 0$ y en consecuencia $(a - ab) \in M$.

Como $M \subseteq \mathbb{Z}$ está conformado por números positivos, es un conjunto bien ordenado y en consecuencia posee un elemento mínimo que aquí se denomina r tal que, $a - bq = r$ y $0 \leq r$.

Sólo falta demostrar que $r < |b|$.

Al suponer lo contrario, esto es, que $r \geq |b| = b$ se encuentra $r = b + t$ donde $t \in \mathbb{N}$ y por esta razón $a - bq = b + t$, así $t = a - b(q + 1)$ y siendo $r = a - bq$, se concluye que $t < r$ lo que es imposible por la elección de r que es el elemento mínimo de M y esta consideración imposibilita otro aún menor que él. En consecuencia $r < |b|$.

ii)) Para $b < 0$ se sigue que $-b > 0$ y según la parte i), $\exists q' \in \mathbb{Z}$, $\exists r \in \mathbb{Z}$ tales que $a = (-b)q + r$ donde $0 \leq r < |b|$ y haciendo $q = -q'$ se puede escribir $a = bq + r$ con $0 \leq r < |b|$.

II. Unicidad de q y de r.

Al suponer $a = bq + r = bq' + r'$, donde $0 \leq r < |b|$ y $0 \leq r' < |b|$, se tiene que $b(q - q') = r' - r$; esto es, $b|(r' - r)$. Aquí puede ocurrir que $r = 0$ o $r \neq 0$; en este momento es claro que $r \neq 0$ no puede ocurrir pues si fuera el caso que $r \neq 0$, siendo $b|(r' - r)$ se seguiría que $|b||r' - r|$. Pero $0 \leq r < |b|$ y $0 \leq r' < |b|$ se tiene que $|r' - r| < |b|$ lo que es imposible.

De modo que lo único que puede ocurrir es que $r' - r = 0$, o mejor, $r' = r$ y siendo $b \neq 0$ se concluye también que $q = q'$, como se quería probar.

Ejemplo:

Sea $a = 2537$ y $b = 7$, así: $2537 = 7(362) + 3$, con $0 \leq 3 < 7$ siendo $q = 362$ y $r = 3$.

Sea $a = 2537$ y $b = -7$, así, $2537 = (-7)(-362) + 3$, con $0 \leq 3 < |-7|$ siendo $q = -362$ y $r = 3$.

Sea $a = -2537$ y $b = 7$, así: $-2537 = 7(-363) + 4$, con $0 \leq 4 < 7$ siendo $q = -363$ y $r = 4$.

Nota. Si $a \in \mathbb{Z}$, $b \in \mathbb{Z}$ y $b \neq 0$ son tales que $a = bq + r$, $0 \leq r < |b|$, entonces $b|a$, si y sólo si, $r = 0$, lo cual se demuestra a continuación.

($\Rightarrow$) Si $b|a$, $\exists k \in \mathbb{Z}$ tal que $a = bk + 0$; pero se sabe que $a = bq + r$ y por la unicidad del algoritmo de la división, se tiene que $q = k$ pero a la vez $r = 0$.

($\Leftarrow$) Sea $r = 0$. Como $a = bq + r$, con $r = 0$ se escribe de inmediato que $a = bq$ y siendo $b \neq 0$, por definición de divisibilidad se tiene que $b|a$.

Definición:

Un número entero n se llama Par si y sólo si $2|n$, de lo contrario se dice que n es Impar.

Ejercicios

¿Cuáles de los siguientes números enteros son pares?

a) $3n^2 + 1\ , n \in \mathbb{N}$
b) $n(n+1), \quad n \in \mathbb{N}$
c) $(n-1)(n+1), n \in \mathbb{N}$
d) $n^3 - n, \ n \in \mathbb{N}$
e) $n(3n+1), n \in \mathbb{N}$
f) $\frac{(n-3)(n-2)(n-1)n}{4}, n \in \mathbb{N}$
g) $(2n+1)^2 - 3, n \in \mathbb{N}$
h) $(2n+1)^2 - (2n-1)^2 - 1, n \in \mathbb{N}$
i) $(2n+1)^3 + (2n-1)^3 + 1, n \in \mathbb{N}$
j) $\frac{n(n+1)(n+2)}{6}, n \in \mathbb{N}$
k) k) $\frac{(2n-3)(2n-1)(2n+1)}{3}, n \in \mathbb{N}$

Ejemplo:

Hallar el residuo de dividir un número n entre 36, sabiendo que al dividir n entre 4, su residuo es 3 y si n se divide entre 9, su residuo es 5.

Solución:

En concordancia con los datos del problema se puede escribir para sendos números enteros q y k que el número n es $n = 4q + 3$ y $n = 9k + 5$; en consecuencia, $4q + 3 = 9k + 5$ o sea $4q - 9k = 2$ que, un poco modificado asegura que, $4(q - 2k) = k + 2$.

Así que, $4|(k+2)$; es decir $k + 2 = 4t$, para algún $t \in \mathbb{Z}$; por ello $k = 4t - 2$.

Al remplazar en n se encuentra: $n = 9(4t - 2) + 5$ y por tanto $n = 36t - 18 + 5$ o mejor $n = 36t - 13 = 36(t-1) + 23$, por lo cual, el cociente es $q = t - 1$ y el residuo es 23.

3.11 El máximo común divisor - MCD

El máximo común divisor de dos enteros resulta ser uno de los conceptos de gran utilidad en la resolución de diversos problemas, sobre todo aquellos relacionados con la teoría de números. Es un concepto en el que se aplica el algoritmo de la división desarrollado por Euclides y que también está relacionado con las fracciones continuas simples.

Definición:

Un número entero positivo d es llamado el Máximo Común Divisor de dos enteros a y b si cumple lo siguiente:

1. $d|a$ y $d|b$
2. Si existe $c \in \mathbb{Z}^+$ tal que $c|a$ y $c|b$, entonces $c|d$.

En el texto Aritmética Elemental de Enzo R. Gentile de la serie de Matemática, divulgado por la secretaría general de la OEA, se adopta como máximo común divisor de los números a y b al valor $d \in \mathbb{N}$ tal que cumple las siguientes dos propiedades:

1. $d|a$ y $d|b$
2. existen los enteros u y v tales que $d = au + bv$.

Hecho que Gentile demuestra utilizando inducción completa y del cual se deja como ejercicio el demostrar que este resultado es equivalente a la definición anterior.

El máximo común divisor de a y b se denota por $d = MCD\ (a,b)$, notación que con frecuencia se simplifica por $d = (a,b)$.

A continuación se presentan algunos ejemplos del Máximo Común Divisor en los que se ha puesto frente a cada uno de ellos, el conjunto de los divisores comunes.

$M.C.D.(6{,}15) = (6{,}15) = 3$	$DC(6{,}15) = \{1,\ 3\}$
$M.C.D.(8{,}20) = (8{,}20) = 4$	$DC(6{,}15) = \{1,\ 2,\ 4\}$
$M.C.D.(5{,}9) = (5{,}9) = 1$	$DC(5{,}9) = \{1\}$
$M.C.D.(20{,}30) = (20{,}30) = 10$	$DC(20{,}30) = \{1,\ 2,\ 5,\ 10\}$
$M.C.D.(12{,}30) = (12{,}30) = 6$	$DC(12{,}30) = \{1,\ 2,\ 3,\ 6\}$

Un procedimiento familiar para encontrar el Máximo Común Divisor de dos números, consiste en aplicar el Teorema Fundamental de la Aritmética y descomponer cada número en sus factores primos y luego conformar el producto de los factores primos comunes tomando el menor exponente.

Por ejemplo, para calcular $d = MCD\ (504{,}540) = (504{,}540)$ se observa que la descomposición de estos números es $504 = 2^3 \times 3^2 \times 7$ y $540 = 2^2 \times 3^3 \times 5$; por lo tanto $d = 2^2 \times 3^2 = 4 \times 9 = 36$.

El $M.C.D.(a,b)$ también se puede encontrar mediante la aplicación reiterada del algoritmo de la división; en este caso, d es el último residuo no nulo. El teorema siguiente, que asegura lo mencionado, se conoce como el algoritmo de Euclides.

Teorema 9

Si $a = bq + r$ en $\mathbb{Z}$, entonces, $MCD\ (a,b) = (a,b) = MCD\ (b,r) = (b,r)$.

Demostración

Sea $d = MCD\ (a,b)$ y $d_1 = MCD\ (b,r)$, entonces, por definición se ve que $d|a$ y $d|b$; en consecuencia, $d|(a - bq)$, es decir, $d|r$.

Ahora, $d_1|b$ y $d_1|r$, por ello, $d_1|(bq + r)$ es decir, $d_1|a$. Esto asegura que, como $d|d_1$ y $d_1|d$; o mejor $d \leq d_1$ y $d_1 \leq d$, de acuerdo con la teoría de divisibilidad, de donde $d = d_1$, tal como se quería demostrar.

A continuación se presenta la generalización del procedimiento. Para ello se considera $0 < b < a$ y por el algoritmo de la división, $\exists q_1$ y $\exists r_1$ en $\mathbb{Z}$ tal que,

P1. $a = bq_1 + r_1$ donde $0 \leq r_1 < b$.

Si $r_1 = 0$ entonces $b|a \ \Rightarrow\ MCD\ (a,b) = b$. Además $b = a \cdot 0 + b \cdot 1$.

Si $r_1 \neq 0$, por el teorema arriba demostrado, se tiene que:

$MCD\ (a,b) = MCD\ (b,r_1)$ y por esto $\exists q_2$ y $\exists r_2$ en $\mathbb{Z}$ tal que,

P2. $b = r_1q_2 + r_2$ donde $0 \leq r_2 < r_1$.

Si $r_2 = 0$ entonces $r_1|b \ \Rightarrow\ MCD\ (b,r_1) = r_1 = MCD\ (a,b)$.

Además $r_1 = a \cdot 1 + b \cdot (-q_1)$.

Si $r_2 \neq 0$ se halla $MCD\ (r_1,r_2) = MCD\ (b,r_1) = M.C.D.(a,b)$ y además $\exists q_3,\ \exists r_3$ en $\mathbb{Z}$ tales que,

P3. $r_1 = r_2q_3 + r_3$ donde $0 \leq r_3 < r_2$.

Si $r_3 = 0$, entonces,

$$r_2|r_1 \ \Rightarrow\ MCD\ (r_1,r_2) = r_2 = MCD\ (b,r_1) = MCD\ (a,b).$$

Además $r_2 = b + r_1 \cdot (-q_2)$ y esto es $= b + [a + b(-q_1)](-q_2)$ que se escribe mejor como $= a(-q_2) + b(1 + q_1q_2)$.

Si $r_3 \neq 0$; $MCD\ (r_2,r_3) = MCD\ (r_2,r_1) = MCD\ (b,r_1) = MCD\ (a,b)$ y además $\exists q_4,\ \exists r_4$ en $\mathbb{Z}$ tales que,

Pk. $r_{k-2} = r_{k-1}q_k + r_k$ con $0 \leq r_k < r_{k-1}$ y debido a que se tiene una cola de descenso finito

$\ldots < r_3 < r_2 < r_1 < b$ en $\mathbb{Z}$ el proceso no continúa indefinidamente, llegando a

P(k+1), paso en el cual se tiene que $r_{k-1} = r_kq_{k+1} + 0$ y por definición de Máximo Común Divisor y por sustituciones consecutivas se ve que,

$M.C.D.(r_k, r_{k-1}) = r_k = MCD\ (r_{k-2}, r_{k-1}) = \ldots MCD\ (b, r_1) = MCD\ (a, b)$, como se quería demostrar.

Además, $\exists x, \exists y$ en $\mathbb{Z}$ tales que $r_k = MCD\ (a, b) = ax + by$; esto es, el máximo común divisor de dos números enteros se puede expresar como una combinación lineal de sus argumentos.

Nota:

Para un par de números enteros no nulos a y b se tiene que:

$$MCD\ (a, b) = MCD\ (b, a) = MCD\ (-a, b) = MCD\ (a, -b) = MCD\ (-a, -b)$$

Ejemplo:

Hallar el $MCD\ (432{,}342)$ y expresarlo como combinación lineal de estos dos enteros.

a) $432 = 2^4 \times 3^3$ y $342 = 2 \times 3^2 \times 19$; así, $MCD\ (432{,}342) = 2 \times 3^2 = 18$.
b) $432 = 342(1) + 90$
$342 = 90(3) + 72$
$90 = 72(1) + 18$
$72 = 18(4) + 0$ de donde,
$18 = 90 + 72(-1) = 90 + [342 + 90(-3)](-1) = 342(-1) + 90(4)$
$= 342(-1) + [432 + 342(-1)](4) = 4(432) + 342(-5)$.

Ejemplo:

Determinar el $MCD\ (432, -342)$:

$432 = (-342)(-1) + 90$
$-342 = 90(-4) + 18$
$90 = 18(5) + 0$ y
$18 = (-342) + 90(4) = (-342) + [432 + (-342)(1)](4)$
$= 4(432) + 5(-342)$.

Igual procedimiento se desarrolla para calcular el máximo común divisor; por ejemplo, de -432 y 342 o si se quiere de -432 y -342.

De hecho, existe el máximo común divisor de a y b $d = MCD\ (a, b)$, si y sólo si $\exists\ x, \exists\ y$ en $\mathbb{Z}$ tales que $d = MCD\ (a, b) = ax + by$; es decir, sí se puede escribir como combinación lineal de sus argumentos.

El algoritmo descrito para calcular el máximo común divisor de dos enteros positivos es susceptible de incorporarse en el sistema de cálculo simbólico Maple puesto que el cálculo de la combinación lineal que lo expresa como combinación lineal de sus argumentos, resulta costoso por la inversión de tiempo. El procedimiento posee la siguiente sintaxis:

```
euclides:=proc(m,n::nonnegint)
local q,r,a,b,a1,b1,c,t,d:nonnegint:
a1:=1; r:=1;
b:=1;
a:=0;
b1:=0;
c:=m;
d:=n;
while r<>0 do
        q:=iquo(c,d):
        r:=irem(c,d);
        if r=0 then RETURN(`El
mcd(`||m||`,`||n||`)=`||d||`=(`||m||`)*(`||a||`)+(`||n||`)*(`||b||`)`
); fi:
   c:=d:
   d:=r:
   t:=a1:
   a1:=a:
   a:=t-q*a:
   t:=b1:
   b1:=b:
   b:=t-q*b:
 od:
 print(``);
 end:
```

Al invocar, por ejemplo, euclides (45454,667676), se consigue lo siguiente:

mcd (45454, 667676)= 2 =(45454)(-22533) + (667676)(1534).

euclides (12345,345); señala que,
mcd (12345,345)=15=(12345)(9) + (345)(-322).

3.12 Fracciones continuas simples

Las fracciones continuas simples se derivan del algoritmo de la división de Euclides y en consecuencia tienen fuerte relación con el máximo común divisor de dos enteros. Una aplicación directa de su uso aparece en la

aproximación a irracionales por racionales lo que se consigue al ir agregando pisos a la representación de un irracional mediante una Fracción Continua Simple Infinita. En este parágrafo se estudian algunos resultados que se evidencian al aplicar un archivo de utilidad escrito para el asistente matemático Derive.

Para encontrar el $M.C.D(a,b)$ se ha aplicado reiteradamente el algoritmo de la división, como se evidencia en el siguiente esquema:

$a = bq_1 + r_1$ donde $0 \leq r_1 < b$
$b = r_1 q_2 + r_2$ con $0 \leq r_2 < r_1$
$r_1 = r_2 q_3 + r_3$ con $0 \leq r_3 < r_2$
...
$r_{k-2} = r_{k-1} q_k + r_k$ con $0 \leq r_k < r_{k-1}$
$r_{k-1} = r_k q_{k+1} + 0$ y por tanto $r_k = M.C.D(a,b)$

Todo esto se puede expresar en términos de fracciones y encontrar el valor aproximado de $\frac{a}{b}$ al número de cifras decimales que se quiera:

$\frac{a}{b} = q_1 + \frac{r_1}{b}$ con $\frac{r_1}{b} < 1$
$\frac{b}{r_1} = q_2 + \frac{r_2}{r_1}$ y $\frac{r_2}{r_1} < 1$
$\frac{r_1}{r_2} = q_3 + \frac{r_3}{r_2}$ con $\frac{r_3}{r_2} < 1$
...
En la primera ecuación se remplaza $\frac{r_1}{b}$ por $\frac{1}{\frac{b}{r_1}}$ para obtener la secuencia $\frac{a}{b} = q_1 + \frac{r_1}{b} = q_1 + \frac{1}{\frac{b}{r_1}} = q_1 + \frac{1}{q_2 + \frac{r_2}{r_1}} = q_1 + \frac{1}{q_2 + \frac{1}{\frac{r_1}{r_2}}} = q_1 + \frac{1}{q_2 + \frac{1}{q_3 + \frac{r_3}{r_2}}} = \ldots$ y así sucesivamente.

Este tipo de escritura por pisos es engorrosa y por ello es preferible escribir, con el mismo significado, de manera horizontal como $\frac{a}{b} = [q_1;\ q_2,\ q_3,\ q_4, \ldots]$. El punto y coma (;) separa la parte entera de la parte fraccionaria cuando se expresa el racional $\frac{a}{b}$ en fracción continua. Las fracciones continuas simples son fracciones compuestas de varios pisos, tales que todos los numeradores son iguales a 1 y los denominadores son números naturales diferentes de 0 y 1.

Ejemplo:

Antes se encontró que,

$$432 = 342(1) + 90$$
$$342 = 90(3) + 72$$
$$90 = 72(1) + 18$$
$$72 = 18(4) + 0$$

En consecuencia, se puede escribir así:

$$\frac{432}{342} = 1 + \frac{90}{342} = 1 + \frac{1}{\frac{342}{90}} = 1 + \frac{1}{3+\frac{72}{90}} = 1 + \frac{1}{3+\frac{1}{\frac{90}{72}}} = 1 + \frac{1}{3+\frac{1}{1+\frac{18}{72}}} = 1 + \frac{1}{3+\frac{1}{1+\frac{1}{\frac{72}{18}}}}$$

expresión que, en definitiva, se escribe como sigue:

$$1 + \frac{1}{3+\frac{1}{1+\frac{1}{4}}} = [1;\ 3,\ 1,\ 4].$$

En este caso $1 + \frac{1}{3+\frac{1}{1+\frac{1}{4}}} = 1 + \frac{1}{3+\frac{1}{\frac{5}{4}}} = 1 + \frac{1}{3+\frac{4}{5}} = 1 + \frac{1}{\frac{19}{5}} = 1 + \frac{5}{19}$; lo que significa que, $\frac{432}{342} = \frac{24}{19}$. Si se corta el último piso o los últimos pisos, se logran aproximaciones del racional en estudio. Con fracciones continuas simples también se puede escribir números irracionales y con ello, cualquier número real y encontrar aproximaciones por defecto o por exceso a cualquier irracional algebraico o trascendente.

Las fracciones continuas juegan un papel importante en algunas ramas de las matemáticas; se utilizan en el aislamiento de raíces reales de polinomios con coeficientes enteros y, como ya se ha mencionado, en el cálculo del máximo común divisor de dos números naturales. El italiano Rafael Bombelli, en los escritos realizados entre 1572 a 1579, los cuales tratan sobre el álgebra, relata sobre una forma de calcular en forma aproximada las raíces que resultan al emplear las fórmulas de Tartaglia, Cardano y Ferrari. El método empleado por Bombelli, hoy se considera como la introducción al mundo académico de las fracciones continuas. Este método aparece explicado en las páginas 61 y 62 del texto *Recorriendo el Álgebra* publicado por la Universidad Nacional de Colombia y escrito por las profesoras Mary Falk de Losada y Miriam Acevedo.

Una tarea de ingente esfuerzo, es la de convertir un racional en fracción continua simple, es decir, en una fracción continua tal que todos sus

numeradores sean 1 y, al contrario, convertir una fracción continua simple en el racional que le corresponde. Dado que una fracción continua puede tener muchos pisos, es preferible dejar esta tarea a las máquinas y en concordancia con ello, se dispone a continuación un archivo que ejecuta las dos acciones de simplificación de manera confiable y rápida, escrito para el programa de asistencia matemática Derive en su versión 5.

Se define un vector vacío:

$v := []$

Se invierte la cadena de entrada del vector:

$u := REVERSE\_VECTOR\ (v)$

Se extrae cualquier elemento del vector invertido, en particular se escoge el último:

$A(m) := ELEMENT(u, m)$

Se define una función recurrente:

$G(s) := IF\ (s = 1, A(1), A(s) + 1/G(s - 1))$

Ahora se define la fracción continua que le corresponde al vector V:

$CONTINUA\ (v) := G(DIMENSION(v))$

Para realizar el procedimiento inverso y dado que la profundidad de cálculo se desconoce, esto es, se ha convertido en un problema abierto, se toma la respuesta hasta el primer infinito que aparezca en su simplificación, primero se define la función:

$R(x) := 1/(x - FLOOR(x))$

Y la función que calcula la fracción continua correspondiente al racional t:

$LINEAL\ (t, n) := FLOOR(ITERATES(R(x), x, t, n))$.

Por ejemplo, para calcular el racional que le corresponde a la fracción continua simple $x = 1 + \frac{1}{3+\frac{1}{1+\frac{1}{4}}}$, es suficiente definir $v := [1,3,1,4]$ y a continuación simplificar la expresión CONTINUA(v) con lo que se encuentra el racional $\frac{24}{19}$.

Para escribir el racional $\frac{35}{143}$ en fracción continua simple, se simplifica la expresión LINEAL (35/143, 6) con lo cual se obtiene el vector $[0,4,11,1,2,\pm\infty,?]$, lo que significa que $\frac{35}{143} = [0; 4,11,1,2]$.

Para las fracciones continuas simples se tienen varios resultados entre los que sobresalen los siguientes:

- Cualquier fracción continua simple finita representa a un número racional y a la inversa, todo número racional se puede expresar de manera única como una fracción continua simple finita.

- Todo número irracional se expresa de manera única mediante una fracción continua simple infinita e inversamente, toda fracción infinita representa a un número irracional.

- Toda fracción continua simple infinita y periódica representa a un irracional de la forma $\sqrt{n}$, donde n es un número natural, por

  ejemplo:$\sqrt{7} = [2; 1,1,1,4,1,1,1,4,..] = \left[2;\ \overline{1,1,4}\right]$.

- Todo irracional de la forma $\sqrt{n^2+1}$. es $\sqrt{n^2+1} = [n; 2n, 2n, 2n,..] = \left[n; \overline{2n}\right]$.

  En efecto, al llamar $x = \sqrt{n^2+1}$ se encuentra de inmediato que $x^2 - n^2 = 1$ y por esto $(x-n)(x+n) = 1$, de donde se obtiene $x - n = \frac{1}{n+x}$; esto es, $x = n + \frac{1}{n+x}$. Ahora basta remplazar de manera reiterada sobre x el valor encontrado; en el siguiente paso se consigue la expresión $x = n + \frac{1}{2n+\frac{1}{1+x}}$. Continuando así se obtiene, tal como se anotó al principio, que,
  $\sqrt{n^2+1} = [n; 2n, 2n, 2n,..] = \left[n; \overline{2n}\right]$.

Este resultado es de importancia en Teoría de Números ya que permite establecer que una fracción continua infinita es la raíz de una ecuación polinómica cuadrática si y sólo si, es periódica. En esta dirección se anotan los dos siguientes resultados.

1. El irracional $[0;\overline{m}]$ es raíz de la ecuación cuadrática $x^2 - mx - 1 = 0$.
2. Si m es un entero mayor que 1, entonces los irracionales $\left[0; m, \overline{1, m-1}\right]$ y $\left[m; \overline{1, m-1}\right]$ satisfacen la ecuación cuadrática $x^2 - (m+1)x + 1 = 0$.

- Todo irracional de la forma $\sqrt{n^4 - 1}$ en su escritura como fracción continua simple infinita es igual a $\sqrt{n^4 - 1} = \left[n^2 - 1;\ \overline{1,\ 2(n^2-1)}\right]$; por ejemplo, $\sqrt{4^4 - 1} = \sqrt{255} = \left[15;\ \overline{1,\ 30}\right]$.

- Todo irracional de la forma $\sqrt{n^4 + 1}$ en su escritura como fracción continua simple infinita es igual a la siguiente expresión: $\sqrt{n^4 + 1} = \left[n^2;\ \overline{2n^2}\right]$.

  Por ejemplo, $\sqrt{4^4 + 1} = \sqrt{257} = \left[16;\ \overline{32}\right]$.

  En efecto, al disponer $\sqrt{257} = x$ se sigue que $x^2 = 257$ de donde $x^2 - 256 = 1$, esto es, $x^2 - 16^2 = 1$ y por consiguiente se tiene que $(x-16)(x+16) = 1$. De aquí se obtiene que, $x - 16 = \frac{1}{(16+x)}$, esto es $x = 16 + \frac{1}{16+x}$. Al remplazar el valor de x en el denominador, se encuentra que, $x = 16 + \frac{1}{32 + \frac{1}{16+x}}$ y así se puede proceder indefinidamente.

  A continuación, se ilustra el procedimiento general para la obtención de la fracción continua simple periódica para este tipo de expresiones. Al llamar $\sqrt{n^4 + 1} = x$, de inmediato se tiene que $x^2 = n^4 + 1$ y en consecuencia, $x^2 - n^4 = 1$ de donde $(x - n^2)(x + n^2) = 1$, y por ello, $x - n^2 =$

$\frac{1}{x+n^2}$, es decir, $x = n^2 + \frac{1}{n^2+x}$. Al remplazar, en esta última expresión el valor de x se tiene,

$$x = n^2 + \frac{1}{2n^2 + \frac{1}{n^2 + x}} = \left[n^2;\quad \overline{2n^2}\right].$$

- Leonhard Euler demostró en 1737que el valor de una fracción continua simple periódica, constituye una irracionalidad cuadrática. Por ejemplo, la fracción $[1; 1,1,1,1,1,1, \dots] = \left[1; \overline{1}\right]$ se corresponde con la razón áurea:

  $\Phi = \frac{1+\sqrt{5}}{2}$.

- En 1770, Joseph Louis Lagrange consigue demostrar el inverso del resultado anterior; es decir, que toda irracionalidad cuadrática se representa mediante una Fracción Continua Simple Periódica.

  El archivo de utilidad escrito antes, para ejecutarlo en el programa Derive, ayuda a evidenciar este hecho, al simplificar expresiones como las dos que se proponen a continuación:

  LINEAL((5+SQRT(7))/3, 12) que produce $[2,1,1,4,1,1,1,4,1,1,1,4,1]$ y esto significa que,

  $\frac{5+\sqrt{7}}{3} = \left[2,1,1,4,\overline{1,1,1,4}\right]$.

  LINEAL((1+5*SQRT(17))/8,20) que al simplificarse determina el vector $[2, 1, 2, 2, 1, 4, 2, 4, 1, 2, 2, 1, 4, 2, 4, 1, 2, 2, 1, 4, 2]$, que se puede escribir de la siguiente manera:

  $\frac{1 + 5\sqrt{17}}{8} = \left[2, \overline{1, 2, 2, 1, 4, 2, 4}\right]$.

- Los números trascendentes admiten escritura como fracción continua simple aperiódica; tal es el caso de los reales π y e.

  En el caso de π, se encuentra que $\pi =$
  [3, 7, 15, 1, 292, 1, 1, 1, 2, 1, 3,...] y con la aproximación

[3, 7, 15, 1] se consigue el racional $\frac{355}{113} \approx \pi$ muy llamativa pues se produce a partir de la repetición en duplas de los primeros tres números impares 113355, bloque que se divide en dos grupos iguales $113|355$ y se configura la fracción de modo que la primera mitad es el denominador y la segunda el numerador.

La escritura de e cómo fracción continua simple, a pesar de carecer de período, posee una regularidad llamativa, y es que a partir del tercer elemento aparece la secuencia de los números pares, siendo que entre dos de ellos se intercalan siempre dos unos. Su escritura como fracción continua es la siguiente:

$$e = [2,\ 1,\ 2,\ 1,\ 1,\ 4,\ 1,\ 1,\ 6,\ 1,\ 1,\ 8,\ 1,\ 1,\ 10,\ 1,\ 1{,}12,\ 1,\ 1,\ 14, \ldots].$$

3.13 Propiedades del máximo común divisor - MCD

A continuación, se presentan algunas propiedades que satisface el máximo común divisor de dos enteros; algunas de ellas tienen fuerte conexión con el álgebra elemental y su demostración es una aplicación directa de alguna identidad algebraica. En cada uno de los casos se presenta una demostración simplificada de la propiedad en estudio y ocasionalmente un ejemplo numérico.

1. Si d es el máximo común divisor de a y b, $MCD\ (a,b) = d$, entonces $MCD\left(\frac{a}{d}, \frac{b}{d}\right) = 1$. En efecto, como $MCD\ (a,b) = d$, existen un par de números x y y en $\mathbb{Z}$ tales que $d = ax + by$ y como $d \neq 0$ y $d > 0$, siendo divisor común de a y b, se escribe $1 = \left(\frac{a}{d}\right)x + \left(\frac{b}{d}\right)$, lo que demuestra que, efectivamente, $MCD\left(\frac{a}{d}, \frac{b}{d}\right) = 1$.

2. Si $MCD\ (a,b) = d$ entonces para cualquier entero λ, siendo $\lambda \neq 0$, se encuentra que $MCD\ (\lambda a, \lambda b) = |\lambda| d$.

   A partir de los resultados anteriores se deduce que, si $d|a$ y $d|b$ implica $\lambda d|\lambda a$ y $\lambda d|\lambda b$; en consecuencia, $\lambda d|(\lambda a \pm \lambda b)$. Ahora, si $d = MCD\ (a,b)$, $\exists x,\ \exists y$ en $\mathbb{Z}$ tales que $d = ax + by$ y como $\lambda \neq 0$, se puede escribir $\lambda d = \lambda ax + \lambda by$, así $MCD\ (\lambda a, \lambda b) = \lambda d$ que se puede anotar como $MCD\ (\lambda a, \lambda b) = |\lambda| d$.

3. Si $MCD\ (a,b) = d$ y $MCD\ (c,b) = 1$, entonces $MCD\ (ac,b) = d$. Esto se deduce porque $d = MCD\ (a,b)$ implica que $d = ax + by$, para algún $x \in \mathbb{Z}$ y para algún $y \in \mathbb{Z}$. De igual modo, si $1 = M.C.D(c,b)$, se tiene que $1 = cm + bn$ para determinados m y n en $\mathbb{Z}$. Al multiplicar estas dos igualdades se consigue $d \cdot 1 = (ax + by) \cdot (cm + bn) = ac(xm) + b(axn + cym + byn)$. Pero las expresiones $(axn + cym + byn) \in \mathbb{Z}$ y $(xm) \in \mathbb{Z}$; esto implica que:

   $d = MCD\ (ac,b)$.

4. Si $a|(b \cdot c)$ y $M.C.D(a,b) = 1$ entonces $a|c$.

   Esto resulta porque $a|(b \cdot c)$ implica la existencia de un entero k tal que $bc = ak$ y siendo $MCD\ (a,b) = 1$, existen enteros x y y para los cuales $1 = ax + by$; multiplicando esta igualdad por c se tiene $c = acx + bcy$ y siendo $bc = ak$ se sigue que $c = acx + aky = a(cx + ky)$ y como $(cx + ky) \in \mathbb{Z}$ se concluye que efectivamente $a|c$.

5. Si $a|c$ y $b|c$ y $MCD\ (a,b) = 1$ se desprende que $(ab)|c$.

   La conclusión es clara, ya que $a|c$ y $b|c$ indica la existencia de los enteros k y t para los cuales se hace evidente que $c = a \cdot k$ y $c = b \cdot t$ y siendo que $MCD\ (a,b) = 1, \exists x \in \mathbb{Z}, \exists y \in \mathbb{Z}$ para los cuales $1 = ax + by$; igualdad que al multiplicarla por c produce: $c = acx + bcy$ y sustituyendo de forma adecuada los valores de c se consigue $c = abty + baky$ que escrito como $c = ab(tx + ky)$ indica que $(ab)|c$ por definición de divisibilidad ya que $(tx + ky) \in \mathbb{Z}$.

6. Si $MCD\ (a,b) = 1$ y además $a > b$, se tiene que $MCD\ (a - b, b) = 1$.

   En efecto; siendo $MCD\ (a,b) = 1$ existen enteros α y β tales que $\alpha a + \beta b = 1$ de donde se encuentra que $\alpha(a - b) + (\alpha + \beta)b = 1$ y esto demuestra que, $M.C.D(a - b, b) = 1$.

7. Para todo par de enteros positivos a y b se tiene que $MCD\ (a,\ ab + 1) = 1$ y $MCD\ (a,\ ab - 1) = 1$.

   Esto se comprueba al escribir $(-b)a + (1)(ab + 1) = 1$ y $(b)a + (-1)(ab - 1) = 1$. Al escoger una potencia n también se evidencia que $MCD\ (a,\ ab^n + 1) = 1$ y $MCD\ (a,\ ab^n - 1) = 1$.

En particular se encuentra que $MCD\ (a,\ a^n + 1) = 1$ y $MCD\ (a,\ a^n - 1) = 1$, para todo natural n cuando se dispone $a = b$.

8. En el caso de tomar $n > m$ entre los naturales y otro entero positivo a se hace evidente que $(-a^{n-m})a^m + (1)(a^n + 1) = 1$; también se encuentra que $(a^{n-m})a^m + (-1)(a^n - 1) = 1$ con lo que se demuestra que:

   $MCD\ (a^m,\ a^n + 1) = 1$ y $MCD\ (a^m,\ a^n - 1) = 1$.

   Por ejemplo,

   $MCD\ (7^8,\ 7^9 + 1) = MCD\ (5764801, 40353608) = 1.$

   $MCD\ (7^8,\ 7^9 - 1) = MCD\ (5764801, 40353606) = 1.$

   En el numeral 7 se probó que $MCD\ (a,\ a^n + 1) = 1$ y $MCD\ (a,\ a^n - 1) = 1$ para cualquier par de naturales a y n; en consecuencia, cualquier potencia de a carece de factores comunes diferentes de la unidad con $a^n + 1$ o con $a^n - 1$ y por ello $MCD\ (a^m,\ a^n + 1) = MCD\ (a^m,\ a^n - 1) = 1$ sin restricción de los valores de n y m.

   Un ejemplo de esta situación se exhibe en los siguientes casos:

   $MCD\ (3^{12},\ 3^8 + 1) = MCD\ (531441{,}6562) = 1.$

   $MCD\ (3^{12},\ 3^8 - 1) = MCD\ (531441{,}6560) = 1.$

9. Para todo par de enteros positivos a y n, un malabar algebraico recuerda que, $a^{n+1} - 1 = (a-1)(1 + a + a^2 + \cdots + a^n)$, expresión que se reescribe como $(1)a^{n+1} + (1-a)(1 + a + a^2 + \cdots + a^n) = 1$ y esto asegura en definitiva que $MCD\ (a^{n+1},\ 1 + a + a^2 + \cdots + a^n)$.

   De aquí también se deriva que $MCD\ (a,\ 1 + a + a^2 + \ldots + a^n) = 1$.

   Para el caso en que $a = 3$ y $n = 6$, se encuentra $MCD\left(3^7,\ \sum_{i=0}^{6} 3^i\right) = MCD\ (2187,\ 1093) = 1$ y si se dispone $a = 8$ y $n = 12$, se halla que,

$$MCD\left(8^{13},\ \sum_{i=0}^{12} 8^i\right) = MCD\ (549755813888,\ 78536544841) = 1.$$

De forma similar, $a^{2n+1}+1=(a+1)(1-a+a^2-\ldots+a^{2n})$ para cualquier par de valores naturales a y n; es decir, $(-1)a^{2n+1}+(a+1)\sum_{i=0}^{2n}(-a)^i=1$ y esto significa que $MCD\left(a^{2n+1},\ \sum_{i=0}^{2n}(-a)^i\right)=1$.

Por ejemplo, al disponer $a=4$ y $n=3$ se halla que:

$$MCD\left(4^7,\ \sum_{i=0}^{6}(-4)^i\right)=MCD\ (16384,\ 3277)=1.$$

10. Una identidad que asombra por la sutileza de la utilización del máximo común divisor sobre tres números enteros fue demostrada hacia 1996 y publicada en la revista Sigma, de la Sociedad Nariñense de Matemáticas en ese mismo año; sin embargo, su demostración atraviesa la teoría de grupos y por ello rebasa los objetivos de este libro. La identidad afirma simplemente que:

$$\frac{MCD\ (n\ MCD\ (a,\ b),\ \ ab)}{MCD\ (n,\ a)\ \times MCD(n,b)}=\frac{MCD\ (a,\ b)}{MCD\left(n,MCD\ (a,\ b)\right)}.$$

o más simplificado,

$$\frac{(n\ (a,\ b),\ \ ab)}{(n,\ a)\times(n,\ b)}=\frac{(a,\ b)}{\left(n,(a,\ b)\right)}.$$

Cada uno de los miembros de la identidad, es un número entero y en consecuencia se evidencia que el producto $MCD\ (n,\ a)\times MCD\ (n,\ b)$ y cada uno de los factores $MCD\ (n,\ a)$ y $MCD\ (n,\ b)$ es un divisor de $MCD\ (n\ MCD\ (a,\ b),ab)$ y también se encuentra que el entero $MCD\left(n,MCD\ (a,\ b)\right)$ es un divisor de $MCD\ (a,b)$.

11. Dos impares inter-consecutivos son primos entre sí. Impares de esta clase son aquellos en los que media otro impar.

Esto se evidencia al utilizar el algoritmo de Euclides puesto que, para los impares $2n+5$ y $2n+1$ se tiene $2n+5=(2n+1)(1)+4$ y por ello,

$MCD\ (2n+5,2n+1) = MCD\ (2n+1,4)$.

Pero ocurre que los impares son de la forma $4m+1$ o de la forma $4m+3$. Para los primeros se tiene $(4m+1)(1)+(4)(-m)=1$ y para los segundos $(4m+3)(-1)+(4)(m+1)=1$. En consecuencia, para cualquier impar $2n+1$ se encuentra que $MCD\ (2n+1,4)=1$.

En definitiva, $MCD\ (2n+5,2n+1)=1$.

12. Si $a, b_1, b_2, b_3, \ldots, b_n$ es una colección de enteros y $MCD\ (a,b_i) = 1, \forall\ i, 1 \leq i \leq n$, entonces,

$$MCD\ (a, b_1 \cdot b_2 \cdot \cdots \cdot b_n) = \left(a, \prod_{i=1}^{n} b_i\right) = 1.$$

Este hecho se demuestra utilizando el Principio de Inducción Completa.

i) Si $n=1$ queda probado que $MCD\ (a,b_1)=1$, y por ello, $\exists\ x_1 \in \mathbb{Z}, \exists\ y_1 \in \mathbb{Z}$ tales que $1 = ax_1 + b_1y_1$.

Sea $MCD\ (a,b_2)=1$ entonces $\exists\ x_2 \in \mathbb{Z}$, $\exists\ y_2 \in \mathbb{Z}$ tales que $1 = ax_2 + b_2y_2$ igualdad que al multiplicarse con el anterior 1 da como resultado el producto:

$$1 = (ax_1 + b_1y_1)(ax_2 + b_2y_2) = a(x_1ax_2 + x_1b_2y_2 + x_2b_1y_1) + b_1b_2(y_1y_2)$$

con lo cual, se tiene que $MCD\ (a, b_1b_2) = 1$.

ii) Si $MCD\ (a, b_1b_2 \ldots b_k) = 1$, entonces, existen una pareja de números enteros X y Y para los cuales $1 = aX + (b_1b_2 \cdots b_k)Y$. Se debe probar que el enunciado es cierto si se escoge otro primo relativo con a.

iii) Como $MCD\ (a, b_{k+1}) = 1$, $\exists \alpha \in \mathbb{Z}$ y $\exists \beta \in \mathbb{Z}$ para los cuales se consigue que $1 = a\alpha + b_{k+1}\beta$.

Al multiplicar esta unidad con la unidad escrita como la combinación lineal del paso ii), se obtiene:

$$1 = a[Xa\alpha + Xb_{k+1}\beta + \alpha(b_1b_2 \ldots b_k)Y] + [b_1b_2 \ldots b_kb_{k+1}]Y\beta.$$

Por esta razón se tiene que, efectivamente, $MCD\ (a, b_1 b_2 \cdots b_k b_{k+1}) = 1$, por lo cual, si $a, b_1, b_2,\ b_3, \ldots,\ b_n$ son enteros tales que $M.C.D(a, b_i) = 1, \forall i, 1 \leq i \leq n$, entonces,

$$MCD\ (a, b_1 \cdot b_2 \cdot \ldots \cdot b_n) = \left(a, \prod_{i=1}^{n} b_i\right) = 1, \forall\ n \in \mathbb{N}.$$

Por ejemplo, el producto de cualquier colección finita de números impares es primo relativo con 2; en particular, la colección puede estar formada por números primos mayores que 2.

Una consecuencia de esta propiedad es que si $MCD\ (a, b) = 1$ se tiene de inmediato que $MCD\ (a^m, b^n) = 1,\ \forall m \in \mathbb{N},\ \forall n \in \mathbb{N}$.

3.14 El mínimo común múltiplo - MCM

El objeto matemático denominado Mínimo Común Múltiplo de dos enteros, está ligado al de Máximo Común Divisor, y por ello es de uso frecuente en la solución de problemas de Teoría de Números.

Definición:

Dados a y b enteros no nulos, un entero positivo m es el Mínimo Común Múltiplo de a y b, denotado como $m = MCM\ (a, b) = [a, b]$, si se satisfacen las dos siguientes propiedades:

1. $a|m$ y $b|m$
2. Si existe $c \in \mathbb{Z}$ tal que $a|c$ y $b|c$ entonces $m|c$.

Como a y b son enteros no nulos, los números ab y $-ab$ son múltiplos comunes de a y de b, y como sólo uno de estos dos números es positivo, el conjunto de los múltiplos comunes de a y b existe y tiene elemento minimal; así, el $MCM\ (a, b)$ existe y es único.

Además, para $a \in \mathbb{Z}$ y $b \in \mathbb{Z}$ se tiene que,

$$MCM\ (a, b) = MCM\ (b, a) = MCM\ (a, -b) = MCM\ (-a, b) = MCM\ (-a, -b).$$

Ejemplo:

El $MCM\ (3,12)$ puede calcularse señalando los conjuntos de los múltiplos de cada uno de los argumentos y a continuación calcular su intersección; de este modo, se tiene:

$$(3) = \{3,\ 6,\ 9,\ 12,\ 15,\ 18,\ 21,\ 24, \ldots\}$$
$$(12) = \{12,\ 24,\ 36,\ 48,\ 60,\ 72,\ 84,\ 96, \ldots\}$$
$$(3) \cap (12) = \{12,\ 24,\ 36,\ 48,\ 60, \ldots\}$$

Así que, $MCM\ (3,12) = 12$.

Una forma frecuente de cálculo del Mínimo Común Múltiplo consiste en descomponer cada uno de los argumentos en sus factores primos, en concordancia con el Teorema Fundamental de la Aritmética, y calcular el producto de los factores primos comunes y no comunes con mayor exponente.

En el ejemplo anterior, siguiendo este procedimiento, se tiene que $3 = 3$ y $12 = 2^2 \cdot 3$, entonces $MCM\ (3,12) = 2^2 \cdot 3 = 12$.

Ejemplo:

Determinar el $MCM\ (8,14)$.

En este caso es obvio que $8 = 2^3$ y $14 = 2 \cdot 7$, y por ello $MCM\ (8,14) = 2^3 \cdot 7 = 56$; resultado al que se llega mediante el cálculo de la intersección de los conjuntos:

$$(8) = \{8,\ 16,\ 24,\ 32,\ 40,\ 48,\ 56, \ldots\}$$
$$(14) = \{14,\ 28,\ 42,\ 56,\ 70,\ 84,\ 98, \ldots\}$$

De donde $(8) \cap (14) = \{56,\ 112,\ 168, \ldots\}$, lo que muestra que $MCM\ (8,14) = 56$.

Ejemplo:

Determinar el $MCM\ (18,15,24)$. Para ello, se descompone cada argumento en sus factores primos, encontrando $18 = 2 \cdot 3^2$, $15 = 3 \cdot 5$ y $24 = 2^3 \cdot 3$ y por ello, $MCM\ (18,15,24) = 2^3 \cdot 3^2 \cdot 5 = 360$.

3.15 Relación entre el máximo común divisor y el mínimo común múltiplo

Teorema 10

Sean a y b enteros no nulos; entonces,

$$MCM\ (a,b) = \frac{|a \cdot b|}{MCD\ (a,b)}.$$

Demostración

Si $m = MCM\ (a,b)$ y $d = MCD\ (a,b)$ entonces $d|a$, $d|b$ y por ello $\exists\ k \in \mathbb{Z}$, $\exists\ t \in \mathbb{Z}$ tales que $a = dk$ y $b = dt$ y sea $m = \frac{|a \cdot b|}{d}$; por ello $m > 0$, siendo además $m \in \mathbb{Z}$. Al escribir $a = d \cdot A$ y $b = d \cdot B$ en lugar de k y t, como d es el máximo común divisor, es claro que $MCD\ (A,B) = 1$ y en consecuencia se ve que $m = \frac{|a \cdot b|}{d} = \frac{|a| \cdot |d \cdot B|}{d} = |a| \cdot |B| = a \cdot (\pm B)$ y por ello $a|m$. Siguiendo el mismo procedimiento se consigue que $b|m$.

Sea $c \in \mathbb{Z}$ tal que $a|c$ y $b|c$ entonces $\exists q \in \mathbb{Z}$ para el cual $c = a \cdot q$ y $\exists s \in \mathbb{Z}$ tal que $c = b \cdot s$, de donde $a \cdot q = b \cdot s$. Pero $a = d \cdot A$ y $b = d \cdot B$ entonces $dAq = dBs$ y así $Aq = Bs$, por tanto, $B|Aq$; y siendo $MCD\ (A,B) = 1$ se consigue que $B|q$ o sea que $\exists p \in \mathbb{Z}$ tal que $q = Bp$. Remplazando en $c = aq = aBp$, teniendo en cuenta que $aB = \pm m$, entonces $c = \pm mp$, de donde $m|c$.

Por tanto $m = M.C.M(a,b)$, tal como se quería demostrar.

Ejemplo:

Dados $MCD\ (a,b) = 24$ y $MCM\ (a,b) = 1440$, determinar a y b.

Como $MCD\ (a,b) = 24$, entonces $24|a$ y $24|b$; esto es, $a = 24A$ y $b = 24B$, siendo $MCD\ (A,B) = 1$. Ahora bien; $m \cdot d = (1440)(24) = (24A) \cdot (24B)$, se consigue que $60 = A \cdot B$.

Ahora corresponde descomponer el número 60 en parejas de factores que sean primos entre sí, encontrando varias posibilidades, así:

$A = 2$	$B = 30$	$a = 24(2) = 48$	$b = 24(30) = 720$
$A = 3$	$B = 20$	$a = 24(3) = 72$	$b = 24(20) = 480$
$A = 4$	$B = 15$	$a = 24(4) = 96$	$b = 24(15) = 360$
$A = 5$	$B = 12$	$a = 24(5) = 120$	$b = 24(12) = 288$
$A = 60$	$B = 1$	$a = 24(60) = 1440$	$b = 24(1) = 24$

Así pues, existen varias parejas de valores a y b que satisfacen las condiciones pedidas.

3.16 La Sucesión de Fibonacci

En su libro "Liber Abacci", el matemático italiano Leonardo de Pisa, más conocido como Fibonacci (Libro del Ábaco) propone el problema de calcular el número de parejas de conejos que nacen en el transcurso de un año, dada una pareja inicial, siendo que estos se reproducen una vez por mes. Por un lado, el libro desempeñó el papel de divulgación del sistema de numeración hindú realizado por los árabes alrededor de los años 1200; y por otro lado, la solución del problema hace apertura a la definición de funciones por recurrencia.

En efecto, al considerar el conjunto de los números naturales $\mathbb{N} = \{1, 2, 3, 4, \ldots\}$, la función recurrente $F: \mathbb{N} \to \mathbb{N}$ definida como sigue, produce como imágenes la secuencia denominada sucesión o serie de Fibonacci, así:

$$F(n) = \begin{cases} 1 & \text{si } n < 3 \\ F(n-1) + F(n-2) & \text{si } n \geq 3 \end{cases}$$

Algunos de los elementos de la secuencia $F(1), F(2), F(3), F(4), \ldots$ son los naturales 1, 1, 2, 3, 5, 8, 13, 21, 34, 55, 89, 144, 233, 377, 610, 987, ... que se denotan por F_1, F_2, F_3, ... de acuerdo con el convenio establecido en la revista *Fibonacci Quarterly,* surgida en 1963.

Esta secuencia, que aparece con frecuencia en problemas relacionados con el estudio de la fenomenología natural, tiene varias propiedades; por ejemplo, puede demostrarse por múltiples sustituciones que,

$$\sum_{i=1}^{n} F(i) = \sum_{i=1}^{n} F_i = F(n+2) - 1 = F_{n+2} - 1.$$

Con esta notación también se tiene que $\sum_{i=1}^{n} F_{2i-1} = F_{2n}$, fórmula que relaciona los números de Fibonacci de posición impar con uno de posición par.

Una de las identidades más populares para los números de Fibonacci la descubrió J. D. Cassini en 1680, relaciona a tres números consecutivos de la secuencia y es $F_{n+1}F_{n-1} - F_n^2 = (-1)^n$ que se demuestra recurriendo al método de inducción o utilizando la identidad $\begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}^n = \begin{pmatrix} F_{n+1} & F_n \\ F_n & F_{n-1} \end{pmatrix}$.

Aplicando el método de inducción matemática se demuestra la importante expresión $F_{n+m} = F_{n-1}F_m + F_nF_{m+1}$ que liga a cada término de la secuencia con cuatro anteriores tomados como pares consecutivos. La demostración parte de las evidencias $F_{n+3} = F_{n+2} + F_{n+1} = 2F_{n+1} + F_n$ y $F_{n+4} = 3F_{n+1} + 2F_n$. Otra propiedad importante es que el cociente de dos elementos consecutivos de la secuencia $\frac{F_n}{F_{n-1}}$, en el infinito, convergen hacia el irracional algebraico $\frac{1+\sqrt{5}}{2}$ que es una de las raíces de la ecuación $x^2 - x - 1 = 0$. Este número se conoce como la razón dorada, número dorado, divina proporción o razón áurea, aunque Euclides lo llamó "la razón extrema y media" y se denota con el símbolo Φ en honor al escultor griego Fidias. De hecho, existen fórmulas que relacionan la razón dorada $\Phi = \frac{1+\sqrt{5}}{2}$, su inversa multiplicativa o la segunda raíz de la ecuación $\frac{1-\sqrt{5}}{2}$ con la serie de Fibonacci, como la siguiente expresión: $F_n = \frac{\left(\frac{1+\sqrt{5}}{2}\right)^n - \left(\frac{1-\sqrt{5}}{2}\right)^n}{\sqrt{5}}$ que se denomina fórmula de Binet en honor de su descubridor. Aquí se redescubre, como la combinación operativa de números irracionales que puede producir números racionales.

Respecto de la relación entre la teoría de la divisibilidad, del máximo común divisor y de la sucesión de Fibonacci, se consignan algunos resultados cuya demostración no corresponde al propósito del texto pero que son, de por si, llamativos. Por ejemplo, a partir de la identidad $F_{n+m} = F_{n-1}F_m + F_nF_{m+1}$ y al tomar m de forma que sea múltiplo de n se consigue por inducción que F_{nk} es múltiplo de F o más escuetamente: si n es divisible por m, entonces F_n también es divisible por F_m. Esto se puede evidenciar entre los valores $F_{20} = 6765$ y $F_{10} = 55$, por ejemplo; pero también significa en la secuencia que cada tercer número es par o cada cuarto número sea múltiplo de tres o cada quinto número sea múltiplo de cinco.

La sucesión $F_1,\ F_2, \ldots,\ F_{n^2-1}$contiene al menos un término divisible por n. Si se dispone $n = 6$, se consigue la secuencia de los 35 números de Fibonacci

1, 1, 2, 5, 8, 13, 21, 34, 55, 89, 144, 233, 377, 610, 987, 1597, 2584, 4181, 6765, 10946,7711, 28657, 46368, 75025, 121393, 196418, 317811, 514229, 832040, 1346269, 2178309, 3524578, 5702887, 9227465 donde el 144 y el 7728 son divisibles por 6.

Una de las más importantes propiedades sobre los números de Fibonacci fue demostrada por el matemático francés François Edouard Anatole Lucas en 1876, y asegura que un número divide a F_m y a F_n si y sólo si es un divisor de F_d donde $d = MCD\ (m, n)$.

En particular,

$$MCD\ (F_n,\ F_m) = F_{MCD(n,\ m)}; \text{ es decir, } (F_n,\ F_m) = F_{(n,\ m)}.$$

Por ejemplo, $(F_{120},\ F_{48}) = (5358359254990966640871840,\ 4807526976) = 46368$; y también se encuentra que, $F_{(120,\ 48)} = F_{24} = 46368$.

Ya se probó que dos números naturales consecutivos son primos entre sí, hecho que al aplicarlo sobre este resultado demuestra que dos elementos consecutivos de la serie de Fibonacci, también son primos relativos.

Del resultado, F_n es divisible por F_m si y sólo si n es divisible por m, se desprenden consecuencias significativas, como los siguientes:

1) Un número de Fibonacci es par si y sólo si su índice es múltiplo de 3.

2) Un número de Fibonacci divisible por 3 si y sólo si su índice es múltiplo de 4.

3) Un número de Fibonacci divisible por 4 si y sólo si su índice es múltiplo de 6.

4) Un número de Fibonacci divisible por 5 si y sólo si su índice es múltiplo de 5.

5) Un número de Fibonacci divisible por 7 si y sólo si su índice es múltiplo de 8.

Y de este modo, el lector puede exhibir otros criterios de divisibilidad para los números de Fibonacci en concordancia con los criterios de divisibilidad existentes para sus índices que son los de la serie natural.

Kepler también estudió esta sucesión por la segunda década de los años 1600 pero el matemático E. Lucas los bautizó con el nombre de los números de Fibonacci. En 1844 G. Lamé utilizó estos números para encontrar la profundidad del algoritmo de Euclides en el cálculo del máximo común divisor de dos enteros, demostrando que si el par de enteros positivos n y m no excedían el valor de F_k, el número máximo de iteraciones es $k+1$ en el cálculo de $MCD\ (m,n)$.

3.17 Teorema fundamental de la aritmética

Determinar si un número cualquiera es primo y descomponer un natural en sus factores primos, tal y como se demuestra en el teorema fundamental de la aritmética, son dos tareas de alta complejidad computacional, pero de gran interés en la criptografía y el desciframiento de códigos. Este teorema de gran importancia en este nuevo mundo de impresionante revolución en el área de la tecnología informática, establece lo siguiente:

Teorema 11

Todo número entero $n > 1$, se puede expresar, en forma única, excepto por el orden de los factores, como un producto de números enteros positivos: $n = p_1 \cdot p_2 \cdot p_3 \ldots p_k$. Si los factores se repiten, entonces $n = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot p_3^{\alpha_3} \ldots p_t^{\alpha_t}$, donde los $\alpha_i \geq 1$ y cada uno de los enteros $p_1,\ p_2, \ldots, p_t$, son distintos dos a dos, y son números primos, pues, se toman positivos, y cada uno conteniendo únicamente dos factores: 1 y $p_i\ \forall i,\ 1 \leq i \leq t$.

Demostración

Si $n = p$, con p primo, entonces se trata de un número primo, y no se tiene nada que demostrar.

Así que, sea $n \neq p$, siendo p cualquier número primo, con esto se construye el conjunto $D_1 = \{q \in \mathbb{Z}:\ q > 1\ \wedge\ q|n\}$.

Al estar constituido D_1 por enteros positivos, tiene un elemento mínimo m que además es primo, pues sólo contiene los factores 1 y m puesto que los valores q de D_1 se van recorriendo en orden. Esto asegura que m es el primer número primo que se encuentra en D_1 y al que se denomina p_1. Siendo así $n = p_1 \cdot q_1$ donde $q_1 > 1$.

En este momento al analizar q_1, puede ocurrir que sea primo o no lo sea. Si q_1 es primo, puede llamarse de inmediato $q_1 = p_2$ y por esta razón $N = p_1 \cdot p_2$, con lo cual termina la prueba.

Si q_1 no es primo, se considera el conjunto $D_2 = \{q \in \mathbb{Z}: \ q > 1 \ \wedge \ q|q_1\}$ con lo cual, y como antes, se llega a escribir $q_1 = p_2 \cdot q_2$, donde p_2 es con certeza, un número primo.

Se repite el argumento con q_2 y de forma reiterada se aplica el mismo proceso, conformando el conjunto $A = \{q_1, q_2, q_3, \ldots\}$cuyos elementos tienen la propiedad: $q_1 \leq q_2 \leq q_3 \leq \cdots$.

Siendo así, el proceso debe terminar en algún primo q_k, pues de no ser así, estos números llegarían a ser más grandes que n, lo cual es imposible. Todos estos q_i al ser primos se denotan como p_i para adornar la escritura, encontrando en definitiva que $n = p_1 \cdot p_2 \cdot p_3 \ldots p_k$, algunos de los cuales pueden aparecer repetidos.

Unicidad

Si $n = p_1 \cdot p_2 \cdot p_3 \ldots p_k = q_1 \cdot q_2 \cdot q_3 \ldots q_t$ son dos escrituras de n como producto de factores primos, se deduce que $p_1|(q_1 \cdot q_2 \cdot q_3 \ldots q_t)$ y al tratarse de números primos, p_1 divide necesariamente a algún q_j que, por comodidad, se identifica con q_1. Pero q_1 es un número primo, por tanto lo único que puede pasar es que $p_1 = q_1$. Aplicando la propiedad cancelativa de la multiplicación sobre $n = p_1 \cdot p_2 \cdot p_3 \ldots p_k = q_1 \cdot q_2 \cdot q_3 \ldots q_t$, se obtiene que $p_2 \cdot p_3 \cdot p_4 \ldots p_k = q_2 \cdot q_3 \cdot q_4 \ldots q_t$. Este procedimiento se repite con el mismo argumento con p_2, p_3,..., p_k consiguiendo que se cancelen hasta $k = t$. De esta manera se evidencia la igualdad entre parejas de factores primos p y q.

Por tanto, $n = p_1 \cdot p_2 \cdot p_3 \ldots p_k$; siendo claro que si aparece multiplicidad en los factores se escribe $n = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot p_3^{\alpha_3} \ldots p_t^{\alpha_t}$; $\alpha_i \geq 1$.

Se escribe a continuación la demostración elaborada por Euclides sobre la demostración de la infinitud de números primos en el conjunto de los números naturales; esta demostración se fundamenta en el método de reducción al absurdo.

Teorema 12

El conjunto de los números primos es infinito.

Demostración

Al suponer que el conjunto de primos naturales es finito, es posible hacer una lista completa de los mismos $P = \{p_1,\ p_2,\ p_3,\ \ldots p_r\}$ y en consecuencia, al considerar el número $n = p_1 \times p_2 \times p_3 \times \ldots \times p_r + 1$ se encuentra que n es primo o n es compuesto. De ser primo, el conjunto Pestaría incompleto y si es compuesto, se encuentra que el conjunto P es incompleto, puesto que al dividir n por cualquiera de los primos de la lista, se evidencia el residuo 1. En consecuencia, cualquiera que sea el caso, el conjunto P queda incompleto y en consecuencia no es posible hacer una lista completa de los números primos, por lo cual, éste es infinito.

CAPÍTULO 4
LOS NÚMEROS RACIONALES

Autor:
Oscar Fernando Soto Ágreda[5]

La Aritmética y la Geometría son las dos cimientes sobre las que ha crecido la matemática. En una amplia variedad de mediciones aparece ese vínculo y, en particular, en la tarea de medir longitudes de segmentos. Particularmente en este proceso de medición de longitudes, y que establecida una unidad o patrón de medida, ella misma no suele estar contenida un número entero de veces sobre el segmento a medir, y en consecuencia, aparece la necesidad de fraccionar la unidad para poder expresar la medida del segmento con más exactitud. Todo esto significa que las fracciones aparecieron de la división y comparación de magnitudes continuas siendo que las primeras magnitudes apropiadas para las mediciones son las de carácter geométrico como las longitudes, áreas, y volúmenes. Las fracciones, ahora llamadas, números racionales, no pudieron surgir desde los números enteros puesto que ellos se aplicaban sobre el significado de objetos enteros, como árbol, cielo, luna, entre otros.

4.1 Revisión de operatoria

La adición y la multiplicación son operaciones binarias en el conjunto de los números enteros, así:

$$+: \mathbb{Z} \times \mathbb{Z} \ \rightarrow \mathbb{Z} \text{ tal que } (a, b) \mapsto a + b$$
$$\cdot: \mathbb{Z} \times \mathbb{Z} \ \rightarrow \mathbb{Z} \text{ tal que } (a, b) \rightarrow a \cdot b$$

Con estas definiciones se estudió el dominio de los números enteros. Sin embargo, el sistema de los números enteros tiene un defecto muy claro; la ecuación $mx + b = 0$, con $m \neq 0$, puede o no tener solución entera debido a que el cociente $\frac{b}{m}$ no siempre es un número entero. Por ejemplo $3x = 6$ tiene como solución $x = 2$ con $2 \in \mathbb{Z}$; en cambio $3x = 7$ no tiene solución en $\mathbb{Z}$. Esto quiere decir que la división como operación inversa de la multiplicación está parcialmente definida en $\mathbb{Z}$.

Esta dificultad se soluciona al adicionar a los números enteros otros elementos que sirven para construir el Sistema de los Números Racionales. El tratamiento de los números racionales como clases de pares de enteros

[5] Profesor Adscrito al Departamento de Matemáticas y Estadística, Universidad de Nariño.

(a, b) con $b \neq 0$ sigue el esquema desarrollado con los números enteros como clases de pares de números naturales.

La motivación para construir el conjunto de los números racionales se basa en la solución de ecuaciones de la forma $bx = a$, siendo $a \in \mathbb{Z}$, $b \in \mathbb{Z}$ y $b \neq 0$.

Definición:

El cociente entre dos números enteros a y b, $b \neq 0$, si existe, se define por $\frac{a}{b} = k$ si y sólo si $a = b \cdot k$ para algún entero k.

Si los cocientes $\frac{a}{b}$ y $\frac{c}{d}$ existen, resulta claro que $\frac{a}{b} = \frac{c}{d} \Leftrightarrow ad = bc$ puesto que, si $\frac{a}{b} = k,\ entonces\ a = b \cdot k$ y $\frac{c}{d} = k$ entonces $c = d \cdot k$, entonces $a \cdot d = b \cdot d \cdot k = b \cdot c, \forall b \neq 0,\ \forall d \neq 0$.

Ejemplo: $\frac{12}{3} = 4 = \frac{-20}{-5} \Leftrightarrow (12)(-5) = -60 = (3)(-20)$.

Definición:

Sea $J = \mathbb{Z} \times \mathbb{Z}^* = \{(a, b): a \in \mathbb{Z},\ b \in \mathbb{Z},\ b \neq 0\}$ se define la relación $R \subseteq J \times J$ tal que $(a, b)\ R\ (c, d) \Leftrightarrow a \cdot d = b \cdot c$, siendo $\mathbb{Z}^* = \mathbb{Z} - \{0\}$.

Teorema 13

R es una relación de equivalencia en J.

Demostración

Se debe probar que la relación R satisface las propiedades reflexiva, simétrica y transitiva. En efecto, sean (a, b), (c, d) y (m, n) en J.

i) $(a, b)\ R\ (a, b)$ ya que $a \cdot b = b \cdot a$.

ii) Si $(a, b)\ R\ (c, d)$ entonces $a \cdot d = b \cdot c$ de donde se sigue que $c \cdot b = d \cdot a$ lo que significa que $(c, d)\ R\ (a, b)$.

iii) Si $(a, b)\ R\ (c, d)$ y $(c, d)\ R\ (m, n)$ entonces $ad = bc$ y $cn = dm$, que multiplicando por n y b, respectivamente, produce: $adn = bcn$ y $bcn = bdm$ lo que asegura que $adn = bdm$, de donde se deduce que $an = bm$; lo cual significa que $(a, b)\ R\ (m, n)$.

Definición:

Una clase de equivalencia se define por:

$$[(a,b)] = [a,b] = \{(x,y) \in J : (x,y)R(a,b)\}$$

o lo que es igual, $[a,b] = \{(x,y) \in J : xb = ya\}$.

Bajo estas condiciones se tiene que $[a,b] = [c,d] \Leftrightarrow (a,b)R(c,d) \Leftrightarrow ad = bc$, y cada clase de equivalencia define un número racional.

Por ejemplo, $[3,4] = \{(x,y) \in \mathbb{Z} \times \mathbb{Z}^* : 4x = 3y\}$ y esto realmente significa que, $[3,4] = \{\ldots, (-6,-8), (-3,-4), (3,4), (6,8), (9,12)\}$. Basta ver, por ejemplo, que $(-6,-8)\ R\ (3,4) \Leftrightarrow (-6)(4) = (-8)(3) = -24$; también se tiene $(3,4)R(9,12)$ ya que $(3)(12) = (4)(9) = 36$.

4.2 Adición y multiplicación de racionales

Antes de definir estas operaciones, se presenta la siguiente consideración: si $\frac{a}{b} = x$; $\frac{c}{d} = y$, donde b y d son enteros diferentes de cero y divisores respectivamente de a y c, entonces $a = bx, c = dy$.

Utilizando las propiedades de los enteros se tiene que $ad = bdx$ y $bc = bdy$, y por tanto $ad + bc = bd(x + y) = da + cb$. Esto asegura que si los pares (a,b) y (c,d) corresponden a los enteros x y y, al entero $x + y$ corresponde el par $(ad + bc, bd)$.

De igual manera, multiplicando las anteriores igualdades se tiene que:

$ac = (bx)(dy) = (bd)(xy)$, lo cual manifiesta que al entero xy corresponde el par (ac, bd) y que en ambos casos se tiene que $bd \neq 0$.

Existen dos números racionales particulares cuyas definiciones son:

$0 = [0,k] \forall k \in \mathbb{Z}^*; \mathbb{Z}^* = \mathbb{Z} - \{0\}$.
$1 = [n,n] \forall n \in \mathbb{Z}^*$.

Así pues, $[0,m] = [0,n] = [0,k]$, $\forall m \neq 0, \forall n \neq 0$ y $\forall k \neq 0$. Y en efecto se tiene que $0 \cdot n = m \cdot 0 = 0 \cdot k$.

También se tiene que $[m,m] = [n,n] = [p,p]\ \forall m \in \mathbb{Z}^*, \forall n \in \mathbb{Z}^*, \forall p \in \mathbb{Z}^*$,... ya que, $m \cdot n = n \cdot m$, y también $np = pn$, y en consecuencia, cada una des estas clases es la representación del 1.

Ahora se está en disposición de definir de manera adecuada las operaciones de adición y multiplicación en el conjunto de números racionales.

Sea $K = \{[a,b]: [a,b]\ es\ clase\ de\ equivalencia\ de\ R\}$ donde R es la relación de equivalencia de la definición anterior.

Definición:

Se define $\oplus: K \times K \to K$ tal que $[a,b] \oplus [c,d] = [ad + bc, bd]$.

Se probará que la operación $\oplus$ está bien definida en K; es decir, es una ley de composición interna en K.

Sea $[a,b] = [m,n]$ y $[c,d] = [p,q]$ entonces $(a,b)\ R\ (m,n)$ y $(c,d)\ R\ (p,q)$ lo cual significa que $an = bm$ y $cq = dp$.

Ahora se considera la suma de clases:

$[a,b] \oplus [c,d] = [ad + bc, bd]$ por definición.

$= [adnq + bcnq, bdnq]$ por definición de uno.

$= [(an)(dq) + (cq)(bn), (bd)(nq)]$ por propiedad asociativa.

$= [(bm)(dq) + (dp)(bn), (bd)(nq)]$ por sustitución.

$= [(bd)(mq + np), (bd)(nq)] = [mq + np, nq][bd, bd]$por factorización.

$= [mq + np, nq]$ debido a que $bd \neq 0$.

$= [m,n] \oplus [p,q]$.

Luego, cualquier clase puede ser remplazada por otra equivalente a ella en cualquier instancia operativa.

Teorema 14

La estructura $(K, \oplus)$ constituye un Grupo Abeliano.

Demostración

La operación $\oplus$ satisface la propiedad asociativa ya que si $[a,b]$, $[c,d]$ y $[m,n]$ son clases en K, entonces:

$([a,b] \oplus [c,d]) \oplus [m,n] = [ad+bc,bd] \oplus [m,n] = [(ad+bc)n + (bd)m, bdn] = [adn + bcn + bdm, bdn]$ de acuerdo al tratamiento que reciben los números en el conjunto de los números enteros.

$= [a(dn) + b(cn+dm), b(dn)]$ en $\mathbb{Z}$.

$= [a,b] \oplus [cn+dm, dn]$ por definición de operación $\oplus$.

$= [a,b] \oplus ([c,d] \oplus [m,n])$ por definición de operación $\oplus$. Lo cual prueba la propiedad asociativa.

La operación $\oplus$ satisface la propiedad modulativa.

En efecto, al suponer que $[x,y]$ es la clase neutra se tiene $[a,b] \oplus [x,y] = [a,b]$, $y \in \mathbb{Z}^*$. De donde se consigue $[ay+bx, by] = [a,b]$ lo que es equivalente a decir $(ay+bx, by)\ R\ (a,b) \Leftrightarrow (ay+bx)\cdot b = bay$. Esto se escribe de mejor manera como $bay + b^2x = bay \Leftrightarrow b^2x = 0$; y como $b \neq 0$, lo único que puede suceder es que $x = 0$. Esto significa que el neutro aditivo es la clase $[0,y]$, $\forall y \neq 0$.

La operación $\oplus$ es invertible.

Para cada clase $[a,b]$ existe una única clase $[\alpha,\beta]$ tal que:

$[a,b] \oplus [\alpha,\beta] = [0,k], \forall k \neq 0,\ \forall \beta \neq 0$.

$[\alpha,\beta]$ es una clase adecuada que debe conseguirse en consonancia con los siguientes pasos.

$[a,b] \oplus [\alpha,\beta] = [0,k] \Leftrightarrow [a\beta + b\alpha, b\beta] = [0,k]$, y así, $(a\beta + b\alpha, b\beta)\ R\ (0,k)$ que es equivalente con la igualdad $(a\beta + b\alpha)\cdot k = b\beta \cdot (0) = 0$; y como $k \neq 0$, se desprende que $a\beta + b\alpha = 0$ que es una ecuación diofántica lineal con infinitas soluciones. Una de ellas se exhibe a continuación: $\alpha = -a$ y $\beta = b$ que se adopta como solución canónica. Esto quiere decir que el inverso aditivo de $[a,b]$ es $[-a,b]$.

La operación $\oplus$ satisface la propiedad conmutativa.

En efecto;

$[a,b] \oplus [c,d] = [ad+bc, bd] = [da+cb, db] = [cb+da, db] = [c,d] \oplus [a,b]$.

Con todo esto, se concluye que efectivamente la estructura $(K,\oplus)$ conforma un grupo abeliano.

Definición:

Se define $\otimes: K \times K \to K$ tal que $[a,b] \otimes [c,d] = [ac, bd]$.

Se probará, primero, que esta operación está bien definida sobre K.

Como antes, sean $[a,b] = [m,n]$ y $[c,d] = [p,q]$ entonces $(a,b)R(m,n)$ y $(c,d)R(p,q)$ lo que significa que $an = bm$ y $cq = dp$.

Ahora se considera el producto de clases:
$[a,b] \otimes [c,d] = [ac, bd]$ por definición.
$= [(ac)(nq), (bd)(nq)]$ por definición de 1 ya que $nq \neq 0$.
$= [(an)(cq), (bd)(nq)]$ por la propiedad conmutativa.
$= [(bm)(dp), (bd)(nq)]$ por sustitución.
$= [(bd)(mp), (bd)(nq)]$ por propiedades conmutativa y asociativa en la multiplicación de enteros.
$= [mp, nq]$ debido a que $bd \neq 0$ y por definición de 1.
$= [m,n] \otimes [p,q]$, como se quería comprobar.

Esto significa que cualquier clase se puede remplazar por otra equivalente cuando de calcular un producto se trata.

Teorema 15

La estructura $(K^*,\otimes)$ conforma un grupo abeliano, donde $K^* = K - \{[0,m]:\ m \in \mathbb{Z}^+\}$.

Demostración

La operación $\otimes$ satisface la propiedad asociativa.

Sean $[a,b]$, $[c,d]$ y $[m,n]$ clases en K entonces:

$([a,b] \otimes [c,d]) \otimes [m,n] = [ac, bd] \otimes [m,n]$

$= [(ac)m, (bd)n] = [a(cm), b(dn)]$, por propiedad asociativa para la multiplicación de enteros.

$= [a, b] \otimes [cm, dn]$ por definición de operación $\otimes$.

$= [a, b] \otimes ([c, d] \otimes [m, n])$ por definición de operación $\otimes$. Y con esto, queda probada la propiedad asociativa.

La operación $\otimes$ satisface la propiedad modulativa, es decir, $\forall [a, b] \in K^*$, existe $[x, y] \in K^*$ tal que $[a, b] \otimes [x, y] = [a, b]$ donde $x \neq 0$ y $y \neq 0$.

En efecto, al suponer que $[a, b] \otimes [x, y] = [a, b]$ con $x \neq 0$ y $y \neq 0$, en, $\mathbb{Z}$ se consigue $[ax, by] = [a, b]$ lo que es equivalente de acuerdo a la relación R a decir $(ax, by)\, R\, (a, b) \Leftrightarrow axb = bya$ y debido a que $ab \neq 0$, es posible cancelar para decidir que $x = y$. Luego el elemento neutro de la multiplicación, también llamado elemento unidad es la clase de equivalencia $[n, n]$ con $n \in \mathbb{Z}$, $n \neq 0$. Esta clase de equivalencia se puede representar simplemente por $[1,1]$.

Como ejemplo de unidades están $[1,1] = [5,5] = [-3, -3] = [15,15]$.

La operación $\otimes$ es invertible, o sea que $\forall [a, b] \in K^*, \exists [\alpha, \beta] \in K^*$ tal que $[a, b] \otimes [\alpha, \beta] = [n, n], \forall n \neq 0$; siendo $[\alpha, \beta]$ una clase adecuada que debe conseguirse en consonancia con los siguientes pasos:

$[a, b] \otimes [\alpha, \beta] = [n, n] \Leftrightarrow [a\alpha, b\beta] = [n, n]$ y así, $(a\alpha, b\beta)R(n, n)$ que es equivalente con la igualdad $a\alpha n = b\beta n$; y como $n \neq 0$, se desprende que $a\alpha - b\beta = 0$ que es una ecuación diofántica lineal con infinitas soluciones; una de ellas es $\alpha = b$ y $\beta = a$ que se adopta como solución canónica.

Esto quiere decir que la clase inversa multiplicativa de $[a, b]$ es la clase $[b, a]$, o mejor $[a, b]^{-1} = [b, a]$.

Por ejemplo $[3,4]^{-1} = [4,3]$ y $[5,3]^{-1} = [3,5]$. Basta ver que $[3,4] \otimes [4,3] = [12,12]$ siendo $12 \neq 0$. Igualmente $[5,3] \otimes [3,5] = [15,15]$ con $15 \neq 0$.

La operación $\otimes$ satisface la propiedad conmutativa. En efecto;

$$[a, b] \otimes [c, d] = [ac, bd] = [ca, db] = [c, d] \otimes [a, b].$$

Con todo esto se concluye que efectivamente la estructura $(K^*, \otimes)$ conforma un grupo abeliano.

Teorema 16

La multiplicación distribuye con respecto a la adición en K.

Demostración

Sean $[a,b]$, $[c,d]$ y $[m,n]$ clases en K entonces:

$[a,b] \otimes ([c,d] \oplus [m,n]) = [a,b] \otimes [cn+dm, dn] = \left[a(cn+dm), b(dn)\right]$
$= [acn + adm, bdn]$ y $\forall b \neq 0$
$= [acbn + adbm, bdbn]$
$= [ac, bd] \oplus [am, bn]$
$= ([a,b] \otimes [c,d]) \oplus ([a,b] \otimes [m,n])$ como se quería demostrar.

De los tres teoremas demostrados se concluye que la estructura $(K,\oplus,\otimes)$ forma un cuerpo o campo, se denomina el cuerpo de los números racionales y se denota por $(\mathbb{Q}, +, \cdot)$.

Teorema 17

Si α, β, γ son números racionales, entonces,

a) $\alpha \oplus \gamma = \beta \oplus \gamma \Rightarrow \alpha = \beta$

b) $\alpha \otimes \gamma = \beta \otimes \gamma$ y además $\gamma \neq 0$, implica que $\alpha = \beta$.

Demostración

Sean $\alpha = [a,b]$, $\beta = [c,d]$ y $\gamma = [m,n]$ entonces:

a) $\alpha \oplus \gamma = [a,b] \oplus [m,n] = [an + bm, bn]$ y $\beta \oplus \gamma = [c,d] \oplus [m,n] = [cn + dm, dn]$, por lo tanto $\alpha \oplus \gamma = \beta \oplus \gamma \Leftrightarrow [an + bm, bn] = [cn + dm, dn]$ y esto a su vez es equivalente con $(an + bm, bn) R (cn + dm, dn) \Leftrightarrow (an + bm)(dn) = (cn + dm)(bn)$, equivalente con $an \cdot dn + bm \cdot dn = cn \cdot bn + dm \cdot bn \Leftrightarrow adn^2 = cbn^2$; como $n^2 \neq 0$ se tiene que $ad = cb$, equivalente a su vez, a decir $(a,b)\ R\ (c,d)$ lo que indica en definitiva que $[a,b] = [c,d]$ o como se dijo al principio, $\alpha = \beta$.

b) $\alpha \otimes \gamma = [a,b] \otimes [m,n] = [am, bn]$ y $\beta \otimes \gamma = [c,d] \otimes [m,n] = [cm, dn]$, por lo tanto $\alpha \otimes \gamma = \beta \otimes \gamma \Leftrightarrow [am, bn] = [cm, dn]$, o sea que:

$(am, bn)\ R\ (cm, dn) \Leftrightarrow am \cdot dn = bn \cdot cm.$

Siendo $mn \neq 0$, se sigue que $ad = bc \Leftrightarrow (a,b)\, R\, (c,d)$ que igualmente es equivalente con $[a,b] = [c,d]$, o mejor $\alpha = \beta$, como se esperaba demostrar.

Teorema 18

Sean α y β números racionales no nulos, entonces se tiene que,

$(\alpha \otimes \beta)^{-1} = \beta^{-1} \otimes \alpha^{-1} = \alpha^{-1} \otimes \beta^{-1}$.

Demostración

Sean $\alpha = [a,b]$, $\beta = [c,d]$ con $a \neq 0$ y $c \neq 0$; de acuerdo a lo demostrado anteriormente se tiene que $\alpha^{-1} = [b,a]$ y $\beta^{-1} = [d,c]$.

De otra parte, es obvio que $\alpha \otimes \beta = [a,b] \otimes [c,d] = [ac,bd]$ y como $ac \neq 0$ se tiene de inmediato que $(\alpha \otimes \beta)^{-1} = [bd,ac] = [db,ca] = [d,c] \otimes [b,a] = \beta^{-1} \otimes \alpha^{-1}$ tal y como se buscaba demostrar. Además, la multiplicación es conmutativa y por ellos se tiene en definitiva que$(\alpha \otimes \beta)^{-1} = \beta^{-1} \otimes \alpha^{-1} = \alpha^{-1} \otimes \beta^{-1}$.

4.3 Orden en los racionales

La extensión del orden definido en los números enteros hacia los números racionales se hace de manera natural y se mantiene la unicidad del elemento que logra el equilibrio al escribir la igualdad.

Definición:

Se dice que $[a,b] > [0,k],\ k \neq 0 \Leftrightarrow ab > 0, \forall a \in \mathbb{Z}$ y $\forall b \in \mathbb{Z}^*$.

El hecho de que $[a,b] > [0,k],\ k \neq 0 \Leftrightarrow ab > 0$ proviene de los números enteros puesto que $\forall a \in \mathbb{Z}$, su representación en clase de equivalencia es $a = [a,1]$ y por ello se tiene que $a = [a,1] > [0,k] \Leftrightarrow a \cdot 1 > 0 \cdot k,\ \forall k \neq 0 \Leftrightarrow a > 0$.

Ahora, dado $b \in \mathbb{Z}^* \Rightarrow b > 0$ o $(-b) > 0$ y por ello $b^2 = b \cdot b = (-b)(-b) > 0$. Así que si $[a,b] > [0,k] \Rightarrow a \cdot b > 0$.

Teorema 19

La condición $[a,b] > [0,k],\ \forall k \neq 0 \ \Leftrightarrow\ a \cdot b > 0$ establece una relación de orden porque es antisimétrica y transitiva.

1) Si $[a,b] > [0,k]$ y $[c,d] > [0,k]$ entonces $[a,b] \oplus [c,d] > [0,k]$

2) Si $[a,b] > [0,k]$ y $[c,d] > [0,k]$ entonces $[a,b] \otimes [c,d] > [0,k]$

3) Se cumple una sola de las tres siguientes condiciones:

   $[a,b] > [0,k]$ o $[-a,b] > [0,k]$ o $[a,b] = [0,k]$, $\forall k \neq 0$.

Demostración

Por definición, si $[a,b] > [0,k] \Leftrightarrow\ a \cdot b > 0$ y también se encuentra que, $[c,d] > [0,k] \Leftrightarrow\ c \cdot d > 0$ y por ello:

1) $[a,b] \oplus [c,d] = [ad + bc, bd]$, por tanto $[ad + bc, bd] > [0,k] \Leftrightarrow (ad + bc)(bd) > 0$ o sea $abd^2 + b^2cd > 0$, ya que $b^2 > 0$, $d^2 > 0$ y también $ab > 0$ y $cd > 0$ en $\mathbb{Z}$ y por esta razón $[a,b] \oplus [c,d] > [0,k]$, $\forall k \neq 0$.

2) $[a,b] \otimes [c,d] = [ac, bd]$ y nuevamente $[ac, bd] > [0,k] \Leftrightarrow (ac) \cdot (bd) > 0$, lo que es cierto ya que $(ac) \cdot (bd) = (ab) \cdot (cd) > 0$ en razón a que $ab > 0$ y $cd > 0$ en $\mathbb{Z}$, y en consecuencia, $[a,b] \otimes [c,d] > [0,k]$, $\forall k \neq 0$.

3) Se cumple la ley de tricotomía ya que dado $[a,b] \in \mathbb{Q}$ se cumple que $ab > 0$ o $-(ab) > 0$ o $ab = 0$.

   Si $ab = 0$ se sigue que $a = 0$ porque se ha tomado $b \neq 0$ y por tanto $[a,b] = [0,k],\ \forall k \neq 0$.

   Si $ab > 0$ entonces $[a,b] > [0,k]$, $\forall k \neq 0$.

   Si $-(ab) > 0 \Rightarrow (-a)(b) = a(-b) > 0$ o sea que,

   $[-a,b] = [a,-b] = -[a,b] > [0,k]$, $\forall k \neq 0$.

   Donde $-[a,b]$ representa la clase opuesta de $[a,b]$.

   Finalmente, se tiene que si $[a,b] > [0,k]$ y $[c,d] \equiv [a,b]$ entonces $[c,d] > [0,k]$.

En efecto, $[c,d]=[a,b] \Leftrightarrow \ (c,d)R(a,b) \Leftrightarrow cb=da$, de donde:

$(cb)^2=(cb)\cdot(da)=(cd)\cdot(ab)>0$ y como $ab>0$ entonces $cd>0$, y en consecuencia, $[c,d]>[0,k]$.

Definición:

Para los racionales $\alpha=[a,b]$ y $\beta=[c,d]$ se define la relación $<$ de modo que, $\alpha<\beta$ si y sólo si $ad<bc$.

Teorema 20 (Propiedad Transitiva).

Para todos los números racionales $\alpha,\ \beta,\ \gamma$ se cumple que si $\alpha<\beta$ y $\beta<\gamma$ entonces $\alpha<\gamma$.

Demostración

Sea $\alpha=[a,b]$; $\beta=[c,d]$ y $\gamma=[m,n]$, entonces $\alpha<\beta$ es equivalente con $[a,b]<[c,d] \Leftrightarrow \ ad<bc$; y $\beta<\gamma \Leftrightarrow [c,d]<[m,n] \Leftrightarrow cn<dm$, como $b\neq 0$, $n\neq 0$. Al considerar $n>0$, se sigue que $bcn\neq 0$ y así $adn<bcn$ y $bcn<bdm$ y por la propiedad transitiva de la relación de orden $<$ (menor que) en el conjunto de los números enteros $\mathbb{Z}$, se tiene que $adn<bdm$. Además $d\neq 0$ y por esta razón se consigue que $an<bm$, lo cual es equivalente a decir $[a,b]<[m,n]$, o mejor, si se quiere $\alpha<\gamma$, como se quería demostrar.

Definición:

Un número racional α se dice positivo si $0<\alpha$.

Teorema 21

Si α y β son números racionales positivos tales que $\alpha<\beta$, entonces $\alpha^{-1}>\beta^{-1}$.

Demostración

Sean $\alpha=[a,b]$ y $\beta=[c,d]$ donde $ab>0$ y $cd>0$, entonces $\alpha<\beta \Leftrightarrow [a,b]<[c,d] \Leftrightarrow ad<bc$.

De otra parte, $\alpha^{-1}=[b,a]$ y $\beta^{-1}=[d,c]$ y en consecuencia $\beta^{-1}<\alpha^{-1}$ es equivalente con $[d,c]<[b,a] \Leftrightarrow ad<bc$; de modo que las dos partes son

equivalentes, esto da constancia de que efectivamente si α y β son números racionales positivos tales que $\alpha < \beta$, entonces $\alpha^{-1} > \beta^{-1}$.

Definición:

Para el racional $\alpha = [a, b]$ y el natural n se define:

$$1 \cdot \alpha = \alpha$$
$$2 \cdot \alpha = 1 \cdot \alpha + \alpha$$
$$\vdots$$
$$(n+1) \cdot \alpha = n \cdot \alpha + \alpha$$

Teorema 22 (Monotonía)

Si $\alpha < \beta$ y $\eta < \lambda$ se sigue que $\alpha + \eta < \beta + \lambda$, donde α, β, η y λ son números racionales.

Demostración

Si $\alpha < \beta$ se tiene $\alpha + \eta < \beta + \eta$ y de $\eta < \lambda$ se sigue que $\beta + \eta < \beta + \lambda$ de donde se obtiene la cadena $\alpha + \eta < \beta + \eta < \beta + \lambda$ y por ello $\alpha + \eta < \beta + \lambda$.

Teorema 23

Si α y β son números racionales tales que $\alpha < \beta$, entonces $\alpha + \lambda < \beta + \lambda$, $\forall \lambda \in \mathbb{Q}$.

Demostración

Sean los racionales $\alpha = [a, b]$, $\beta = [c, d]$ y $\lambda = [p, q]$ de modo que $\alpha < \beta$, esto significa que $ad < bc$ en el conjunto de los números enteros; ahora bien, $q \in \mathbb{Z}^*$ y por ello $q^2 \in \mathbb{Z}^+$ de modo que a partir de que, $ad < bc$ por propiedades de la relación de orden *menor que* en los enteros, se sigue que $adq^2 < bcq^2$, y de allí que, $adq^2 + bdpq < bcq^2 + bdpq$, o mejor, $(aq + bp)dq < (cq + dp)bq$ de donde se encuentra que, $[aq + bp, bq] < [cq + dp, dq]$ o lo que es igual a que, $[a, b] + [p, q] < [c, d] + [p, q]$. Por ello, siempre que α y β sean números racionales tales que $\alpha < \beta$, se implica que $\alpha + \lambda < \beta + \lambda$, $\forall \lambda \in \mathbb{Q}$.

Teorema 24

Si α y β son números racionales, tales que $\alpha < \beta$, entonces $\forall n \in \mathbb{N}^*$ se tiene que, $n\alpha < n\beta$.

Demostración

Se recurre al método de inducción completa sobre n.

i) Si $\alpha < \beta$ y $n = 1$ se tiene que $1 \cdot \alpha < 1 \cdot \beta$ por simple hipótesis.
ii) Al suponer que el enunciado es válido para $n = k$, se tiene que $k \cdot \alpha < k \cdot \beta$
iii) De acuerdo con el teorema anterior y la definición anterior, se conjuntan las partes i) y ii) para concluir que $k \cdot \alpha + 1 \cdot \alpha < k \cdot \beta + 1 \cdot \beta$, es decir $(k + 1) \cdot \alpha < (k + 1) \cdot \beta$ y por ello $n\alpha < n\beta$, $\forall n \in \mathbb{N}$.

Teorema 25

Si α y β son números racionales positivos tales que $\alpha < \beta$, entonces $\exists \delta \in \mathbb{Q}$ tal que, $\alpha < \delta < \beta$.

Demostración

Si $\alpha < \beta$ entonces $\alpha + \alpha < \alpha + \beta$ y $\alpha + \beta < \beta + \beta$ y por esta razón se puede escribir $2\alpha < \alpha + \beta < 2\beta$, lo que implica $\alpha < \frac{\alpha+\beta}{2} < \beta$ y llamando $\frac{\alpha+\beta}{2} = \delta$ queda demostrado que $\alpha < \delta < \beta$. De hecho, si $\alpha = [a, b]$ y $\beta = [c, d]$ se encuentra que $\delta = [ad + bc, 2bd]$ y δ recibe el nombre de promedio aritmético de α y β.

Es evidente que el mismo proceso de interponer un racional entre otros dos puede repetirse con $\alpha < \delta$ y con la parte $\delta < \beta$, proceso que puede reiterarse un número infinito de veces, lo que significa que *entre dos números racionales hay un número infinito de números racionales.*

El siguiente teorema se fundamenta en los llamados promedios ponderaros en la Estadística y muestra de manera evidente que entre dos racionales cualesquiera se puede intercalar una multitud de números racionales.

Teorema 26

Si α y β son números racionales tales que $\alpha < \beta$, entonces $\forall n \in \mathbb{N}^*$ y $\forall m \in \mathbb{N}^*$ se tiene que $\alpha < \frac{n\alpha+m\beta}{n+m} < \beta$.

Demostración

Si $\alpha < \beta$ siendo $m > 0$, por el Teorema anterior se tiene que, $m\alpha < m\beta$ y como también $n\alpha = n\alpha$, al sumar estas dos expresiones a miembros, y por la ley de monotonía. se encuentra que $(n+m)\alpha < n\alpha + m\beta \quad (I)$.

De igual modo, si $\alpha < \beta$, como $n > 0$ se tiene $n\alpha < n\beta$ y además $m\beta = m\beta$; se tiene como antes, que $n\alpha + m\beta < (n+m)\beta \quad (II)$.

Conjuntando (I) y (II) se consigue la cadena $(n+m)\alpha < n\alpha + m\beta < (n+m)\beta$ y como $\frac{1}{n+m} > 0$, al multiplicar por esta última expresión se tiene que, $\alpha < \frac{n\alpha+m\beta}{n+m} < \beta$.

Es importante recalcar que al cambiar los valores de n y m que puede hacerse de manera indefinida, pueden intercalarse entre α y β infinitos números racionales, en particular, si $n = 1$ y $m = 1$ se consigue el promedio aritmético de los racionales α y β. como lo indica el Teorema anterior.

Teorema 27 (Propiedad arquimediana)

Si α y β son números racionales positivos, entonces $\exists n \in \mathbb{Z}^+$ tal que $n\alpha \geq \beta$.

Demostración

Sean $\alpha = [a, b]$ y $\beta = [c, d]$ tales que $ab > 0$ y $cd > 0$; entonces, $2\alpha = [a, b] \oplus [a, b] = [ab + ba, bb] = [2ab, bb] = [2a, b], \quad \forall b \neq 0$ y siguiendo de esta manera: $3\alpha = 2\alpha + \alpha = [2a, b] \oplus [a, b] = [2ab + ba, bb] = [3ab, bb] = [3a, b], \forall b \neq 0$; ..., $n\alpha = [na, b]$; entonces $n[a, b] > [c, d] \Leftrightarrow [na, b] > [c, d] \Leftrightarrow nad > bc$.

Como $ad \geq 1$, se tiene $2ad > 1$. Luego, basta escribir $n = 2bc$ para obtener que, $n\alpha > \beta$.

CAPÍTULO 5
LOS NÚMEROS REALES

Autor:
Segundo Javier Caicedo Zambrano[6]

Los números racionales son aquellos que corresponden al cociente o razón entre dos números enteros, y los irracionales los que no permiten tal cociente. La unión de estos dos conjuntos, racionales e irracionales, constituye el conjunto de los números reales. En los trabajos cotidianos referidos, por ejemplo, a los términos bancarios o comerciales, a las mediciones de tiempo, de edad, a las referencias de distancias entre ciudades, entre otros, lo común es el uso de números racionales, y esto induce la creencia de que sólo existen los números racionales. Sin embargo, los números racionales flotan en un mar de irracionales. El matemático alemán de origen ruso, Georg Cantor (1845-1918), desarrolló una teoría de los números irracionales y demostró que en cantidad son mucho más que los números racionales, puesto que no son numerables.

El conjunto de los números reales, por tanto, tiene una cardinalidad mayor que el de los números racionales y tal valor, definido por Cantor, es el transfinito $\aleph_1 = 2^{\aleph_0}$ que se denomina el cardinal del continuo. Por increíble que parezca, al escoger un número real cualquiera, lo más probable es que se trate de un irracional.

La diferencia mayor entre esta clase de números radica en que los racionales en su expansión decimal infinita posee ciclos repetitivos, llamados periodos, mientras que los irracionales carecen de estos ciclos repetitivos.

5.1 Necesidad operativa

A partir del conjunto de los números naturales se han definido las operaciones de adición y multiplicación con sus respectivas propiedades fundamentales. Al considerar la sustracción como operación inversa de la adición, se hizo necesario introducir nuevos elementos (los enteros negativos) y mediante una relación de equivalencia se construyó el sistema de los números enteros, el cual conserva las propiedades de los números naturales. Debido a que la división, como operación inversa de la multiplicación. no siempre es posible en los números enteros, es necesario introducir nuevos elementos (fraccionarios), definir una relación de

[6] Profesor Adscrito al Departamento de Matemáticas y Estadística, Universidad de Nariño.

equivalencia y construir con esas clases el sistema de los números racionales, pero conservando las propiedades demostradas para los números enteros. La única restricción impuesta es que la división por cero no existe.

Por tanto, en el sistema de los números racionales es factible realizar, sin ninguna restricción, las operaciones de adición, sustracción, multiplicación y división (excepto por cero). Así, se construyó el cuerpo de los números racionales.

Además, entre los números racionales cualesquiera, hay un número infinito de racionales. Para ilustrar este hecho, basta tomar el punto medio de cada par de números racionales, que equivale a su promedio aritmético, tal como se demostró anteriormente. Esto quiere decir que los números racionales recubren densamente a la línea recta, denominada recta numérica.

A pesar de la densidad de los números racionales, hay números que no se pueden expresar como cociente de dos números enteros $\frac{a}{b}$, $a,\ b$ en $\mathbb{Z}$ y $b \neq 0$, como sucede con $\sqrt{2}$ o con el número π (Figura 21).

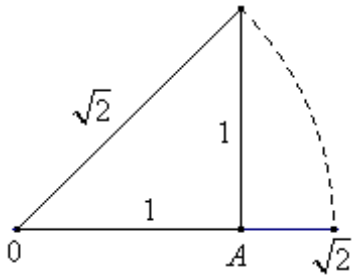

Figura 21. Representación de $\sqrt{2}$

Es suficiente ver que la hipotenusa de un triángulo rectángulo isósceles es inconmensurable con su lado, o bien, que la circunferencia es inconmensurable con su diámetro. Esto es, el diámetro no cabe un número exacto de veces en un arco total de circunferencia.

Estas consideraciones conllevan a definir los números irracionales y a concluir que la recta real está totalmente recubierta por los puntos racionales y los irracionales conformando el llamado continuo numérico, que corresponde al conjunto de los números reales, simbolizado por $\mathbb{R}$. Dicho de otra manera, hay una correspondencia biunívoca entre los números reales y los puntos de la línea recta. Cada número real viene dado por un decimal que tiene infinito número de cifras.

Por ejemplo, los siguientes son números irracionales:

$$\sqrt{2} = 1.414213562\ldots;\ \sqrt{3} = 1.732050808\ldots;\pi = 3.141592654\ldots$$

Ya se estableció que existe una correspondencia biunívoca entre los puntos de una recta y los números reales, de manera que a cada punto P de la recta se le asigna una y sólo una abscisa $P(a)$. Dicha coordenada puede ser positiva, negativa o cero, según cómo se ubique con respecto a un punto de referencia llamado origen de componentes (Figura 22).

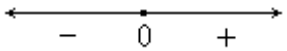

Figura 22

5.2 Construcción de números irracionales

Los números reales no sólo se clasifican en racionales e irracionales, sino también en otras dos categorías, a saber, números algebraicos y trascendentes. Los primeros son aquellos que corresponden a soluciones de ecuaciones algebraicas en una variable y coeficientes enteros; y los segundos, los que no aparecen como raíces de tales ecuaciones. Algunos números algebraicos son racionales y otros irracionales, sin embargo, todos los números trascendentes son irracionales. Los números que corresponden a esta segunda categoría han sido motivo de estudio y han trascendido en los ámbitos académico y cultural; entre los números reales trascendentes más famosos, están π y e.

Los números racionales son cerrados para la adición, sustracción, multiplicación y la división (excepto por cero). Los números irracionales no poseen tales propiedades. Sin embargo, a partir de cualquier número irracional α se puede construir una infinidad de números irracionales.

En efecto, siendo α un número irracional, n un número entero y r un racional, las siguientes combinaciones son números irracionales: $\frac{\alpha}{n}$, $n\alpha$, α^n, $\alpha + r$, $\alpha - r$, $r - \alpha$, $r \cdot \alpha$, $\frac{\alpha}{r}$ y $\frac{r}{\alpha}$, entre otras. Para demostrar que efectivamente son irracionales se aplica el método de reducción al absurdo, para lo cual, se supone que cada expresión corresponde a un número racional y se llega a la contradicción de que α es irracional y racional al mismo tiempo.

Así, por ejemplo, al suponer que $\alpha + r = r_1$, donde $r_1 \in \mathbb{Q}$ se devela por simple despeje que $\alpha = r_1 - r$ y siendo $\mathbb{Q}$ cerrado para la sustracción, se sigue que $r_1 - r$ es racional, es decir α es racional; resultado que constituye un absurdo ya que por hipótesis se trata de un irracional. Por esta razón no se puede suponer que $\alpha + r$ sea un número racional siendo α irracional.

Ejemplo:

Sean $\alpha = \sqrt{3}$ y $\frac{2}{5} \in \mathbb{Q}$. Las siguientes combinaciones son números irracionales: $\sqrt{3} + \frac{2}{5}$,

$$\frac{2}{5} - \sqrt{3}, \frac{2}{5\sqrt{3}}, \frac{2\sqrt{3}}{5}, \frac{\sqrt{3}}{\frac{2}{5}} = \frac{5\sqrt{3}}{2}, -\frac{2}{5}\sqrt{3}.$$

Ejemplo:

A partir de los números irracionales construidos en el ejemplo anterior, es factible construir otros números irracionales como los que se observan a continuación, para los cuales se ha tomado como centro al irracional $\frac{2\sqrt{3}}{5}$:

$$\frac{2\sqrt{3}}{5} - \frac{2}{5}, \frac{2}{5}\left(\frac{2}{5}\sqrt{3}\right), \frac{2\sqrt{3}}{5} \div \frac{2}{5} = \sqrt{3}, \frac{2}{5}\left(\frac{2}{5\sqrt{3}}\right), \ldots$$

Si α es irracional y β es irracional, $\alpha + \beta$ no necesariamente es irracional, esto ocurre, por ejemplo, tomando $\alpha = 3 + \sqrt{5}$ y $\beta = 2 - \sqrt{5}$ para los cuales es claro que $\alpha + \beta = 5 \in \mathbb{Q}$.

También es posible proponer ejemplos sobre los cuales el producto, el cociente y la diferencia de irracionales no producen irracionales.

Por ejemplo, si $\alpha = 3 + \sqrt{3}$ y $\beta = 6 - 2\sqrt{3}$, se tiene que, $\alpha \cdot \beta = \left(3 + \sqrt{3}\right)\left(6 - 2\sqrt{3}\right) = 2(3^2 - 3) = 12$; y si $\alpha = 4 + 2\sqrt{17}$ y $\beta = 2 + \sqrt{17}$; es obvio que $\frac{\alpha}{\beta} = 2$.

5.2.1 Ecuaciones algebraicas

La irracionalidad de algunos números como $\sqrt{3}$, $\sqrt{5}$, $\sqrt[3]{6}$ ... se suele demostrar mediante las ecuaciones algebraicas como las que se proponen enseguida, cuyas raíces son los números que se han expuesto en cada una:

a) $x^2 - 3 = 0 \Rightarrow x = \sqrt{3}$
b) $x^2 - 5 = 0 \Rightarrow x = \sqrt{5}$
c) $x^3 - 6 = 0 \Rightarrow x = \sqrt[3]{6}$

Un polinomio de grado n en la indeterminada x viene dado por la expresión $p(x) = \sum_{i=0}^{n} a_i x^i = a_0 + a_1 x^1 + a_2 x^2 + \ldots + a_n x^n$ donde $a_n \neq 0$ y $n \in \mathbb{Z}^+ \cup \{0\}$. En el caso en que $n = 0$, se trata de constantes y se adoptan como polinomios constantes.

Si $p(x) = 0$ se tiene una ecuación polinómica. En general, los coeficientes a_i se toman en el conjunto de los números enteros $\mathbb{Z}$, pero indistintamente se pueden tomar también en $\mathbb{Q}$ o en $\mathbb{R}$.

Teorema 28 (Teorema de Beazout).

Las raíces racionales $\frac{\alpha}{\beta}$ con $\beta \neq 0$, de la ecuación polinómica que determina $p(x)$: $a_0 + a_1 x^1 + a_2 x^2 + \ldots + a_n x^n = 0$, donde $a_i \in \mathbb{Z}$ y $n \in \mathbb{Z}^+$, se determinan cuando α es divisor de a_0 y β es divisor de a_n.

Demostración

Sea $\frac{\alpha}{\beta}$, en sus términos mínimos, una raíz de la ecuación $p(x) = 0$; $a_0 + a_1 x^1 + a_2 x^2 + \ldots + a_n x^n = 0$, $a_i \in \mathbb{Z}$, $n \in \mathbb{Z}^+$; entonces se satisface la igualdad al remplazar x por $\frac{\alpha}{\beta}$, así: $a_0 + a_1 \left(\frac{\alpha}{\beta}\right)^1 + a_2 \left(\frac{\alpha}{\beta}\right)^2 + \ldots + a_n \left(\frac{\alpha}{\beta}\right)^n = 0$; multiplicando todo por β^n se consigue $a_0\beta^n + a_1\alpha\beta^{n-1} + a_2\alpha^2\beta^{n-2} + \ldots + a_n\alpha^n = 0$;y por ello, $-a_n\alpha^n = a_0\beta^n + a_1\alpha\beta^{n-1} + a_2\alpha^2\beta^{n-2} + \ldots + a_{n-1}\alpha^{n-1}\beta$, expresión que se escribe como $-a_n\alpha^n = \beta(a_0\beta^{n-1} + a_1\alpha\beta^{n-2} + a_2\alpha^2\beta^{n-3} + \ldots + a_{n-1}\alpha^{n-1})$. Esto indica que $\beta | a_n\alpha^n$ y siendo que $\frac{\alpha}{\beta}$ aparece escrito de manera que α y β son primos relativos, lo único que puede ocurrir es que $\beta | a_n$; es decir, β es divisor del coeficiente director a_n.

Por otra parte, $a_1\alpha\beta^{n-1} + a_2\alpha^2\beta^{n-2} + \ldots + a_n\alpha^n = -a_0\beta^n$, que al factorizar α produce $\alpha(a_1\beta^{n-1} + a_2\alpha^1\beta^{n-2} + \ldots + a_n\alpha^{n-1}) = -a_0\beta^n$, lo que asegura que α es un divisor de $a_0\beta^n$ y como $\frac{\alpha}{\beta}$ está escrito en términos mínimos, lo único que puede ocurrir es que $\alpha | a_0$.

Ejemplo:

Demostrar que $\sqrt[3]{6}$ es irracional.

Solución

Se sabe que $\sqrt[3]{6}$ es una raíz de la ecuación polinómica $x^3 - 6 = 0$.

Partiendo del supuesto que $\sqrt[3]{6} = \frac{\alpha}{\beta}$, donde α y β son números enteros y que está escrito en términos mínimos en concordancia con el Teorema anterior, se tiene que, siendo $\frac{\alpha}{\beta}$ una raíz racional de $x^3 - 6 = 0$, es obvio que $\alpha|6$ y $\beta|1$; pero $D(6) = \{\pm 1,\ \pm 2,\ \pm 3,\ \pm 6\}$ y $D(1) = \{\pm 1\}$, por lo que al ser $\frac{\alpha}{\beta}$ una raíz racional de la ecuación polinómica, necesariamente debe pertenecer al conjunto $\{\pm 1,\ \pm 2,\ \pm 3,\ \pm 6\}$; al remplazar estos valores en la ecuación, ninguno produce cero.

En consecuencia $\sqrt[3]{6}$ no es racional.

Ejemplo:

Demostrar que $\sqrt{3} + \sqrt{5}$ es irracional.

Solución

Llamando $x = \sqrt{3} + \sqrt{5}$ se tiene que $x - \sqrt{3} = \sqrt{5}$ y elevando al cuadrado se sigue que $\left(x - \sqrt{3}\right)^2 = \left(\sqrt{5}\right)^2$, o mejor, $x^2 - 2x\sqrt{3} + 3 = 5$ que reorganizando adecuadamente produce $x^2 - 2 = 2x\sqrt{3}$, y elevando nuevamente al cuadrado, se encuentra $x^4 - 4x^2 + 4 = 4x^2(3)$, de donde $x^4 - 16x^2 + 4 = 0$, ecuación de coeficientes enteros cuyas únicas posibles raíces racionales deben pertenecer al conjunto $\{\pm 1,\ \pm 2, \pm 4\}$.

Dado que, ninguno de estos valores produce cero, las raíces reales de la ecuación $x^4 - 16x^2 + 4 = 0$ son irracionales; en particular, la raíz $x = \sqrt{3} + \sqrt{5}$.

Es factible aprovechar la función *DIVISORS* contenido en el archivo *Number.mth* del asistente matemático Derive, y definir unas funciones que

apliquen el teorema de Beazout, dado que el reconocimiento de raíces racionales exige la inversión de mucho tiempo.

Ejemplo:

Con la función *DIVISORS* activa, se definen las expresiones:

$$V:=[]$$
$$v\_0(v):=DIVISORS(-ABS(ELEMENT(v,DIM(v))))$$
$$v\_n(v):=DIVISORS(ABS(ELEMENT(v,1)))$$
$$p(x):=SUM(ELEMENT(v,i)\cdot x\hat{}(DIM(v)-i),i,1,DIM(v))$$
$$beazout(n,m):=IF(p(ELEMENT(v\_0(v),n)/ELEMENT(v\_n(v),m))=0,$$
$$[ELEMENT(v\_0(v),n)/ELEMENT(v\_n(v),m),\text{"Es raiz"}],[ELEMENT(v\_0(v),$$
$$n)/ELEMENT(v\_n(v),m),\text{"No es raiz"}])$$
$$prueba\_beazout(v):$$
$$=VECTOR(VECTOR(beazout(i,j),i,1,DIM(v\_0(v))),j,1,DIM(v\_n(v)))$$

El polinomio $x^4-16x^2+4=0$ del ejemplo anterior, se introduce como $v:=[1,0,-16,0,4]$ y al simplificar la expresión $prueba\_beazout(v)$, se encuentra la matriz:

$$\begin{Vmatrix} -4 & No\ es\ raiz \\ -2 & No\ es\ raiz \\ -1 & No\ es\ raiz \\ 1 & No\ es\ raiz \\ 2 & No\ es\ raiz \\ 4 & No\ es\ raiz \end{Vmatrix}$$

Y en consecuencia, el polinomio $x^4-16x^2+4=0$ carece de raíces racionales, por lo cual, todas sus raíces reales son irracionales; una de ellas, es el real $\sqrt{3}+\sqrt{5}$.

Con este recurso, para demostrar la irracionalidad de $x=\sqrt{2}-\sqrt{3}$, se aplica la prueba_beazout al polinomio $x^4-10x^2+1=0$. Para ello se define el vector $v:=[1,0,-10,0,1]$; y al simplificar $prueba\_beazout(v)$, se encuentra que,

$$\begin{Vmatrix} -1 & No\ es\ raiz \\ 1 & No\ es\ raiz \end{Vmatrix}$$

En consecuencia, las raíces del polinomio dado son números irracionales.

Definición:

Si a y b son números reales y $a < b$, se definen los siguientes intervalos:

$(a, b) = \{x \in \mathbb{R}: a < x < b\}$; intervalo abierto de extremos a y b.
$[a, b] = \{x \in \mathbb{R}: a \leq x \leq b\}$; intervalo cerrado de extremos a y b.
$(a, b] = \{x \in \mathbb{R}: a < x \leq b\}$; intervalo semiabierto a izquierda de extremos a y b.
$[a, b) = \{x \in \mathbb{R}: a \leq x < b\}$; intervalo semiabierto a derecha de extremos a y b.

La diferencia entre sus extremos se llama longitud del intervalo: $l = b - a$; también es usual llamar a esta diferencia, el calibre del conjunto (Figura 23).

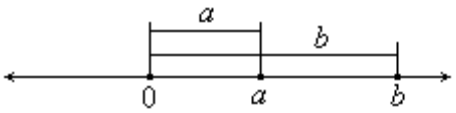

Figura 23

La notación $X(x)$ establece la relación biunívoca entre los puntos Xde la recta y los números reales x; es usual llamar a x la abscisa del punto X.

Ejemplo:

Si $P(5)$ y $Q(12)$, entonces $l = 12 - 5 = 7\ unidades$.
Si $P(-4)$ y $Q(3)$, entonces $l = 3 - (-4) = 7\ unidades$.
Si $P(-8)$ y $Q(-1)$, entonces $l = -1 - (-8) = 7\ unidades$.
Si $P(-3)$ y $Q(6)$, entonces $l = 6 - (-3) = 9\ unidades$.

Además, se definen los intervalos infinitos o semirrectas como los siguientes (*Figura 24* y *Figura* 25):

$$(a, \infty) = \{x \in \mathbb{R}: a < x\}$$

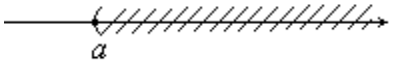

Figura 24

$$(-\infty, a) = \{x \in \mathbb{R}: x < a\}$$

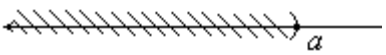

Figura 25

De igual manera se pueden definir los intervalos infinitos o impropios semicerrados, así: $[a, \infty)$ y $(-\infty, a]$.

Algunos intervalos se pueden representar utilizando el concepto de valor absoluto, tal como se indica a continuación.

$|x| \leq a \Leftrightarrow -a \leq x \leq a, \quad \forall a > 0$. Si se tiene $|x - k| \leq a$ se está representando al conjunto de valores x tales que $-a \leq x - k \leq a$ que es equivalente a escribir que $k - a \leq x \leq k + a$, conjunto que representa a un intervalo cerrado con punto medio k y longitud o calibre $2a$ (Figura 26).

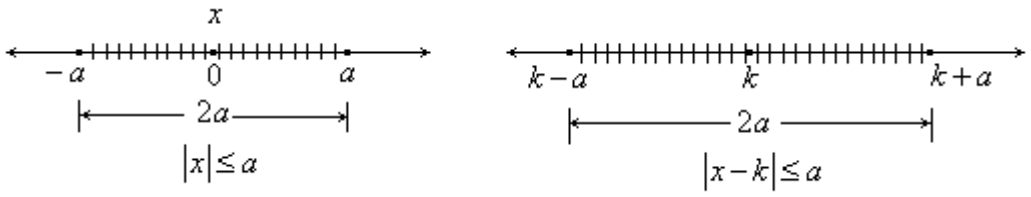

Figura 26

El uso de la función valor absoluto facilita el estudio de los intervalos configurados por números reales.

5.3 Encajes de intervalos

La medición de una distancia entre dos puntos $P(a)$ y $Q(b)$, puede hacerse por aproximaciones sucesivas, bien sea formando valores superiores o valores inferiores al calibre del intervalo $|b - a|$ (Figura 27).

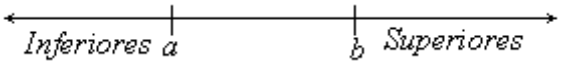

Figura 27

Es decir, es factible acercarse a cualquiera de los extremos de un intervalo por izquierda o por derecha. Entre más fina sea la aproximación, más exacto es el valor del calibre del intervalo.

Como a todo número real corresponde uno y sólo un punto de la línea recta, la aproximación a él puede realizarse mediante una sucesión de intervalos encajados $[a_1, b_1], [a_2, b_2], \ldots, [a_n, b_n]$ de manera que,

1.- $[a_k, b_k] \subseteq [a_{k-1}, b_{k-1}]$

2.- El calibre de cada intervalo disminuya al crecer k.

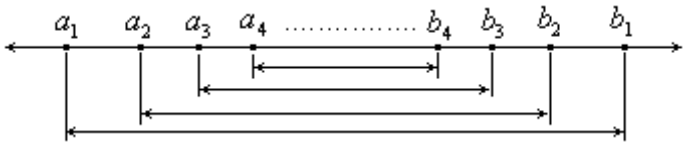

Figura 28

Por ejemplo, el valor $\sqrt{7}$ está comprendido en el siguiente encaje de intervalos; $[2,3], [2.6,2.7], [2.64,2.65], [2.645,2.646]$, ... donde los puntos de la izquierda son aproximaciones racionales por defecto y los puntos de la derecha, por exceso. A medida que se refine cada intervalo, es más fina la aproximación al valor $\sqrt{7}$, el cual, como se evidencia, se ubica en la intersección de todos los intervalos (Figura 28).

Según lo anterior, es fácil entender que un mismo número real puede ser definido por distintos encajes de intervalos, tomando otras formas de aproximación racional por izquierda y por derecha. Basta, para ello, relacionar las sucesiones de intervalos.

Definición:

Se dice que los encajes de intervalos $E_1: [a_1, b_1], [a_2, b_2], \dots, [a_n, b_n]$ y $E_2: [c_1, d_1], [c_2, d_2], \dots, [c_n, d_n]$ determinan un mismo número real si y sólo si $a_i \leq d_j$ y $c_i \leq b_j$ para cualquier par de índices i, j e independientemente de la tendencia de n hacia el infinito.

Por tanto, se asegura que E_1 está relacionado con E_2 si y sólo si $a_i \leq d_j$ y $c_i \leq b_j \ \forall i, \forall j$ y con esta definición se puede demostrar que la relación establecida para los encajes es de equivalencia. Cada clase de equivalencia de estos encajes define a un número real; en consecuencia, se adopta la siguiente definición.

Definición:

Un encaje infinito de intervalos cerrados con extremos racionales es toda sucesión de intervalos $E: [a_1, b_1], [a_2, b_2], \dots, [a_n, b_n], \dots$ cada uno contenido propiamente en el anterior; es decir, $[a_n, b_n] \subseteq [a_{n-1}, b_{n-1}]$, tal que dado un número $\varepsilon > 0$ arbitrario, tan pequeño como se quiera, se tiene que $b_n - a_n < \varepsilon$ para n suficientemente grande (mayor que n_0, el cual depende del ε dado). Esto garantiza que el calibre entre los encajes sea decreciente.

La sucesión $\{a_1, a_2, a_3, \dots\}$ de números racionales conformada por los extremos izquierdos del encaje infinito E tiende al número real P, lo mismo que la sucesión de los extremos derechos $\{b_1,\ b_2,\ b_3, \dots\}$; la una por izquierda y la otra por derecha.

Al utilizar la relación de equivalencia de la presente definición entre sucesiones de intervalos, se tiene la definición que sigue.

Definición:

Un número real P es una clase de equivalencia de encajes de intervalos cerrados con extremos racionales:

$$E_1: [a_1, b_1], [a_2, b_2], \dots, [a_n, b_n], \dots$$
$$E_2: [c_1, d_1], [c_2, d_2], \dots, [c_n, d_n], \dots$$

respecto a la relación de equivalencia definida por $a_i \leq d_j$ y $c_i \leq b_j\ \forall i, \forall j$.

De aquí en adelante todas las propiedades algebraicas de los números reales vienen dadas en términos de clases.

Queda claro que las propiedades ya demostradas para los números racionales siguen siendo perfectamente válidas para el conjunto de los números reales.

5.4 Operatoria en el cuerpo de los números reales

Definición:

Sean P y Q dos números reales, definidos por los encajes infinitos de intervalos:

$$P: [a_1, b_1], [a_2, b_2], [a_3, b_3], \dots, [a_n, b_n], \dots$$
$$Q: [c_1, d_1], [c_2, d_2], [c_3, d_3], \dots, [c_n, d_n], \dots$$

La suma y el producto de P y Q, vienen dados por los siguientes encajes de intervalos:

$$P + Q: [a_1 + c_1, b_1 + d_1], [a_2 + c_2, b_2 + d_2], [a_3 + c_3, b_3 + d_3], \dots, [a_n + c_n, b_n + d_n], \dots$$
$$PQ: [a_1 \cdot c_1, b_1 \cdot d_1], [a_2 \cdot c_2, b_2 \cdot d_2], [a_3 \cdot c_3, b_3 \cdot d_3], \dots, [a_n \cdot c_n, b_n \cdot d_n], \dots$$

y por tanto, también son números reales.

Ejemplo:

Determinar los valores de $\sqrt{3}+\sqrt{5}$ y de $\sqrt{3}\cdot\sqrt{5}$ mediante encajes de intervalos.

$\sqrt{3}$: $[1,2], [1.7,1.8], [1.72,1.73], [1.731,1.732], \ldots$
$\sqrt{5}$: $[2,3], [2.2,2.3], [2.22,2.23], [2.235,2.236], \ldots$
$\sqrt{3}+\sqrt{5}$: $[3,5], [3.9,4.1], [3.94,3.96], [3.966,3.968], \ldots$
$\sqrt{3}\cdot\sqrt{5}$: $[2,6], [3.7,4.1], [3.82,3.86], [3.869,3.873], \ldots$

En notación decimal se encuentra que:

$\sqrt{3} = 1.732050808 \ldots ; \sqrt{5} = 2.236067977 \ldots$
$\sqrt{3}+\sqrt{5} = 3.968118785 \ldots ; \sqrt{3}\cdot\sqrt{5} = 3.872983346 \ldots$

5.5 Orden en el conjunto de los números reales

Un número real P definido por un encaje infinito de intervalos cerrados, con extremos racionales: $P: [a_1, b_1], [a_2, b_2], [a_3, b_3], \ldots, [a_n, b_n], \ldots$ es llamado positivo si $\exists M \in \mathbb{N}$ tal que $a_n > 0, \forall n > M$ (se debe determinar a tal M). Este hecho se simboliza como $P > 0$.

El número real P es negativo, cuando $\exists S \in \mathbb{N}$ tal que $b_n < 0$, $\forall n > S$. (Se debe determinar tal S). Este hecho se simboliza como $P < 0$. Es claro que, si no ocurre ninguno de los dos casos mencionados, se encuentra que $P = 0$.

De acuerdo con lo visto en los números racionales se establece que:

$$\forall\, P \in \mathbb{R}\, y\, \forall\, Q \in \mathbb{R}: P \leq Q \Leftrightarrow \exists K \in \mathbb{R}^+ \cup \{0\}\, P + K = Q.$$

Por satisfacer las propiedades aditivas, multiplicativas y distributivas que poseen las estructuras de cuerpo, las propiedades de orden enunciadas y por no dejar ningún escaño vacío en su representación sobre una recta consolidando continuidad, puesto que a cada punto de ella le corresponde de manera biunívoca un número real, se hace evidente que los números reales tienen la estructura de cuerpo ordenado y completo. Además, dados los números reales P y Q tales que $0 < P < Q, \exists n \in \mathbb{N}\ tal\ que\ nP > Q$; este resultado se conoce como propiedad arquimedeana de los números reales y se demuestro anteriormente en un teorema. En consecuencia, la estructura algebraica $(\mathbb{R}, +, \cdot)$ constituye un cuerpo ordenado, completo y arquimediano.

Definición:

Un conjunto de números reales S se dice acotado superiormente si existe un número real M tal que $x \leq M, \forall\, x \in S$.

Teorema 29

El conjunto de los números naturales $\mathbb{N}$ no está acotado superiormente.

Demostración

Al suponer que $\mathbb{N}$ está acotado superiormente, se encuentra que existe $M \in \mathbb{R}$ tal que $n \leq M, \forall\, n \in \mathbb{N}$. Pero M es un número real y por ello se define a través de un encaje infinito de intervalos con extremos racionales; por lo cual, se puede escoger $n \in \mathbb{N}$ de modo que, $M \in (n-2, n+2)$; y siendo $n+2$ un número natural, es claro que M no es cota superior de $\mathbb{N}$. Como esto ocurre para cualquier real M que se escoja, se hace evidente que $\mathbb{N}$ no está acotado superiormente.

Teorema 30

Para cada real x se tiene un número natural n tal que $n > x$.

Demostración

Si ocurriera lo contrario, esto es, que $n \leq x, \forall\, n \in \mathbb{N}$, se tendría que el conjunto de los números naturales es acotado superiormente; hecho contrario a lo demostrado en el teorema anterior.

Teorema 31 (Propiedad arquimediana de los números reales)

Dados los números reales P y Q tales que $0 < P < Q$, $\exists\, n \in \mathbb{N}$ tal que $nP > Q$.

Demostración

Es suficiente con llamar $x = \frac{Q}{P}$ y aplicar el teorema anterior. Así que, dados los reales P y Q mayores que 0, existe $n \in \mathbb{N}$ tal que $n > \frac{Q}{P}$, de donde por propiedad de monotonía, se deduce que $nP > Q$.

La propiedad arquimediana se extiende de manera evidente para el caso en que $P > 0$ y $Q < 0$ puesto que con estas condiciones $nP > Q$, $\forall n \in \mathbb{N}$.

Actualmente se define a los números reales de manera axiomática, como la estructura $(\mathbb{R}, +, \cdot, \leq)$ como un cuerpo, ordenado, completo y arquimediano. Esta presentación se debe al gran matemático alemán David Hilbert (1862-1943).

5.6 El número Pi

El número π, irracional trascendente, goza de tanta fama en la matemática, tal como el número *e* que es la base de los logaritmos neperianos o naturales; la preocupación por su estudio se remonta a la antigüedad. En el libro I de Reyes, capitulo 7, versículo 23, al hablar de la construcción del palacio de Salomón, se lee:

> *Hizo así mismo un mar de fundición de 10 codos del uno al otro lado, redondo y de 5 codos de alto, y señaló en derredor un cordón de 30 codos.*

Este mar redondo, no era más que un pozo donde los egipcios se bañaban por costumbre. Según lo explica el versículo, el diámetro del pozo es de 10 codos y la longitud de la circunferencia es de 30 codos; existe pues, entre la longitud de la circunferencia y su diámetro, una razón de 3 que es el valor de π revelado en la Biblia.

Los egipcios, 40 siglos antes de Cristo, al estudiar el área de la esfera encontraron una aproximación a π con un valor igual al cuadrado de la fracción $\frac{16}{9}$ o sea $\frac{256}{81} = 3.160493$ que es un valor de π con un error de aproximadamente 2 centésimas. Arquímedes, en el siglo III a. C. mostró que π está comprendido entre las fracciones $\frac{223}{71}$ y $\frac{22}{7}$ y se debe observar que $\frac{223}{71} = 3{,}140845070422535211267605633802 8$,
resultado asombrosamente más cercano a π.

Ha sido abundante la preocupación por π: los poetas le han cantado y se han ideado versos como reglas mnemotécnicas en diversos idiomas.

En el libro de *Las Matemáticas y la Imaginación* de Kasner y Newman en la página 59 aparece:

> *Recurriendo a las series convergentes, Abrhamn Sharp en 1669, calculó π con 71 decimales. Dase, calculador rápido como el relámpago, orientado por Gauss, calculó en 1824 el número π con 200 decimales. En 1854 el alemán Ritcher*

halló 500 decimales para π y Shanks, algebrista inglés, alcanzó la inmortalidad de los geómetras, determinando el número π con 707 cifras decimales.

Es de anotar que, William Shanks trabajó durante 20 años para obtener su resultado.

Se comprobó, mucho más tarde (en 1945), que este último cálculo falla a partir de la cifra 528. Hacia 1980 se había calculado a π con más de diez mil cifras decimales. Actualmente π se ha calculado con más de un millón de cifras, y una pareja de japoneses escribieron el que se conoce como el libro más aburrido del mundo, de 800 páginas, que contiene las primeras 16 millones de cifras decimales de π.

Existen muchas fracciones que se aproximan de forma sorprendente a π, una de ellas fue descubierta por Tsu Ch'ung Chih, astrónomo chino, en el siglo V de nuestra era, lo que indica un adelanto de mil años a los matemáticos occidentales. La fracción descubierta por el chino se puede formar mediante un truco de prestidigitación, basta tomar los tres primeros números naturales impares y escribirlos por pares; 1, 1; 3, 3; 5,5 y a continuación los tres últimos se ubican sobre los tres primeros formando el fraccionario $\frac{355}{113}$. Es increíble de creer, pero el cociente determina que $\frac{355}{113} = 3{,}14159292035398230088495575221 24$ mientras que π con treinta cifras de aproximación es 3.14159265358979323846264338327; lo que señala que la fracción tiene las seis primeras cifras decimales igual a las de π.

En la antigüedad se tomaba a π aproximadamente igual a la raíz cuadrada de 10, donde $\sqrt{10}\cong$3.162277660, valor un poco alejado de este número trascendente. La raíz cúbica de 31 se aproxima mucho más, tal número es igual a $\sqrt[3]{31}$=3.14138065239139; la suma de las raíces cuadradas de 2 y de 3, también es una buena aproximación $\sqrt{2}+\sqrt{3}$=3.14626436994197.

Las primeras tentativas para determinar el valor exacto de π están ligadas al problema de la cuadratura del círculo; a partir de la búsqueda de la solución de este problema han aparecido varias construcciones gráficas que se aproximan a π. Una de las más sencillas se debe a Tsu Ch'ung Chih que se mencionó arriba y procede como sigue. Se construye el primer cuadrante de una circunferencia de radio 1 (Figura 29), con las líneas que se dibujan en la Figura 29, de tal modo que bc sea $\frac{7}{8}$ del radio, dg sea $\frac{1}{2}$ del radio, de paralelo con ac y df paralelo con be. Se puede demostrar que la

distancia fg es igual a $\frac{16}{113} = 0{,}14159292035398 23 \ldots$ Como $\frac{355}{113} = 3 + \frac{16}{113}$, si se dibuja un segmento igual al triple del radio y se le suma el segmento fg, el segmento resultante difiere de π en menos de una millonésima de unidad.

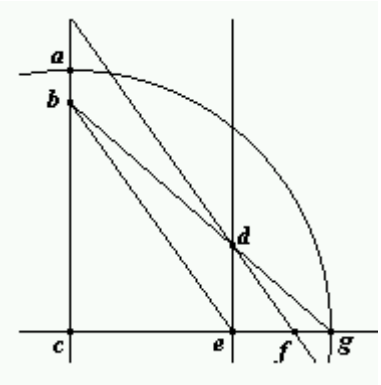

Figura 29. Cuadratura del círculo

Quienes trabajando en el problema de la cuadratura del círculo han creído haber descubierto el valor exacto de π, constituyen un gran contingente; ninguno tan terco ni caprichoso como el filósofo inglés Thomas Hobbes (1588-1679), quien combinó su elevado pensamiento con la más profunda ignorancia. En la época de Hobbes no se enseñaba matemáticas a los ingleses cultivados y éste leyó por primera vez los Elementos de Euclides cuando ya había cumplido los cuarenta años. Al llegar al teorema de Pitágoras exclamó asombrado: "¡Por Dios! ¡Esto no es posible!" Y repasó con mucho juicio la demostración hasta que se convenció. Durante el resto de su vida se entregó al estudio de la geometría. Afirmaba que "La geometría tiene algo que se parece al vino" (Anécdotas matemáticas, 1982). A los 67 años de edad, publicó el libro *De corpore* (Sobre los cuerpos) el cual contiene un curioso método para cuadrar el círculo; como todos los que existen, se trataba de una buena aproximación; no obstante, el autor estaba convencido que se trataba de un método exacto.

Por su parte, Jhon Wallis (1616-1703) matemático y criptógrafo inglés, publicó un folleto en el que establece los errores de Hobbes, y con esta publicación surge uno de los más largos, divertidos y estériles duelos, librado por dos espíritus selectos. Durante más de 25 años se dirigieron sarcasmos y críticas.

Con algunas treguas, la disputa continuó hasta la muerte de Hobbes que ocurrió cuando ya tenía 91 años; en uno de los últimos ataques, Hobbes

escribió: “El señor Hobbes jamás ha intentado provocar a nadie, pero quien lo provoque descubrirá que su pluma es al menos tan hiriente como la suya. Todos vuestros escritos no son sino errores o sarcasmos; esto es, nauseabundos flatos, hedores de mulo viejo cinchado con exceso tras un hartazgo. Yo he cumplido. Os he tenido en consideración por esta vez, pero no lo repetiré…” (Wikipedia, s.f.).

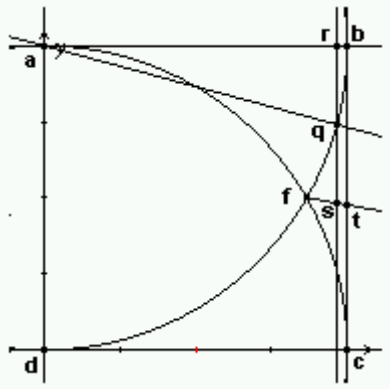

Figura 30. Método de Hobbes para cuadrar el círculo

Por su parte, Wallis se ufanaba de explicar a los demás de la “incapacidad del Señor Hobbes para aprender lo que no sabe”. Hobbes publicó cerca de una docena de métodos diferentes para cuadrar el círculo. El primero, que es uno de los mejores se muestra a continuación y se corresponde con la Figura 30.

Hobbes, en 1965, en su obra “De corpore”, presentó un método para cuadrar el círculo, como sigue: en un cuadrado de lado unidad, se trazan los arcos ac y bd, que son cuadrantes de sendas circunferencias de radio unidad (ver Figura 30). Se biseca el arco bf y se rotula como q, a este punto medio. Se traza la recta rq paralela a un lado del cuadrado y se prolonga hasta que qs sea igual a rq. Se dibuja a continuación la recta fs que corta al lado del cuadrado en t. Hobbes mantenía que la longitud del arco bf es exactamente igual a la del segmento bt. Dado que la circunferencia contiene 12 veces el arco bf, π sería seis veces la longitud del segmento bt. De este modo el valor de π sería 3.1419 …. (Falletti, 1999)[7].

Hoy se sabe que ninguna construcción puede dar el valor exacto de π; asombra conocer que Wallis sabía que la única forma posible de calcular su valor exacto era a través de un procedimiento algorítmico infinito que

7 Falletti, A. (1999). La cuadratura del círculo. Consultado 06/09/2022 en https://jmhernandez.tech/pi/pi_cuadr01.htm

converja hacia π. Él mismo, descubrió uno de los más sencillos que tiene un asombroso parecido con la regla descubierta por el chino Tsu Ch'ung Chih, que se presenta por el siguiente cálculo:

$$\pi = 2\left(\frac{2}{1}\times\frac{2}{3}\times\frac{4}{3}\times\frac{4}{5}\times\frac{6}{5}\times\frac{6}{7}\times\frac{8}{7}\times\frac{8}{9}\times\frac{10}{9}\times\frac{10}{11}\times\ldots\right)$$

Una de las más curiosas características del cálculo de las 707 cifras calculadas por el inglés William Shanks es su aversión al 7, y es que cada uno de los dígitos aparece en promedio 70 veces, excepto el 7 que sólo aparece 51; pero es maravilloso saber que después de corregir los errores mencionados en los cálculos (falla a partir de la cifra 528) los 7 que hacían falta aparecieron inmediatamente; más aún, hay varias ternas de sietes en la expresión decimal de π, se han encontrado quíntuplas de 7's; de hecho, se encuentran infinidad de ternas de cada uno de los dígitos, varias series de 7777 y la sorprendente 999999.

Para terminar esta sección sobre el número π, se presenta una relación histórica que muestra los espacios históricos de todos los calculadores de π y de todos los que han creído tener la solución al problema de la cuadratura del círculo.

π= 3	Oriente, Babilonia año 2000 a. C.
π= 3	Libro I de Reyes, capitulo 7, versículo 23
π= 3.16	Papiro de Rhind, Egipto, 1700 a.C.
π= 3.1410	Arquímedes, Sicilia, siglo III a.C.
π= 3.1416	Ptolomeo, Egipto, siglo II d.C.
π= 3.14159	Lien Huei, China, siglo III d.C.
π= 3. 1415926	Tsu Chung Chih, China, siglo V d.C.
π= 3.1415926535	FranÇois Viète, Francia, 1579.
π= 3.14159265358979323846264338327950	Ludolf van Ceulen, Holanda, en 1596.
π = con 808 cifras	D.F Ferguson, Inglaterra, 1946.

Por último y en una excelente relación entre la literatura y la Matemática que se logra con π, es de anotar que en el periódico ***Al Día*** del Viernes 4 de octubre de 1996, periódico de la Ciudad de Málaga, al sur de España, apareció la siguiente noticia: la academia sueca sorprende con el nóbel a la poetisa polaca Wislawa Szymborska. Traducida a varios Idiomas, a los 73 años nunca ha abandonado su Cracovia Natal. A la fecha, esta poetisa sólo tenía dos poemas traducidos al castellano, uno de ellos es al famoso número π.

EL NÚMERO Pi

El número Pi es digno de admiración
tres coma uno cuatro uno
todas sus cifras siguientes también son iniciales
cinco nueve dos, porque nunca se termina.
No permite abarcarlo con la mirada seis cinco tres cinco
con un cálculo ocho nueve
con la imaginación siete nueve
o en broma tres dos tres, es decir, por comparación
cuatro seis con cualquier otra cosa
dos seis cuatro tres en el mundo.

La más larga serpiente después de varios metros se interrumpe
Igualmente, aunque un poco más tarde, hacen las serpientes fabulosas.
El cortejo de cifras que forman el número Pi
no se detiene en el margen de un folio,
es capaz de prolongarse por la mesa, a través del aire,
a través del muro, de una hoja, del nido de un pájaro,
de las nubes, directamente al cielo
a través de la total hinchazón e inmensidad del cielo.

¡Oh qué corta es la cola del cometa, como la de un ratón!
¡Qué frágil el rayo de la estrella que se encorva en cualquier espacio!

Pero aquí dos tres quince trescientos noventa
mi número de teléfono la talla de tu camisa
año mil novecientos setenta y tres sexto piso
número de habitantes sesenta y cinco décimos
la medida de la cadera dos dedos la charada y el código
en la que mi ruiseñor vuela y canta
y pide un comportamiento tranquilo
también transcurren la tierra y el cielo
pero no el número Pi, éste no,
él es todavía un buen cinco
no es un ocho cualquiera
ni el último siete
metiendo prisa, oh, metiendo prisa a la perezosa eternidad
para la permanencia (Szymborska, s.f.).

5.7 El número e

El número e, aproximadamente igual a 2.71828182845904523536 es un número real trascendente, cuya fama es equivalente a la de π; fue introducido en el ambiente matemático por el prolífico Leonhard Euler y empleado por el matemático escocés John Napier o John Neper (1550-

1617) quien introdujo el primer sistema de logaritmos, descrito en *Mirifici logarithmorum canonis descriptio* (1614) para facilitar los cálculos en astronomía, y además, según sus propias palabras, "reducir el trabajo a la mitad." El sistema establecido por Napier se conoce como Logaritmos Naturales o Logaritmos Neperianos.

El número e se calcula a través de aproximaciones sucesivas de números racionales de la forma $\left(1+\frac{1}{n}\right)^n$, tal como se puede apreciar en la Tabla 6.

***Tabla 6**. Aproximaciones al número e*

n	$\left(1+\frac{1}{n}\right)^n$	n	$\left(1+\frac{1}{n}\right)^n$
3	2.370370370	500	2.715568520
10	2.593742460	1000	2.716923932
50	2.691588029	2000	2.717602570
100	2.704813829	5000	2.718010046
200	2.711517122	10000	2.718145918

En consecuencia, la definición del número trascendente e, se adopta como el siguiente límite:

$$\lim_{n\to\infty}\left(1+\frac{1}{n}\right)^n = e.$$

Por lo tanto, los límites de la forma 1^∞ dependen de e, por ejemplo:

$$\lim_{n\to\infty}\left(1-\frac{1}{n}\right)^{3n} = e^{-3};\ \lim_{n\to\infty}\left(1-\frac{1}{n}\right)^{n} = \frac{1}{e};\ \lim_{n\to\infty}\left(1-\frac{1}{2n}\right)^{n} = \frac{\sqrt{e}}{e}.$$

Contrario a lo que un neófito supondría, la aparición de e es muy frecuente. En el mundo comercial aparece en los cálculos financieros, en particular, en los cálculos relacionados con interés compuesto; en los procesos de crecimiento y decrecimiento de poblaciones; en el cálculo de probabilidades, donde se establece a través de la distribución normal; en las funciones trigonométricas; en las ecuaciones diferenciales; en la teoría de series, entre otros temas.

CAPÍTULO 6.
LOS NÚMEROS COMPLEJOS

Coautores:
Oscar Fernando Soto Ágreda[8]
Segundo Javier Caicedo Zambrano[9]

Al estudiar los números reales, se vio que la raíz cuadrada de los negativos carecía de sentido en razón a que los cuadrados de reales son reales positivos, y en el peor de los casos es cero. Las necesidades científicas obligaron a considerar expresiones de la forma $a + b\sqrt{-1}$ como números especiales que se denominaron imaginarios por antagonismo con los reales. Con el tiempo, su nombre cambió al de números complejos y se estudiaron bajo el supuesto de que estaban sujetos a las mismas leyes y propiedades de los números reales.

Los matemáticos de los siglos XVII y XVIII dudaron de la validez del uso de esta clase de números que en la operatoria básica suelen producir resultados sorprendentes; por ejemplo, no es posible extender la noción de orden entre ellos y la suma, el producto o el cociente o la diferencia de dos de ellos, puede ser un número real. Todas las dudas se esfumaron en los albores del siglo XIX cuando se estableció una función biyectiva entre los números complejos y los puntos del plano cartesiano. Algunos años más tarde el matemático húngaro János Bolyai (1802-1860) y el matemático irlandés William Rowan Hamilton (1805-1865) establecieron la fundamentación aritmética de los números complejos tratando a cada número complejo como un par ordenado susceptible de representarse en el plano cartesiano.

[8] Profesor Adscrito al Departamento de Matemáticas y Estadística, Universidad de Nariño.
[9] Profesor Adscrito al Departamento de Matemáticas y Estadística, Universidad de Nariño.

6.1 Necesidad operativa

Se ha visto que al ascender de un sistema numérico a otro, se van eliminando restricciones y, por tanto, se adquiere mayor libertad para realizar cálculos. Por ejemplo, la ecuación $x^2 - 2 = 0$ no tiene solución en $\mathbb{Q}$, con lo cual se crea la necesidad de introducir los números irracionales $\pm\sqrt{2}$. Sin embargo, no toda ecuación de segundo grado tiene solución en $\mathbb{R}$, puesto que el cuadrado de cualquier número real nunca es negativo. De manera que, para evitar esta dificultad se introduce la llamada unidad imaginaria, así:

$$i = \sqrt{-1} \;\Leftrightarrow\; i^2 = -1.$$

Por tanto, el símbolo i carece de sentido si se trabaja en los números reales. Lo mismo sucede, por ejemplo, con $\sqrt{-9}, \sqrt{-27}, (-3)^{\frac{3}{4}}$ puesto que se pueden escribir como sigue:

$$\sqrt{-9} = \sqrt{(9)(-1)} = \sqrt{9}\sqrt{-1} = 3i.$$
$$\sqrt{-27} = \sqrt{(9)(3)(-1)} = \sqrt{9}\sqrt{3}\sqrt{-1} = 3\sqrt{3}\ i.$$

Siendo $i^2 = -1$, no es válido pensar que se comporta como un número real, porque de hacerlo así, se podría escribir incorrectamente, como sigue:

$$i^2 = \left(\sqrt{-1}\right)^2 = \sqrt{-1}\cdot\sqrt{-1} = \sqrt{(-1)(-1)} = \sqrt{1} = 1.$$

La expresión $a + bi$ es un binomio (polinomio) aritmético, donde a y b son reales e i la unidad imaginaria, llamado Número Complejo; a es la parte real y se denota como $Re(a + bi) = a$, b es la parte imaginaria y se denota como $Im(a + bi) = b$. Es claro que si $b = 0$ se tiene que $a + bi = a + oi = a \in \mathbb{R}$, lo que ilustra cómo $\mathbb{R} \subset \mathbb{C}$.

El concepto de número complejo surgió de manera natural al tratar de resolver sin ninguna restricción la ecuación general de segundo grado en una variable. El concepto se debe al esfuerzo de muchas investigaciones y por ello no es creación de una sola persona.

Sea $ax^2 + bx + c = 0$ donde $a \neq 0$; al dividir por a se escribe $x^2 + \frac{b}{a}x = -\frac{c}{a}$ y completando el cuadrado se tiene: $x^2 + \frac{b}{a}x + \left[\frac{b}{2a}\right]^2 = \left[\frac{b}{2a}\right]^2 - \frac{c}{a}$ y por

lo tanto, $\left(x+\frac{b}{2a}\right)^2=\frac{b^2-4ac}{4a^2}$; y así: $x+\frac{b}{2a}=\pm\sqrt{\frac{b^2-4ac}{4a^2}}=\pm\frac{\sqrt{b^2-4ac}}{2a}$, de donde en definitiva se obtiene que, $x=\frac{-b\pm\sqrt{b^2-4ac}}{2a}$.

Si $b^2-4ac>0$, se obtienen dos raíces reales diferentes.
Si $b^2-4ac=0$ se obtienen dos raíces reales iguales y corresponde a una raíz real de multiplicidad dos.
Si $b^2-4ac<0$ se obtienen dos raíces complejas diferentes.

La aparición de valores complejos se debe a que en este caso a que:

$$\sqrt{b^2-4ac}=\sqrt{(-1)(4ac-b^2)}=\sqrt{4ac-b^2}\ i.$$

Además, en concordancia con la expresión $x=\frac{-b\pm\sqrt{b^2-4ac}}{2a}$ para este caso se obtiene que $x=\frac{-b\pm\sqrt{4ac-b^2}i}{2a}$, raíces denominadas conjugadas, tal como se definirán más adelante.

Ejemplo:

Al resolver la ecuación $x^2-2x+2=0$ se tiene,

$$x=\frac{2\pm\sqrt{4-(4)(2)}}{2}=\frac{2\pm\sqrt{-4}}{2}=\frac{2\pm 2i}{2}$$

Esto significa que las raíces son $x_1=1+i$, $x_2=1-i$, hecho que se comprueba al remplazarlos valores en la ecuación original, tal como se procede enseguida:

$$(1+i)^2-2(1+i)+2=1+2i+i^2-2-2i+2=0.$$

$$(1-i)^2-2(1-i)+2=1-2i+i^2-2+2i+2=0.$$

Ejemplo:

Determinar el polinomio cuadrático de coeficientes enteros cuyas raíces son $2+3i$ y $2-3i$.

Solución:

Si $2+3i$ es raíz, entonces $x-(2+3i)=0$

Si $2-3i$ es raíz, entonces $x-(2-3i)=0$; y como el producto de ceros es igual a cero, se tiene: $[x-(2+3i)]\cdot[x-(2-3i)]=0$. Multiplicando entre términos, en definitiva se obtiene: $x^2-4x+13=0$ que es la ecuación pedida.

En efecto,

$$(2+3i)^2-4(2+3i)+13=4+12i-9-8-12i+13=0.$$
$$(2-3i)^2-4(2-3i)+13=4-12i-9-8+12i+13=0.$$

Por tanto, la ecuación determinada, es correcta.

Definición:

Con los binomios $a+bi$ se forma el conjunto $\mathbb{C}=\{a+bi: a\in\mathbb{R},\ b\in\mathbb{R};\ i^2=-1\}$ donde $a+bi=c+di\Leftrightarrow a=c$ y $b=d$.

Definición:

En $\mathbb{C}$, se define dos operaciones binarias, una es de carácter aditivo y la otra de carácter multiplicativo, así:

$$+:\mathbb{C}\times\mathbb{C}\to\mathbb{C}, \text{tal que}, (a+bi,c+di)\mapsto(a+c)+(b+d)i.$$
$$\cdot:\mathbb{C}\times\mathbb{C}\to\mathbb{C}, \text{tal que } (a+bi,c+di)\mapsto(ac-bd)+(ad+bc)i$$

Para encontrar el inverso multiplicativo de un número complejo distinto de cero, es necesario definir el concepto de conjugado de un número complejo.

Definición:

Si $z=a+bi$ entonces, el complejo $\overline{z}=\overline{a+bi}=a-bi$ es el conjugado de z. Cabe anotar que $z\cdot\overline{z}=(a+bi)(a-bi)=a^2+b^2\in\mathbb{R}$.

El inverso multiplicativo de $a+bi$ en $\mathbb{C}^*$ es, en consecuencia:

$$\frac{a-bi}{a^2+b^2}.$$

De la definición anterior, al realizar los cálculos, se desprende que, $\overline{z_1+z_2}=\overline{z_1}+\overline{z_2}$ y también $\overline{z_1\cdot z_2}=\overline{z_1}\cdot\overline{z_2}$ para cualquier par de números complejos z_1 y z_2; además, $\overline{\overline{z}}=z, \forall\ z\in\mathbb{C}$; en particular, $\overline{z_1\cdot\overline{z_2}}=\overline{z_1}\cdot z_2$.

Bajo estas condiciones, se demuestra que la estructura algebraica $(\mathbb{C},+,\cdot)$ forma un cuerpo o campo. Sin embargo, $\mathbb{C}$ no es ordenado. Al suponer que existe una parte positiva de los números complejos $\mathbb{C}^+$ y que $i \in \mathbb{C}^+$, entonces, $i \cdot i = i^2 = -1 \in \mathbb{C}^+$ y por ello $(-1)\cdot i = -i \in \mathbb{C}^+$, lo cual es imposible, porque en los cuerpos ordenados, los elementos opuestos no nulos no pueden pertenecer a la misma parte. De este modo, no puede suponerse una partición de los números complejos en la que exista una parte positiva $\mathbb{C}^+$, que sea cerrada para la multiplicación y la adición.

Ejemplo:

Determinar el valor de la siguiente expresión:

$$2\sqrt{-3} - 3\sqrt{-2} + 5\left(-\sqrt{-2}\right) + 4\left(-\sqrt{-3}\right).$$

Solución:

Basta asociar los términos semejantes:

$$2\sqrt{-3} - 3\sqrt{-2} + 5\left(-\sqrt{-2}\right) + 4\left(-\sqrt{-3}\right) = (2-5)\sqrt{-2} - (3+4)\sqrt{-3} =$$

$$= -3\sqrt{-2} - 7\sqrt{-3} = -\left(3\sqrt{2} + 7\sqrt{3}\right) i.$$

Las potencias de i tienen un carácter cíclico de orden cuatro, el cual cumple la siguiente regla:

$$i = i^5 = i^9 = i^{13} = \cdots = i^{4n+1}$$
$$i^2 = -1 = i^6 = i^{10} = i^{14} = \cdots = i^{4n+2}$$
$$i^3 = -i = i^7 = i^{10} = i^{14} = \cdots = i^{4n+3}$$
$$i^4 = 1 = i^8 = i^{12} = i^{16} = \cdots = i^{4n}$$

Ejemplo:

Calcular $3i^{37} + 2i^{43} - 5i^{23} + 4i^{18}$.

Solución:

Con la aplicación del carácter cíclico de las potencias de la unidad imaginaria i, se encuentra que,

$$3i^{37} + 2i^{43} - 5i^{23} + 4i^{18} = 3i^{36+1} + 2i^{40+3} - 5i^{20+3} + 4i^{16+2}$$
$$= 3i + 2i^3 - 5i^3 + 4i^2 = 3i - 2i + 5i - 4 = -4 + 6i.$$

Ejemplo:

Determinar $x,\ y$ en $\mathbb{R}$ de modo que, $2x-1+(y-3)i=5x-4yi$.

Solución:

Por la igualdad entre números complejos, es claro que $2x-1=5x$, mientras que, $y-3=-4y$. De la primera ecuación se obtiene $x=-\frac{1}{3}$; de la segunda, $y=\frac{3}{5}$.

Ejemplo:

Resolver la ecuación $3-4i+2ix=3i-(1-i)x$.

Solución:

Como la incógnita es x, se separa: $[2i+(1-i)]x=3i+4i-3$; es decir $(1+i)x=7i-3$, de donde se encuentra como $x=\frac{7i-3}{1+i}$.

Ahora, al multiplicar numerador y denominador por el conjugado del denominador, se obtiene:

$$x=\frac{(7i-3)(1-i)}{(1+i)(1-i)}=\frac{4+10i}{2}=2+5i$$

Con el fin de verificar si es correcta la solución determinada, se puede remplazar el valor de x en la expresión inicial.

La representación de un número complejo como una pareja ordenada, adquiere mayor generalidad y carácter abstracto cuando se adopta el concepto de par ordenado $\mathbb{C}=\{(a,b):a\in\mathbb{R},\ b\in\mathbb{R}\}$, donde $(a,b)=(c,d)\Leftrightarrow a=c,\ b=d$.

Las operaciones de adición y multiplicación se definen como sigue:

Definición:

Sean los números complejos (a,b) y (c,d), se definen las siguientes operaciones: de adición y multiplicación:

Adición: $(a,b)+(c,d)=(a+c,b+d)$.

Multiplicación: $(a,b)\cdot(c,d)=(ac-bd,ad+bc)$.

Bajo estas condiciones se prueba que la estructura algebraica $(\mathbb{C}, +, \cdot)$ constituye una una estructura de cuerpo.

6.2 Representación gráfica

La interpretación geométrica de los números complejos que se deriva de su representación como par ordenado en el plano cartesiano, imprimió mayor naturalidad a las operaciones, porque utilizó representaciones por construcciones y motivó sus aplicaciones en Física.

Un número complejo $z = a + bi$ representa un punto $P(a, b)$ en el plano. Es claro que a se mide en el eje x (eje real) y b se mide en el eje y (eje imaginario). Por tanto, a cada punto del plano corresponde un número complejo.

6.3 Valor absoluto o norma

Es evidente que el conjugado de $a + bi$ es simétrico con respecto al eje x.

El valor absoluto de un número complejo, que se denota como $|a + bi|$, se representa por la distancia desde el origen de coordenadas al punto $P(a, b)$, tal como se ilustra en la Figura 31.

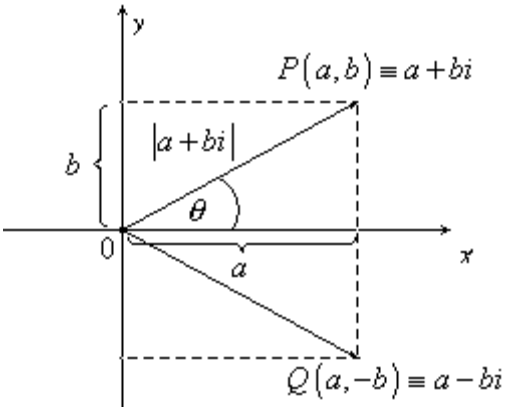

Figura 31. Valor absoluto de un complejo

Es decir, $|a + bi| = \sqrt{a^2 + b^2}$ que corresponde al módulo de $a + bi$. Además, un simple cálculo muestra que $(a + bi)(a - bi) = a^2 + b^2$, esto es, $z\overline{z} = |z|^2$ para todo número complejo.

Ejemplo:

$$|-5 + 7i| = \sqrt{(-5)^2 + 7^2} = \sqrt{74}.$$
$$|-3 - 4i| = \sqrt{(-3)^2 + (-4)^2} = \sqrt{25} = 5.$$

Los números complejos de módulo 1 se ubican sobre la circunferencia unitaria con centro en el origen de coordenadas, esto es: $x^2 + y^2 = 1$.

Definición:

Para el número complejo $z = a + bi$ se define la parte real de z como el número real a y se escribe $Re(z) = a$; la parte imaginaria de z corresponde al número real b, y se denota como $Im(z) = b$.

De este modo, las partes real e imaginaria de un número complejo son números reales, y en consecuencia, satisfacen las dos siguientes propiedades de orden:

$$a)\ Re(z) \leq |Re(z)| \leq |z|;\ b)\ Im(z) \leq |Im(z)| \leq |z|$$

De hecho, se puede establecer mediante cálculos sencillos que,

$$z + \overline{z} = 2\,Re(z)\,;\ z - \overline{z} = 2\,Im(z)$$

Propiedad

El módulo de una suma de dos números complejos cumple la desigualdad triangular, esto es:

$$|z_1 + z_2| \leq |z_1| + |z_2|$$

Además, se cumple que,

$$|z_1 \cdot z_2| = |z_1| \cdot |z_2|;\ |z_1| = |\overline{z_1}|$$

Demostración:

En efecto, si $z_1 = a + bi$ y $z_2 = c + di$; entonces,

$$z_1 + z_2 = (a + c) + (c + di)$$
$$z_1 \cdot z_2 = (ac - bd) + (ad + bc)i$$
$$\overline{z_1} = a - bi$$

1. $|z_1 \cdot z_2| = \sqrt{(ac - bd)^2 + (ad + bc)^2} = \sqrt{(ac)^2 + (bd)^2 + (ad)^2 + (bc)^2}$

   $= \sqrt{a^2(c^2 + d^2) + b^2(c^2 + d^2)} = \sqrt{(a^2 + b^2)(c^2 + d^2)} = |z_1| \cdot |z_2|.$

   De este modo $|z_1 \cdot z_2| = |z_1| \cdot |z_2|$, para cualquier par de números complejos z_1 y z_2.

2. Si $z_1 \in \mathbb{C}$ y $z_2 \in \mathbb{C}$, se tiene que,

$$|z_1 + z_2|^2 = (z_1 + z_2)\left(\overline{z_1 + z_2}\right) = (z_1 + z_2)(\overline{z_1} + \overline{z_2})$$
$$= z_1\overline{z_1} + z_2\overline{z_2} + z_1\overline{z_2} + \overline{z_1}z_2$$
$$= z_1\overline{z_1} + z_2\overline{z_2} + z_1\overline{z_2} + \overline{z_1\overline{z_2}}$$
$$= |z_1|^2 + |z_2|^2 + 2\,Re(z_1\overline{z_2}) \leq$$
$$\leq |z_1|^2 + |z_2|^2 + 2|z_1||z_2| = (|z_1| + |z_2|)^2$$

   De $|z_1 + z_2|^2 = (|z_1| + |z_2|)^2$, al extraer raíz cuadrada, se obtiene que, $|z_1 + z_2| \leq |z_1| + |z_2|$.

3. Si $z = a + bi$, entonces $\overline{z} = a - bi$; y es claro que, $|z| = \sqrt{a^2 + b^2}$, como también $|\overline{z}| = \sqrt{a^2 + (-b)^2} = \sqrt{a^2 + b^2} = |z|$.

En la demostración de la propiedad triangular, a saber, $|\boldsymbol{z_1 + z_2}| \leq |\boldsymbol{z_1}| + |\boldsymbol{z_2}|$, para cualquier par de complejos $\boldsymbol{z_1}$ y $\boldsymbol{z_2}$, se utilizó propiedades ya mencionadas, entre las que se destacan: $\boldsymbol{Re(z)} \leq |\boldsymbol{z}|$ y $\boldsymbol{z + \overline{z} = 2\,Re(z)}$, $\forall \boldsymbol{z} \in \mathbb{C}$.

6.4 El argumento de un número complejo

Definición:

El ángulo θ formado por la parte positiva del eje x y el radio vector $\overrightarrow{OP}$ que representa al complejo $z = a + bi$, se denomina argumento del número complejo $z = a + bi$ y se denota como $arg(z)$.

Se debe tener en cuenta que el argumento de $\overline{z}$ es el opuesto del argumento de z. En las demostraciones es útil tomar el menor valor θ tal que $0 < \theta \leq 2\pi$, con lo cual se puede representar a cualquier complejo. A este menor valor del argumento se le denomina *argumento principal;* de este modo, se establece una función llamada *Argumento Principal* entre los números complejos y el intervalo $0{,}2\pi$.

6.5 Forma polar de un complejo

Todo número complejo $z = a + bi$ puede expresarse en forma trigonométrica, mediante la utilización del argumento θ y el radio vector r (ver Figura 32).
En efecto se tiene:
$a = r\ Cos\theta$ y $b = r\ Sen\theta$, por tanto, se escribe $a + bi = r\ Cos\theta + i\ r\ Sen\theta$; en consecuencia, $z = r(Cos\theta + i\ Sen\theta)$, siendo $r = \sqrt{a^2 + b^2}$.

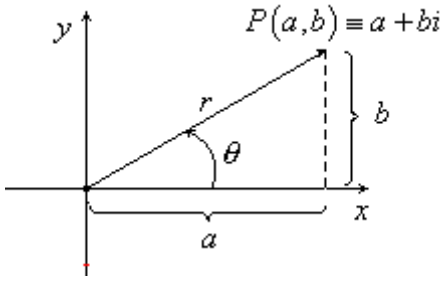

Figura 32. Forma polar de un número complejo

Los números reales r y θ se denominan coordenadas polares del punto P, y el origen de coordenadas se denomina Polo. Por tanto, $P(a, b)$ equivale a $P(r, \theta)$, y se puede pasar sin dificulta de un sistema uno a otro.

Sin embargo, la representación polar de un número complejo no es única debido al carácter periódico de las funciones trigonométricas. Por ejemplo:

$$Cos\ \theta = Cos(\theta = \theta + 2k\pi);\ Sen\ \theta = Sen(\theta = \theta + 2k\pi), \forall\ k \in \mathbb{Z}.$$

Cada uno de los valores $\theta + 2k\pi$ se denomina argumento del número complejo.

Ejemplo:

Determinar el módulo y el argumento principal del número complejo $z = 3 + 2i$.

Solución:

El módulo de este complejo es: $|z| = \sqrt{3^2 + 2^2} = \sqrt{13} \in \mathbb{R}$.
El argumento θ es tal que $Tan(\theta) = \frac{2}{3}$ y entonces $\theta = Arc\ tan\left(\frac{2}{3}\right)$ que, en grados sexagesimales, es aproximadamente igual a $\theta = 33^o\ 41'$.

El producto, la potencia y el cociente de complejos escritos en forma polar, se convierte en una operación bastante simple.

En efecto, sean $z_1 = r_1(Cos\alpha + iSen\alpha)$, $z_2 = r_2(Cos\beta + iSen\beta)$.

El producto es,

$$z_1 \cdot z_2 = r_1 \cdot r_2[(Cos\alpha Cos\beta - Sen\alpha Sen\beta) + i(Cos\alpha Sen\beta + Sen\alpha Cos\beta)]$$

Por tanto,

$$z_1 \cdot z_2 = r_1 \cdot r_2[Cos(\alpha + \beta) + iSen(\alpha + \beta)].$$

Para la potenciación se induce que, si $z_1 = z_2 = z$, siendo $z = r(Cos\alpha + iSen\alpha)$, se tiene como producto inicial, su cuadrado $z^2 = r^2(Cos\alpha + iSen\alpha)^2 = r^2(Cos2\alpha + iSen2\alpha)$, y en general, $\forall n > 1$ en el conjunto de los naturales se tiene $z^n = r^n(Cosn\alpha + iSenn\alpha)$, expresión conocida como la fórmula de De Moivre, la cual se demuestra por inducción completa, como sigue.

i) Para $n = 1$ se tiene que,

$$z^n = z^1 = z = r(Cos\alpha + iSen\alpha) = r^1(Cos1 \cdot \alpha + iSen1 \cdot \alpha)$$
$$= r^n(Cosn\alpha + iSenn\alpha)$$

ii) Se supone que el enunciado es válido para $n = k$, y por ello se tiene que,

$$z^k = r^k(Cosk\alpha + iSenk\alpha)$$

iii) Se demuestra que también es cierto para $n = k + 1$.

En este caso, de manera evidente se tiene que:

$$z^{k+1} = z^k \cdot z = \left(r^1(Cos1 \cdot \alpha + iSen1 \cdot \alpha)\right)$$
$$= r^{k+1}(Cosk\alpha + iSenk\alpha)(Cos\alpha + iSen\alpha)$$
$$= r^{k+1}\left((Cosk\alpha Cos\alpha - Senk\alpha Sen\alpha) + i(Senk\alpha Cos\alpha + Sen\alpha Cosk\alpha)\right)$$
$$= r^{k+1}(Cos(k+1)\alpha + iSen(k+1)\alpha).$$

Por esta razón,

$$z^n = r^n(Cosn\alpha + iSenn\alpha), \forall n \in \mathbb{N}.$$

Para el conjugado de $z = r(Cos\alpha + iSen\alpha)$, $\overline{z} = r(Cos\alpha - iSen\alpha)$, también se encuentra que $(\overline{z})^n = r^n(Cosn\alpha - iSenn\alpha), \forall n \in \mathbb{N}$; resultado que también se demuestra por inducción completa.

El cociente también adquiere una forma más simple, así:

$$\frac{z_1}{z_2} = \frac{r_1(Cos\alpha + iSen\alpha)}{r_2(Cos\beta + iSen\beta)} = \frac{r_1}{r_2} \cdot \frac{(Cos\alpha + iSen\alpha) \cdot (Cos\beta - iSen\beta)}{Cos^2\beta + Sen^2\beta}$$
$$= \frac{r_1}{r_2} \cdot [(Cos\alpha Cos\beta + Sen\alpha Sen\beta) + i(Sen\alpha Cos\beta - Cos\alpha Sen\beta)]$$
$$= \frac{r_1}{r_2} \cdot [Cos(\alpha - \beta) + iSen(\alpha - \beta)]$$

Si en la fórmula de De Moivre, se toma $r = 1$ y se expande de conformidad con el binomio de Newton, se tiene $\forall n > 1$ que, $(Cos\theta + iSen\theta)^n = Cosn\theta + iSennn\theta$; es decir, $Cos\, n\theta + iSen\, n\theta = \sum_{k=0}^{n} Cos^{n-k}\theta \cdot (iSen\theta)^k$; al igualar respectivamente las partes reales y las partes imaginarias, se obtienen identidades para los ángulos múltiples.

Por ejemplo, cuando $n = 2$, en la fórmula de De Moivre, se tiene:

$$(Cos\theta + iSen\theta)^2 = Cos^2\theta + 2iCos\theta Sen\theta - Sen^2\theta = Cos2\theta + iSen2\theta$$

Separando las partes real e imaginaria, se tiene que,

$$Cos2\theta = Cos^2\theta - Sen^2\theta$$
$$Sen\, 2\theta = 2sen\theta cos\theta$$

Para $n = 3$ se encuentra lo siguiente:

$$(Cos\theta + iSen\theta)^3 = Cos^3\theta + 3iCos^2\theta Sen\theta + 3Cos\theta(iSen\theta)^2 + (iSen\theta)^3$$
$$= Cos3\theta + iSen\theta$$
$$= Cos^3\theta - 3Cos\theta Sen^2\theta + i(3Cos^2\theta Sen\theta - Sen^3\theta).$$

Por lo tanto,

$$Cos3\theta = Cos^3\theta - 3Cos\theta Sen^2\theta$$
$$Sen3\theta = 3Cos^2\theta Sen\theta - Sen^3\theta$$

Para el caso en que $n < 0$; se escribe $n = -k$, con $k > 0$, lo que en la fórmula de De Moivre produce:

$$(Cos\theta + iSen\theta)^n = (Cos\theta + iSen\theta)^{-k} = ((Cos\theta + iSen\theta)^{-1})^k$$
$$= \left(\frac{Cos\theta - iSen\theta}{Cos^2\theta + Sen^2\theta}\right)^k = (Cos\theta - iSen\theta)^k = Cosk\theta - iSenk\theta$$
$$= Cos(-k\theta) + iSen(-k\theta)$$
$$= Cos(n\theta) + iSen(n\theta).$$

Por ello, $(Cos\theta + iSen\theta)^n = Cosn\theta + iSenn\theta$, $\forall n \in \mathbb{Z}$.

La Fórmula de De Moivre constituye una excelente herramienta para deducir identidades trigonométricas referidas a ángulos múltiples al separar las partes real e imaginaria en la expansión del Binomio de Newton cuando se combina con las fórmulas de Euler, a saber:

$$e^{i\theta} = Cos\theta + iSen\theta$$
$$e^{-i\theta} = Cos\theta - iSen\theta$$

En particular, al utilizar la primera fórmula de Euler, se determina que $e^{i\pi} + 1 = 0$, que condensa en una igualdad cinco de los más famosos símbolos numéricos que posee la matemática.

Entre otras identidades que utilizan las fórmulas de Euler, están las que se presentan en seguida.

$$e^{i(5\theta)} = \left(e^{i\theta}\right)^5 = (Cos\,\theta + iSen\,\theta)^5$$

Al igualar las partes real e imaginaria de la expresión anterior, se tiene:

$$Cos\,5\theta = 16Cos^5\theta - 20Cos^3\theta + 5Cos\theta$$
$$Sen\,5\theta = 16Sen^5\theta - 20Sen^3\theta + 5Sen\theta$$

Otros resultados que se pueden obtener con este procedimiento, son:

$$Cos\,6\theta = 32Cos^6\theta - 48Cos^4\theta + 18Cos^2\theta - 1$$
$$Sen\,6\theta = 32Sen\theta Cos^5\theta - 32Sen\theta Cos^3\theta + 6Sen\theta Cos\theta$$
$$Cos\,7\theta = 64Cos^7\theta - 112Cos^5\theta + 56Cos^3\theta - 7Cos\theta$$
$$Sen\,7\theta = -64Sen^7\theta + 112Sen^5\theta - 56Sen^3\theta + 7Sen\theta$$

6.6 Raíces de un número complejo

Los valores de $(Cos\theta + iSen\theta)^{\frac{1}{n}}$, $\forall n \in \mathbb{Z}^+$ se definen como los números complejos de la forma $Cos\alpha + iSen\alpha$ que tienen su n-ésima potencia igual a $Cos\theta + iSen\theta$; por ello se tiene $(Cos\alpha + iSen\alpha)^n = Cos\theta + iSen\theta$, ó mejor $Cosn\alpha + iSenn\alpha = Cos\theta + iSen\theta$, y en consecuencia, $\alpha = \frac{\theta}{n}$, o mejor aún, $\alpha = \frac{\theta+2k\pi}{n}$, donde $k \in \mathbb{Z}$.

En consideración a esto, se tiene,

$$(Cos\theta + iSen\theta)^{\frac{1}{n}} = Cos\left(\frac{\theta + 2k\pi}{n}\right) + iSen\left(\frac{\theta + 2k\pi}{n}\right), k \in \mathbb{Z}$$

Se encuentran n valores distintos al proponer para k cualquier conjunto de n enteros consecutivos; en particular, los valores $0, 1, 2, 3, \ldots, n-1$.

Siendo $z = r(Cos\theta + iSen\theta), m \in \mathbb{Z}^+$ y $n \in \mathbb{Z}^+$, para calcular las raíces n-ésimas de z^m se dispone $z^{\frac{m}{n}} = R(Cos\alpha + iSen\alpha)$ y utilizando la fórmula de De Moivre, se encuentra en primera instancia que $z^m = R^n(Cosn\alpha + iSenn\alpha)$, y al aplicarla una segunda ocasión se halla $r^m(Cosm\theta + iSenm\theta) = R^n(Cosn\alpha + iSenn\alpha)$. Luego se obtienen las raíces n-ésimas en los dos miembros de la igualdad para obtener, en definitiva:

$$r^{\frac{m}{n}}\left(Cos\left(\frac{m\theta + 2k\pi}{n}\right) + iSen\left(\frac{m\theta + 2k\pi}{n}\right)\right) = \left(r(Cos\theta + iSen\theta)\right)^{\frac{m}{n}} = z^{\frac{m}{n}}.$$

Los n valores distintos se encuentran al disponer para k, n valores consecutivos entre los números enteros.

Ejemplo:

Calcular las raíces n -ésimas de 1.

Solución:

En este caso, $r = 1$ y $\theta = 0$; entonces $(1 + 0i)^{\frac{1}{n}} = Cos\left(\frac{2k\pi}{n}\right) + iSen\left(\frac{2k\pi}{n}\right)$ donde $k \in \{0,\ 1,\ 2,\ 3, \ldots,\ n-1\}$. Por tanto, para $n = 3$ se obtiene:

$$(1 + 0i)^{\frac{1}{3}} = Cos\left(\frac{2k\pi}{3}\right) + iSen\left(\frac{2k\pi}{3}\right), \text{donde } k \in \{0,\ 1,\ 2\}$$

$$k = 0 \text{ implica } r_0 = Cos0 + iSen0 = 1 + 0i = 1$$

$$k = 1 \text{ implica } r_1 = Cos\frac{2\pi}{3} + iSen\frac{2\pi}{3} = -\frac{1}{2} + i\frac{\sqrt{3}}{2}$$

$$k = 2 \text{ implica } r_2 = Cos\frac{4\pi}{3} + iSen\frac{4\pi}{3} = -\frac{1}{2} - i\frac{\sqrt{3}}{2}$$

Geométricamente, estas raíces representan los vértices de un triángulo equilátero inscrito en la circunferencia unitaria tal y como se puede a apreciar en la Figura 33.

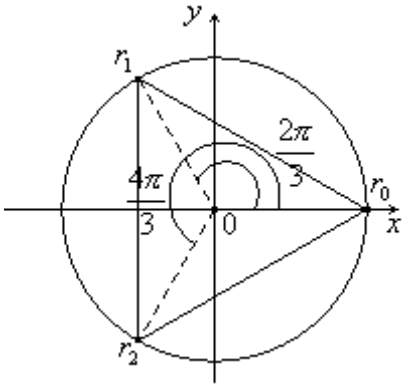

Figura 33. Raíces cúbicas de la unidad

Ejemplo:

Determinar las raíces quintas de $-2+2i$.

Solución:

$$a)\ r=\sqrt{a^2+b^2}=\sqrt{2^2+2^2}=\sqrt{8}=2^{\frac{3}{2}}$$

$$b)\ Tan\theta=\frac{b}{a}=\frac{2}{-2}=-1 \text{ lo que implica que } \theta=Arc\,tan(-1)=\frac{3\pi}{4}=135^o$$

$$c)\ -2+2i=2^{\frac{3}{2}}(Cos135^0+iSen135^o)$$

$$d)\ (-2+2i)^{\frac{1}{5}}=\left(2^{\frac{3}{2}}\right)^{\frac{1}{5}}\left[Cos\left(\frac{135^0+k\cdot 360^o}{5}\right)+iSen\left(\frac{135^0+k\cdot 360^o}{5}\right)\right]$$

De aquí se obtiene:

$$r_0=2^{\frac{3}{10}}(Cos27^o+iSen27^o)$$

$$r_1=2^{\frac{3}{10}}\left[Cos\left(\frac{135^o+360^o}{5}\right)+iSen\left(\frac{135^o+360^o}{5}\right)\right]=2^{\frac{3}{10}}(Cos99^o+iSen99^o)$$

$$r_2=2^{\frac{3}{10}}\left[Cos\left(\frac{135^o+720^o}{5}\right)+iSen\left(\frac{135^o+720^o}{5}\right)\right]=2^{\frac{3}{10}}(Cos171^o+iSen171^o)$$

$$r_3=2^{\frac{3}{10}}\left[Cos\left(\frac{135^o+1080^o}{5}\right)+iSen\left(\frac{135^o+1080^o}{5}\right)\right]=2^{\frac{3}{10}}(Cos243^o+iSen243^o)$$

$$r_4=2^{\frac{3}{10}}\left[Cos\left(\frac{135^o+1440^o}{5}\right)+iSen\left(\frac{135^o+1440^o}{5}\right)\right]=2^{\frac{3}{10}}(Cos315^o+iSen315^o)$$

Ejemplo:

El cálculo de las raíces n -ésimas de un número complejo exige gran cantidad de operaciones que logran desviar la esencia misma del problema. Las siguientes líneas permiten realizar esta tarea dentro del sistema *Derive*, con gran confiabilidad y para cualquier número complejo.

```
NUM(a,b):=a+b*#i
MODU(a,b):=ABS(NUM(a,b))
RAIN(a,b,n):=ABS(NUM(a,b))^(1/n)
ANG(a,b):=ACOS(a/ABS(NUM(a,b)))
RAICES(a,b,n):=VECTOR(RAIN(a,b,n)*(COS((ANG(a,b)+ 2*pi*k )/n) +
#i*SIN((ANG(a,b)+2*pi*k)/n)),k,0,n-1)
PUNTOS(a,b,n):=VECTOR([RAIN(a,b,n)*COS((ANG(a,b)+ 2* pi*k) /n),
RAIN(a,b,n)*SIN((ANG(a,b) + 2*pi*k)/n)] ,k,0,n)
```

Para calcular las raíces sextas de la unidad, utilizando el sistema Derive mediante el uso del archivo de utilidad diseñado por las expresiones mencionadas, es suficiente con simplificar la orden RAICES (1,0,6), con lo cual se obtiene el siguiente vector de raíces:

$$\left[\frac{1}{2},\ \frac{1+\sqrt{3}i}{2},\ \frac{-1+\sqrt{3}i}{2},\ -1,\ \frac{-1-\sqrt{3}i}{2},\ \frac{1-\sqrt{3}i}{2}\right]$$

Al simplificar la expresión PUNTOS (1,0,6) se obtiene la matriz de puntos, vértices del hexágono que determinan estas raíces (Figura 34).

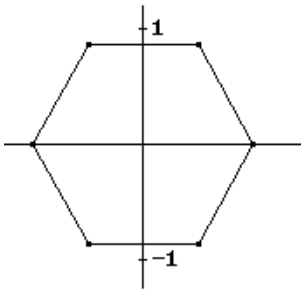

Figura 34. Raíces sextas de la unidad

Con la orden PUNTOS (-2,2,5) se encuentran los vértices del pentágono regular que se corresponden con las raíces quintas del complejo $-2+2i$, cuya gráfica aparece en la Figura 35.

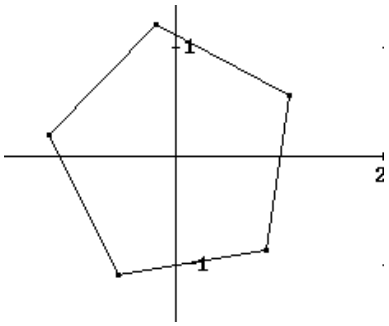

Figura 35. Raíces quintas de $-2+2i$

Con grandes detalles, se ha expuesto en el caso particular de la multiplicación que la esencia de ella cuando se aplica sobre $\mathbb{R}$ aparece por la posibilidad de dilatar, contraer o puntificar segmentos y a la vez poder cambiar de sentido en segmentos dirigidos cuando de multiplicar por un real negativo se trata. En el caso de los números complejos $\mathbb{C}$ surge la posibilidad de rotar vectores; este es el caso de multiplicar, por ejemplo, por i para lograr el efecto de que todo el plano rote un ángulo recto. Este tipo de hechos se deben destacar en los cursos regulares como un testimonio claro de la fuerte relación existente entre la aritmética y la geometría, lo que a su vez posibilita pensar en la existencia de estructuras más grandes como la de los hipercomplejos o cuaterniones de Hamilton, donde se pierde la conmutatividad de la multiplicación, y la de los Octonios en la que se pierde la asociatividad.

Contrarias a la dificultad histórica y dialéctica de la aparición y aceptación de los números complejos, han surgido ramas especializadas donde su tratamiento es eje fundamental y aplicaciones técnicas de gran trascendencia: muchos resultados del análisis en variable real se consiguen al atravesar el análisis en variable compleja; las funciones conformes de argumentos complejos se utilizan en la aviación. Dentro del campo formal, el campo de los complejos ha logrado enriquecer los fundamentos teóricos de los sistemas numéricos ya que aceptan varias formas de representación y sin duda, una prueba de su importancia, es la cantidad de representaciones que tiene un objeto. Una de las variadas formas de representar a los complejos es a través de matrices reales 2×2, con la cual se deja entrever que las estructuras $(\mathbb{C},\ +\ ,.)$ y $\left(\begin{pmatrix} a & -b \\ b & a \end{pmatrix} \in \mathbb{R}^{2\times 2},\ +,\ .\right)$ son indistinguibles, y con ello se determina cómo $(\mathbb{C},\ +\ ,.)$ es una subestructura del anillo $(\mathbb{R}^{2\times 2},\ +,\ .)$, y este a su vez, es un claro ejemplo que las subestructuras pueden ser más poderosas que las estructuras ya que los complejos configuran un campo, mientras la estructura que lo contiene es tan solo un anillo.

Sobre la representación en curso se deben ejecutar las siguientes identificaciones:

$1 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$, $i = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ y de esta manera, cualquier complejo $a + bi$ se puede representar de la siguiente manera:

$$a + bi = a\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} + b\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} a & -b \\ b & a \end{pmatrix}.$$

En el caso de los cuaterniones de Hamilton se pueden elaborar separaciones de la forma $H = \mathbb{R} + Im(H)$, donde la parte imaginaria $Im(H)$ se confunde en todos sus aspectos con $\mathbb{R}^3$, y por lo cual, cuando $p \in Im(H)$ y $q \in Im(H)$ se tiene que p y q están en $\mathbb{R}^3$, por ello ocurre que $pq = -p.q + p \times q$ donde ". " indica producto escalar y " $\times$ " el producto vectorial; el producto escalar respeta traslaciones y el productor vectorial respeta volúmenes. Esto señala cómo en los cuaterniones de Hamilton se encuentra comprometido el cálculo vectorial y una disculpa para estudiar a fondo este constructo que acarrea la curiosa anécdota de que Hamilton obligaba a sus hijos todas las mañanas a preguntarse si ya había encontrado la forma de multiplicar en $\mathbb{R}^3$.

EJERCICIOS

Capítulo 1. Generalidades de los sistemas numéricos

1. Explicar las propiedades que satisface el conjunto de los números naturales con la adición.

2. Explicar las propiedades que satisface el conjunto de los números naturales con la multiplicación.

3. Determinar un criterio para reconocer cuando dos números naturales son iguales o diferentes.

4. Explicar el por qué la suma y el producto de dos naturales múltiplos de 7 también son múltiplos de 7.

5. Estudiar y determine la cardinalidad de los conjuntos de los números naturales, los enteros, los racionales, los reales y los complejos.

6. ¿Cuántos subconjuntos de los naturales existen con la misma cardinalidad que los naturales?

7. Determinar algoritmos de carácter geométrico para determinar la suma, el producto y el cociente de dos enteros no negativos.

8. Construir con regla y compás números irracionales de la forma $\sqrt{\frac{n}{n+1}}$.

9. Establecer una forma de reconocer cuando dos números complejos son iguales.

10. ¿Por qué razón, si utiliza coordenadas polares para representar complejos, tal representación no es única?

11. Indicar algunas situaciones donde el conjunto de los números enteros deja de ser suficiente para resolver el problema.

12. Argumentar las razones del por qué ningún conjunto de siete elementos puede ser igual a uno de ocho elementos.

13. Proponer ejemplos de conjuntos infinitos que posean la misma cardinalidad.

1. Demostrar que cualquier número natural $n \neq 0$ es e la forma $n = m^*$ para algún natural m.

2. Demostrar que para todo natural m es válida la fórmula $m^* = m + 0^*$.

3. Demostrar que para todo natural m es cierto que $m \neq m^*$.

4. Demostrar que en el conjunto de los números naturales $m + n = 0$ si y sólo si $m = 0$ y $n = 0$.

5. Demostrar en el conjunto de los números enteros que $m^2 = 0$ si y sólo si $m = 0$.

6. Demostrar que si m y n son números naturales, la expresión $mn = 0$ es cierta sólo si $m = 0$ o $n = 0$.

7. Demostrar que $n + 1 = 1 + n$, $\forall n \in \mathbb{N}$.

8. Demostrar que en el conjunto de los números naturales si $n^2 \neq 0$ entonces $n > 1$.

9. Demostrar que para cualquier número natural n se tiene que $n < n^*$.

10. Demostrar para el conjunto de los números naturales que si $n < m$ y $m < s$ entonces $n < s$.

11. Demostrar que si $n < s$ dentro del conjunto de los naturales, se encuentra que $n + p < s + p$ cualquiera que sea $p \in \mathbb{N}$.

12. Demostrar que $(m + n)^* \neq m$ para cualquier par de valores m y n en $\mathbb{N}$.

13. Demostrar que la relación “menor que” es transitiva pero no reflexiva ni simétrica.

14. Demostrar para el conjunto de los números naturales que si $m < n^*$ entonces
$m \leq n$.

15. Demostrar para cualquier número natural n cada una de las siguientes proposiciones:

    $3^{2n+2} + 2^{8n+1}$ es múltiplo de 11.

    $3^{4n+2} + 2 \cdot 4^{3n+1}$ es un múltiplo de 17.

    $n^2 - 2$ no es divisible por 3.

    $n^7 - n$ es divisible por 42.

16. Para qué valores de $n \in \mathbb{N}$ se encuentra que:

    $n - 2$ es un divisor de $2n$.

    $n - 3$ es un divisor de $n^2 + 1$.

    $n - 1$ es un divisor de $n^2 - 4$.

17. Probar que la suma entre 1 y el producto de cuatro naturales consecutivos se consigue un cuadrado.

18. Probar que la suma entre 1 y el producto de dos naturales impares consecutivos se consigue un cuadrado.

19. Probar que la suma entre 1 y el producto de dos naturales pares consecutivos se consigue un cuadrado.

20. Probar que el producto de cuatro naturales consecutivos no puede ser un cuadrado.

21. Demostrar por inducción la veracidad de cada una de las fórmulas siguientes:

$$\sum_{i=1}^{n} (2i - 1) = n^2$$

$$\sum_{i=1}^{n} i^2 = \frac{n(n+1)(2n+1)}{6}$$

$$\sum_{i=1}^{n} 2^i = 2(2^n - 1)$$

$$\sum_{i=1}^{n} \frac{1}{i(i+1)} = \frac{n}{n+1}$$

En $\mathbb{N} \times \mathbb{N}$ se definió la relación de equivalencia $(a,b) \sim (c,d) \Leftrightarrow a+d = b+c$ y se establecieron las clases $[a,b] = \{(x,y) \in \mathbb{N} \times \mathbb{N}: x+b = y+a\}$; teniendo en cuenta esta situación y las definiciones establecidas para sumar y multiplicar clases, demostrar las siguientes proposiciones:

(a) $[a*,a] = 1$ y $[a,a*] = -1$
(b) $[a+b,b] = [a*,1]$
(c) $[a,b] + [c,c] = [a,b]$
(d) $[a,b] \cdot [c,c] = [c,c]$
(e) $[a,b] \cdot [c*,c] = [a,b]$
(f) $[a,b] + [b,a] = [a,a]$

Demostrar que la fórmula $F_n = \frac{\sqrt{5}}{5}\left[\left(\frac{1+\sqrt{5}}{2}\right)^n - \left(\frac{1-\sqrt{5}}{2}\right)^n\right]$ produce la secuencia de Fibonacci $1,\ 1,\ 2,\ 3,\ 5,\ 8,\ 13, \ldots$. $\frac{1+\sqrt{5}}{2} = \Phi$ es llamada la razón áurea y es una de las raíces de la ecuación $x^2 - x - 1 = 0$.

Demostrar que si a y b están en $\mathbb{Z}$ entonces $ab = 0$ si y sólo si $a = 0$ o $b = 0$.

Demostrar que si a y b están en $\mathbb{Z}$ entonces $|ab| = |a||b|$.

Demostrar que $a - b < a + b$, $\forall b \in \mathbb{Z}^+$.

Enunciar y demostrar la propiedad cancelativa para la multiplicación de enteros.

Aplicar el algoritmo de la división de Euclides a los siguientes pares de números:
123 y 14 1787 y 456 454545 y 46676

Calcular el Máximo Común Divisor de los siguientes pares de números y escribirlos como combinación lineal de ellos:
12345 y 3450 454787 y 45451 454545 y 38787

Calcular el Mínimo Común Múltiplo de los pares de enteros del problema anterior.

Sea d un divisor común de a y b, probar que $M.C.M\left(\frac{a}{d}, \frac{b}{d}\right) = \frac{M.C.M(a,b)}{d}$.

Hallar un par de enteros a y b tales que $a + b = 54$ y $M.C.M(a,b) = 231$.

Hallar un par de enteros a y b tales que $a + b = 69$ y $M.C.M(a,b) = 270$.

Hallar un par de enteros a y b tales que $a + b = 27$ y $M.C.D(a, b) = 3$.

Hallar un par de enteros a y b tales que $a + b = 91$ y $M.C.D(a, b) = 7$.

Probar que ningún número entero puede ser par e impar a la vez.

Demostrar que si $M.C.D(a, b) = d$ entonces $M.C.D(a^n, b^n) = d^n$, $\forall n \in \mathbb{N}$.

Probar que si p es un número primo, entonces p es divisor del combinatorio $\binom{p}{k}$ donde k está entre 1 y $p - 1$ inclusive.

Demostrar que para todo $n \in \mathbb{N}$ el combinatorio $\binom{2n}{n}$ es divisible por $n + 1$.

Probar que si p es un número primo diferente de 2 y de 3, entonces es de la forma $6m - 1$ o de la forma $6m + 1$ para algún m en $\mathbb{Z}$.

Calcular los números primos p para los cuales la terna p, $p + 2$ y $p + 4$ está formada sólo por números primos.

Probar que el producto de los enteros $2n$, $2n + 1$ y $2n + 2$ es múltiplo de 24.

Para los enteros positivos n, m y a con $a > 1$, demostrar que $a^n - 1$ es un divisor de $a^m - 1$ si y sólo si n es un divisor de m.

Demostrar que para todo natural n y cualquier par de enteros a y b se tiene que $a - b$ es un divisor de $a^n - b^n$.

Demostrar que para todo natural par n y cualquier par de enteros a y b se tiene que $a + b$ es un divisor de $a^n - b^n$.

Demostrar que todo entero cuadrado perfecto es de la forma $4m$ o $4m + 1$ para algún entero m.

¿Cuáles de los siguientes números enteros son impares?

$n^2 - 3$ $\quad n^3 + 1$ $\quad 2n^3 + 3$ $\quad (2n - 1)(2n + 1)$
$(4n - 1)(4n + 1)$ $\quad n! + 3$ $\quad (-1)^n \cdot 3 + (-1)^{n-1} \cdot 3$ $\quad n^5 - n$

Demostrar que el único primo par que existe es el 2.

Demostrar que cualquier par de números primos son primos entre sí.

Demostrar que existen infinitos números primos terminados en 999.

Demostrar que existen infinitos números primos terminados en cualquier cadena de unos $(\ldots 111.)$

Encontrar un algoritmo que permita calcular el número de divisores de cualquier entero n.

Encontrar un algoritmo que permita calcular la suma de los divisores de cualquier entero n.

Calcular todos los números de cuatro cifras que a la vez sean divisibles por 15 y por 17.

Capítulo 4. Los números racionales

Parte 1:

4.4 EJERCICIOS

Demostrar que:

1. $[-a,-b]=[a,b]$
2. $-[-a,b]=-[a,-b]=[a,b]$
3. $-(-[a,b])=[a,b]$
4. $(-[a,b])\otimes(-[c,d])=[a,b]\otimes[c,d]$
5. $[1,a]>[0,k]\Leftrightarrow a>0$
6. $\beta>\alpha>0\Rightarrow\alpha^{-1}>\beta^{-1}>0$
7. $[a,b]\oplus[a,c]=[a,b+c]\Rightarrow a=0$
8. $(\alpha+\beta<\gamma+\beta)\Leftrightarrow(\alpha<\gamma)$
9. Cuando $\gamma>0,\ \alpha\cdot\gamma<\beta\cdot\gamma\Leftrightarrow\alpha<\beta$
10. Cuando $\gamma<0,\ \alpha\cdot\gamma<\beta\cdot\gamma\Leftrightarrow\alpha>\beta$
11. Si $\alpha,\ \beta$ están en $\mathbb{Q}$ y $\alpha\cdot\beta=0\Rightarrow\alpha=0$ o $\beta=0$

12. Si $[m,n] > [p,q]$ y si $[s,t] \in \mathbb{Q}^+$ entonces:

    a. $[m,n] \oplus [s,t] > [p,q]$
    b. $[m,n] \oplus [s,t] > [p,q] \oplus [s,t]$
    c. $[m,n] \oplus [s,t] > [p,q] \oplus [-s,t]$
    d. $[m,n] \oplus [-s,t] > [p,q] \oplus [-s,t]$

13. Demostrar que,

14. si $[a,b] < [c,d]$ y $[m,n] < [p,q]$ se tiene que $[a,b] \oplus [m,n] < [c,d] \oplus [p,q]$

15. $\forall [a,b] \in \mathbb{Q}$: $[a,b] \otimes [a,b] \geq [0,k]$, $k \neq 0$ y si $[a,b] \neq [0,k]$, entonces se implica $[a,b] \otimes [a,b] > [0,k]$.

16. Dados $a \in \mathbb{Q}$ y $p \in \mathbb{Q}^+$ determinar explícitamente el conjunto de todos los $x \in \mathbb{Q}$ tales que:

    e. $|x-a| < p$
    f. $|x-a| > p$
    g. $|x-a| \leq p$
    h. $|x-a| \geq p$

Parte 2:

Dadas las clases de equivalencia que construyen a los números racionales y sus operaciones de adición y multiplicación, demostrar las siguientes proposiciones:

(a) $[a,b] + [0,c] = [a,b]$ (b) $[a,b] + [-a,b] = [0,b]$
(c) $[a,b] \cdot [0,c] = [0,b]$ (d) $[a,b] \cdot [b,a] = [b,b]$

Demostrar que si x y y son dos números racionales tales que $x < y$ siempre existe un número racional z tal que $x < z < y$.

Demostrar que si $n \in \mathbb{N}$ y $n > 1$ entonces $\sum_{i=1}^{n} \frac{1}{i}$ no es un entero.

Demostrar que si $ad - bc = \pm 1$ entonces la fracción $\frac{a+d}{b+c}$ es irreducible.

Demostrar que entre los racionales $\frac{2}{10}$ y $\frac{3}{10}$ existe una infinidad de números racionales.

Llevar a la forma $\frac{a}{b}$ los siguientes racionales expresados como fracciones continuas simples:

$r = [2; 1,2,3,1,2]$ $r = [3; 2,3,2,1,2,1,5]$ $r = [3; 2,3,3,3,2,2,5,2,7]$

Transformar en fracciones continua simples los siguientes números racionales:

$\frac{43}{30}$ $\frac{280}{87}$ $\frac{985}{408}$ $\frac{21}{13}$ $\frac{28196}{19939}$ $\frac{611}{185}$

Calcula la expansión decimal infinita y periódica de los siguientes números racionales:

$\frac{11}{13}$ $\frac{17}{13}$ $\frac{23}{19}$ $\frac{19}{23}$ $\frac{7}{29}$ $\frac{12}{13}$

Demostrar que todo decimal periódico representa a un número racional.

Capítulo 5. Los números reales

Expresar como fracciones continuas simples los siguientes números reales:

$\sqrt{7}$ $\sqrt{10}$ $\sqrt{\frac{2}{3}}$ $\sqrt{15}$ $\sqrt{21}$ $\sqrt{33}$

Empleando la fracciones continuas simples infinitas y periódicas encontradas en el problema anterior, calcular aproximaciones racionales para cada uno de los números irracionales descritos.

Calcular los números reales que a continuación se expresan como fracciones continuas simples infinitas y periódicas:

$x = [1; \overline{3}]$ $x = [1; \overline{3,2}]$ $x = [1; 1, \overline{2,3}]$ $x = [1; 1,2, \overline{2,1,3}]$

Argumente la razón por la cual en número $\sum_{i=0}^{\infty} \frac{1}{10^{i!}}$ es un irracional.

Calcular algunas aproximaciones racionales de la razón dorada $\Phi = \frac{1+\sqrt{5}}{2}$.

Ordenar de mayor a menor el siguiente conjunto de números reales positivos:

$$\pi^e,\ e^\pi,\ e^e,\ \pi^\pi,\ \left(\frac{e}{\pi}\right)^\pi,\ \left(\frac{e}{\pi}\right)^e,\ \left(\frac{\pi}{e}\right)^e,\ \left(\frac{\pi}{e}\right)^\pi$$

Demostrar que la aplicación $f:\mathbb{C}\to\mathbb{C}$ tal que $f(z)=\overline{z}$ es una función biyectiva.

Demostrar que el valor absoluto del producto de dos complejos es el producto de sus valores absolutos y el argumento del producto es la suma de sus argumentos.

Demostrar que el valor absoluto del cociente de dos complejos es el cociente de sus valores absolutos y el argumento del cociente es el argumento del numerador menos el argumentos del denominador.

Hallar las raíces sextas de 1 y comprobar que entre ellas se encuentran las raíces cuartas y las raíces cúbicas de 1.

Demostrar que el conjugado del conjugado de un complejo z es el mismo z.

Hallar las raíces cúbicas, cuartas, quintas y sextas de los siguientes complejos.

8 $\quad 2+3i$ $\quad i$ $\quad 1$ $\quad 1+\sqrt{3}i$ $\quad -1$

Demostrar que la suma de las raíces enésimas de 1 es cero.

REFERENCIAS BIBLIOGRÁFICAS

Acevedo, M. & Falk, M. (1997). *Recorriendo el Álgebra: de la solución de ecuaciones al álgebra abstracta*. Universidad Nacional de Colombia.

Alexandrov, D., Kolmogorov, A., Laurentiev, M. & Otros. (1979). *La Matemática, su contenido, métodos y significado*. Alianza Universidad.

Ayres, F. (1978). *Álgebra Moderna*. McGraw-Hill.

Clawson, C. (1999). *Misterios Matemáticos, Magia y belleza de los números*. Editorial Diana.

Euclides (2000). *Elementos*. Biblioteca Clásica GREDOS, Traducción de Puertas Castaños María Luisa, Gráficas Cóndor.

Fraleigh, J. (1988). *Álgebra Abstracta*. Addison-Wesley Iberoamericana.

G. Bush, G. & Obreanu, P. (1972). *Introducción a la Matemática Superior*. Editorial Trillas.

Gentile, E. (1985). *Aritmética Elemental*. Secretaría General de la Organización de los Estados Americanos.

Gómez, C, Mosquera, S & Soto, F. (2002). *Matemáticas Fundamentales con Derive*. Universidad de Nariño.

Guedjj, D. (1987). *El imperio de las Cifras y los números*. Biblioteca de Bolsillo CLAVES.

Herstein, I. (1979). Álgebra Moderna. Trillas.

Jiménez, R. & otros. (2004). *Teoría de Números para Principiantes*. Universidad Nacional de Colombia.

Kline, M. (1979). *El Pensamiento Matemático de la Antigüedad a Nuestros Días*. Alianza Universidad.

Los Sofistas. (2009). Bibliografías. http://lossofistasut.blogspot.com/2009/05/bibliografias.html

Nachbin, L. (1986). *Álgebra Elemental*. Secretaría General de la Organización de los Estados Americanos.

Oostra, A. (2003). Acerca del Artículo On The Logic of Number de Charles Sanders Peirce. *Boletín de Matemática, X*(1), 13-20.

Pinzón, A. (1986). *Conjuntos y Estructuras*. Colección Harper.

Saldarriaga, P. (2013). Breve historia de la lógica. Consultado: septiembre de 2022, en https://pedrosaldarriaga.blogspot.com/2013/08/breve-historia-de-la-logica-en-un.html

Sanders, C. (2003). Peirce. Sobre la Lógica del Número. *Boletín de Matemática*, *X*(1), 1-12.

Soto, F. (1996). Sobre el Máximo Común Divisor de dos Enteros. *Sigma*, *7*, 3-11.

Soto, F. (1998). Fracciones Continuas y Derive, *RECYM*, (2), 71-84.

Soto, F., Osejo, E. & Caballero, R. (1996). Acerca de una enumeración peirceana de los racionales*. Boletín de Matemáticas*, III(2). 83-96.

Soto, O.F., Caicedo, S. J. & Escobar, H.A. (2021). *Lecciones de Aritmética: Un recurso para docentes*. Colombia: Editorial Universidad de Nariño. ISBN Digital 978-958-5123-71-7. Disponible en: https://sired.udenar.edu.co/7444/1/LIBRO%20Lecciones%20de%20Aritme%CC%81tica.pdf

Szymborska, W. (s.f.). El número Pi. Consultado: septiembre de 2022, en: https://www.madrimasd.org/cienciaysociedad/poemas/poesia.asp?id=606

Thomas, H. (1956). *The Thirteen Books of Euclid's Elements* (Segunda Edición). Dover Publications, Inc.

Trejo, C. (1985). *El Concepto de Número. Aritmética Elemental (*Tercera edición). Secretaría General de la Organización de los Estados Americanos.

Vera, F. (s.f.). *Veinte Matemáticos Célebres*. Texto preparado por Patricio Barros para Internet.

Vinogradov, I. (1971). *Fundamento de la Teoría de Números*, Editorial Mir.

Vorobiov, N. (1974). *Números de Fibonacci. Lecciones Populares de Matemáticas*, Editorial MIR.

Wikipedia (s.f.). Hobbes–Wallis controversy. Consultado: septiembre de 2022, en https://en.wikipedia.org/wiki/Hobbes%E2%80%93Wallis_controversy#cite_note-Skinner-3.

Williams, J. (1974). *Álgebra de Números Complejos*. Limusa.

ACERCA DE LOS AUTORES

Oscar Fernando Soto-Agreda. Docente adscrito al Departamento de Matemáticas y Estadística, Facultad de Ciencias Exactas y Naturales, Universidad de Nariño. Magister en Modelos de Enseñanza Problémica. Licenciado en Matemáticas y Física, Universidad de Nariño. Especialista en Computación para la Docencia, Universidad Mariana. Profesor Tiemplo Completo Universidad de Nariño.

Correo electrónico: oscarfdosoto@gmail.com; fsoto@udenar.edu.co.

Segundo Javier Caicedo-Zambrano. Docente adscrito al Departamento de Matemáticas y Estadística, Facultad de Ciencias Exactas y Naturales, Universidad de Nariño. Doctor en Ciencias de la Educación, Universidad del Tolima. Licenciado en Matemáticas y Física, Universidad de Nariño. Ingeniero de Sistemas, Universidad Antonio Nariño. Especialista en Computación para la Docencia, Universidad Mariana. Especialista en Multimedia Educativa, Universidad Antonio Nariño. Magister en Software Libre, Universidad Autónoma de Bucaramanga. Asesor de Desarrollo Académico, Universidad de Nariño. Profesor Tiempo Completo Universidad de Nariño.

Correo electrónico: jacaza1@gmail.com; jacaza1@udenar.edu.co.

La historia verifica cómo el hombre tardó miles de años en pasar del manejo de las cantidades al concepto de número; este concepto que subyace en el mundo incorruptible de las ideas y que hoy aparece tan sencillo, trivial y evidente es el producto de un largo trabajo de abstracción. Seguramente el mediador elemental para conseguir este resultado se encuentra en la diferencia entre lo singular y lo plural, mirando en cada objeto la existencia de la unidad y escindiendo, en la pluralidad, las diferencias particulares. Y es que el número convive en el límite entre lo parecido y lo diferente ya que las cosas que se enumeran son aparentemente parecidas y justamente se rotulan con cifras distintas porque a la vez son diferentes.

Las marcas y el emparejamiento son los primeros vestigios de la conservación de los números y su consecuente propiedad operativa y para su memorización recurrieron al cuerpo y muy especialmente a los dedos y las articulaciones.
El siguiente paso fue convertir el conocimiento numérico forjado en la práctica de una simbología primaria y de la necesidad de operar con las cantidades en un sistema de representación de los mismos que hoy se denomina numeración. La numeración actual, y que nos parece rutinaria, se caracteriza por varios aspectos mágicos que se ponen de relieve al analizar su sencillez e importancia; en principio alcanza formas de representación visual, oral y escrita, lo que se traduce en la posibilidad de su captura óptica, su expresión verbal o nombre y su representación simbólica a través de la escritura. Debe recordarse que la aparición de la escritura es el paso gigantesco que parte en dos la historia de la humanidad y permitió el paso a lo que se llama civilización.

El presente libro expone una perspectiva histórica epistemológica que, aunado al concepto de número, muestra cómo se fueron constituyendo los sistemas numéricos a partir de los números naturales: enteros, racionales, reales y complejos. Se evidencia las razones por las cuales se tuvo la necesidad de disponer de un nuevo sistema numérico que dé soporte a las operaciones de adición, multiplicación, inversos aditivos y multiplicativos en la resolución de problemas algebraicos.

El libro constituye una guía y fuente de consulta para estudiantes, docentes y comunidad académica en general de los programas en cuyo proceso de formación se requiera fundamentación matemática.

9 786287 509771

Universidad de Nariño
FUNDADA EN 1904

Universidad de Nariño
ACREDITADA DE ALTA CALIDAD
RESOLUCIÓN MEN 10567 - MAYO 23 DE 2017

Editorial
Universidad de Nariño