ALGORITMO GENERAL PARA DETERMINAR CRITERIOS DE DIVISIBILIDAD EN CUALQUIER BASE NUMÉRICA MEDIADA POR EL ENTORNO VIRTUAL APP-INVENTOR

JANNICK ANDRÉS LUGO GARCÍA

UNIVERSIDAD PEDAGÓGICA NACIONAL
FACULTAD DE CIENCIA Y TECNOLOGÍA
DEPARTAMENTO DE MATEMÁTICAS
LICENCIATURA EN MATEMÁTICAS
BOGOTÁ, D.C.
2021

ALGORITMO GENERAL PARA DETERMINAR CRITERIOS DE DIVISIBILIDAD EN CUALQUIER BASE NUMÉRICA MEDIADA POR EL ENTORNO VIRTUAL APP-INVENTOR

Trabajo de grado presentado como requisito parcial para optar por el título de Licenciado en Matemáticas

JANNICK ANDRÉS LUGO GARCÍA

Cód. 2016240045

Director:

WILLIAM ALFREDO JIMÉNEZ GÓMEZ

Magister en Docencia de la Matemática

UNIVERSIDAD PEDAGÓGICA NACIONAL
FACULTAD DE CIENCIA Y TECNOLOGÍA
DEPARTAMENTO DE MATEMÁTICAS
LICENCIATURA EN MATEMÁTICAS
BOGOTÁ, D.C.

2021

FACULTAD DE CIENCIA Y TECNOLOGÍA

DEPARTAMENTO DE MATEMÁTICAS

LICENCIATURA EN MATEMÁTICAS

ACTA DE EVALUACIÓN DE TRABAJO DE GRADO

Presentados y aprobados el documento escrito y la sustentación del Trabajo de Grado titulado "ALGORITMO GENERAL PARA DETERMINAR CRITERIOS DE DIVISIBILIDAD EN CUALQUIER BASE NUMÉRICA MEDIADA POR EL ENTORNO VIRTUAL APP-INVENTOR", elaborado por el estudiante **JANNICK ANDRÉS LUGO GARCÍA,** identificado con el Código **2016240045** y Cédula **1014214848** el equipo evaluador, abajo firmante, asigna como calificación **treinta y siete** (37**)** puntos.

El mismo equipo evaluador recomienda la siguiente sugerencia de distinción:

Ninguna ☒ Meritoria ☐ Laureada ☐

El Trabajo de Grado, presentado como monografía, constituye un requisito parcial para optar al título de **Licenciado en Matemáticas**.

En constancia se firma a los quince (20) días del mes de septiembre de 2021.

Mg. WILLIAM ALFREDO JIMÉNEZ GÓMEZ
Director del Trabajo de grado

Dra. LEONOR CAMARGO URIBE
Jurado del Trabajo de grado

Mg. NATALIA MORALES ROZO
Jurado del Trabajo de grado

A mis padres y a mi abuela por su apoyo incondicional.

Jannick Lugo

Resumen

En este trabajo se realizó un algoritmo para determinar criterios de divisibilidad en cualquier base sustentado a partir del trabajo realizado por Ruíz y Carvajal (2002) y de los aportes descritos en el libro *Teoría de números para principiantes* (escrito por Rubiano, G., Jiménez y Gordillo (2004)), los cuales están relacionados con la divisibilidad. A través de la búsqueda de trabajos previos orientados a encontrar este tipo de algoritmos y del estudio de la forma polinómica de un número como lo presentaban Osorio y Castañeda (2014), se llegó a considerar el análisis de la cifra de las unidades como pieza fundamental en la determinación de criterios. Esto se ve reflejado en uno de los teoremas resultado de este trabajo, el cual recibe el nombre de Criterio de las Cifras de las Unidades (CCU) el cual considera que, si la cifra de las unidades de un número no es múltiplo del máximo común divisor de la base y un posible divisor, entonces este último no divide al número. Teniendo en cuenta el potencial del algoritmo, se ejecuta a una aplicación en el entorno virtual *App-Inventor,* en donde un usuario deberá ingresar la base, el número escrito en esta base y el posible divisor para encontrar el criterio de divisibilidad correspondiente.

Palabras claves: Criterios de divisibilidad, Base numérica, Divisor, Forma polinómica de un número.

Contenido

Tablas

Ilustraciones

Introducción

Durante el semestre académico 2016-II, en el espacio académico de *Aritmética* de la tercera versión del plan de estudios de la Licenciatura en Matemáticas de la Universidad Pedagógica Nacional, que fue orientado por el profesor William Jiménez, se estudiaron algunos procedimientos para encontrar criterios de divisibilidad en diferentes bases; estos estaban asociados a reescribir la base como una combinación lineal donde uno de sus sumandos es múltiplo de un posible divisor, al escribir el número como sumas de potencias de la base. A su vez, en el curso surgió la idea de no reescribir todas las potencias como una combinación lineal, excepto la que acompaña la cifra de las unidades.

Después de estudiar la relación del máximo común divisor con la cifra de las unidades, se extiende el algoritmo para determinar criterios, en lo que apareció la condición que restringe la posibilidad de considerar cualquier cifra de las unidades para ejecutar el algoritmo. De aquí nació la necesidad de caracterizar los números en dos categorías: la primera, los números cuya cifra de las unidades es divisible por el máximo común divisor de la base y el posible divisor; y la segunda, aquellos números cuya cifra de las unidades no es múltiplo de este posible divisor. De acuerdo con lo anterior, se obtuvo un teorema que permite descartar la segunda categoría.

A partir de estos resultados se desarrolló una aplicación que permite determinar criterios de divisibilidad en cualquier base y posible divisor, todo este contenido se desarrolla en cuatro capítulos los cuales se describen brevemente a continuación:

En el primer capítulo, se realizó la revisión de los teoremas relacionados con los algoritmos para generar criterios de divisibilidad uno en base diez y los otros en diferentes bases.

En el segundo capítulo, se realizó una recopilación de resultados obtenidos en trabajos asociados a las propiedades fundamentales de la divisibilidad desde la construcción del conjunto de los números enteros, también se tienen en cuenta los aportes de autores como Blaise Pascal (1665), el cual determinó criterios de divisibilidad para números escritos en diferentes bases. Además, se resaltó la importancia de usar un entorno virtual (*App*-Inventor) para la aplicación de algunos conceptos matemáticos y las formas de usar sus herramientas;

teniendo en cuenta los aportes de Martin (2001) y Sánchez (2002), quienes indican que las habilidades que emergen del uso de un software son aspectos primarios para el desarrollo del pensamiento de orden superior.

En el tercer capítulo se desarrolla, desde la teoría propuesta de este documento, la creación del algoritmo que determina los criterios de divisibilidad para un número escrito en cualquier base, se dan a conocer dos teoremas fundamentales: El primero, permite considerar números en cualquier base para determinar criterios de divisibilidad, con la restricción que la cifra de las unidades debe ser múltiplo del máximo común divisor de la base en la que está escrito el número y el posible divisor; el segundo, considera cuáles números no son divisibles por otro a partir de la relación de la cifra de las unidades con este máximo común divisor. Sin embargo, ambos teoremas forman el Algoritmo único de divisibilidad, el cual permite extender o "eliminar" la restricción del primer teorema y, permite generalizar un proceso para determinar la divisibilidad de un número.

También, se programó el algoritmo descrito en el teorema *Algoritmo parcial de divisibilidad* a una herramienta virtual (software) o programa, donde se muestra una descripción breve del entorno de la herramienta *App-Inventor* y se exponen los pasos fundamentales que se tuvieron en cuenta para la elaboración de la aplicación.

Finalmente, en el cuarto capítulo se plasmaron unas consideraciones que posibilitan dar respuestas a los objetivos planteados en el trabajo, donde se exponen ideas de orden matemático y tecnológico, limitaciones del estudio y futuras adecuaciones que pueden emerger; en términos generales, esta propuesta facilita el proceso para determinar criterios de divisibilidad considerando cualquier base y un posible divisor.

Justificación

Ante la variedad de propuestas para encontrar criterios de divisibilidad, se fomentan procesos de conjeturación y justificación, los cuales son una constante en el curso de *Aritmética*. En este sentido, la propuesta de buscar criterios nuevos no deja de ser un trabajo enriquecedor para la formación como docente de matemáticas, ya que posibilita potenciar dichos procesos y realizar producción matemática.

La tarea diaria de los matemáticos de realizar la transición entre lo particular a lo general es primordial, ya que algunas veces solo pueden mantenerse en el plano de lo abstracto y donde la manipulación solo se puede hacer a través del pensamiento. Por su parte, en otras ocasiones, se pueden evidenciar patrones que hacen posible que se determinen algoritmos y se diseñe un programa que facilite la tarea de encontrar resultados en menos tiempo. Sumado a ello, los intentos de algunos autores como Osorio y Castañeda (2014) de escribir un algoritmo que permita determinar criterios de divisibilidad no solo en una base numérica, motivó a que se estudiará la posibilidad de buscar un algoritmo que permita determinar criterios y construirlo de la manera más general posible.

De esta manera, el trabajo busca diseñar un código accesible para que sea ejecutado en una aplicación, permitiendo a un usuario ver los resultados de dicho algoritmo y que esté al alcance de cualquier persona interesada en el tema o que requiera observar, analizar o conjeturar acerca de los criterios de divisibilidad; conjeturar, justificar estas proposiciones y algunas veces traducir a un lenguaje de programación, permiten aportar al conocimiento de esta las matemáticas o para estudiarla. Este andamiaje se trabaja en cursos como *Aritmética* y en grupos de investigación como el Seminario de Álgebra de la Universidad Pedagógica Nacional, donde precisamente surgió la propuesta del presente trabajo.

La iniciativa de encontrar criterios en diferentes bases, a partir de algunos casos (los cuales son muy comunes en la comunidad educativa) como los criterios del 2, 3 y 5 en base 10, llevó a que se desarrollaran diferentes propuestas. Algunas de estas involucraron todas las cifras del número para determinar dichos criterios, otras solo consideraban la cifra de las unidades

para hacer la misma tarea; esta última llamó la atención del docente William y del mismo autor, por esta razón, se comenzó a trabajar en torno a esta idea.

Después de indagar algunos documentos relacionados a determinar criterios de divisibilidad, se encontró que algunos estudiaban criterios en diferentes bases con algunas características particulares. En otros se abordan criterios para una misma base para cualquier divisor, sin embargo, aparte del resultado propuesto por Pascal (1665), no se encontró algún otro que permitiera de forma general considerar cualquier número, base y divisor; dado lo anterior, esto llevó a que se pensara en desarrollar un algoritmo que considere cualquier base y al mismo tiempo que solo se tenga en cuenta la cifra de las unidades (como fue trabajado por Ruíz y Carvajal (2002)) para determinar el criterio.

Este trabajo de grado promueve una experiencia desde un orden matemático, creando más conocimiento en esta ciencia, lo cual enriquece el proceso de formación del licenciado en matemáticas; los diferentes aportes sobre algoritmos que contribuyen a determinar criterios de divisibilidad permiten ver los diferentes caminos con un mismo propósito, algo que sin duda ofrece las Matemáticas, de encontrar diversas soluciones a un mismo problema. Este documento recoge esas ideas que también sirvieron de inspiración para el desarrollo de este trabajo y que pueden servir de material de consulta para estudiantes de Matemáticas, Licenciatura en Matemáticas o para la comunidad académica en general.

Objetivos

Objetivo general

Construir un algoritmo general que determine criterios de divisibilidad en cualquier base numérica el cual sea ejecutado por un usuario a través de una *App*.

Objetivos específicos

- Seleccionar los principales teoremas sobre la divisibilidad y la caracterización del conjunto numérico de los enteros, con el fin de justificar los algoritmos propuestos.
- Demostrar el algoritmo general de divisibilidad basado en el estudio de criterios y sus respectivos algoritmos en diferentes bases numéricas.
- Diseñar una *App* que ejecute el algoritmo general y al mismo tiempo muestre el criterio correspondiente.

1. Antecedentes

A partir del surgimiento de esta propuesta, se empezó con una búsqueda de trabajos elaborados que estuvieran relacionados con teoremas de divisibilidad; esta búsqueda inicia con el planteamiento propuesto por Pascal (1623-1662), luego se revisaron trabajos recientes como los de Ruíz y Carvajal (2002); y Osorio y Castañeda (2014). En ese sentido, se encuentran algunas relaciones de orden matemático en sus planteamientos que posibilitaron dar un horizonte al presente trabajo, el cual se encaminó (en un principio) a definir y nombrar teoremas asociados a la divisibilidad y todos los posibles términos que lo implican: algoritmo de la división, máximo común divisor, números primos, primos relativos, expresión de números en diferentes bases.

De esta manera, estos autores dejan abierta la posibilidad de estudiar criterios de divisibilidad en diferentes bases numéricas y al mismo tiempo, buscar algoritmos y métodos no tan extensos de hacer operaciones para llegar a nuevos criterios; además, se buscaron fuentes correspondientes al uso de software para la aplicación de conceptos matemáticos. En las siguientes tablas se muestran las fichas que resumen el objetivo del trabajo por cada autor, su relación y diferencias con el desarrollo de esta propuesta más adelante en el marco de referencia se profundizara en cada uno de los resultados resumidos en la siguiente tabla:

<table>
<tr><td colspan="3">El siguiente es un resultado de Ruíz, F., & Carvajal, J. (2002), en su trabajo titulado Un criterio universal de divisibilidad</td></tr>
<tr><td colspan="3">Teorema Criterio universal de divisibilidad (CUD): Si $b \in Z$ y $b \neq 0$ es un entero primo relativo con 10, entonces, existe un entero a tal que para cualquier número natural n, donde $n = 10d + u; 0 \leq u \leq 9$, se tiene que, $b|n \leftrightarrow b|(d - au)$</td></tr>
<tr><td>¿Qué se desarrolló en el trabajo?</td><td>Diferencia con lo planteado en esta propuesta</td><td>¿De qué manera contribuye a esta propuesta?</td></tr>
<tr><td>Es un resultado que es muy cercano a lo que se pretende realizar en este</td><td>• Solo consideran la base diez.</td><td>Esta muestra otra forma de realizar la demostración de enunciar y sintetizar un resultado en un teorema que es muy</td></tr>
</table>

trabajo de grado. En este consideran también un algoritmo para determinar criterios que se caracterizan por considerar la cifra de las unidades y el número sin dicha cifra. También tienen en cuenta la combinación lineal del máximo común divisor que en este caso siempre va a ser uno, debido a que se buscan números que sean primos relativos con diez. Los criterios tienen la característica que se debe sumar el número sin la cifra de las unidades más el sumando de dicha combinación lineal en el cual uno de sus factores es la cifra de las unidades. Con este método que proponen estos autores se puede extender el resultado a más bases que cumplan la condición de ser primos relativos con el número por el cual se desea dividir.	• Solo se tienen en cuenta números que sean primos relativos con diez (la base).	similar; también deja ver en su demostración una forma de escribir el número dado sin la cifra de las unidades de una manera muy compacta, la cual se tendrá en cuenta al momento de plantear los resultados de la investigación. Esta forma es $n = 10d + u; 0 \leq u \leq 9$ Donde u es la cifra de las unidades y aunque no se menciona explícitamente el número d qué representa, este se puede obtener de factorizar 10 de la forma polinómica de n, es decir, $n = c_n \times 10^k + c_{k-1} \times 10^{k-1} + \cdots + c_1 \times 10 +$ donde $0 \leq c_i \leq 9$ Factorizando 10, $n = 10[c_k \times 10^{k-1} + c_{k-1} \times 10^{k-2} + \cdots + c_1] + u$ Haciendo $d = c_k \times 10^{k-1} + c_{k-1} \times 10^{k-2} + \cdots + c_1$, es decir d es el número sin la cifra de las unidades.

Tabla 1: Teorema Criterio universal de divisibilidad (CUD)

El siguiente es un teorema propuesto por Blaise Pascal (Glaser,1971; citado en Osorio, K., & Castañeda, E. (2014)
Teorema Criterio General de Divisibilidad Extendido (CGDE): El número $n = a_t b^t + a_{t-1} b^{t-1} + \cdots + a_1 b + a_0$ en base b es divisible por p si y solo si $b \mid T$, donde $T =$

$a_tR_t + a_{t-1}R_{t-1} + \cdots + a_1R_1 + a_0$ y $bR_{i-1} = px_i + R_i$, para cada $i = 1,2, \ldots, t$, teniendo en cuenta que $R_0 = 1$.		
¿Qué se desarrolló en el trabajo?	**Diferencia con lo planteado en esta propuesta**	**¿De qué manera contribuye a esta propuesta?**
Este es un algoritmo que a simple vista lo hace cuestionar a uno de la razón de su existencia, debido a que se está escribiendo nuevamente una expresión con la misma cantidad de sumandos que tiene la forma polinómica del número, solo que esta vez los factores de los sumandos que multiplican a cada una de las cifras son residuos y no potencias de la base. Esto hace pensar que hacer la suma de esta nueva forma de escribir el número es equivalente a hacer la de la forma polinómica. Al aplicar el teorema, uno se puede dar cuenta de su potencial, ya que los residuos pueden ser cero, eliminando muchos sumandos. Esto hace que el criterio sea más fácil que realizar la suma de cada uno de los productos indicados en la forma polinómica para determinar la divisibilidad del número por otro. Por ejemplo, si se quiere saber una condición necesaria y suficiente de cuando un número escrito en base 10 es divisible por 2. Sea n natural y $n = a_t10^t + a_{t-1}10^{t-1} + \cdots + a_110 + a_0 = \sum_{i=0}^{t} a_i10^i$, calculando los residuos R_i para cada $i = 1, \ldots, t$, teniendo en cuenta que $R_0 = 1$ y que $10R_i = 2(5R_i)$ para cada i entonces $T = a_0$ ya que los demás residuos valen 0. De esta manera se	● Considera los residuos de divisiones sucesivas $bR_{i-1} = px_i + R_i$ para cada $i = 1, \ldots, t$, donde t es el exponente más alto al escribir el número en su forma polinómica. ● Considera todas las cifras del número en el algoritmo.	Este es el más general encontrado en la consulta que se realizó, debido a que se puede considerar cualquier base y cualquier número por el que se desea dividir el número que se escribe en dicha base.

puede concluir que $2\|n$ si y solo si $2\|a_0$.		

Tabla 2: Teorema Criterio General de Divisibilidad Extendido (CGDE)

Teorema criterios de divisibilidad en diferentes bases (CDDB)

1. En cualquier base b un número n es divisible por b si y solo si la cifra de las unidades es cero.
2. En cualquier base b un número n es divisible por $b-1$ si y solo si la suma de sus cifras es múltiplo de $b-1$.
3. En cualquier base b un número n, es divisible por $b+1$ si y solo si la suma entre el número conformado por las cifras de n excepto la de las unidades y el producto resultante de multiplicar esta cifra por b es múltiplo de $b+1$.
4. En cualquier base b un número n, es divisible por $b+1$ si y solo si la diferencia entre el resultado de sumar las cifras de posiciones impares y el resultado de sumar las cifras de posiciones pares de n es múltiplo de $b+1$.

Teorema Criterios de divisibilidad particulares (CDP)

Un número n en base de la forma **(2)** es divisible por **(1)** si y solo si **(3).**

Divisor (1)	**Base (2)**	**Criterio (3)**
2	*2k*	La cifra de las unidades es múltiplo de 2
	2k+1	La suma de las cifras es múltiplo de 2
3	*3k*	La cifra de las unidades es múltiplo de 3
	3k+1	La suma de las cifras es múltiplo de 3
	3k+2	La diferencia entre la suma de las cifras de posición par más los de posición impar es múltiplo de 3.
5	*5k*	La cifra de las unidades es múltiplo de 5
	5k+1	La suma de las cifras es múltiplo de 5

	5k+2	La diferencia entre el número n sin la cifra de las unidades y dos veces esta cifra es múltiplo de 5
	5k+3	La suma entre el número n sin la cifra de las unidades y dos veces esta cifra es múltiplo de 5
	5k+4	La diferencia entre el número sin la cifra de las unidades y esta cifra es múltiplo de 5
7	*7k*	La cifra de las unidades es múltiplo de 7
	7k+1	La suma de las cifras es múltiplo de 7
	7k+2	La diferencia entre el número n sin la cifra de las unidades y tres veces esta cifra es múltiplo de 7
	7k+3	La diferencia entre el número n sin la cifra de las unidades y dos veces esta cifra es múltiplo de 7
	7k+4	La diferencia entre el número n sin la cifra de la unidad y cinco veces esta cifra es múltiplo de 7
	7k+5	La diferencia entre el número n sin la cifra de la unidad y cuatro veces esta cifra es múltiplo de 7
	7k+6	La diferencia entre la suma de las cifras de posición par y la suma de los de posición impar es múltiplo de 7
11	*11k*	La cifra de las unidades es múltiplo de 11
	11k+1	La suma de las cifras es múltiplo de 11
	11k+2	La diferencia entre dos veces el número n sin la cifra de las unidades y esta cifra es múltiplo de 11

	11k+3	La diferencia entre el número n sin la cifra de las unidades y siete veces esta cifra es múltiplo de 11
	11k+4	La suma entre el número n sin la cifra de las unidades y tres veces esta cifra es múltiplo de 11
	11k+5	La diferencia entre el número n sin la cifra de las unidades y dos veces esta cifra es múltiplo de 11
	11k+6	La suma entre el número n sin la cifra de las unidades y dos veces esta cifra es múltiplo de 11
	11k+7	La suma entre el número n sin la cifra de las unidades y once veces esta cifra es múltiplo de 11
	11k+8	La diferencia entre el número n sin la cifra de las unidades y cuatro veces esta cifra es múltiplo de 11
	11k+9	La diferencia entre el número n sin la cifra de las unidades y seis veces esta cifra es múltiplo de 11
	11k+10	La diferencia entre la suma de las cifras de posición par y la suma de las de posición impar es múltiplo de 11

¿Qué se desarrolló en el trabajo?	**Diferencia con lo planteado en esta propuesta**	**¿De qué manera contribuye a esta propuesta?**
En general se puede dividir los resultados de este trabajo de grado en dos situaciones: En la primera se proponen criterios en cualquier base de la	Se consideran diferentes casos para determinar criterios. No hay un algoritmo general que agrupe todos los casos.	● Recoge los criterios de divisibilidad más populares, por ejemplo, el del 2, 3,5, 7 y 11. Y mediante la forma en que se construyen algunos de

forma (b), y el número por el cual se desea dividir debe ser de la forma $b, b-1$ o $b+1$. En la segunda se hace una clasificación de criterios de 2,3,4,5,6,7,8,9,10 y 11, teniendo en cuenta si el número al cual se le desea determinar la divisibilidad es de la forma $ak+i$ donde $a = 2,3 \dots ,11; k \in Z; i = 1,2,3, \dots a$.		estos criterios se consideran más casos.
Estos son una serie de resultados tomados de Osorio, K., & Castañeda, E. (2014) en su tesis titulada *Criterios de divisibilidad en diferentes bases*		

Tabla 3: Teorema criterios de divisibilidad en diferentes bases (CDDB)

2. Marco de referencia

A continuación, se darán a conocer una algunas definiciones y teoremas que se relacionan con la divisibilidad entre números enteros; un ejemplo de estos es el Algoritmo de Euclides y el máximo común divisor de dos números representado como una combinación lineal, que servirán para sustentar la propuesta de este trabajo. A su vez, se recopila una serie de teoremas asociados a criterios de divisibilidad, a diferencia de lo anterior, estos tienen la característica de aplicarse en diferentes bases y ofrecen un método para determinar relaciones y posibles criterios de divisibilidad.

2.1. Componente matemático

En la primera parte se asumen los resultados de la construcción de los naturales por medio de los axiomas de Peano con la operación de la suma y multiplicación. Asimismo, se tienen en cuenta las propiedades de la relación de orden en este conjunto, el buen orden (cualquier subconjunto no vacío de N existe un elemento mínimo) el cual será clave para demostrar el *algoritmo de la división* y que es totalmente ordenado ($a, b \in N, a < b$ si y solo si $b = a + k$ para algún $k \in N$). También es importante tener en cuenta que la relación

igualdad entre los enteros es una relación de equivalencia (es reflexiva, simétrica y transitiva) y esta se tiene en cuenta para las demostraciones correspondientes a los números enteros. De acuerdo con lo anterior, se enfoca el estudio desde los números enteros, inicialmente con la operación suma, multiplicación y dotado de un orden, luego se continúa con los principales resultados de divisibilidad, que permiten sentar una base de los teoremas que se propondrán en este trabajo de grado. Todos los teoremas se construyen a partir del conjunto de los enteros, por eso se considera oportuno realizar un estudio previo de este conjunto numérico.

En la segunda parte, hay cuatro teoremas importantes asociados a determinar criterios de divisibilidad; dos de ellos recopilan los aportes de Osorio y Castañeda (2014), otro es un algoritmo propuesto por Ruíz y Carvajal (2002) y el último es una extensión de un algoritmo planteado en González (2004).

2.1.1. Construcción del conjunto numérico de los enteros

La construcción de los enteros se realizará a partir de los aportes de Rubiano, G., Jiménez, L., & Gordillo, J. (2004), estos autores presentan una definición de los números enteros (Z), así como también de la suma, la multiplicación y la relación de orden en este conjunto y con esto desarrollan algunas propiedades; de esta manera, se proponen las respectivas demostraciones, las cuales son desarrolladas por el autor de este trabajo de la siguiente manera:

Definición 1 (D1): $Z = \{-n | \, n \in N, n \neq 0\} \cup N$

Operación de la adición:

Definición 2 (D2): Se define la adición en Z mediante las siguientes reglas:

2.1 (D2.1) Si $x, y \in N$ la suma $x + y$ es la misma que se maneja en N.

2.2 (D2.2) Para todo $x \in Z$ se define $x + 0 = 0 + x = x$

2.3 (D2.3) Si m y n son números naturales diferentes de cero y $m = n + k$ para algún $k \in N$, se define:

a) $m + (-n) = (-n) + m = k$

b) $(-m) + n = n + (-m) = \{-k\ si\ k \neq 0\ \ 0\ \ si\ k = 0\}$

c) $(-m) + (-n) = -(m + n)$

Usualmente se escribe $m - n$ en vez de $m + (-n)$.

Esta operación tiene las siguientes propiedades:

Teorema 1 (T1). ***Propiedad Asociativa de la suma*****:** Si $x, y, z \in Z$ entonces

$(x + y) + z = x + (y + z)$

Demostración Si se considera $x, y, z \in N$ la propiedad se cumple debido a que la asociatividad de la suma en N se toma como válida.

Para el caso en que $x, y, z \in Z - N$ se tiene que $x = -r, y = -t$ y $z = -u$ con $r, t, u \in N$ por **D1**. Entonces

$$x + (y + z) = -r + [(-t) + (-u)]$$

Por **D2.3c** se tiene que,

$$= -r - (t + u) = -r + [-(t + u)]$$

Nuevamente por **D2.3c**

$$= -[r + (t + u)]$$

Por propiedad asociativa de la suma en N,

$$= -[(r + t) + u]$$

Aplicando **D2.3c** iteradamente queda que

$$= (-r - t) - u$$

Y sustituyendo x, y y z en la última expresión se concluye que

$$= (x + y) + z$$

Es decir

$$x + (y + z) = (x + y) + z$$

Ahora, se considera el caso en el que $x \in Z - N$ y $y, z \in N$. Por **D1** $x = -r$, con $r \in N$. Entonces

$$x + (y + z) = -r + (y + z) = k_1$$

por **D2.3**, $-r + y = k_2$ que es lo mismo a tener que $y = r + k_2$ y $y + z = r + k_1$. Al sustituir y en esta última igualdad queda que

$$(r + k_2) + z = r + k_1$$

Por las propiedades asociativa y cancelativa en N

$$k_2 + z = k_1$$

Sustituyendo k_2,

$$(-r + y) + z = k_1$$

Sustituyendo x se tiene que

$$(x + y) + z = k_1 = x + (y + z)$$

Por un razonamiento análogo se concluye que para los casos $y \in Z - N$ y $x, z \in N$ y $z \in Z - N$ y $x, y \in N$ también se cumple la propiedad.

Teniendo en cuenta ahora que $x, y \in Z - N$ y $z \in N$, por **D1**, $x = -r$ y $y = -t$ para $r, t \in N$. Luego

$$(x + y) + z = k_1 = (-r - t) + z$$

Por **D2.3c**

$$= -(r + t) + z$$

Por **D2.3**

$$z = (r + t) + k_1$$

También $z = t + k_2$ por la misma definición y este a su vez se puede escribir como $k_2 = z - t$. Igualando las dos últimas igualdades se tiene que

$$t + k_2 = (r + t) + k_1$$

Por propiedad conmutativa, asociativa y cancelativa en N

$k_2 = r + k_1$, que por **D2. 3a** queda como $k_2 - r = -r + k_2 = k_1$. Sustituyendo k_2 en esta última igualdad,

$$-r + (-t + z) = k_1$$

Sustituyendo x y y,

$$x + (y + z) = k_1 = (x + y) + z$$

Para los casos en los que $x, z \in Z - N$ y $y \in N$ y $y, z \in Z - N$ y $x \in N$ las demostraciones son similares a la anterior.

Teorema 2 (T2). ***Propiedad conmutativa de la suma*****:** Si $x, y \in Z$ entonces $x + y = y + x$

Demostración. Se puede omitir el caso en que $x, y \in N$ debido a que ya se asume la conmutatividad de la suma en los números naturales.

Se considera entonces el caso en que $x \in N$ y $y \in Z - N$. Luego $y = -t$ con $t \in N - \{0\}$. Sin pérdida de generalidad se puede tomar $x > t$. Esto significa que $x = t + k_1$ para algún $k_1 \in N$ por el orden total en N. Luego al sustituir el valor de y en $x + y$ se tiene que

$$x + y = x + (-t)$$

Por **D2. 3a,**

$$= -t + x$$

Sustituyendo nuevamente el valor de y,

$$= y + x$$

Por lo tanto $x + y = y + x$.

Para el caso en que $x = t$ se tiene que $0 + x = t$ por **D2.2.** Luego

$$x + y = x + (-t)$$

Por **D2.3b**

$$= -t + x$$

Sustituyendo el valor de y

$$= y + x$$

Si $x < t$ se llega a que $t = x + k_2$ para algún $k_2 \in N$ por el orden total en N, haciendo u proceso análogo a lo anterior se escribe,

$$x + y = x + (-t)$$

De D2.3b se obtiene que

$$= (-t) + x$$

Que al sustituir nuevamente el valor de y

$$= y + x$$

Si $y \in N$ y $x \in Z - N$ la demostración es similar a lo anterior.

Queda por probar la conmutatividad cuando $x, y \in Z - N$. Luego $x = -r, y = -t$ con $r, t \in N - \{0\}$. Sustituyendo los valores de x y y en $x + y$ se tiene que

$$x + y = -r - t$$

Por **D2.3c** se llega a

$$= -(r + t)$$

y por propiedad conmutativa de la suma en los números naturales.

$$= -(t + r)$$

aplicando nuevamente **D2.3c**

$$= -t - r$$

Sustituyendo nuevamente los valores de x y y queda

$$= y + x$$

por transitividad de la igualdad se concluye que $x + y = y + x$.

Teorema 3 (T3): Para todo $x \in Z$, existe $y \in Z$ tal que $x + y = 0$

Demostración. Se considera $x \in N$. Por propiedad del elemento neutro en la suma en los números naturales se tiene que $x = x + 0 = 0 + x$. Si $x = 0$ se cumple que $0 + 0 = 0$, luego $y = 0$. Si $x \neq 0$, por **D2.3b** se llega a que $x - x = 0$.

Queda entonces que $y = -x$.

Para el caso en que $x \in Z - N$ se tiene que $x = -r$ para algún $r \in N - \{0\}$ nuevamente por la propiedad del elemento neutro de la suma en N, se tiene que $r =$

$r + 0$ y por **D2.3b,** $-r + r = 0$. Sustituyendo el valor de x en esta última igualdad, queda que

$x - x = 0$.

El número $y = -x$ es el opuesto de x.

Operación multiplicación

Definición 3 (D3): Se define la multiplicación en Z mediante las siguientes reglas:

3.1 (D3.1) Si $x, y \in N$ se usa la multiplicación definida en N

3.2 (D3.2) Para todo $x \in Z$, se define $x(0) = (0)x = 0$

3.3 (D3.3) Si m, n son naturales diferentes de cero, se define:

a) $(-m)n = n(-m) = -(mn)$

b) $(-m)(-n) = mn$

Esta operación tiene las siguientes propiedades:

Teorema 4 (T4).*Propiedad Asociativa de la multiplicación*: Si $x, y, z \in Z$ entonces $(xy)z = x(yz)$.

Demostración. Se consideran los siguientes casos con su correspondiente demostración:

Caso 1: $x, y, z \in N$.

Esta propiedad se cumple, debido a que se asume así para este conjunto numérico.

Caso 2: $x, y \in N$ y $z \in Z - N$.

Se tiene que $z = -u$ con $u \in N$. Por lo tanto $(xy)z = (xy)(-u)$ que por **D3. 3a** obtiene $(xy)(-u) = -[(xy)u]$. Por asociatividad de la suma en los números naturales el segundo miembro de la última igualdad se convierte en $-[(xy)u] = -[x(yu)]$ y al aplicar la **D3. 3a** *iteradamente* se llega a lo siguiente

$$-[x(yu)] = x[-(yu)] = x[y(-u)]$$

Que al sustituir z en la última expresión,

$$x[y(-u)] = x(yz)$$

Finalmente, se obtiene que $(xy)z = x(yz)$ para este caso. Se van a tener otros dos casos análogos a este, los cuales son: caso 3: $x, z \in N$ y $y \in Z - N$ y caso 4: $y, z \in N$ y $x \in Z - N$ las demostraciones son similares a la del caso 2.

Caso 5: $x \in N$ y $y, z \in Z - N$.

Sea $y = -t$ y $z = -u$ con $t, u \in N$, por definición de número entero. Luego $x(yz) = x[(-t)(-u)] = x(tu)$, esta segunda igualdad se da por **D3.3b**. El último miembro de la igualdad se puede reescribir como $x(tu) = (xt)u$ por asociatividad de la multiplicación en los números naturales, que a su vez es igual a tener

$$(xt)u = [-(xt)](-u) = [x(-t)](-u) = (xy)z$$

por las **D3.3b** y **D3. 3a** respectivamente y sustituyendo nuevamente y y z. De esta cadena de igualdades se concluye que $(xy)z = x(yz)$.

Nuevamente se tienen otros dos casos análogos y sus demostraciones son similares al caso 5. Estos casos son: caso 6: $y \in N$ y $x, z \in Z - N$ y caso 7: $z \in N$ y $x, y \in Z - N$.

Caso 8: $x, y, z \in Z - N$.

Por definición de número entero se tiene que $x = -r, y = -t$ y $z = -u$ con $r, t, u \in N$. Luego $(xy)z = [(-r)(-t)](-u)$. Por **D3.3b** y **D3. 3a** se tiene que $[(-r)(-t)](-u) = [rt](-u) = -[(rt)u]$. Por asociatividad de la multiplicación en N se llega a que $-[(rt)u] = -[r(tu)]$. Por **D3. 3a** y **D3.3b** $-[r(tu)] = (-r)[(tu)] = (-r)[(-t)(-u)]$. Sustituyendo x, y y z en esta última expresión queda que $(-r)[(-t)(-u)] = x(yz)$. De aquí que $(xy)z = x(yz)$.

Teorema 5 (T5). ***Propiedad Conmutativa de la multiplicación*****:** Si $x, y \in Z$ entonces $xy = yx$.

Demostración. Para el caso en que $x, y \in N$ se cumple la propiedad debido a que se asume esta propiedad para los números naturales.

Sin pérdida de generalidad se escoge $x \in N$ y $y \in Z - N$, se tiene que $y = -t$ con $t \in N - \{0\}$.

Luego $xy = x(-t) = -(xt)$ por **D3. 3a** . Por propiedad conmutativa de la multiplicación en los naturales se cumple que $-(xt) = -(tx)$, usando nuevamente de **D3. 3a** se llega a que $-(tx) = (-t)x = yx$, y por propiedad transitiva de la igualdad se concluye que $xy = yx$.

Para el caso en que $x, y \in Z - N$, se hace $x = -r, y = -t$ con $r, t \in N - \{0\}$. Luego $xy = (-r)(-t) = rt$ por **D3.3b**. Por propiedad conmutativa en N, el último miembro de la igualdad queda cómo $rt = tr$ y usando nuevamente **D3.3b** se tiene que $tr = (-t)(-r) = yx$. Luego $xy = yx$.

Teorema 6 (T6). ***Elemento neutro*****:** Para todo $x \in Z$, $x(1) = x$.

Demostración. Si $x \in N$ se cumple, por propiedad del elemento neutro o módulo de la multiplicación en los números naturales.

Se considera entonces $x \in Z - N$. Luego $x = -r$ con $r \in N - \{0\}$. Luego, $x(1) = (-r)(1) = -(r1)$ por **D3. 3a.** Así, esta última expresión se puede reescribir como $-(r1) = -r = x$ y sustituyendo por propiedad del módulo de la multiplicación en los números naturales. De aquí que $x(1) = x$.

Teorema 7 (T7). ***propiedad distributiva de la multiplicación respecto a la suma*****:** Para todo $x, y, z \in Z$, $x(y + z) = xy + xz$.

Demostración Se consideran varios casos para esta prueba.

Caso 1: $x, y, z \in N$.

En este caso se cumple que $x(y + z) = xy + xz$, debido a que se asume válida esta propiedade en N.

Caso 2: $x, y, z \in Z - N$.

Por **D1,** $x = -r, y = -t$ y $z = -u$, con $r, t, u \in N$. Luego

$$x(y + z) = -r[(-t) + (-u)]$$

Por **D2.3c,**

$$= -r[-(t + u)]$$

De **D3.3b,**

$$= r(t + u)$$

por la propiedad distributiva de la multiplicación respecto a la suma en N

$$= rt + ru$$

De **D3.3b**

$$= -r(-t) + (-r)(-u)$$

Sustituyendo los valores correspondientes a x, y y z en esta última expresión,

$$= xy + xz$$

es decir, $x(y + z) = xy + xz$.

Caso 3: $x \in N$ y $y, z \in Z - N$.

Por **D1,** $y = -t$ y $z = -u$ con $t, u \in N$. Luego

$$x(y + z) = x[-(t + u)]$$

de **D2.3c,**

$$= x[-(t + u)]$$

De **D3. 3a,**

$$= -[x(t + u)]$$

por la propiedad distributiva de la multiplicación respecto a la suma en N

$$= -[xt + xu]$$

nuevamente usando **D2.3c,**

$$= -(xt) + [-(xu)]$$

de **D3. 3a,**

$$= x(-t) + x(-u)$$

Finalmente, sustituyendo los valores correspondientes a y y z, y por propiedad transitiva de la igualdad se concluye que $x(y + z) = xy + xz$.

Caso 4: $x \in Z - N$ y $y, z \in N$.

Por **D1** $x = -r$ con $r \in N$. Luego

$$x(y + z) = -r(y + z)$$

Por **D3. 3a**,

$$= -[r(y + z)]$$

que usando la propiedad distributiva de la multiplicación respecto a la suma en N

$$= -[ry + rz]$$

De **D2.3c**,

$$= -(ry) + (-rz)$$

Que usando **D3. 3a**

$$= (-r)y + (-r)z$$

Sustituyendo el valor de x se concluye que $x(y + z) = xy + xz$.

Caso 5: $x, y \in N$ y $z \in Z - N$.

Por **D1**, $z = -u$ con $u \in N$. Suponer que $y > u$ con el orden de N. Luego por orden total en N se llega a $y = u + k$ para algún $k \in N$.

De **D2.3** se tiene que $y - u = k$ entonces

$$x(y + z) = x(y - u) = xk$$

Y $xk = xk + 0$ ya que $xk, xu \in N$ (la multiplicación es cerrada en N) y por propiedad de elemento neutro de la suma en N. Esta última expresión se puede reescribir como

$xk + 0 = xk + (xu - xu)$, por **T3**

Por T1,

$$= (xk + xu) - xu$$

Por propiedad distributiva de la multiplicación respecto a la suma y por propiedad conmutativa en N,

$$= x(u + k) - xu \qquad (1)$$

Debido a que $y - u = k$ por **D2.3** se tiene que $y = u + k$, sustituyendo y en (1),

$$= xy - xu$$

Por **D3. 3a**

$$= xy + x(-u)$$

Sustituyendo el valor de z en esta última expresión,

$$= xy + xz$$

De aquí que $x(y+z) = xy + xz$.

Ahora se considera $y < u$, nuevamente por orden total en N se tiene que $u = y + k$. Por lo tanto,

$$x(y+z) = x(y-u) = x(-k) = -(xk)$$

La primera igualdad se obtiene de sustituir el valor de $z = -u$ en la primera expresión. La segunda se da por la sustitución de $-k$ en la segunda expresión, y la tercera se tiene por **D3. 3a.**

Por **D2.2**,

$$-(xk) = -(xk) + [xy - (xy)]$$

Por T2 y luego T1 se tiene que

$$= xy + [-(xk) - (xy)]$$

Por **D2.3c**

$$= xy - [xk + xy]$$

De la propiedad distributiva de la multiplicación respecto a la suma en N,

$$= xy - [x(k+y)]$$

Sustituyendo $u = y + k$ en esta última expresión,

$$= xy - (xu)$$

Por **D3. 3a**

$$= xy + x(-u)$$

Y sustituyendo en esta el valor de z,

$$= xy + xz$$

Por propiedad transitiva de la igualdad se concluye que $x(y+z) = xy + xz$.

Considerando ahora que $y = u$. Por **D2.3** $y = u + 0$ y por **D2.3b** se tiene que

$y - u = 0$. Luego

$$x(y-u)=x(0)$$

Esta última expresión se puede escribir como $x(0)=0$ que al tener que $xy \in N$ (la multiplicación es cerrada en N) se tiene que $0=xy-xy$ por **T3.**

Como $y=u$ entonces al sustituir en la última expresión,

$$xy-xy \ = xy-xu$$

Usando **D3. 3a**

$$= xy+x(-u)$$

Y sustituyendo el valor de z en este último sumando se tiene que

$$= xy+xz$$

Concluyendo que $x(y+z)=xy+x$.

Para el caso en que $x,z \in N$ y $y \in Z-N$ la demostración es análoga a la del caso anterior (caso 5).

Teorema 8 (T8): Si $x,y \in Z$ con $x \neq 0, y \neq 0$ entonces $xy \neq 0$.

Demostración. Si $x,y \in N$ se cumple la propiedad debido a que se asume dicha proposición para N.

Ahora se considera $x \in N-\{0\}$ y $y \in Z-N$. Por **D1** $y=-t$ y para algún

$t \in N-\{0\}$, es decir $x>0$ y $t>0$. Además $xy=x(-t)=-(xt)$ por **D3. 3a.** Por propiedad del orden de los números naturales $xt>0$, y esto implica que $xt \neq 0$ por tricotomía en N. Luego por definición de número entero

$-(xt) \in Z-N$, de aquí que $-(xt) \neq 0$. Y como

$-(xt)=x(-t)=xy$ debido a **D3. 3a** y de sustituir y en $x(-t)$, entonces $xy \neq 0$.

Si se tiene en cuenta que $x \in N-\{0\}$ y $y \in Z-N$, la demostración es similar al caso anterior.

Suponer que $x, y \in Z - N$. Por **D1**, $x = -r$ y $y = -t$ para $r, t \in N - \{0\}$. De aquí que $r > 0$ y $t > 0$. Y por la propiedad del orden de los números naturales $rt > 0$, por lo tanto $rt \neq 0$ por tricotomía en N. Cómo $rt = (-r)(-t)$ por **D3.3b** y este último miembro queda como $(-r)(-t) = xy$ al realizar la sustitución de x y y; se concluye que $xy \neq 0$.

Teorema 9 (T9): Si $x, y, z \in Z$, $z \neq 0$ tales que $xz = yz$ entonces $x = y$.

Demostración. Dados $x, y, z \in Z$, $z \neq 0$, se parte de considerar el caso en el que $x, y, z \in N$. Esto se cumple en este conjunto debido a que se asumen las propiedades de la multiplicación en N.

Sean entonces $x, y \in N$ y $z \in Z - N$. Por **D1** $z = -u$, con $u \in N - \{0\}$.

Como,

$$xz = yz,$$

Sustituyendo el valor de z queda que

$$x(-u) = y(-u),$$

Por **D3. 3a**

$$-(xu) = -(yu) \quad (2)$$

Como el producto $xu, yu \in N$ debido a que la multiplicación es cerrada en N. Entonces por **D1,** $-(xu), -(yu) \in Z$.

por **T3**,

$$yu - (yu) = 0,$$

De **T5**,

$$uy - (ux) = 0,$$

luego por **T7,**

$$u(y - x) = 0.$$

Usando el contrarrecíproco de **T8** se tiene que,

$u = 0$ o $y - x = 0$,

pero como $u \neq 0$ por **D1,** por lo tanto, se debe tener que $y - x = 0$.

Si y o x son nulos, pero no ambos, por **D2.2** no se puede dar la anterior igualdad.

De aquí que o $x, y \in \{0\}$ o $x, y \in N - \{0\}$.

Si ambos son nulos se cumple $x = y$. Ahora si ambos son naturales positivos, por **D2.3** la expresión $y - x = 0$ se puede escribir como $x = y + 0$ y por **D2.2** se tiene que $x = y$.

Para los casos en los que $x, y, z \in Z - N$, $x, y \in Z - N$ y $z \in N$, las demostraciones son similares a la anterior.

Si $x, z \in N$ y $y \in Z - N$ con $z \neq 0$, se tiene que $y = -t$ para $t \in N$ y $t \neq 0$.

Luego sustituyendo y en la expresión $xz = yz$ queda que $xz = (-t)z$, que por **D3. 3a** se puede escribir como

$xz = -(tz)$ (3)

Además, como la multiplicación en N es cerrada, entonces $xz \in N$ y por (3) se deduce que $-(tz) \in N$. Y por **D1,** $tz \in N$.

De la suma $tz - (tz) = 0$, y por propiedad de la suma de los números naturales ($m, n \in N$, si $m + n = 0$ entonces $m = 0$ y $n = 0$) se tiene que $tz = 0$. Luego por (3), $xz = 0$ y de aquí que $t = 0$ o $z = 0$ y $x = 0$ o $z = 0$ por propiedad de la multiplicación en N ($m, n \in N$ si $mn = 0$ entonces $m = 0$ o $n = 0$). Pero como $z \neq 0$, se debe tener entonces que $t = 0$ y $x = 0$. Y como se había dicho inicialmente que $t \neq 0$, esto lleva a una contradicción por tricotomía en N.

Con esto se concluye que el caso $x, z \in N$ y $y \in Z - N$ con $z \neq 0$ no se puede dar. Con este mismo argumento se descartan también los casos $y, z \in N$ y $x \in Z - N$, $x \in N$ y $y, z \in Z - N$ y $y \in N$ y $x, z \in Z - N$.

Orden en los números enteros

Definición 4 (D4): Sean $x, y \in Z$ se define $x \leq y$ si y solo si $y - x \in N$,

$x \leq y$ también se puede representar como $y \geq x$. Esta relación tiene las siguientes reglas:

4.1 (D4.1) Si $x \leq y$ y $x \neq y$ se escribe $x < y$.

4.2 (D4.2) Si $0 < x$ se dice que x es un *entero positivo*. El conjunto de los enteros positivos se denota como Z^+. También se puede usar $x > 0$.

4.3 (D4.3) Los enteros x que satisfacen $-x > 0$ se denominan *negativos*, que también se puede escribir como $x < 0$.

Teorema 10 (T10): Dados $x, y \in Z, x \leq y$ si y solo si existe $s \in N$ tal que $x + s = y$. (orden total)

Demostración. →) Sea $x, y \in Z$ con $x \leq y$. Por **D4** $y - x \in N$, es decir $y - x = s$, con $s \in N$ y por **D2.3** se tiene que $y = x + s$.

←) Ahora se considera $x + s = y$. Por **D2.3** se tiene que $y - x = s$, $y - x = 0$, o $y - x = -s$.

Para los dos primeros casos como $0, s \in N$ entonces $y - x \in N$ por lo tanto $x \leq y$ por **D4.**

Para el tercer caso ($y - x = -s$) por D2.3 se tiene que $x = y + s$ luego por **D2.3b** se concluye que $y \leq x$.

Teorema 11 (T11): La relación $x \leq y$ con $x, y \in Z$ es una relación de orden (reflexiva, antisimétrica y transitiva)

Demostración. Sea $x \in Z$, por **T3** existe $-x \in Z$ tal que $x - x = 0$, como $0 \in N$ se tiene que $x - x \in N$ y por **D4** se cumple que $x \leq x$. Esto quiere decir que la relación es reflexiva.

Sean $x \leq y$ y $y \leq x$. Por **D4** $y - x \in N$ y $x - y \in N$ al sumar

$$(y - x) + (x - y) = (y - x) + (-y + x) = y + (-x - y) + x = y + (-y - x) + x$$
$$= (y - y) + (x - x) = 0 + 0 = 0$$

La primera igualdad se da por **T2**, la segunda por **T1**, la tercera y cuarta nuevamente por **T2** y **T1** respectivamente, la quinta igualdad se da por **T3** y la sexta es una propiedad del elemento cero que se asume demostrada ya que esta se hace en el estudio de los números naturales.

Por la propiedad transitiva de la igualdad $(y - x) + (x - y) = 0$, y considerando la proposición *"si la suma de dos números naturales es cero entonces cada uno de sus sumandos es cero*" se deduce que $y - x = 0$ y $x - y = 0$. De esta última igualdad se suma y a ambos miembros de la igualdad, es decir,

$$(x - y) + y = 0 + y$$

Por **T1** se llega a

$$x + (-y + y) = 0 + y$$

de **T3** se tiene,

$$x + 0 = 0 + y$$

Y por **D2.2**

$$x = y$$

Por lo tanto, la relación es antisimétrica.

Se supone ahora que $x \leq y$ y $y \leq z$ con $x, y, z \in Z$. Por **D4** $(y - x), (z - y) \in N$, como la suma es cerrada en los naturales entonces $(y - x) + (z - y) \in N$, y esta suma es igual a tener,

$$(y - x) + (z - y) = (z - y) + (y - x) = \big(z + (-y + y)\big) - x = (z + 0) - x = z - x$$

La primera igualdad se obtiene por **T2**, la segunda por **T1**, la tercera por **T3** y la cuarta por **D2.2.** Con esto se asegura que $z - x \in N$ y por **D4**, $x \leq z$. Esto prueba que la relación es transitiva.

Como la relación es reflexiva, antisimétrica y transitiva entonces es de orden.

Teorema 12 (12): $Z^+ = N - \{0\}$.

Demostración. Sea $x \in Z^+$ por **D4.2** se tiene que $0 < x$, luego $x - 0 \in N$ por **D4,** y como $x + 0 = x$ por **D2.2**, entonces $x \in N$. Cómo $0 < x$ entonces por propiedad de la tricotomía de los números naturales $x \neq 0$, de aquí que $x \in N - \{0\}$, por lo tanto

$Z^+ \subseteq N - \{0\}$.

Sea $x \in N - \{0\}$ entonces $x \neq 0$ y x no puede ser menor que 0 debido a que en los axiomas de Peano el cero es el primer elemento. Por lo tanto $0 < x$ y por **D4.2** se concluye que $x \in Z^+$, entonces $N - \{0\} \subseteq Z^+$. Esto permite concluir que $Z^+ = N - \{0\}$.

Ahora bien, el orden definido sobre Z tiene las siguientes propiedades:

Teorema 13 (T13): Si $x, y \in Z^+$ entonces $x + y \in Z^+$ y $xy \in Z^+$.

Demostración. Dado que $x, y \in Z^+$ entonces $x, y \in N - \{0\}$ por **T12.** Como x y y son números naturales entonces $(x + y)$ y $xy \in N$. Además, por **D4.2** $0 < x$ y $0 < y$. Por **D4,** $x + 0 \in N$ y por **T3** se tiene que $x + 0 = x + (y - y)$, que por T1 este último miembro de la igualdad queda

$$x + (y - y) = (x + y) - y$$

Por transitividad de la igualdad, $x + 0 = (x + y) - y$ por lo tanto $(x + y) - y \in N$ y con esto se cumple que $0 < y \leq x + y$. Por propiedad de la transitiva de la relación de orden **T11** se concluye que $0 < x + y$, y por **D4.2** $x + y \in Z^+$.

La propiedad de la tricotomía en los números naturales permite inferir que $x \neq 0$ y $y \neq 0$, luego por **T8,** $xy \neq 0$. Como no se puede tener que $xy < 0$ debido a que $xy \in N$ y 0 es el primer elemento de N entonces, de nuevo por la propiedad de la tricotomía $0 < xy$. Por lo tanto, se llega a que $xy \in Z^+$ por **D4.2.**

Teorema 14 (T14): Si $x, y \in Z$ entonces una y solo una de las siguientes afirmaciones es verdadera

$$x < y, x = y, y < x.$$

Demostración. Se da por hecho que $x < y$. Por **D4.1** se tiene que $x \neq y$.
Ahora, si se considera que también se da que $y < x$, por **T11 (**propiedad transitiva del orden**)** queda que $x < x$. En este punto se pueden dar dos casos. El primero es que $x \in N$, pero por la propiedad de la tricotomía en N esto no puede pasar ya que $x = x$. El segundo es cuando $x \in Z - N$. Por **D1** se tiene que $x = -r$ para $r \in N$, entonces tener $x < x$ es lo mismo que $-r < -r$, y por **T10** se tiene que
$-r = -r + k$ con $k \in N$.
Como $k > 0$ (ya que si fuera llevaría a que $-r = -r$ lo cual no puede darse), al sumar r en ambos miembros de la igualdad queda que

$$r - r = r + (-r + k)$$

Por T1 y T3 se deduce que

$$0 = k$$

Esto es una contradicción por propiedad de la tricotomía en N debido a que ya se tenía que $k > 0$. Por lo tanto, solo se puede dar que $x < y$.

Mediante un razonamiento análogo se demuestra que si se da que $y < x$ entonces $y \neq x$ y que no se puede dar que $x < y$.

Si se toma como verdadero que $x = y$ queda claro que no se puede dar $x < y$ o $y < x$ ya que esto es lo mismo a tener que $x < x$. Pero esto no se puede dar, debido al argumento descrito en el primer párrafo de la demostración.

Teorema 15 (T15): Si $x, y \in Z$ son tales que $x \leq y$ entonces para todo z, $x + z \leq y + z$.

Demostración. Dados $x, y \in Z$ tales que $x \leq y$. Por **D4** $y - x \in N$. Por propiedad del modula de la suma en N se tiene que

$$y - x = y - x + 0$$

Por **T3,**

$y - x + 0 = (y - x) + (z - z)$, para $z \in Z$

Por **T1,**

$$= y + (-x + z) - z$$

De **T2** se tiene,

$$= y + (z - x) - z$$

Nuevamente por **T1**,

$$= (y + z) + (-x - z)$$

Por **D2.3c**

$$= (y + z) - (x + z)$$

Cómo $y - x \in N$ y por la propiedad transitiva de la igualdad $y - x = (y + z) - (x + z)$, entonces $(y + z) - (x + z) \in N$. Y por **D4** se concluye que $x + z \leq y + z$.

Teorema 16 (T16): Si $x, y, z, w \in Z$ son tales que $x \leq y$ y $z \leq w$ entonces $x + z \leq y + w$.

Demostración. Dado que se tiene $x, y, z, w \in Z$ y $x \leq y$ y $z \leq w$. Por el teorema anterior (**T15**) se cumple que $x + z \leq y + z$ y que $y + z \leq y + w$. Por la propiedad transitiva del orden en Z (**T11)** se concluye que $x + z \leq y + w$.

Teorema 17 (T17): Si $x, y \in Z$ son tales que $x \leq y$ y $z > 0$ entonces $xz \leq yz$.

Demostración. Si $x, y \in Z$ con $x \leq y$ y $z > 0$. Por **D4** $y - x \in N$. Además, $z \in Z^+$ por **D4.2;** y por T10, $z \in N - \{0\}$.

Cómo la multiplicación es cerrada en los números naturales se cumple que $z(y - x) \in N$. Por **T7** se tiene que

$$z(y - x) = zy + z(-x)$$

Por propiedad conmutativa en Z

$$= yz + (-x)z$$

Por D3. 3a,

$$= yz - (xz)$$

Por transitividad de la igualdad $z(y - x) = yz - (xz)$, luego $yz - (xz) \in N$ y por **D4** $xz \leq yz$.

Teorema 18 (T18): Si $x, y \in Z$ son tales que $x \leq y$ y $z < 0$ entonces $yz \leq xz$.

Demostración. Dado $x, y \in Z$ con $x \leq y$ y $z < 0$. Por **D4.3** $-z > 0$ y por **D4**, $y - x \in N$. Luego $-z \in Z^+$ por **D4.2.**

Se consideran dos casos. Cuando $y - x = 0$ o cuando $y - x > 0$.

Si $y - x = 0$, al multiplicar por $-z$ esta última igualdad, se tiene que

$$-z(y - x) = -z(0)$$

Por **T7**,

$$-zy - z(-x) = -z(0)$$

Por **D3.3b**,

$$-zy + zx = -z(0)$$

de **T2** y

$$zx - zy = -z(0)$$

y por **D3.2** se llega a

$$zx - zy = 0$$

Como $0 \in N$, entonces $zx - zy \in N$, y por **D4** $yz \leq xz$.

Para el segundo caso $y - x > 0$; por **D4.2** se tiene que $y - x \in Z^+$ y como $-z \in Z^+$ por **T13** se llega a que $-z(y - x) \in Z^+$ que es equivalente a decir que $-z(y - x) > 0$, por lo tanto $-z(y - x) \in N$, y como ya se sabe que $-z(y - x) = zx - zy$ (por el argumento anterior) por lo tanto $zx - zy \in N$, luego se concluye que $yz \leq xz$ por **D4**.

2.1.2. La divisibilidad entre los números enteros

A partir de aquí, las definiciones y teoremas estarán enfocados al concepto de divisibilidad, ya que en algunas ocasiones se usan de manera errada sin notar la diferencia. Por eso se hará precisión de estos para evitar ambigüedades. De acuerdo lo anterior, La siguiente definición recoge los conceptos asociados a divisibilidad que fueron trabajados por González (2004):

Definición 5 (D5): Sean $a,b \in Z$ tales que $a \neq 0$. Se dice que *a divide* a b si existe un número $q \in Z$ tal que $b = aq$. Esto se denota como $a|b$.

Expresiones equivalentes a "a *divide* a b" son "a es un divisor de b" o "b es múltiplo de a" o "b es divisible por a ".

Ahora bien, para el desarrollo de algunas propiedades que se establecen en la relación "ser múltiplo de…" mencionada anteriormente, se tiene en cuenta el trabajo hecho por Rubiano et al. (2004):

Teorema 19 (T19): Supongamos que $a, b, c \in Z$. Entonces:

19.1. Si $a \neq 0$ entonces $a|0$, $a|a, a|(-a)$.

19.2. $1|a, (-1)|a$.

19.3. Si $a|b$ entonces $a|bc$.

19.4. Si $a|b$ y $b|c$ entonces $a|c$.

19.5. Si $a|b\ y\ a|c$ entonces para todo $x, y \in Z$, $a|(bx + cy)$.

19.6 Si $a|(b + c)$ y $a|b$ entonces $a|c$.

Demostración.

Prueba de 19.1: Por **D3.2** se tiene que $a(0) = 0$, y dado que $a \neq 0$ por **D5** se cumple que $a|0$. Por **D3.2** se tiene que $a(1) = a$ y por **D5**, $a|a$.

Ahora, como $-a = -a(1) = a(-1)$, la primera igualdad se da por **D3.2** y la segunda por **D3. 3a;** y de **D5** se concluye que $a|(-a)$.

Prueba de 19.2: Dado que por **D3.2** para cualquier $a \in Z$ se tiene que $a(1) = a$, y por **T2** $1(a) = a$ y usando **D5** se concluye que $1|a$.

Prueba de 19.3: Por hipótesis $a|b$ esto quiere decir por **D5** que $ak = b$, con $a \neq 0$ si se multiplica por c en ambos miembros de la igualdad y aplicar **T1**, se tiene que $a(kc) = bc$ luego por **D5** $a|bc$, lo cual prueba a T19.3.

Prueba de 19.4: De **D5** se tiene que $ak = b$ y $bt = c$ para k y t enteros. Si se toma la primera igualdad y la multiplicamos por t se llega a que $akt = bt = c$ de aquí que $a|c$. Esto demuestra 1.4.

Prueba de 19.5: Por hipótesis y **D5**, existen $r, s \in Z$ tal que $b = ar$ y $c = as$.

Sean $x, y \in Z$ entonces

$$bx + cy = (ar)x + (as)y = a(rx + sy) \qquad (4)$$

La primera igualdad se da por la sustitución de b y c en la primera expresión y la segunda se tiene por **T1** y **T7.**

De (4) se concluye que $a|(bx + cy)$ por **D5.**

Prueba de 19.6: Como $a|(b+c)$ y $a|b$, por **T19.5,** $a|[(b+c)-b]$.

Por **T1** y **T2** se tiene que

$$a|[b+(-b+c)]$$

Nuevamente por **T1**,

$$a|[(b-b)+c)]$$

por **T3,**

$$a|(0+c)$$

Y por **D2.2**

$$a|c$$

Ahora bien, un uso que se le da al principio del buen orden es el algoritmo de la división, siendo este último de mayor importancia, ya que dota sentido al algoritmo de Euclides; en este caso, los avances de Rubiano, G., Jiménez, L., & Gordillo, J. (2004), permiten que se demuestre de la siguiente manera:

Teorema 20 (T20). ***Algoritmo de la división:*** Sean $a, b \in Z$ con $b > 0$. Entonces existen enteros únicos q, r tales que

$$a = bq + r \text{ con } 0 \leq r < b.$$

Demostración: Sea el conjunto $S = \{a - bx : x \in Z \; y \; a - bx \geq 0\}$, se debe comprobar que $S \neq \emptyset$.

Como a no tiene alguna condición salvo ser entero, entonces se considera los casos en que $a \geq 0$ y $a < 0$. Para el primer caso ($a \geq 0$) se tiene que $a = a + 0 = a + (0)b$ por **D2.2** y **D3.2** por lo tanto a se puede escribir de la forma $a - xb$ con $x = 0$, esto quiere decir que $a \in S$. En el segundo caso ($a < 0$) y dado que $b > 0$ por lo tanto $b \geq 1$, de aquí que $1 - b \leq 0$, luego $a(1-b) = a - ab \geq 0$, con esto se prueba que $a - ab \in S$ al hacer

$x = a$. Esto demuestra que $S \neq \emptyset$.

Por el principio de buen orden se llega a que S posee un mínimo $r = a - qb$. Ahora se debe probar si $r < b$. Si se supone que no, es decir se debe considerar que $r \geq b$ que es lo mismo a tener que $r - b \geq 0$ (2) y que al hacer la sustitución de r en (2) se convierte en

$(a - qb) - b \geq 0$. Esto se puede reescribir como $a - (q + 1)b \geq 0$ por **T1** y **D2.3c.** Luego se tiene que $r - b \in S$ lo cual lleva a una contradicción con el hecho de que r es el mínimo. Por lo tanto, se debe tener que $r < b$.

Ahora se procede a demostrar la unicidad. Se toma como válido que q, r no son únicos es decir que $a = bq + r$ y $a = bq' + r'$ con $q \neq q'$, $r \neq r'$, $0 \leq r < b$ y $0 \leq r' < b$.

Si se considera que $q' < q$ entonces $q' + 1 \leq q$, por lo tanto

$$r = a - bq \leq a - b(q' + 1) = (a - bq') - b = r' - b < 0$$

Lo cual es una contradicción. De manera análoga se llega a una contradicción si se considera $q' > q$. Por lo tanto, se debe tener que $q = q'$ y $r = r'$.

Teniendo como base el algoritmo de la división, Zalamea (2008) propone la definición de máximo común divisor de dos números de la siguiente manera:

Definición 6 (D6): Dados $a, b \in Z$, el máximo común divisor de a y b se denota como $mcd\ (a, b)$ y se define mediante las condiciones:

i. $mcd\ (a, b) > 0$
ii. $mcd(a, b)|a$ y $mcd(a, b)|b$
iii. Si $d'|a$ y $d'|b$ entonces $d'|mcd(a, b)$.

El siguiente algoritmo determina el $mcd\ (a, b)$ por medio de divisiones sucesivas y además permite encontrar una combinación lineal de este, en términos de dichos números.

Se puede suponer que a y b son dos enteros positivos y que $a > b$ de esta manera por el algoritmo de la división se tiene que:

$$a = bq_1 + r_1 \text{ con } 0 \leq r_1 < b$$

$$b = r_1q_2 + r_2 \text{ con } 0 \leq r_2 < r_1$$

$$r_1 = r_2q_3 + r_3 \text{ con } 0 \leq r_3 < r_2$$

…

$$r_{n-2} = r_{n-1}q_n + r_n \text{ con } 0 \leq r_n < r_{n-1}$$

$$r_{n-1} = r_nq_n + 0$$

Este algoritmo recibe el nombre de *Algoritmo de Euclides* y termina en el momento en el que se obtiene un residuo igual a cero. De no ser así, se obtendría una cadena infinita descendente de naturales lo cual sería una contradicción con el hecho de que cualquier subconjunto de los naturales posee un primer elemento por el principio del buen orden.

Para desarrollar el teorema cuyo enunciado es $r_n = mcd\ (a, b)$, se requiere aclarar lo siguiente:

Teorema 21 (T21): Sean $a, q \in Z$. Si $a = qb + r$ con $0 \leq r < b$ entonces

$mcd\ (a, b) = mcd\ (b, r)$.

Demostración: Como $a = bq + r$ entonces $r = a - bq$ por lo tanto r es una combinación lineal a y b y por **T19.5** se tiene que si $mcd\ (a, b) = d$ entonces $d|r$. De aquí que $mcd\ (a, b)$ es un divisor común de b y r. Se procede ahora a demostrar por contradicción que $mcd\ (a, b) = mcd\ (b, r)$. Esto quiere decir que existe $d' = mcd\ (b, r)$ y $d' > d$. Y por el mismo razonamiento inicial se tiene que a es una combinación lineal de b y r y por **T19.5** se tiene que $d'|a$ por lo tanto $d \neq mcd\ (a, b)$ lo cual es una contradicción. De aquí que $mcd\ (b, r) = mcd\ (a, b)$.

Teorema 22 (T22): Sea $a, b \in Z$ teniendo en cuenta el proceso descrito anteriormente se tiene que $r_n = mcd\ (a, b)$.

Demostración: Como se tiene que $r_{n-1} = r_nq_n + 0$, por **D5** $r_n|r_{n-1}$ por lo tanto

$mcd\ (r_{n-1}, r_n) = r_n$ aplicando reiteradamente (**T21)** se tiene lo siguiente:

$r_n = mcd\ (r_{n-1}, r_n) = mcd\ (r_{n-2}, r_{n-1}) = \cdots = mcd\ (r_2, r_1) = mcd\ (b, r_1) = mcd\ (a, b)$

es decir $r_n = mcd\ (a, b)$.

Definición 7 (D7): Si $a, b, c\ \in Z$, $a \neq 0$ y $b \neq 0$, toda ecuación lineal de la forma

$ax + by = c$, con $x, y\ \in\ Z$ se dice una ecuación **diofántica lineal en dos variables**.

Como en este documento solo se van a considerar este tipo de ecuaciones (diofántica lineal en dos variables) no hay la posibilidad de que se confunda con otros tipos de ecuaciones diofánticas. Por lo tanto, se hará referencia de estas simplemente como ecuaciones diofánticas.

Teorema 23 (T23): Sean a y b dos enteros no ambos iguales a cero. El $mcd\ (a, b)$ es el menor entero positivo que pueda escribirse en la forma $ax + by$ con $x, y\ \in\ Z$.

*Demostración***:** Se parte de que el $mcd\ (a, b) = d$. Sea

$$S = \{z \in Z^+ |\ z = ax + by, x, y \in Z\ \}.$$

Como $aa + bb = z$ se tiene que $z \in S$ por lo tanto $S \neq \emptyset$, luego S posee un mínimo g por el principio del buen orden. Luego $g = ax_0 + by_0$, debido a que $g \in\ S$. Ahora lo que sigue es probar que $g = d$.

Por **T22** se tiene que:

$$a = qg + r \text{ con } 0 \leq r < g$$

Al sustituir g,

$$r = a - qg = a - q(ax_0 + by_0) = a(1 - qx_0) + b(-qy_0) = ax_1 + by_1$$

Si $r \neq 0$ se tendría que $r \in S$ y además g no es mínimo (por la condición $r < g$) lo cual es una contradicción. Por lo tanto $r = 0$, de aquí que $g|a$ y siguiendo un razonamiento análogo también se tiene que $g|b$, con lo que se puede concluir que $g \leq d$ debido a que g es un divisor común. Como se tiene que $g = ax_0 + by_0$, $d|a$ y $d|b$ por el **T19.5** se llega a que $d|\ ax_0 + by_0$ es decir que $d|g$ luego $d \leq g$ y como

ya se tenía que $g \leq d$ se concluye que $g = d$. Luego el $mcd\ (a, b)$ es el menor entero que puede escribirse como una combinación lineal de a y b.

Esto permite garantizar la existencia y unicidad del máximo común divisor de dos números, debido a que el mínimo de un conjunto es único.

Teorema 24 (T24): Si $a|bc$ y $mcd\ (a, b) = 1$ entonces $a|c$.

Demostración. Como $a|bc$ entonces existe $k \in Z$ tal que $bc = ak$ por **D5**.
Además, dado que $mcd\ (a, b) = 1$ por **T23** se tiene que existen $x, y \in Z$ tales que $1 = ax + by$

Por lo tanto,

$$c = c(1) = c(ax + by) = c(ax) + c(by) = a(cx) + (cb)y = a(cx) + (ak)y \\ = a(cx + ky)$$

La primera igualdad se da por **T6,** la segunda por la sustitución de la combinación lineal en 1, la tercera por **T7,** la cuarta por **T1**, la quinta se tiene de hacer la sustitución de $bc = ak$ en la expresión anterior, la sexta de **T1** y **T7.**

Por propiedad transitiva de la igualdad se llega a que $c = a(cx + ky)$ y por **D5** se concluye que $a|c$.

Teorema 25 (T25): La ecuación $ax + by = c$ diofántica tiene solución si y solo si $d|c$ donde $d = mcd\ (a, b)$.

Demostración: →) Dado que $d = mcd\ (a, b)$, por **D5** $a = dl$ y $b = dm$. Si se supone que $ax + by = c$ al sustituir a y b en esta expresión se tiene que,

$$(dl)x + (dm)y = c$$

Luego, por **T1** y **T7**

$$d(lx + my) = c$$

Por lo tanto $d|c$

←) Ahora si se considera que $d|c$, por definición $c = dp$ para algún $p \in Z$ y teniendo en cuenta que por **D6** $a = dl$ y $b = dm$, se tiene que existen x'', y' tal que

$$ax' + by' = d, \text{ por } \mathbf{T23}$$

Multiplicando por p,

$$(ax')p + (by')p = dp$$

Sustituyendo por c y por **T1**

$$a(x'p) + b(y'p) = c$$

Por lo tanto, existen x e y con $x = x'p$ y $y = y'p$ tal que

$$ax + by = c$$

Teorema 26 (T26): Sea $x_0 = 0, x_1 = 1, y_0 = 1, y_1 = -q_1$ y las fórmulas de recurrencia

$$x_i = x_{i-2} - x_{i-1}q_i,$$

$$y_i = y_{i-2} - y_{i-1}q_i,$$

Se tiene entonces que

$$ax_{i-1} + by_{i-1} = r_{i-1}, \text{ Para } i = 2, \dots, k. \qquad (5)$$

Demostración. Aplicando el algoritmo de Euclides se tiene que

$$a = bq_1 + r_1, \quad 0 \le r_1 < b$$
$$b = r_1q_2 + r_2, \quad 0 < r_2 < r_1$$
$$r_1 = r_2q_3 + r_3, \quad 0 < r_3 < r_2$$
$$\dots$$
$$r_{k-2} = r_{k-1}q_k + r_k, \quad 0 < r_k < r_{k-1}$$
$$r_{k-1} = r_kq_{k+1} + 0.$$

Sea S el conjunto de los $i \in Z$ tales que $1 \le i \le k$ y para los cuales la afirmación (5) es cierta.

Cuando $i = 2$ se tiene que,

$$ax_1 + by_1 = a(1) + b(-q_1) = r_1$$

Ahora se supone que (5) es cierta para $i \leq j$ donde $2 \leq j \leq k$. Por las fórmulas de recurrencia se tiene que:

$$ax_{j+1} + by_{j+1} = a\left(x_{j-1} - x_j q_{j+1}\right) + b\left(y_{j-1} - y_j q_{j+1}\right)$$
$$= \left(ax_{j-1} + by_{j-1}\right) - \left(ax_j + by_j\right) q_{j+1}$$
$$= r_{j-1} - r_j q_{j+1}.$$

Además, puesto que $r_{j-1} = r_j q_{j+1} + r_{j+1}$ se tiene que $ax_{j+1} + by_{j+1} = r_{j+1}$. Por el principio de inducción la igualdad (2) es cierta para $i = 1,2, \dots, k$.

Dado a que es de vital importancia para este trabajo escribir un número natural como la suma de potencias de la base respectiva, González (2004) establece una demostración de la siguiente manera:

Teorema 27 (T27): Dados dos números enteros positivos n y b con $b \geq 2$, pueden encontrarse k enteros no negativos c_k únicos, tales que

$$n = c_k b^k + c_{k-1} b^{k-1} + \cdots + c_2 b^2 + c_1 b + c_0 = \sum_{i=0}^{k} c_i b^i$$

Donde $i \geq 0$, $c_k \neq 0$ y $0 \leq c_i < b$ para todo $i = 0,1,2, \dots, k$.

Demostración. Dados n y b, por el *Algoritmo de la división* existirán q_1 y a_0, únicos, tales que

$$n = bq_1 + a_0, \text{ con } 0 \leq a_0 < b, \text{ y } q_1 < n.$$

Aplicando nuevamente el algoritmo, esta vez tomando q_1 y b, pueden encontrarse q_2 y a_1, únicos, tales que

$$q_1 = bq_2 + a_1 \text{ con } 0 \leq a_1 < b, \text{ y } q_2 < q_1.$$

Reiterando el proceso,

$$q_2 = bq_3 + a_2 \text{ con } 0 \leq a_2 < b, \text{ y } q_3 < q_2$$

$$q_3 = bq_4 + a_3 \text{ con } 0 \leq a_3 < b, \text{ y } q_4 < q_3$$

y así sucesivamente.

Se tendrá entonces una sucesión de enteros positivos

$$n, q_1, q_2, q_3, q_4, \ldots$$

tal que

$$n > q_1 > q_2 > q_3 > q_4 > \cdots$$

y que, por el *principio del buen orden*, tiene un primer elemento q_k, tal que

$$q_k = b(0) + a_k, \text{ con } 0 \leq a_k < b$$

y a_k debe ser distinto de cero ya que de lo contrario q_k sería cero, contradiciendo el hecho de que este es positivo.

Sustituyendo el valor de q_1 en n,

$$n = (bq_2 + a_1)b + a_0 = q_2 b^2 + a_1 b + a_0$$

y sustituyendo en este resultado el valor de q_2

$$n = (bq_3 + a_2)b^2 + a_1 b + a_0 = q_3 b^3 + a_2 b^2 + a_1 b + a_0$$

Repitiendo el proceso hasta q_k,

$$n = a_k b^k + a_{k-1} b^{k-1} + \cdots + a_3 b^3 + a_2 b^2 + a_1 b + a_0$$

La expresión obtenida es la *descomposición polinómica* de n en la base b.

Este teorema permite que, en el desarrollo del trabajo, se considere cualquier número entero como el resultado de una sumatoria de términos, que vendrían siendo las cifras; es importante que se tenga en cuenta la última cifra del número a trabajar.

2.1.3. Criterios de divisibilidad

Entrando en el principal foco de estudio, a partir de ahora, si se desea saber cuándo un número divide a otro, el primer número recibe el nombre de *presunto divisor*. En los siguientes teoremas se empiezan a estudiar algoritmos para obtener criterios de divisibilidad;

cada uno ofrece un método distinto, uno abarca cualquier presunto divisor (pero en una base específica- base 10), otro considera cualquier base y cualquier presunto divisor y, otro agrupa números con ciertas características determinando para cada grupo, un algoritmo diferente.

A través de los años se han realizado estudios enfocados a determinar criterios de divisibilidad, un panorama detallado de este rastreo histórico se puede ver en el trabajo realizado por Osorio y Castañeda (2014). En este, resaltan la labor de Blaise Pascal, quien determinó resultados significativos en el estudio de la divisibilidad, enunciando un algoritmo para determinar criterios de divisibilidad que se extienden a diferentes bases numéricas (el cual se presentará como un teorema en este documento).

Es evidente el interés a través de los años de buscar criterios, este interés todavía está vivo y es evidente en los centros educativos cuando se presentan criterios, por ejemplo, para saber cuándo un número es divisible por 2 se debe mirar si la cifra de las unidades es múltiplo de dos; para saber si un número es divisible por 3, se deben sumar las cifras de este y verificar si la suma es múltiplo de tres. Estos criterios se pueden enunciar de una manera más precisa de la siguiente manera:

- *Múltiplo de dos:* un número es divisible por dos si y solo si la cifra de las unidades es múltiplo de dos
- *Múltiplo de tres:* un número es divisible por tres si y solo si la suma de sus dígitos es múltiplo de tres.

Una de las aplicaciones que se les da a los criterios de divisibilidad es la de simplificar fracciones reduciendo procedimientos de cálculo o (relaciones entre números y la operación división). Aunque muchos de estos criterios no son tan prácticos en el sentido de que, en ocasiones resulta más fácil hacer la división, no deja de ser interesante ver la variedad de caminos para saber si un número es divisible por otro.

El siguiente teorema propuesto por Ruíz y Carvajal (2002) considera cualquier presunto divisor para determinar el criterio, sin embargo, el número por el cual se desea determinar la divisibilidad debe estar en base 10. De esta manera, en la compilación que hace Hardy (2008), indica que es de vital importancia entender cómo se comportan dos números enteros cuando

no tienen un divisor común diferente a 1, además la forma en que se puede demostrar por medio del algoritmo de Euclides; por eso se define en primer lugar el concepto de primos relativos.

Definición 8 (D8): Sean $a, b \in Z$, se dice que son primos relativos (o coprimos) si no tienen ningún factor primo en común, es decir, si no tienen otro divisor común más que 1, o cumplen que el $mcd\ (a, b) = 1$.

Teorema Criterio universal de divisibilidad (CUD): Si $b \in Z$, donde $b \neq 0$ y primo relativo con 10, entonces, existe un entero a tal que para cualquier número natural n, donde $n = 10d + u; 0 \leq u \leq 9$, se tiene que $b|n \leftrightarrow b|(d - au)$.

Demostración: Como b y 10 son primos relativos, entonces, el $(b, 10) = 1$; Por **T23** existen enteros x e y, tales que $bx + 10y = 1$ (3)

Si se hace $y = -a$, la ecuación se transforma en $bx = 10a + 1$. Si se reescribe a n se puede sustituir bx tal y como se muestra a continuación:

$$n = 10d + u$$

Por **D2.2** y **T3**

$$n = 10d + (-10au + 10au) + u$$

De **T1** y **T7,**

$$n = 10(d - au) + u(10a + 1)$$

Al sustituir bx que se obtiene de despejar (3) en la anterior igualdad,

$$n = 10(d - au) + u(bx)$$

Nuevamente por **T1**

$$n = 10(d - au) + b(ux)$$

De aquí que $b|n \leftrightarrow b|(d - au)$ por **T19.6.**

Ejemplo 1: ¿335257 es divisible por 13?

Solución

Hay que determinar a para usar el teorema anterior; para esto, se puede resolver la ecuación diofántica $13x - 10a = 1$ como se muestra a continuación;

$$13 = 10(1) + 3 \qquad (6)$$

$$10 = 3(3) + 1 \qquad (7)$$

$$3 = 3(1) + 0$$

Sumando -10 en (6) y reemplazando 3 en (7) se tiene que

$$10 = 3[13 - 10(1)] + 1$$

$10(4) + 13(-3) = 1$,

por lo tanto $a = -4$, de esta manera

$$13|335257 \leftrightarrow 13|[33525 + 4(7)]$$

$$\leftrightarrow 13|33553$$

$$\leftrightarrow 13|[3355 + 4(3)]$$

$$\leftrightarrow 13|3367$$

$$\leftrightarrow 13|[336 + 4(7)]$$

$$\leftrightarrow 13|364$$

$$\leftrightarrow 13|[36 + 4(4)]$$

$$\leftrightarrow 13|52$$

$$\leftrightarrow 13|[5 + 4(2)]$$

$$\leftrightarrow 13|13$$

Por lo tanto $13|335257$.

Criterios de divisibilidad para diferentes bases

Ahora bien, durante este marco se han mencionado los teoremas que resumen las formas de encontrar criterios de divisibilidad cuando se trabaja en base diez (10), sin embargo, los resultados de Osorio, K., & Castañeda, E. (2014), muestran los adelantos en la teoría de números para determinar criterios de divisibilidad en diferentes bases que fueron trabajados desde Pascal.

El siguiente teorema es una extensión del teorema Criterio General de Divisibilidad[1] planteado por González, F. (2004). Este autor lo considera para base 10, aunque ya Blaise Pascal había enunciado el teorema considerando cualquier base (Glaser, 1971; citado en Osorio, K., & Castañeda, E., 2014) tal y como se describe a continuación:

Teorema Criterio General de Divisibilidad Extendido (CGDE): El número $n = a_t b^t + a_{t-1} b^{t-1} + \cdots + a_1 b + a_0$ en base b es divisible por p si y solo si $b|T$, donde $T = a_t R_t + a_{t-1} R_{t-1} + \cdots + a_1 R_1 + a_0$ y $bR_{i-1} = px_i + R_i$, para cada $i = 1,2, \ldots, t$, teniendo en cuenta que $R_0 = 1$.

Demostración: →)Partamos de que $p|n$, es decir que

$n = a_t b^t + a_{t-1} b^{t-1} + \cdots + a_1 b + a_0 = pl$, para algún $l \in N$

Teniendo en cuenta que $bR_{i-1} = px_i + R_i$, para cada $i = 1,2, \ldots, t$ se tiene que:

$$b = px_1 + R_1$$

$$bR_1 = px_2 + R_2$$

$$bR_2 = px_3 + R_3$$

…

$$bR_{t-1} = px_n + R_t$$

Al despejar cada uno de los residuos y sustituir se llega a lo siguiente:

$$R_1 = b - px_1$$

$$R_2 = bR_1 - px_2 = b(b - px_1) - px_2 = b^2 - p(bx_1 + x_2)$$

$$R_3 = bR_2 - px_3 = b[b^2 - p(bx_1 + x_2)] - px_3 = b^3 - p[b(bx_1 + x_2) + x_3] = b^3 - p(b^2 x_1 + bx_2 + x_3)$$

…

$$R_t = b^t - p(b^{t-1} x_1 + b^{t-2} x_2 + \cdots + bx_{t-1} + x_t)$$

Si a cada factor de p de las anteriores igualdades lo sustituimos por un k_i , se tiene entonces que

[1] Sea n un entero positivo, sea $\sum_{i=1}^{k} a_i 10^i$ su representación decimal, y sean r_i los restos de la división de 10^i por $p \geq 2, i = 1, .., k$. Entonces n es divisible por p si y sólo si lo es $\sum_{i=1}^{k} a_i r_i$. González, F. (2004).

$$R_i = b^i + pk_i$$

Como $T = a_t R_t + a_{t-1} R_{t-1} + \cdots + a_1 R_1 + a_0$ podemos reescribir de la siguiente manera:

$$T = a_t R_t + a_{t-1} R_{t-1} + \cdots + a_1 R_1 + a_0 = \sum_{i=1}^{t} a_i R_i + a_0$$

Sustituyendo R_i en esta última expresión,

$$T = \sum_{i=1}^{t} a_i (b^i + pk_i) + a_0 = \sum_{i=1}^{t} a_i b^i + \sum_{i=1}^{t} a_i pk_i + a_0 = \sum_{i=1}^{t} a_i b^i + a_0 + p \sum_{i=1}^{t} a_i k_i$$

$$= n + p \sum_{i=1}^{t} a_i k_i = pl + p \sum_{i=1}^{t} a_i k_i$$

Luego,

$$T = p\left(l + \sum_{i=1}^{t} a_i k_i\right)$$

Por lo tanto $p|T$.

←) Ahora supongamos que $p|T$ esto quiere decir que $T = pm$ para algún entero m. Teniendo en cuenta el análisis anterior podemos escribir a T como $T = n + p\sum_{i=1}^{t} a_i k_i$ al sustituir T en esta última expresión queda que

$$pm = n + p \sum_{i=1}^{t} a_i k_i$$

Sumando $-p\sum_{i=1}^{t} a_i k_i$ en ambos miembros de la igualdad,

$$n = pm - p \sum_{i=1}^{t} a_i k_i = p\left(m - \sum_{i=1}^{t} a_i k_i\right)$$

Lo cual permite concluir que $p|n$.

Ejemplo 2:

a) Obtener una condición necesaria y suficiente para que un natural sea divisible por 2.

Solución

Sea n natural y $n = a_t 10^t + a_{t-1}10^{t-1} + \cdots + a_1 10 + a_0 = \sum_{i=0}^{t} a_i 10^i$ su representación polinómica. Calculando los residuos R_i para cada $i = 0,1, \ldots, t$, teniendo en cuenta que $R_0 = 1$ y que $10R_i = 2(5R_i)$ para cada i entonces $T = a_0$ ya que los demás residuos valen 0. De esta manera se puede concluir que $2|n$ si y solo si $2|a_0$ por **CGDE**.

b) Determinar si el número 3654 en base 7 es divisible por 6.

Solución

Calculando los residuos,

$$R_0 = 1$$

$$R_1 = 1 = R_2 = R_3$$

Luego $T = 3 + 6 + 5 + 4 = 24$ en base 7 si repetimos nuevamente el proceso para 24 se llega a que $T' = 2 + 4 = 6$. Como $6|T'$ por **CGDE** $6|24$, es decir, $6|T$ y nuevamente por **CGDE** se concluye que $6|3654$.

A continuación, se darán a conocer dos teoremas que resumen la propuesta hecha por Osorio, K., & Castañeda, E. (2014), en donde se presentan una serie de casos para determinar criterios de divisibilidad; de esta manera, las demostraciones para ambos teoremas fueron desarrollados en su mismo trabajo. Ahora bien, el siguiente teorema generaliza algunos criterios en diferentes bases, con las condiciones de que si b es la base, entonces el número por el que se desea dividir son de la forma $b, b-1$ o $b+1$.

Teorema criterios de divisibilidad en diferentes bases (CDDB)

1. En cualquier base b un número n es divisible por b si y solo si la cifra de las unidades es cero.
2. En cualquier base b un número n es divisible por $b-1$ si y solo si la suma de sus cifras es múltiplo de $b-1$.

3. En cualquier base b un número n, es divisible por $b+1$ si y solo si la suma entre el número conformado por las cifras de n excepto la de las unidades y el producto resultante de multiplicar esta cifra por b es múltiplo de $b+1$.
4. En cualquier base b un número n, es divisible por $b+1$ si y solo si la diferencia entre el resultado de sumar las cifras de posiciones impares y el resultado de sumar las cifras de posiciones pares de n es múltiplo de $b+1$.

Para poder visualizar este teorema, se presenta a continuación el ejemplo:

Ejemplo 3: Determinar si los siguientes números en base 16 son divisibles por 16 y por 15:

a) 156980
b) $98465ABB65D7844C$
c) $2C9C83A65B$

Solución

Como el único que termina en cero es el número 156980 entonces es el único de los tres que es divisible por 16 por el inciso 1 del teorema **CDDB**. La suma de las cifras de cada uno es 29, 123, 78 respectivamente. Como la suma de los dígitos de 78 es 15 se puede concluir por **CDDB** numeral 2 que el número $2C9C83A65B$ es el único de los tres que es divisible por 15.

A continuación, se dará a conocer el segundo teorema que resume una serie de resultados donde se caracterizan o agrupan criterios, teniendo en cuenta el "presunto divisor" a, la base en la que está escrito un número debe ser de la forma $ak+c$ con $0 \leq c < a$, con $k, c \in N$.

Teorema Criterios de divisibilidad particulares (CDP)

*Un número n en base de la forma **(2)** es divisible por **(1)** si y solo si **(3).***

Debido a la cantidad de resultados obtenidos por Osorio, K., & Castañeda, E. (2014), y viendo la forma en que ellos enunciaron estos teoremas, se pudo apreciar que estos están escritos bajo una estructura que se repite, aunque sean distintos dichos teoremas. Se ha hecho una tabla con el objetivo de no escribir las palabras que se vuelven recurrentes en cada una de las proposiciones. Cada uno de los criterios se agrupan de acuerdo con la base y esta a su

vez depende del "presunto divisor". Las frases que se repiten en cada uno de los enunciados (aunque no necesariamente están escritos con las mismas palabras por los autores) son: "Un número n en base de la forma", "es divisible por", "si y solo si".

De esta manera la tabla está compuesta por las palabras o números que completan estos enunciados, la primera columna numerada con 1 y con nombre "Divisor", corresponde al "presunto divisor"; la segunda columna corresponde a la base en la que está escrito el número n y la tercera columna, es la condición necesaria y suficiente para que n sea múltiplo de uno de los números de la primera columna.

Por ejemplo, si se considera el número 3 de la primera columna con la base escrita de la forma $3k + 1$. Entonces le corresponde la condición "la suma de las cifras es múltiplo de 3". La proposición queda completa si se sustituyen en las etiquetas (1), (2) y (3) los números o palabras correspondientes a la columna, es decir, "*Un número en base de la forma* $3k + 1$ *es divisible por 3 si y solo si la suma de las cifras es múltiplo de 3".*

Divisor (1)	**Base (2)**	**Criterio (3)**
2	2*k*	La cifra de las unidades es múltiplo de 2
	2*k*+1	La suma de las cifras es múltiplo de 2
3	3*k*	La cifra de las unidades es múltiplo de 3
	3*k*+1	La suma de las cifras es múltiplo de 3
	3*k*+2	La diferencia entre la suma de las cifras de posición par más los de posición impar es múltiplo de 3.
5	5*k*	La cifra de las unidades es múltiplo de 5
	5*k*+1	La suma de las cifras es múltiplo de 5
	5*k*+2	La diferencia entre el número n sin la cifra de las unidades y dos veces esta cifra es múltiplo de 5

	$5k+3$	La suma entre el número n sin la cifra de las unidades y dos veces esta cifra es múltiplo de 5
	$5k+4$	La diferencia entre el número sin la cifra de las unidades y esta cifra es múltiplo de 5
7	$7k$	La cifra de las unidades es múltiplo de 7
	$7k+1$	La suma de las cifras es múltiplo de 7
	$7k+2$	La diferencia entre el número n sin la cifra de las unidades y tres veces esta cifra es múltiplo de 7
	$7k+3$	La diferencia entre el número n sin la cifra de las unidades y dos veces esta cifra es múltiplo de 7
	$7k+4$	La diferencia entre el número n sin la cifra de la unidad y cinco veces esta cifra es múltiplo de 7
	$7k+5$	La diferencia entre el número n sin la cifra de la unidad y cuatro veces esta cifra es múltiplo de 7
	$7k+6$	La diferencia entre la suma de las cifras de posición par y la suma de los de posición impar es múltiplo de 7
11	$11k$	La cifra de las unidades es múltiplo de 11
	$11k+1$	La suma de las cifras es múltiplo de 11
	$11k+2$	La diferencia entre dos veces el número n sin la cifra de las unidades y esta cifra es múltiplo de 11
	$11k+3$	La diferencia entre el número n sin la cifra de las unidades y siete veces esta cifra es múltiplo de 11

	$11k$+4	La suma entre el número n sin la cifra de las unidades y tres veces esta cifra es múltiplo de 11
	$11k$+5	La diferencia entre el número n sin la cifra de las unidades y dos veces esta cifra es múltiplo de 11
	$11k$+6	La suma entre el número n sin la cifra de las unidades y dos veces esta cifra es múltiplo de 11
	$11k$+7	La suma entre el número n sin la cifra de las unidades y once veces esta cifra es múltiplo de 11
	$11k$+8	La diferencia entre el número n sin la cifra de las unidades y cuatro veces esta cifra es múltiplo de 11
	$11k$+9	La diferencia entre el número n sin la cifra de las unidades y seis veces esta cifra es múltiplo de 11
	$11k$+10	La diferencia entre la suma de las cifras de posición par y la suma de las de posición impar es múltiplo de 11

Tabla 4: Criterios de divisibilidad particulares

Ejemplo 4: Determinar la divisibilidad de los siguientes números:

a) 98766 en base 11 ¿es divisible por 3?
b) 56844 en base 12 ¿es divisible por 2?
c) $576A14BC9$ en base 15 ¿es divisible por 5?

Solución

- En la situación (a) nos ubicamos en la fila dos de la tabla (1) del teorema **CDP** y como 11 se puede escribir de la forma $3k + 2$, se debe entonces sumar los dígitos de las posiciones pares y los de las posiciones impares y luego hacer la diferencia de estas

dos sumas. Esto es $22 - 14 = 8$ como 8 no es múltiplo de 3 entonces el número no es divisible por 3.

- Para el caso (b) nos ubicamos en la primera fila; ahora bien, como 12 es par y como la cifra de las unidades es 4 (que es múltiplo de 2), entonces 56844 es divisible por 2.
- En (c) es posible ubicar la fila 3, como 15 es múltiplo de 5 y la cifra de las unidades del número $576A14BC9$ es decir, 9 no es múltiplo de cinco, entonces el número no es divisible por 5.

Como se puede apreciar que estos teoremas buscan generalizar un proceso para determinar criterios, algunos tienen la característica de considerar solo la base diez como es el caso del **CUD**, aunque en este vale la pena decir que se puede extender a otras bases teniendo en cuenta que se puede escribir a un número $n = bP + u; 0 \leq u \leq b - 1$, donde b es la base; si $(p, b) = 1$ se puede usar un argumento análogo a la demostración de **CUD** para probar que $b|n \leftrightarrow b|(d - au)$.

Otros resultados en cambio hacen una clasificación considerando una "familia" de números donde determinan criterios por diferentes procedimientos como es el caso de los criterios propuestos por Osorio, K., & Castañeda, E. (2014). También se puede ver el algoritmo **CGDE** donde se incluye cualquier base, desarrollando un procedimiento que involucra a todas las cifras del número por el cual se desea saber si es divisible por otro.

Teniendo en cuenta estos resultados surge la inquietud de si es posible un algoritmo general tal vez un poco menos laborioso que el de Pascal, en el sentido de no considerar todas sus cifras para desarrollar su procedimiento, en donde se determine un criterio que incluya cualquier base y que no se limite a la condición que se puede abstraer de **AUD** (la base y el divisor son primos relativos).

Bajo estos parámetros se traza una ruta que permita construir un algoritmo con estas características, uno de los objetivos de este trabajo es generar dicho algoritmo y, al mismo tiempo, programar estas condiciones y que sean ejecutadas por medio de una *App*.

2.2. Componente tecnológico

Esta propuesta considera importante la aplicación de criterios de divisibilidad en diferentes bases por medio de una *App*, debido a que la persona (usuario) al poner en marcha las funciones de la *App*, puede abarcar conocimientos conceptuales y conocimientos procedimentales. Según Diaz & Hernández (2002), los conocimientos conceptuales se construyen por medio del aprendizaje abstracto que constituyen los conceptos, principios, axiomas o teoremas; por otro lado, el conocimiento procedimental en matemáticas, lo consideran como la ejecución de estrategias, procedimientos, métodos, etc.

De esta manera, las acciones que el "usuario" va a ejercer con respecto al campo matemático y al campo tecnológico están estrechamente relacionadas con procesos cognoscitivos y metacognitivos (Sánchez, 2002); así mismo, haciendo un uso guiado de la *App*, se podrían generar procesos de observación, ejecución, análisis, inferencias; además de ello, se puede dotar de sentido al pensamiento a través de otros procesos como la planificación, la ejecución y evaluación.

De acuerdo con Ángel y Bautista (2001), el uso de un software donde se puedan aplicar conceptos de las matemáticas crea y proporciona un ambiente de trabajo dinámico e interactivo; para estos autores, estas habilidades pueden ser desarrolladas integrando al trabajo intelectual del estudiante el software matemático. En tal sentido, con el uso del software, la atención se enfoca en facilitar que el estudiante aprenda a procesar la información, así como, en la transferencia y generalización de los aprendizajes a otros aspectos académicos; para Martín (2001) y Sánchez (2002), estos aspectos son primarios para el desarrollo de las habilidades del pensamiento de orden superior.

2.2.1. Caracterización de la App

MIT App-Inventor es una herramienta de programación intuitiva que permite que las personas desde edades tempranas puedan crear aplicaciones para Android; al no manejar una sintaxis o un lenguaje propio, hace que sea más rápido de entender y el usuario solo debe centrarse en la lógica del programa que desee desarrollar.

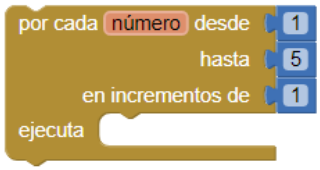
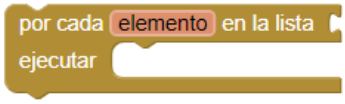
El entorno es visual y al permitir interactuar con figuras conocidas como bloques arrastrándolas, uniendo, separando y ver casi de forma inmediata si funciona cada paso del proceso para desarrollar la aplicación lo hace muy llamativo y divertido. Además, permite diseñar al mismo tiempo los diferentes elementos que quieren que se vea en la pantalla cuando se ejecute la aplicación; estos elementos pueden ser sonidos, animaciones, botones, entre otros.

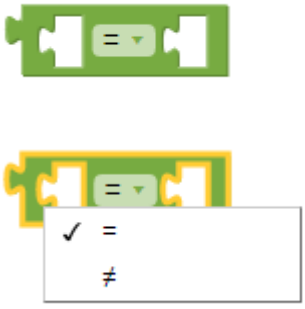
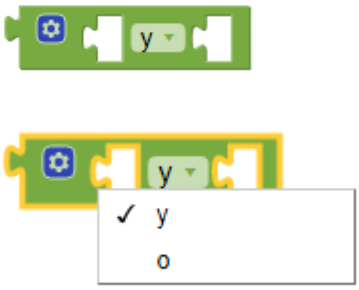
A continuación, se muestra un resumen de las funciones de los bloques más importantes para el desarrollo de la aplicación que se desea hacer y se expondrán los pasos más relevantes de dicho programa[2].

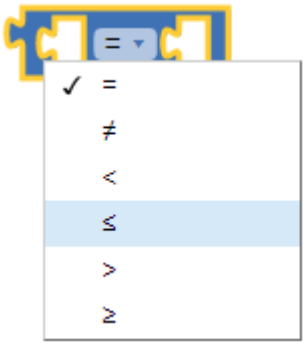
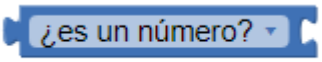
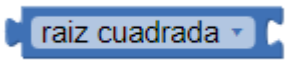
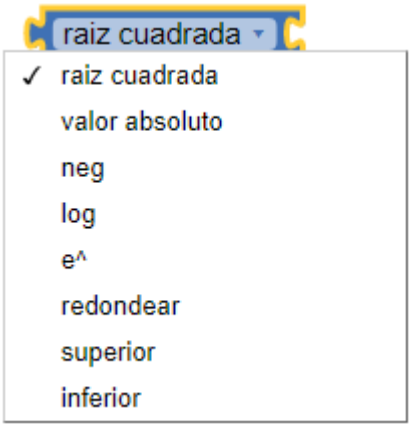
Los bloques están clasificados por categorías, agrupándolos por colores. En la siguiente tabla se darán a conocer estas categorías con sus correspondientes bloques.

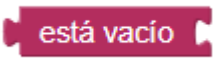
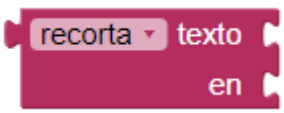
Categoría	Bloque	Descripción
Control		Este bloque evalúa una condición, si es verdadera, ejecuta la acción anidada en el espacio inferior del bloque. En caso contrario el bloque no devuelve un valor.

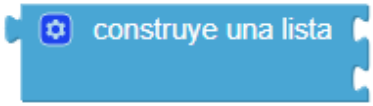
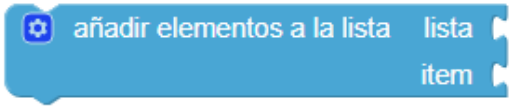
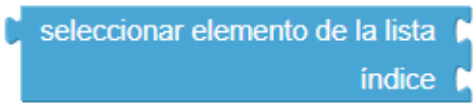
[2] Las descripciones de los diferentes bloques se pueden encontrar en el sitio web http://ai2.*App*inventor.mit.edu/reference/blocks/

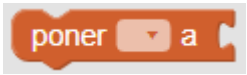
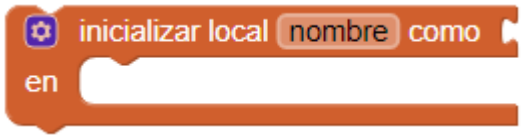
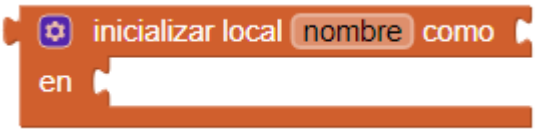
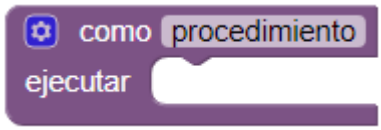
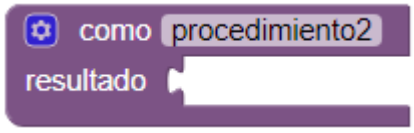
		Este es un complemento del anterior. Ahora cuando la proposición no es verdadera ya no devuelve un valor, sino que, al contrario, ejecuta una acción anidada en el espacio inferior.
		Ejecuta los bloques que engloba en una secuencia de incrementos dados hasta cierto valor.
		Toma cada elemento de una lista y ejecuta los bloques englobados
		Ejecuta los bloques ubicados en el espacio de la parte inferior hasta que se deje de cumplir la

		condición incrustada en la parte superior.
Lógica		Establece si una proposición es verdadera o falsa.
		Devuelve el valor de verdad opuesto a la entrada.
		Comprueba si dos cosas (no solo números) son iguales o en su variante, si son diferentes.
		Comprueba el valor de verdad de una serie de proposiciones conectadas por la disyunción. En su variante las proposiciones están unidas por la conjunción.

Matemáticas		Suma dos o más valores numéricos
		Realiza la división de dos valores numéricos
	 	Comprueba si dos números son iguales o diferentes en su variante.
		Valida si la entrada es un número
	 	Devuelve la raíz cuadrada, el valor absoluto, logaritmo natural, o permite redondear al entero más próximo superior o inferior.

		Determina el residuo.
Texto		Se puede escribir cualquier carácter o número en este bloque
		Elimina todos los espacios al inicio y final de una cadena y devuelve el resultado
		Anexa todas las cadenas para hacer una sola.
		Devuelve el número de caracteres o espacios de una cadena
		Verifica si la cadena está vacía o no
		Recorta una cadena indicada en el espacio con la etiqueta “en” y devuelve una lista

		con esta modificación
Listas		Crea una lista sin elementos
		Crea una lista cuyos elementos son las entradas.
		Añade elementos al final de una lista
		Devuelve el número de elementos que tiene la lista
		Selecciona un elemento de la lista indicando la posición de este en el índice.
		Inicia o crea variables, permitiendo modificar el nombre de esta en el espacio con etiqueta “nombre”

Variables		Llama cualquier variable que se haya creado
		Le asigna a una variable un valor específico
		Permite crear variables que solamente son accesibles en la parte ejecutar de este bloque
		Permite crear variables que solamente son accesibles en la sección resultado de este bloque
		Recoge una secuencia de bloques y no devuelve algún valor
		Recoge la secuencia de bloques y arroja un resultado

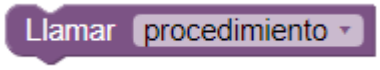
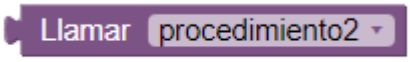
Procedimientos		Llama un procedimiento que no devuelve un valor
		Llama un procedimiento que devuelve un valor

Tabla 5: Descripción de los bloques de App-Inventor

3. Desarrollo de la propuesta

En el siguiente apartado, se va a desarrollar la propuesta desde dos aspectos: el primero que está relacionado a lo matemático, es decir, por medio de un algoritmo único de divisibilidad y su respectiva demostración, se llegará a encontrar el posible criterio de divisibilidad para cualquier número entero escrito en cualquier base; por otro lado, se plantean unas ideas desde lo tecnológico que permiten describir la relación que tendría la *App* (con sus respectivas funciones) con el algoritmo anteriormente mencionado.

3.1. Una mirada desde lo matemático

A partir de la forma polinómica de un número en base diez (caso particular de **T25**) se realizó un trabajo de indagación para encontrar criterios de divisibilidad. En principio se consideró el mismo método que usan Osorio y Castañeda (2014) en sus demostraciones para argumentar los criterios de **CDP.** En este se escribe el número diez en cada potencia como una combinación lineal, de tal manera que uno de sus sumandos sea múltiplo del presunto divisor. En el siguiente ejemplo se puede observar la manera cómo se construye el criterio con dichas observaciones.

Ejemplo 5: Mostrar que una condición necesaria y suficiente para que un número escrito en base 10 sea múltiplo de 3 es que la suma de sus cifras también debe serlo.

Sea $n \in N$, por **T25** se tiene que

$$n = c_k 10^k + c_{k-1} 10^{k-1} + \cdots + c_2 10^2 + c_1 10 + c_0 = \sum_{i=0}^{k} c_i 10^i \quad (8)$$

Donde $i \geq 0$, $c_k \neq 0$ y $0 \leq c_i < 10$ para todo $i = 0,1,2, \ldots, k$.

La expresión (8) se puede escribir de la siguiente manera

$$\sum_{i=0}^{k} c_i (9+1)^i$$

Aplicando el principio de inducción matemática se tiene que:

i. Para $k = 1$

$$\sum_{i=0}^{1} c_i(9+1)^i = c_1(9+1) + c_0 = 9c_1 + c_1 + c_0$$

Como $3|9$ por **T19.3** se tiene que $3|9c_1$ **y** para que $3|(9c_1 + c_1 + c_0)$ por **T19.6** se debe tener que $3|(c_1 + c_0)$. Por lo tanto, se cumple el criterio para este caso.

ii. Ahora se supone que se cumple para un $k > 1$ y se debe llegar que también se satisface para $k + 1$.

Por Teorema del binomio[3]

$$(9+1)^{k+1} = \sum_{i=0}^{k+1} \left(\frac{k+1}{i}\right) 9^{(k+1)-i} 1^i = 1 + \sum_{i=0}^{k} \left(\frac{k+1}{i}\right) 9^{(k+1)-i}$$

De aquí que $3|\sum_{i=0}^{k} \left(\frac{k+1}{i}\right) 9^{(k+1)-i}$.

Como

$$c_{k+1}(9+1)^{k+1} + c_k(9+1)^k + \cdots + c_2(9+1)^2 + c_1(9+1) + c_0$$

$$= c_{k+1}\left[1 + \sum_{i=0}^{k} \left(\frac{k+1}{i}\right) 9^{(k+1)-i}\right] + \sum_{i=0}^{k} c_i(9+1)^i$$

$$= c_{k+1} + c_{k+1} \sum_{i=0}^{k} \left(\frac{k+1}{i}\right) 9^{(k+1)-i} + \sum_{i=0}^{k} c_i(9+1)^i$$

Por **T19.6** se debe tener que $3|c_{k+1}$ y como por hipótesis $3|\sum_{i=0}^{k} c_i$ entonces por **T19.5** se tiene que $3|\sum_{i=0}^{k+1} c_i$ lo cual demuestra la proposición.

Después de estudiar varios ejemplos en los que se obtienen criterios de manera análoga, se quiso estudiar otra forma de ver el polinomio. En esta se considera la cifra de las unidades como $c_0 = 1(c_0)$ y se llegó a una expresión, en la que solo se debe cambiar a 1 por una combinación lineal de 10 y el "presunto divisor". A continuación, se ejemplifica lo anterior: Se desea determinar una condición para que un número escrito en base 10 sea divisible por 7.

---

[3] ***Teorema del binomio***: $(a+b)^n = \sum_{k=0}^{n} \binom{n}{k} a^{n-k} b^k$. Donde $\binom{n}{k} = \frac{n!}{k!(n-k)!}$.
La demostración de este teorema se encuentra en Osorio, K., & Castañeda, E. (2014).

Como $1 = 3(7) - 2(10)$

$$n = c_k 10^k + \cdots + c_2 10^2 + c_1 10^1 + (21 - 20)a_0$$

Al factorizar el producto común 10, esto se puede reescribir como

$$10[(c_k 10^{k-1} + \cdots + c_2 10^1 + c_1) - 2c_0] + 21c_0$$

De aquí que el factor de 10 debe ser múltiplo de 7 para que 7 divida a n, ya que 7 divide a $21a_0$, por lo tanto, el criterio es el siguiente:

Si la diferencia del número n sin la cifra de las unidades y dos veces esta cifra es múltiplo de 7 entonces 7 divide a n.

Para el caso en el que el presunto divisor es 9 se tiene que:

$$n = c_k 10^k + \cdots + c_2 10^2 + c_1 10^1 + (10 - 9)c_0$$

Esto se puede reescribir como

$$10[(c_k 10^{k-1} + \cdots + c_2 10^1 + c_1) + c_0] - 9c_0$$

De aquí que el factor de 10 debe ser múltiplo de 9 para que 9 divida a n, por lo tanto, el criterio es el siguiente:

Si la suma del número n sin la cifra de las unidades más esta cifra es múltiplo de 9 entonces 9 divide a n.

Lo interesante de este método es que permite encontrar criterios no solo en la base 10 sino que también en otras bases como se ejemplifica a continuación:

Ejemplo 6: Sea n un natural en base 11 y se quiere determinar una condición para que sea divisible por 8.

Dado que $1 = 3(11) - 4(8)$. Al sustituir esto en (8) queda que

$$n = c_k 11^k + \cdots + c_2 11^2 + c_1 11^1 + (33 - 32)c_0$$

que es equivalente a,

$$11[(c_k 11^{k-1} + \cdots + c_2 11^1 + c_1) + 3c_0] - 32c_0$$

Razonando de manera análoga a los procedimientos anteriores, se tiene que el criterio para este caso es: *si la suma del número n sin la cifra de las unidades más tres veces esta cifra es múltiplo de 8 entonces 8 divide a n*. De esta manera se pueden determinar más criterios y no solo en una base.

3.1.1. Un cambio en la notación polinómica

Viendo el resultado de Ruíz y Carvajal (2002) de solo tener en cuenta la cifra de las unidades para determinar criterios, que se puede considerar en cualquier base y la forma en que su notación sintetiza la forma polinómica de un número; de ahora en adelante se considera la notación descrita en **CUD,** es decir el número n escrito en su forma polinómica en base x es

$$n = c_k x^k + c_{k-1} x^{k-1} + \cdots + c_2 x^2 + c_1 x + c_0$$

factorizando x,

$$= x[c_k x^{k-1} + c_{k-1} x^{k-2} + \cdots + c_2 x + c_1] + c_0$$

Haciendo $c_k x^{k-1} + c_{k-1} x^{k-2} + \cdots + c_2 x + c_1 = P$ y $c_0 = u$ queda que $n = xP + u$.
Se realiza la siguiente conjetura:
Si se desea encontrar un condición necesaria y suficiente para que un número n escrito en base x sea múltiplo de y donde $mcd\,(x, y) = 1$; solo se debe considerar la siguiente operación $P + mu$, donde m resulta de $1 = mx + ny$ para $x, y \in N$ por **T23**. Con esta observación, es posible pensar en un algoritmo que sintetice el anterior procedimiento para calcular criterios y así mismo, considerar una notación que resuma el criterio correspondiente. Este algoritmo se describe a continuación:

1. Escribir a 1 como una combinación lineal de x y y, es decir $1 = mx + ny$
2. Escribir el criterio teniendo en cuenta las siguientes condiciones:
   $P + mu$ es múltiplo de y entonces $y|n$

a) Si $m > 0$ entonces el criterio es: $(m, +)$
b) Si $m < 0$ entonces el criterio es: $(m, -)$.

A continuación, se describen los criterios encontrados anteriormente con su correspondiente notación mencionada en el paso 2 del algoritmo:

- Si $P + 2u$ es múltiplo de 7 entonces $7|n$. Se denota como $(2, +)$.
- Si $P + u$ es múltiplo de 9 entonces $9|n$. Se denota como $(1, +)$.
- Si $P + 3u$ es múltiplo de 8 entonces $11|n$. Se denota como $(3, +)$.

Los siguientes son ejemplos de la aplicación del anterior algoritmo.

Ejemplo 6: Sea un natural n en base 13 , determinar una condición para que n sea múltiplo de 5.

Solución

Se escribe la ecuación diofántica asociada.

$$13m + 5n = 1$$

Aplicando el Algoritmo de Euclides,

$$13 = 5(2) + 3$$
$$5 = 3(1) + 2$$
$$3 = 2(1) + 1$$
$$2 = 1(2) + 0$$

Ahora se reescribe el penúltimo residuo (que en este caso es el 1) como una combinación lineal de 13 y 5, para hacer esto se despeja cada uno de los residuos obtenidos de la primera a la penúltima ecuación

$$1 = 3 - 2(1)$$
$$2 = 5 - 3(1)$$
$$3 = 13 - 5(2)$$

y se sustituye el 2 de la segunda igualdad en la primera y luego el 3 de la tercera igualdad en la expresión obtenida previamente.

$$1 = 3 - \big(5 - 3(1)\big)(1) = 2(3) - 5 = 2\big(13 - 5(2)\big) - 5 = 2(13) - 5(5)$$

Los pasos anteriores no están expresados en los pasos descritos antes…

De esta manera se concluye que

$$1 = 13(2) + 5(-5)$$

Es decir que $m = 2$ y $n = -5$

Por lo tanto, aplicando el algoritmo descrito anteriormente se tiene que: *si la suma del número n sin la cifra de las unidades más dos veces esta cifra es múltiplo de 5 entonces 5 divide a n, que en notación se escribe como* $(2, +)$.

Ejemplo 7: Sea un natural n en base 5 , determinar una condición para que n sea múltiplo de 6.

Solución

Se escribe la ecuación diofántica asociada.

$$5m + 6n = 1$$

Aplicando el Algoritmo de Euclides,

$$6 = 5(1) + 1$$

$$5 = 1(5) + 0$$

Luego,

$$1 = 5(-1) + 6(1)$$

Es decir que $m = -1$ y $n = 1$, por lo tanto, el criterio es: *si la diferencia del número n sin la cifra de las unidades y esta cifra es múltiplo de 6 entonces 6 divide a n, que en notación se escribe como* $(1, -)$.

A continuación, en la Tabla 6 se muestran diferentes criterios donde las columnas están las bases del 2 al 20 y en la fila los presuntos divisores (etiquetado como divisor) también del 2 al 20. En la explicación de la tabla se tendrá en cuenta la notación usada anteriormente es decir $n = xP + u$, donde x es la base en la que está escrito n, u corresponde a las cifras de las unidades de n; y y es el presunto divisor.

Base \ Divisor	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
2	T0	(1,-)		(2,-)		(3,-)		(4,-)		(5,-)		(6,-)		(7,-)		(8,-)		(9,-)	
3	(1,+)	T0	(1,-)	(2,+)		(2,-)	(3,+)		(3,-)	(4,+)		(4,-)	(5,+)		(5,-)	(6,+)		(6,-)	(7,+)
4		(1,+)	T0	(1,-)		(2,+)		(2,-)		(3,+)		(3,-)		(4,+)		(4,-)		(5,+)	
5	(1,+)	(1,-)	(1,+)	T0	(1,-)	(3,+)	(3,-)	(2,+)		(2,-)	(5,+)	(5,-)	(3,+)		(3,-)	(7,+)	(7,-)	(4,+)	
6				(1,+)	T0	(1,-)				(2,+)		(2,-)				(3,+)		(3,-)	
7	(1,+)	(1,+)	(1,-)	(2,-)	(1,+)	T0	(1,-)	(4,+)	(3,+)	(3,-)	(5,-)	(2,+)		(2,-)	(7,+)	(5,+)	(5,-)	(8,-)	(3,+)
8		(1,-)		(2,+)		(1,+)	T0	(1,-)		(4,-)		(5,+)		(2,+)		(2,-)		(7,-)	
9	(1,+)		(1,+)	(1,-)		(3,-)	(1,+)	T0	(1,-)	(5,+)		(3,+)	(3,-)		(7,-)	(2,+)		(2,-)	(9,+)
10		(1,+)				(2,-)		(1,+)	T0	(1,-)		(4,+)				(5,-)		(2,+)	
11	(1,+)	(1,-)	(1,-)	(1,+)	(1,-)	(2,+)	(3,+)	(4,-)	(1,+)	T0	(1,-)	(6,+)	(5,-)	(4,-)	(3,+)	(3,-)	(5,+)	(7,+)	(9,-)
12				(2,-)		(3,+)				(1,+)	T0	(1,-)				(7,-)		(8,+)	
13	(1,+)	(1,+)	(1,+)	(2,+)	(1,+)	(1,-)	(3,-)	(2,-)	(3,-)	(5,-)	(1,+)	T0	(1,-)	(7,+)	(5,+)	(4,+)	(7,+)	(3,+)	(3,-)
14		(1,-)		(1,-)				(2,+)		(4,+)		(1,+)	T0	(1,-)		(6,-)		(4,-)	
15	(1,+)		(1,-)			(1,+)	(1,-)			(3,+)		(6,-)	(1,+)	T0	(1,-)	(8,+)		(5,-)	
16		(1,+)		(1,+)		(3,-)		(4,+)		(2,-)		(4,-)		(1,+)	T0	(1,-)		(6,+)	
17	(1,+)	(1,-)	(1,+)	(2,-)	(1,-)	(2,-)	(1,+)	(1,-)	(3,+)	(2,+)	(5,+)	(3,-)	(5,+)	(7,-)	(1,+)	T0	(1,-)	(9,+)	(7,-)
18				(2,+)		(2,+)				(3,-)		(5,-)				(1,+)	T0	(1,-)	
19	(1,+)	(1,+)	(1,-)	(1,-)	(1,+)	(3,+)	(3,+)	(1,+)	(1,-)	(4,-)	(5,-)	(2,-)	(3,+)	(4,+)	(5,-)	(8,-)	(1,+)	T0	(1,-)
20		(1,-)				(1,-)		(4,-)		(5,+)		(2,+)				(6,+)		(1,+)	T0

Tabla 6: Criterios de divisibilidad desde la base 2 hasta la base 20

En principio, la Tabla 6 se hizo con la intención de encontrar una regularidad para ver si era posible determinar criterios sin tener que recurrir al algoritmo; de hecho, en algunos casos como las tres primeras filas y columnas se intentó encontrar una regularidad, pero no fue posible[4].

Los espacios donde están marcados como T0, indican que el criterio para esa pareja (esa base y el presunto divisor) se reduce a verificar si $u = 0$; si es así, entonces n es múltiplo de y. Se

[4] Se invita al lector a estudiar la tabla y encontrar posibles regularidades; de esta manera, se podría determinar una vía más corta en la construcción de criterios con estas características

puede observar en la tabla, que en los casos donde ocurre esto, es cuando $x = y$. En otras palabras

$$si\ x = y\ entonces\ y|n\ si\ y\ solo\ si\ u = 0$$

Esto se justifica por **CDDB1**.

Como se puede observar en la tabla, hay algunos espacios en blanco esto se debe a que no es posible encontrar un criterio para estas parejas de números por el método descrito anteriormente, debido a que no se puede escribir a uno como una combinación lineal de x y y. Esto se justifica por el **T25** y debido a que $mcd\ (x, y) \neq 1$ y $mcd\ (x, y) \nmid 1$.

Se puede afirmar que el número más pequeño para las combinaciones lineales de las parejas de números donde están estos espacios, son los máximos comunes divisores de dichos números por **T25**. Teniendo en cuenta esta observación, se puede extender la idea inicial para que los casos en los que el $mcd\ (x, y) \neq 1$ se pueda encontrar un criterio para cada uno y con esto completar la tabla.

Considerar el caso en que la base es 9 y el presunto divisor es 6. Se desea determinar una condición para que 6 divida a un número n escrito en dicha base.

Sea n tal que

$$n = 9P + u \quad (3)$$

Se debe tener en cuenta que $mcd\ (9,6) = 3$ y se supone que $u = 3s$, es decir, u es un múltiplo del $mcd\ (9,6)$, esto último se hace para poder escribir a 3 como una combinación lineal de la base y el presunto divisor; que en este caso es $9(1) + 6(-1) = 3$. Reescribiendo la expresión (3) se tiene que:

$$n = 9P + 3s = 6t$$

Sustituyendo la combinación lineal,

$$9P + (9 - 6)s = 6t$$

Por **T2** y **T7,**

$$9P + 9s - 6s = 2t,$$

Por **T7**, y por **T9**

$$3(P + s) - 2s = 2t$$

Como $2|2s$ y $2|[3(P + s) - 2s]$ por **T19.6**, se tiene que $2|3(P + s)$ y como como $mcd\ (2,3) = 1$ entonces por **T24,** $2|(P + s)$.

lo cual nos da el criterio siguiente: con la condición de que $mcd\ (x, y)|u$.

Si la suma del número n sin la cifra de las unidades más la tercera parte de esta cifra es múltiplo de 2 entonces 6 divide a n.

Se pueden hacer por lo menos dos observaciones del anterior procedimiento: la primera tiene que ver con que se le adicionó una condición a u ($mcd\ (x, y)|u$), de aquí que si no se cumple esa condición un algoritmo que se deduzca a partir de este procedimiento no va a funcionar. La segunda es que el criterio ya no depende del divisor 6 si no que ahora depende de 2; esto tampoco ocurría en el algoritmo que se estudió inicialmente, por lo tanto, la notación que se venía manejando no se puede usar para este caso ya que no recoge toda la información para describir el criterio. Esto se debe principalmente al hecho de que en la notación no era importante considerar el presunto divisor, puesto a que en todos los criterios la condición siempre era ser múltiplo de este, en cambio en este último procedimiento la condición es ser múltiplo de 2 que en este caso no es el presunto divisor dado.

3.1.2. Generalización del algoritmo

Nota: Los siguientes dos teoremas son resultados propios de este trabajo; a continuación, se extiende la idea del último procedimiento por medio de un teorema el cual recibirá el nombre de Algoritmo único de divisibilidad (AUD).

Antes de enunciar el siguiente teorema se realizarán algunas aclaraciones sobre la notación usada en este. Se tendrá en cuenta un número natural n escrito en base x y se desea saber si

es divisible por y. También se considerarán los valores $r, s \in Z$ tales que $y = mcd\ (x, y)(r)$ y $u = mcd\ (x, y)(s)$. Además $mcd\ (x, y) = mx + ny$ para $m, n \in Z$.

Teorema Algoritmo parcial de divisibilidad (APD): Sea $n, x, y \in N$ donde n escrito en base x con

$n = xP + u$, y $mcd\ (x, y)|u$ entonces $y|n$ si y solo si $r|(P + ms)$.

Demostración. →) Se toma como dado $n = xP + u$, $mcd\ (x, y)|u$ y $y|n$. Se supone que $mcd\ (x, y) = d$. Por **D5**

$$u = d(s) \qquad (9)$$

Existen $m, n \in Z$ tales que $d = mx + ny$ por **T23**. Al sustituir esto último en (9) se llega a

$$u = (mx + ny)s \qquad (10)$$

Nuevamente se hace una sustitución de n en la expresión $y|n$, es decir,

$$y|(xP + u) \qquad (11)$$

Sustituyendo (10) en (11) se obtiene que

$$y|[xP + (mx + ny)s]$$

Por **T2** y luego **T7** la última expresión queda como

$$y|\{xP + [s(mx) + s(ny)]\}$$

Por **T1** y luego **T2** esto último se puede reescribir como

$$y|\{xP + [x(ms) + y(ns]\}$$

Nuevamente por **T1**

$$y|\{[xP + x(ms)] + y(ns)\}$$

Y por **T7**

$$y|\{x[P + ms] + y(ns)\}$$

Como $d|y$ y $d|x$ por Dmcd entonces $y = dr,\ x = dt$ y

$$x(P + ms) + y(ns) = yk, \text{ para algún } k \in Z, \text{ por } \mathbf{D5}$$

Sustituyendo los valores de x y y en esta última expresión se tiene que

$$dt(P + ms) + dr(ns) = (dr)k$$

Por **T7** y **T4**,

$$d[t(P + ms) + r(ns)] = d(rk)$$

Por **T9,**

$$t(P + ms) + r(ns) = rk$$

Sumando a ambos miembros de la igualdad $-r(ns)$ se tiene que

$$[t(P + ms) + r(ns)] - r(ns) = rk - r(ns)$$

Que por **T1**, **T3** y **D2.2** queda,

$$t(P + ms) = rk - r(ns)$$

Por **T7**,

$$t(P + ms) = r[k - (ns)]$$

Luego por **D5,**

$$r|t(P + ms) \qquad (12)$$

Se debe tener que $mcd\ (r, t) = 1$, ya que si no fuera así se tendría que $mcd\ (r, t) = d' > 1$. De aquí que $r = d'k_1$ y $t = d'k_2$. Y como antes se tenía que $x = dt$ y $y = dr$ al sustituir los valores de t y r respectivamente en las últimas dos igualdades se tiene,

$$x = d(d'k_2) \text{ y } \ y = d(d'k_1)$$

De aquí que

$$dd'|x \text{ y } dd'|y \ (13)$$

Además, como $d' > 1$ entonces $d' - 1 > 0$ y por **D4.2** $(d' - 1) \in Z^+$. Teniendo en cuenta también que $d > 0$ por Dmcd se tiene que $d \in Z^+$; luego por T12 se deduce que $d(d' - 1) \in Z^+$, y como $d(d' - 1) = dd' - d$, con esto se puede asegurar que $(dd' - d) \in Z^+$, que por

D4.2 se tiene que $dd' - d > 0$ y sumando d en la desigualdad se concluye que $dd' > d$. Esto último sumado a la proposición (13) contradice el hecho de que $d = mcd(x, y)$. Por lo tanto, se debe tener que r y t son primos relativos.

De (12) y debido a que $mcd\ (r, t) = 1$ por T se deduce,

$$r|(P + ms)$$

←) Ahora se supone que $r|(P + ms)$ por T.

$$r|t(P + ms)$$

Además, como $r|r$ por T entonces $r|r(ns)$ por T y por T se tiene que

$$r|[t(P + ms) + r(ns)]$$

Por **D5,**

$$t(P + ms) + r(ns) = rk, \text{ con } k \in Z$$

Multiplicando la igualdad por d

$$dt(P + ms) + dr(ns) = drk$$

Sustituyendo los valores de x y y,

$$x(P + ms) + y(ns) = yk$$

Por **T7,**

$$xP + xms + y(ns) = yk$$

Por **T4**, **T5** y **T7**,

$$xP + s(xm + yn) = yk$$

Sustituyendo la combinación lineal de d,

$$xP + sd = yk$$

Sustituyendo el valor de u

$$xP + u = yk$$

Sustituyendo n

$$n = yk$$

Y por **D5**

$y|n.$

Ejemplo 8: Determinar una condición necesaria para que un número en base 14 sea divisible por 21.

Solución

Como el $mcd\ (14{,}21) = 7$, una combinación lineal para 7 en términos de la base y el divisor es:

$$7 = 21(1) - 14(1)$$

entonces por **APD** y teniendo en cuenta la notación de este teorema y que $7|u$ se tiene que la condición es:

$3|(P + s)$, donde s se obtiene de hacer $7s = u$

El teorema anterior permite encontrar criterio para el caso en que la cifra de las unidades sea múltiplo del máximo común divisor de la base (x) y el presunto divisor (y), lo cual es una condición que hace que no se tengan en cuenta muchos números (números cuya cifra de las unidades no sea múltiplo del $mcd\ (x, y)$). A partir de esto surgen las siguientes preguntas: ¿qué pasa si la cifra de las unidades no es múltiplo de dicho número? ¿Cómo se escribe este tipo de números teniendo en cuenta $mcd\ (x, y)$)? ¿Es posible usar un razonamiento análogo a la demostración de **APD** para considerar dichos casos y hacer el algoritmo más general?

Al intentar responder las preguntas, se describe un proceso que sirve para descartar los números cuyas cifras de las unidades no son múltiplos de $mcd\ (x, y)$; la idea surgió a partir de ver algunos ejemplos de casos particulares en el que la condición $mcd\ (x, y)|a_0$ no se cumple y se llegaba a que $y \nmid n$ teniendo en cuenta la notación de **APD**. Uno de los ejemplos que se consideró fue el siguiente:

Ejemplo 9: Determinar la divisibilidad de 1458 en base 9 por 12.

Solución

1458 en base 9. Se tiene que $mcd\ (9{,}12) = 3$, $3 \nmid 8$ y $12 \nmid 1458$

A continuación, se generaliza esta idea de la siguiente manera:

Teorema criterio de las cifras de las unidades (CCU): Sean $n, y \in N$ con $n = xP + u$ en base x. Si $y|n$ entonces $mcd\ (x, y)|u$.

Demostración. Como $y|n$ entonces $y|(xP + u)$. Además, como $mcd\ (x, y)|y$ y $mcd\ (x, y)|x$, por **T11(*transitiva*)**, $mcd\ (x, y)|(xP + u)$ y por **T19.3,** $mcd\ (x, y)|xP$. Luego $mcd\ (x, y)|[(xP + u) - xP]$ por **T19.5,** y por **T2** y **T1** queda que $mcd\ (x, y)|[u + (xP - xP)]$. Finalmente $mcd\ (x, y)|(u + 0)$, que es lo mismo a tener $mcd\ (x, y)|u$.

Ejemplo 10: Sea el número 5678 en base 9 y se quiere determinar la divisibilidad por 6 y por 7. Para el primer caso como $mcd\ (6{,}9) = 3$ y $3 \nmid 8$ (3 no divide a la cifra de las unidades) entonces por **CCU** se tiene que $3 \nmid 5678$. Por otro lado $mcd\ (7{,}9) = 1$ y como $1|8$ entonces no podemos usar **CCU** para saber si 5678 es divisible por 7.

Como más adelante se ejemplifica, la proposición que tendrá mayor utilidad es la contrarrecíproca de **CCU**. Básicamente esta utilidad radica en que se pueden descartar los números con las cifras de las unidades que no sean múltiplos del $mcd\ (x, y)$, debido a que los números con dichas cifras no serán divisibles por y.

Teniendo en cuenta los pasos de la demostración de **APD** y de la proposición que resulta del contrarrecíproco de **CCU**, se puede describir un proceso que se denominará el *Algoritmo único de divisibilidad.* para determinar si un número n es divisible por un presunto divisor.

Algoritmo único de divisibilidad

Teniendo en cuenta que $n, y \in N$, n escrito en base x y $n = xP + u$. Se puede determinar si $y|n$ o $y \nmid n$ mediante los siguientes pasos:

1. Determinar el $mcd\ (x, y)$. Podemos garantizar su existencia por **T23.**

2. Comprobar si el número del paso anterior divide a u. Si es así proceda con los siguientes pasos, sino entonces el número no es divisible por y. Esto se garantiza por **CCU.**
3. Reescriba el $mcd\ (x, y)$ como una combinación lineal de la base y del presunto divisor, es decir, $mcd\ (x, y) = mx + ty$. Esto se puede hacer por **T23.**
4. El número m obtenido en el paso 3 se debe multiplicar por s. Donde s resulta de $u = mcd\ (x, y)(s)$. Esto se obtiene debido a que $mcd\ (x, y)|u$ por el paso 2 y **D5**.
5. Sume el número obtenido en el paso 4 con *P* (el número n sin la cifra de las unidades). Si esta suma es múltiplo de r, donde r se obtiene de $y = mcd\ (x, y)(r)$ este existe debido a que $mcd\ (x, y)|y$ y **D5**, entonces $y|n$. En caso contrario $y \nmid n$. Esto se garantiza por **APD.**

Ejemplo 11: determinar si los siguientes números en base 14 son divisibles por 8.

Solución

a) $18B36D$
   1. $mcd\ (14,8) = 2$
   2. $2 \nmid D$ por lo tanto $8 \nmid 18B36D$

b) $18B36C$
   1. $mcd\ (14,8) = 2$
   2. $2|C$
   3. $2 = 2(8) - 1(14)$, entonces $m = -1$
   4. Como $C = 6[mcd(14,8)]$ entonces se hace $-1(6)$= - 6
   5. $8|18B36D \leftrightarrow 4|(18B36 - 6) = 18B30 \leftrightarrow 2|(18B3 - 0) = 18B3$

   Por el ítem 2 se puede decir que $18B36C$ no es divisible por 8 ya que la cifra de las unidades del número $18B3$ no es divisible por 2 ($2 \nmid 3$).

c) 25488
   1. $mcd\ (14,8) = 2$
   2. $2|8$
   3. $2 = 16 - 14 = 2(8) - 1(14)$, entonces $m = -1$

4. Como $8 = 4[mcd(14,8)]$ entonces se hace $-1(4)$
5. $8|25488 \leftrightarrow 4|(2548-4) = 2544 \leftrightarrow 2|(254-2) = 252 \leftrightarrow 1|(25-1) = 24$

Por lo tanto $8|25488$.

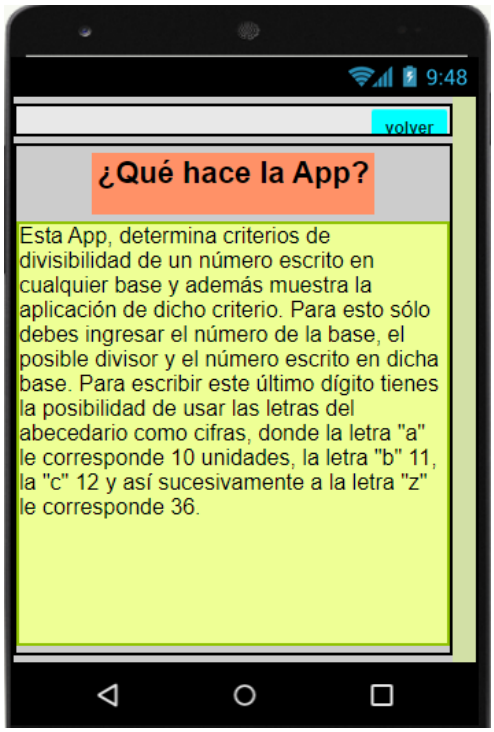
Teniendo en cuenta que se ha encontrado un algoritmo para determinar criterios que puede abarcar todos los posibles casos (cualquier base y cualquier divisor), se ve la necesidad de llevarlo a un software que sea de fácil acceso e intuitivo de usar. Por eso y entre otras razones se escogió el entorno de programación *MIT App-Inventor*; el objetivo principal debe ser que cualquier persona pueda tener acceso, localizar un número (con su respectiva base y presunto divisor), para luego observar el algoritmo único de divisibilidad.

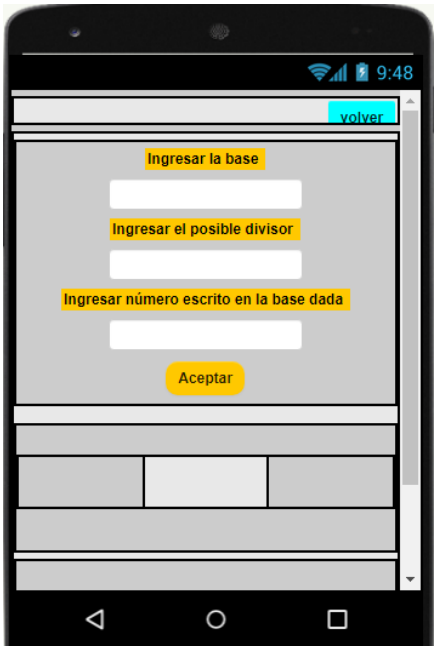
El tener el algoritmo debe permitir a la persona entender y usar el programa como una "calculadora" donde se obtienen criterios como resultados; de esta manera se pueden obtener posibles conjeturas, hipótesis, encontrar regularidades entre los criterios o describir las diferencias.

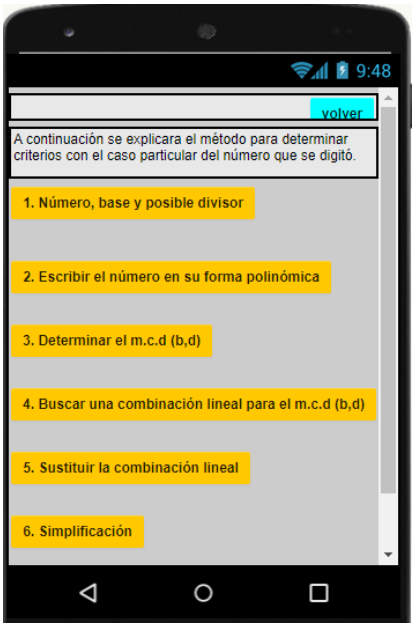
3.2. Desde una mirada tecnológica

A continuación, se presenta una tabla y una descripción de algunas imágenes correspondientes a los bloques (código) que resumirá el contenido de la aplicación desarrollada con nombre *Algoritmo único de divisibilidad.* En la primera se darán a conocer las ventanas que conforman la *App*, mostrando lo que ve el usuario y una descripción breve de dicha ventana tal y como se muestra a continuación:

DESCRIPCIÓN DE LAS VENTANAS DE LA *APP*	
VENTANA 1	Es la primera ventana que ve el usuario. En esta se habilitan dos botones que tienen etiqueta "¿Qué hace la *App*?" y "Continuar". Al dar clic en el primer botón el usuario podrá ver una ventana 2 en donde se describe la función de la *App*.

 *Ilustración 1: Ventana 1 - Presentación*	Si el usuario presiona el botón "Continuar". Podrá ver la ventana 3 donde se le pedirá ingrese tres datos.
VENTANA 2  *Ilustración 2: Ventana 2 - Propósito de la*	En esta ventana se describe la función de la *App*, y también las condiciones en las que debe ingresar los datos de la ventana 3.

VENTANA 3  *Ilustración 3: Ventana 3 - Recolección de datos*  *Ilustración 4: Ventana 3 - Botones habilitados*	En esta ventana se le permite al usuario ingresar el número de la base, el posible divisor y el número escrito en dicha base. Una vez hecho esto deberá oprimir el botón “Aceptar” para que se habiliten los otros botones, bajo una condición; y es que las cifras del número escrito deben ser estrictamente menores a la base dada. Si se cumple este requisito se habilitan los botones los cuales son: “Determinar el criterio” o “Aplicar el criterio”. Al oprimir cualquiera de estos dos botones se habilitarán otros dos. Uno de estos últimos es para ver la construcción del criterio paso a paso o para aplicar el criterio. El otro deja ver el criterio sin mostrar los pasos previos para su construcción o deja ver si el número es divisible por ese posible divisor dado.

VENTANA 4  *Ilustración 5: Ventana 4 - Determinar paso a paso el criterio*	En esta ventana se dan a conocer los diferentes pasos para determinar el criterio, es decir se aplica el teorema **APD.** Al dar clic a cada uno de los botones que indican dichos pasos se hace visible la información relacionada a dicho paso, justificando cada uno de estos.
VENTANA 5	En esta se da a conocer la aplicación de los teoremas **APD** y **CCU.** Cuando se oprime el botón ver criterio, se muestra el criterio obtenido en la ventana 4, y si el usuario selecciona el botón “ver proceso” la *App* dejará ver los diferentes pasos donde se realiza el proceso de suprimir la cifra de las unidades al número para luego sumarle a este un múltiplo de esta.

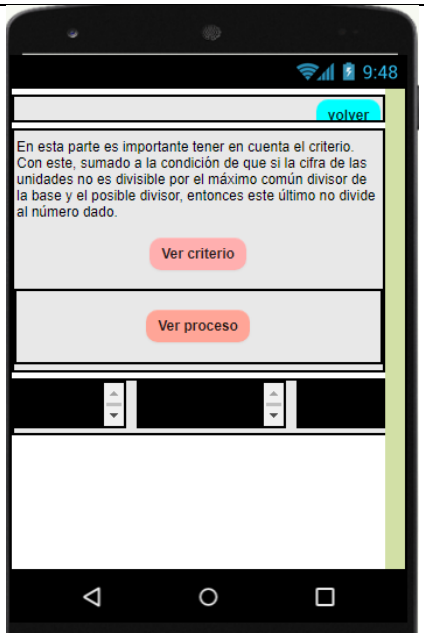
 *Ilustración 6: Ventana 5 - Aplicar el criterio*	

Tabla 7: Descripción de ventanas App

Como se pudo evidenciar, las ventanas en donde están involucrados los teoremas obtenidos en este trabajo (**APD** y **CCU**) son las ventanas 4 y 5. Por eso, a continuación, se hace una recopilación del código que se considera más relevante para llevar a cabo el funcionamiento de esta *App* relacionado a dichas ventanas.

En la ventana 4 se separan las cifras del número escrito en la base dada digitado por el usuario por medio del bloque "recorta" y se guarda cada cifra en una lista, tal y cómo se muestra en la *ilustración 7*. Esto se hace con el fin de poder escribir el número de la forma polinómica dejando a cada una de sus cifras con su correspondiente potencia de la base, que es precisamente lo que se hace en los bloques de la *ilustración 11*. Para esto se tiene en cuenta que después del último sumando, no se debe colocar el signo más, por eso se usa el bloque "si-entonces-sino", para escribir todos los sumandos que tienen como factor las cifras del número excepto el de la cifra de las unidades con el signo +, y luego imprimir el sumando donde está cifra el cual no debe llevar este símbolo.

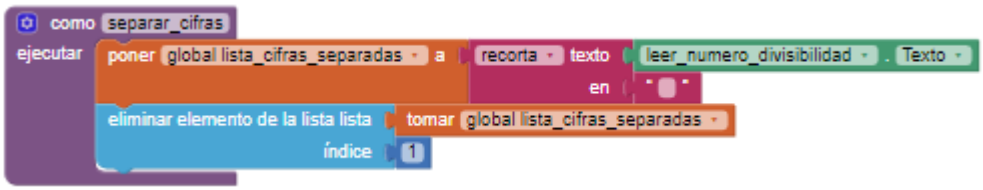


Ilustración 7: Bloques para recortar las cifras del número ingresado y hacer una lista con estas

En la Ilustración 8 se da a conocer los bloques que realizan el proceso de asignarle a cada letra (si las hay) que representa una de las cifras del número dado, el número correspondiente teniendo en cuenta el orden alfabético, al escribir bases mayores que diez. La importancia de hacer esta asignación radica en que las sumas entre el número sin las cifras de las unidades con el múltiplo de esta cifra al aplicar el *algoritmo único de divisibilidad* se realizaron en base 10. Luego mediante un proceso análogo al mostrado en la *imagen 8* se le asigna a cada suma la representación correspondiente al número teniendo en cuenta la base dada. Esto último se hace mediante los bloques mostrados en la Ilustración 12.

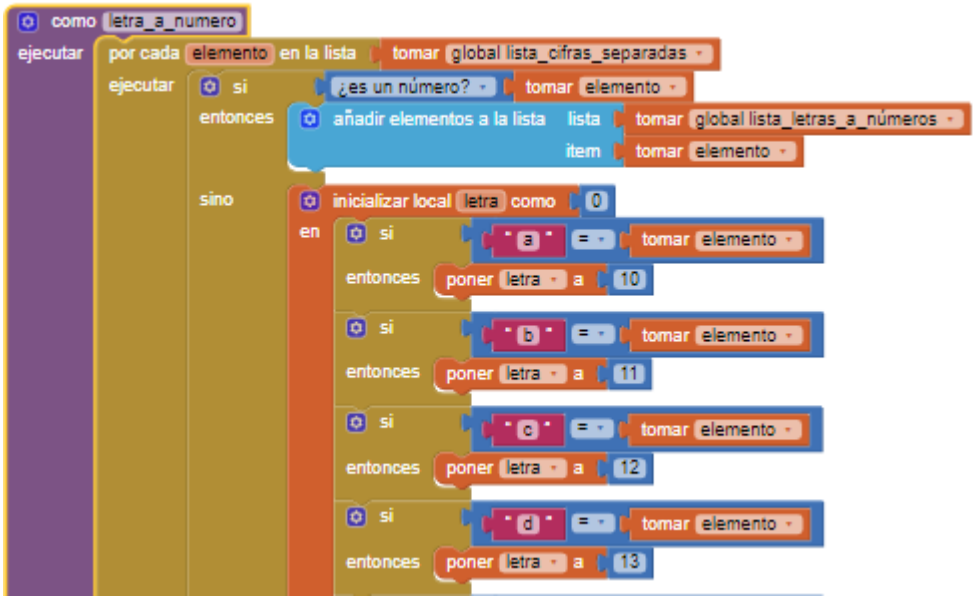


Ilustración 8: Bloques para asignarle a cada letra un número

En la Ilustración 9 se deja ver los bloques para determinar el máximo común divisor de la base y el presunto divisor. Este está inspirado en el *algoritmo de Euclides.*

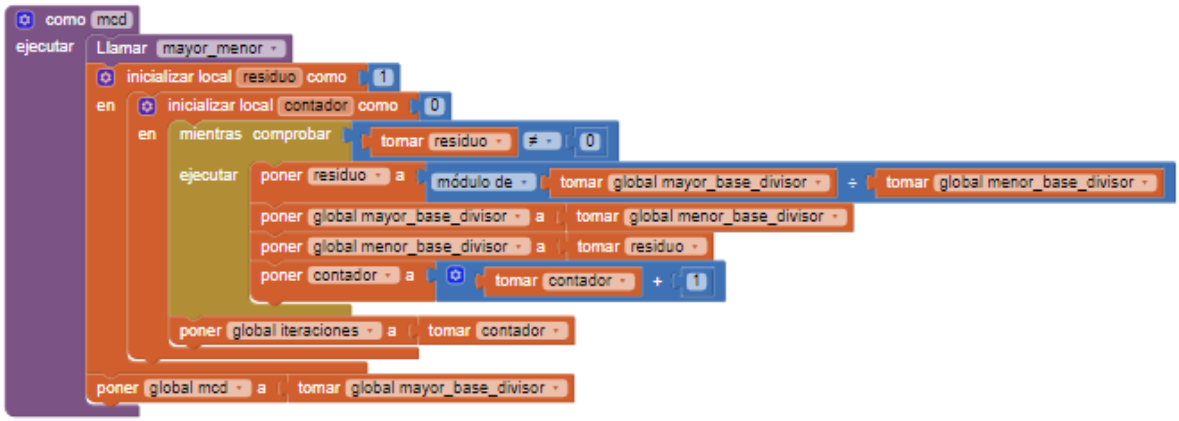


Ilustración 9:Bloques para determinar el máximo común divisor de la base y el posible divisor

En la Ilustración 10 se puede observar parte de los bloques que se usaron para determinar la combinación lineal del máximo común divisor de la base y el posible divisor. Este describe el algoritmo presentado en **T26.**

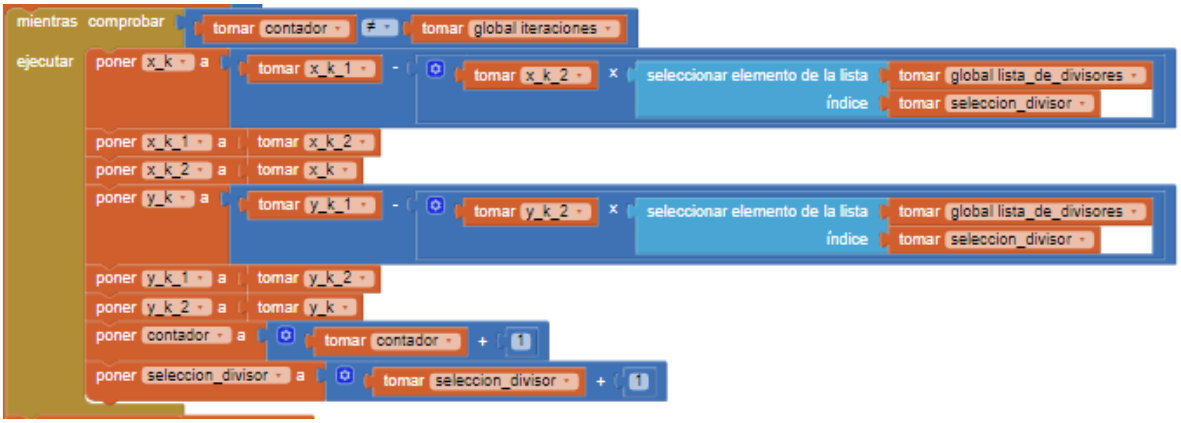


Ilustración 10: Bloques para determinar la combinación lineal del máximo común divisor

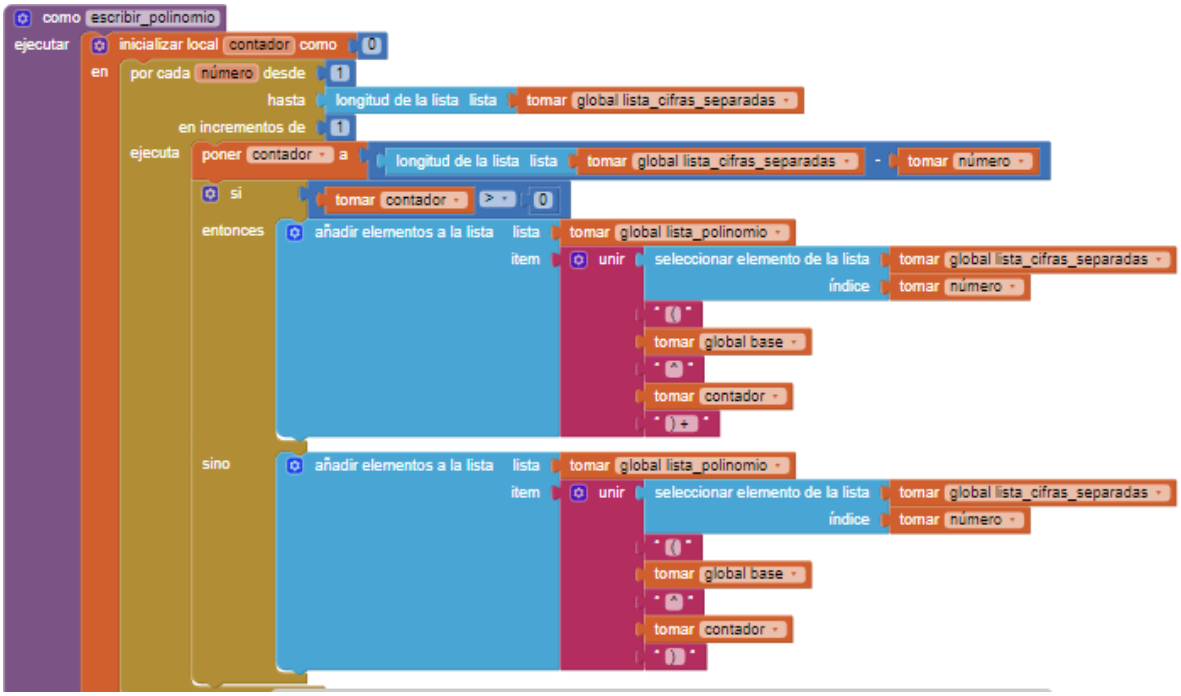


Ilustración 11: Bloques para escribir la forma polinómica de un número

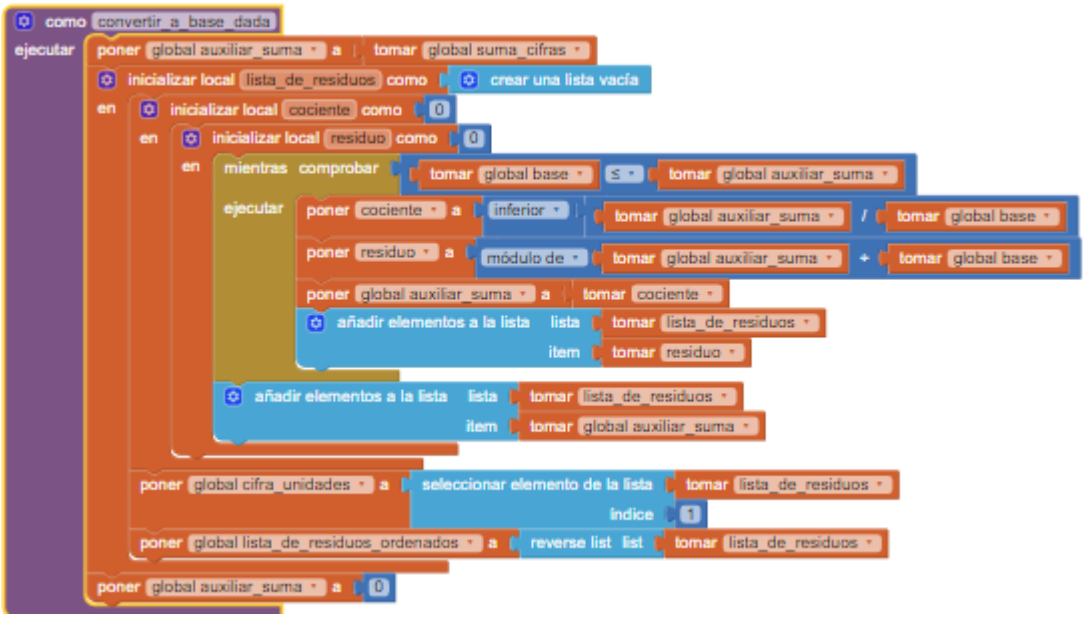


Ilustración 12: Bloque para escribir un número a la base dada

En el siguiente link se puede ver un tutorial de la aplicación

https://youtu.be/Buj9WGiE7G0

Mediante el siguiente código QR se puede descargar la aplicación

O mediante el siguiente link se puede descargar desde la Play Store

https://play.google.com/store/apps/details?id=appinventor.ai_grupoalgebraupn.Algoritmo_unico_de_divisibilidad

4. Conclusiones

En este apartado se presentan las conclusiones del trabajo, las cuales están direccionadas a los objetivos del estudio, las limitaciones/fortalezas y falencias que se presentaron y, los aportes de dichos resultados a la formación en Educación Matemática.

4.1. Respuesta a los objetivos

Los dos teoremas fundamentales propuestos en este trabajo *algoritmo parcial de divisibilidad* (**APD) y** *criterio de la cifra de las unidades* (**CCU)** fueron las piezas claves que permitieron dar cumplimiento parcial con el objetivo general. Al usar estos dos algoritmos "combinados", se determinó un algoritmo general que considera cualquier número escrito en cualquier base, dado un posible divisor para determinar la divisibilidad de un número por otro.

El algoritmo descrito en **APD** no recogió todos los posibles casos (los casos en que el máximo común divisor de la base y el posible divisor no divida a la cifra de las unidades), para determinar un método general para encontrar criterios de divisibilidad y al intentar encontrar un método que determinara criterios de manera análoga a los casos en los que sí funciona el algoritmo, surgió **CCU**, el cual permite descartar que el posible divisor divide a este número.

Con esto se llegó a un algoritmo que determina criterios de divisibilidad bajo una restricción (**APD**), por lo tanto, no podemos decir que es general, pero sí se encontró un algoritmo general para determinar la divisibilidad de un número dado y un posible divisor (**AUD**).

Estos algoritmos se pudieron llevar a una *App*, la cual permite ver los resultados de la combinación de ambos algoritmos aplicados a casos particulares, donde el usuario puede ingresar un número escrito en cualquier base, la base y el posible divisor y así, obtener un criterio de divisibilidad que se cumpla para estas condiciones. La *App* permite ver no solo el criterio, sino que también da a conocer la unión de ambos algoritmos, nombrado ***Algoritmo único de divisibilidad;*** de acuerdo con lo anterior, se puede garantizar el cumplimiento parcial del objetivo general de este trabajo.

Además, teniendo en cuenta los planteamientos de Osorio, K., & Castañeda, E. (2014) y Ruíz, F., & Carvajal, J. (2002), junto con la revisión de los principales teoremas de divisibilidad, se pudo llegar a la demostración del ***Algoritmo único de divisibilidad,*** donde su forma final fue:

Algoritmo parcial de divisibilidad (**APD)**	***Criterio de la cifra de las unidades*** (**CCU)**
Sea $n, x, y \in N$ escrito en base x con $n = xP + u$, y $mcd\ (x, y)\|u$ entonces $y\|n$ si y solo si $r\|(P + ms)$.	Sean $n, y \in N$ con $n = xP + u$ en base x. Si $y\|n$ entonces $mcd\ (x, y)\|u$.

Algoritmo único de divisibilidad

Teniendo en cuenta que $n, y \in N$, n escrito en base x y $n = xP + u$. Se puede determinar si $y|n$ o $y \nmid n$ mediante los siguientes pasos:

1. Determinar el $mcd\ (x, y)$
2. Comprobar si el número del paso anterior divide a u. Si es así proceda con los siguientes pasos, sino entonces el número no es divisible por y.
3. Reescriba el $mcd\ (x, y)$ como una combinación lineal de la base y del presunto divisor, es decir, $mcd\ (x, y) = mx + ny$.
4. El número m obtenido en el paso 3 se debe multiplicar por s. Donde s resulta de $u = mcd\ (x, y)(s)$.
5. Sume el número obtenido en el paso 4 con P (el número n sin la cifra de las unidades). Si esta suma es múltiplo de r donde r se obtiene de $y = mcd\ (x, y)(r)$, entonces $y|n$. En caso contrario $y \nmid n$.

Tabla 8: Algoritmo general de divisibilidad

Es interesante el resultado de **CCU** que permite hacer una inspección casi "superficial" para descartar una infinidad de números que no son divisibles por un número dado con solo "mirar" la cifra de las unidades, además que permite acotar los posibles candidatos a ser divisibles. Algo que no se esperaba de este proceso, era determinar si un número es múltiplo

de otro, teniendo que comprobar la divisibilidad por un número menor al presunto divisor dado; usualmente con los métodos estudiados previamente, los autores consideraban al mismo posible divisor y así construir la condición para caracterizar la divisibilidad de un número. Es importante aclarar que se pueden obtener una infinidad de criterios para una misma base y posible divisor teniendo en cuenta el **APD**, porque es posible escribir infinitas combinaciones lineales iguales al máximo común divisor, debido al tipo de ecuaciones diofánticas que se obtienen en dicho algoritmo.

4.2. Limitaciones y falencias del estudio

El método descrito en este trabajo para determinar criterios de divisibilidad puede ser más largo que aplicar el algoritmo de la división para saber si un número es divisible o no por un número dado. Cabe aclarar que no se pretendía encontrar un resultado que reemplazara dicho algoritmo ni los resultados relacionados a determinar criterios; en ese orden de ideas, se hace evidente que en el proceso para usar el *algoritmo único de divisibilidad* se debe determinar el máximo común divisor de la base y el posible divisor y, una combinación lineal de estos dos para poder ejecutarlo. Puede tomar mucho tiempo si se usa el algoritmo de Euclides o procesos de ensayo y error para determinar la combinación lineal, así al dar un buen uso a herramientas tecnológicas es posible calcularla de manera más rápida, comprender los algoritmos relacionados a la divisibilidad e ir más allá de un resultado (Sánchez, 2002).

Aunque se pudo traducir el algoritmo desde un lenguaje matemático a un lenguaje de programación en la *App*, es evidente que este presenta falencias al mostrar algunos pasos, debido a que algunos números que muestra la *App* están entre paréntesis (cuando no es necesario) y también muestra números con el formato de número decimal (una representación de los números racionales), que aunque son equivalentes a los valores esperados, no se deberían presentar así ya que se están considerando solo números enteros. Esto ocurre por ejemplo cuando se espera obtener una expresión cómo la que sigue $2548 - 4 = 2544$, la

App arroja el siguiente resultado $(2548) - (4) = (2544.0)$. Esta es una limitación desde el planteamiento teórico inicial de trabajar con un solo conjunto numérico (ver *imagen 13*).

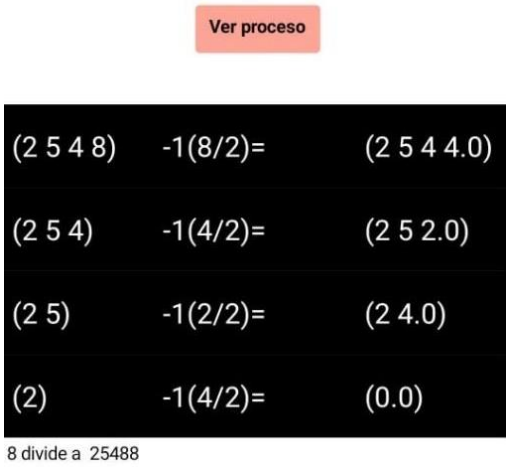


Ilustración 13: Captura de la App en donde se aplica el criterio

4.3. Aportes y proyecciones a la formación en educación matemática

El desarrollo del trabajo desde el aspecto matemático permitió construir una base para la formación profesional donde el rigor de la escritura y la construcción de una demostración fueron fundamentales; además, permitió evaluar y repensar la manera en que se comunican las ideas matemáticas, así como también desarrollar habilidades lectoescritoras y matemáticas. Ahora bien, desde el aspecto tecnológico es un avance enorme por el hecho de llevar un lenguaje matemático a un lenguaje de programación, donde el usuario que desee hacer uso de la *App* tenga la posibilidad de interpretar, comparar, entender e interactuar con los criterios que el Algoritmo general le arroje.

Como maestro en formación, este trabajo me permitió cuestionar cada proceso encontrado al momento de determinar criterios de divisibilidad y me ayudó a desarrollar una actitud de permanente inquietud, cuestionando cada algoritmo para obtener criterios, lo cual considero que nutre mi conocimiento en matemáticas y el hecho de llevarlo a un software me ayudó a ejercitar las nociones de programación adquiridas en la carrera y conocer mejor este entorno para hacer aplicaciones; considero completamente oportuno y eficiente este trabajo, ya que

permite mejorar mis acciones y prácticas como docente en donde el pilar en la enseñanza de las matemáticas sea la apropiación de conceptos matemáticos aplicados a otras ciencias como la programación.

En cuanto a la interfaz de la aplicación, me llamó mucho la atención el diseño del software de *App*-Inventor, como docente en formación considero que los bloques, sus colores y la facilidad para manipularlos, lo hace una herramienta muy atractiva y dinámica para cualquier usuario. Esto puede ser una forma de motivar a los estudiantes de temprana edad a estudiar temas de matemáticas de manera indirecta, al promoverse la construcción de aplicaciones donde se pueda ejecutar algunos conceptos y procesos matemáticos (Ángel y Bautista, 2001).

Por último, espero que este trabajo pueda ser de utilidad para próximas consultas bibliográficas de estudiantes no solo de la Licenciatura en Matemáticas de la Universidad Pedagógica Nacional, sino para otras personas que estén en proceso de formación en el campo de las Matemáticas y afines que estén en búsqueda de respuestas asociadas a criterios de divisibilidad en diferentes bases numéricas, su aplicación en entornos virtuales y el análisis de algoritmos respectivos; aún queda abierta la puerta para pensar otros algoritmos, viendo el potencial de reescribir la forma polinómica de un número, esto se hizo evidente en los resultados de este trabajo y así mismo buscar relaciones o generalidades de los criterios demostrados en esta propuesta; también es posible minimizar el código de programación, ejecutándolo en cualquier otro Software.

Referencias

Ángel, J., & Bautista, G. (2001). Didácticas de las matemáticas en enseñanza superior: La utilización de software especializado. Recuperado el 12 de enero de 2005, de http:// www.uoc.edu/web/esp/art/uoc/0107030/mates.html

Crawford Pokress, S., & Dominguez Veiga, J. J. (2013). *MIT App Inventor: Enabling Personal Mobile Computing*. *arXiv*, arXiv-1310.

Cuicas, M., Debel, E., Casadei, L. & Alvarez, Z. (2007). El software matemático como herramienta para el desarrollo de habilidades del pensamiento y mejoramiento del aprendizaje de las matemáticas. *Actualidades Investigativas en Educación*, 7(2), 1 - 36. https://www.redalyc.org/articulo.oa?id=44770209

Díaz, F., & Hernández, G. (2002). *Estrategias docentes para un aprendizaje significativo: Una interpretación constructivista* (2a ed.). México, D.F.: McGrawHill Interamericana

González, F. (2004). *Apuntes de Matemática discreta. Divisibilidad. El algoritmo de la división.* Cádiz, España: Universidad de Cádiz.

Hardy, G.H.; Wright, E. M. (2008). *An Introduction to the Theory of Numbers* (en inglés) (6ª edición). Oxford University Press. ISBN 978-0-19-921986-5.

Martín, J. (2001). Enseñanza de procesos de pensamiento: Metodología, metacognición y transferencia. Recuperado 12 de febrero de 2005, de http://www.uv.es/RELIEVE/v7n2/RELIEVEv7n2_2.htm

MIT App Inventor. (s.f.). Obtenido de https://*App*inventor.mit.edu

Osorio, K., & Castañeda, E. (2014). Criterios de divisibilidad en diferentes bases. *(Tesis pregrado para optar título de licenciado en matemáticas).* Universidad Pedagógica Nacional, Bogotá, Colombia.

Rubiano, G., Jiménez, L., & Gordillo, J. (2004). *Teoría de números para principiantes* (segunda ed.). Bogotá, Colombia: Pro-Offset Editorial Ltda.

Ruíz, F., & Carvajal, J. (2002). Un criterio universal de divisibilidad.

Sánchez, M. (2002). La investigación sobre el desarrollo y la enseñanza de las habilidades de pensamiento . *REDIE. Revista Electrónica de Investigación Educativa*, 4(1), . ISSN: . Disponible en: https://www.redalyc.org/articulo.oa?id=15504108

Zalamea, F. (2008). *Fundamentos de Matemáticas* (Primera ed.). Bogotá, Colombia: Universidad Nacional de Colombia, Unibiblos.