Índice general

Capítulo 1

INTRODUCCIÓN

"Desde la linde a la espesura de un bosque conducen muchos senderos. Son sinuosos, se juntan, se separan de nuevo y se cruzan. Paseando podemos notar su gran cantidad, recorre algunos de ellos y ver cómo se internan en las frondas.
Si se quiere estudiar seriamente un bosque es necesario seguir sus senderos mientras se los pueda distinguir entre la pinocha seca y las mas pequeñas matas de arándano. Para poder aprovechar los dones del bosque hay que abandonar por completo los caminos trillados y abrirse paso a través del entrelazamiento de ramas espinosas"(Vorobiov; p. 3; 1975).
La presente Monografía puede considerarse como descripción de uno de los posibles paseos por la linde de las matemáticas contemporáneas. La exposición de los datos básicos referentes a la divisibilidad, nos obliga a incluir en esta monografía algunas cuestiones bastante abstractas de las matemáticas discretas. A estas pertenecen las propiedades de la teoría elemental de números que están agrupadas en torno al análisis de las descomposiciones un número en sus factores primos, luego la propia divisibilidad de los números se examina como una relación definida en el conjunto de los enteros y finalmente, los criterios de divisibilidad se tratan aquí como algoritmos que transforma cada número en respuesta a la interrogación, ¿se divide o no por el número dado?
Además que para el estudiante de secundaria de nuestro medio, le es dificultoso familiarizarse con las matemáticas, es más se podría afirmar que para muchos de ellos existe un abismo entre la matemática y ellos, esta afirmación se saca de la misma experiencia pedagógica que viven los estudiantes de matemáticas del INSSB en el módulo de práctica docente.

Razones para el surgimiento de este problema en la enseñanza de la matemática hay muchas como la falta de interés del alumno, el pésimo control de los padres de estos en su educación, la poca prioridad que da el Estado a la educación, la poca preparación del docente, etc.

Capítulo 2

PRESENTACIÓN DEL TEMA DE ESTUDIO

2.1. Metodología

El método descriptivo

"El objeto de la investigación descriptiva consiste en describir y evaluar ciertas características de una situación particular en uno o más puntos del tiempo" (Hayman, p. 92). En la investigación descriptiva se analizan los datos reunidos para descubrir así, cuáles variables están relacionadas entre sí. Sin embargo, "es habitualmente difícil interpretar qué significan estas relaciones.

El investigador puede interpretar los resultados de una manera, pero desgraciadamente ésta será a menudo sólo una de las varias maneras de interpretarlos". (Hayman, p. 135).

La metodología que se utilizó en este análisis es el método descriptivo, que se utiliza para recoger, organizar, presentar, analizar, los resultados de las observaciones.

"Este método implica la recopilación y presentación sistemática de datos para dar una ideas clara de una determinada situación. Las ventajas que tiene este estudio es que la: metodología es fácil de corto tiempo y económica. En el estudio descriptivo el propósito del investigador es describir situaciones y eventos. Esto es, decir como es y se manifiesta determinado fenómeno."(Zorrilla, p.53, 1996)

En la presente investigación monografica en el que es preciso analizar, estudiar y exponer

ideas ya establecidas, mediante la recolección de datos, un sistema de fichas, además de la revision de cuadernos de resúmenes y organizándola para presentarla finalmente en el presente trabajo.

2.2. Objetivos

2.2.1. Objetivo general

Hallar el algoritmo de la divisibilidad, por el que se pueda determinar la divisibilidad de un número por otro.

2.2.2. Objetivos específicos

- ⋆ Revisar un conjunto de teorías que hablan acerca de la divisibilidad.
- ⋆ Describir las propiedades elementales de los números enteros, que facilitaran el estudio de la teoría de la divisibilidad.
- ⋆ Describir las propiedades de la división, que nos permita determinar la divisibilidad de un número por otro.
- ⋆ Elaborar las conclusiones finales.
- ⋆ Proponer un conjunto de recomendaciones, que permitan facilitar el estudio de la divisibilidad, en el proceso de Enseñanza y Aprendizaje.

2.3. Justificación

La importancia de este trabajo monografico encuentra sentido en que es necesario que el maestro pueda mejorar el trabajo docente mediante una investigación mucho más profunda de la matemática. De ahí que parte del aporte que se quiere hacer con el presente trabajo descriptivo, es el de sugerir que el maestro este más preparado, más actualizado en su área. “Como todos los educándos los maestros mismos deben recibir ayuda para su aprendizaje si es que van a adquirir la capacidad de ayudar al aprendizaje de sus

alumnos."(MOLL, p. 236); además que la propia Reforma Educativa que dice "**Articulo 14º** La carrera docente depende del constante mejoramiento en actualización permanente y formación profesional. [...] "(Ley 1565, R.E., DS 23968, 24 de febrero de 1995, p.139), de esto podemos decir que no sólo el alumno esta en la responsabilidad de aprender y el maestro en enseñarle, sino que el maestro esta en la obligación de saber mucho mas que el alumno; aportando de esta manera a la Educación secundaria .

Por otro lado es importante estudiar "divisibilidad", pues al desarrollar un número mediante productos, permiten escribir números con pocas cifras, que nos permitan operar rápidamente con ellos, factorizar un número, conocer sus divisores además de estudiar sus propiedades. También es preciso decir que Factorizar es una forma de expresar un número mediante productos de números primos, proporcionando información considerable sobre el número, sus divisores y sus múltiplos, acción que se ejecuta en cualquier rama de la matemática y principalmente en los primeros niveles de secundaria donde el estudiante toma sus primera armas para enfrentar posteriormente a una matemática mas abstracta. Además que el estudio de la teoría de números, es uno de los principales ejemplos de matemática pura, que, si es estudiado con interés por parte del estudiante le sera de gran utilidad en la transición de este a la universidad.

Ahora *¿De que hablamos, cuando hablamos de divisibilidad?*

En muchas situaciones los docentes responden al planteamiento anterior en términos muy simples: de criterios de divisibilidad (por 2, por 3, etc.), de descomposición de un número en factores primos para calcular el máximo común divisor o el mínimo común múltiplo de dos números, y ya. Y todo lo anterior tratado de una forma práctica, reducida a cómo se hacen las cosas, a las reglas correspondientes a cada caso.

Sin embargo y como lo iremos viendo a lo largo de este trabajo monografico, el tema de la divisibilidad se refiere al estudio de los números enteros, es decir, pensando en que todo número entero siempre puede describirse como producto de varios factores. De esta consideración tan sencilla y de la curiosidad e intuición de algunas personas arrancó en la historia de la matemática un estudio muy amplio que abarca conceptos, relaciones, propiedades, regularidades y también aplicaciones.

Es importante porque el alumno experimenta de manera concreta el trabajo matemático que realiza un "matemático puro", la teoría de la divisibilidad es importante porque el alumno trabaja en un contexto netamente matemático, donde ve de que manera se aplica

las propiedades de los números enteros para encontrar otras propiedades.

Capítulo 3

EL ESTUDIO DE LA DIVISIBILIDAD (Fundamento teórico)

3.1. Problema

El problema detectado es, que se requiere demostrar o describir el algoritmo de la división, es así que nos planteamos en la presente investigación descriptiva: ¿Es posible hallar y/o demostrar la divisibilidad de un número entero hacia otro entero?
Nos planteamos la interrogante a partir de lo siguiente: Es claro que existe un Algoritmo de la división "$a = bq+r$", donde la división de un número por otro es exacta o inexacta, pero sólo para un número determinado, pero no tenemos un criterio general de la divisibilidad de un número, donde el número es divisible por algún otro.
Luego, a partir de una investigación descriptiva, recogiendo información,
analizando llegaremos a exponer los resultados a que llegará este estudio de la Teoría de la Divisibilidad.

3.2. Consideraciones preliminares

3.2.1. Propiedades Básicas de (+, *)

En los enunciados que siguen sean a, d, c y d elementos cualesquiera de $\mathbb{Z}$

Propiedades de la igualdad

Reflexividad: $a = a$ para todo a.
Simetría: Si $a = b$, entonces $b = a$
Transitividad: Si $a = b$ y $b = c$, entonces $a = c$.

Propiedades de la suma y de la multiplicación

Bien definida: Si $a = b$ y $c = d$, entonces $a + c = b + d$ y $a \times c = b \times d$.
Cerrada: $a + b \in \mathbb{Z}$ y $a \times b \in \mathbb{Z}$.
Conmutatividad: $a + b = b + a$ y $a \times b = b \times a$.
Asociatividad: $(a + b) + c = a + (b + c)$ y $(a \times b) \times c = a \times (b \times c)$.
Identidad: Existe un elemento 0 tal que $a + 0 = 0 + a = a$; existe un elemento 1 tal que $a \times 1 = 1 \times a = a$.
Inverso: Para cada a existe un elemento $-a$ tal que $a + (-a) = (-a) + a = 0$.
Cancelación: Si $a \times c = b \times c$ cuando $c \neq 0$, entonces $a = b$.
Distributividad: $a \times (b + c) = (a \times b) + (a \times c)$; $(b + c) \times a = (b \times a) + (c \times a)$.

Propiedades de la desigualdad ($a < b \Leftrightarrow b > a$)

Tricotomía: Para cada par de elementos a y b, sólo uno de los siguientes enunciados es verdadero:

$$a < b,\ a = b,\ \text{ó}\ b < a.$$

Suma: Si $a < b$, entonces $a + c < b + c$
*Multiplicación:*Si $a < b$y $c > 0$, entonces $a \times c < b \times c$.
Transitividad: Si $a < b$ y $b < c$, Entonces $a < c$
Muchos de los teoremas pueden ser demostrados cómo consecuencias de las propiedades

básicas de la igualdad, suma y multiplicación; entre ellos están los siguientes:
Propiedad del cero de la multiplicación: $a \times 0 = 0$
Producto cero: Si $a \times b = 0$, entonces $a = 0$ o $b = 0$

Principio del buen orden (P.B.O.)

Todo subconjunto no vacío de los enteros ($\mathbb{Z}^+$) positivos tiene un elemento mínimo.
El principio del buen orden nos garantiza que cualquier subconjunto del conjunto de los enteros que contiene solo números positivos, contiene un entero positivo menor menor que todos los demás. Por ejemplo, el conjunto de los enteros positivos pares tiene un menor elemento, el 2.
Sea el subconjunto

$$S \subset \mathbb{Z}^+ \Rightarrow \exists a \in S : a \leq s; \forall s \in S$$

Obs:

- El axioma no es valido en todo $\mathbb{Z}^+$ porque no puede haber un entero negativo menor.
- El axioma no es valido en $\mathbb{Q}$

3.3. Divisibilidad

Divisibilidad, es parte de la teoría de los números que estudia las condiciones que debe reunir un numeral para ser divisible entre otro y las consecuencias que de este hecho se derivan.
"El estudio de las propiedades de los números enteros positivos es el objetivo central de la teoría de números: Teoría Elemental, Teoría Analítica, Teoría Algebraica "(De oliveira, Plinio; p. 2; 2000)
En esta monografía nos limitamos a la parte elemental, donde se presenta demostraciones básicas, que según Plinio de Oliveira son necesarias para el estudio de las partes Analítica y Algebraica, como también para las demás ramas de las matemáticas.
Estudiaremos las propiedades elementales de la divisibilidad en el conjunto de los enteros, siendo el algoritmo de la división el enunciado mas importante, pues a partir del cual,

podremos pasar a estudiar los Números Primos, el MCD (Máximo común divisor), además del algoritmo euclidiano, para finalmente llegar a Los Criterios de divisibilidad

3.3.1. Divisibilidad entre números naturales

Calcular el cociente 12:3 o 12/3, o dividir 12 por 3, significa hallar un número tal que da resultado 12 si se multiplica por tres.

Entonces 12:3=4 puesto que 12=4·3

y en general

a:b=c significa que a=c·b.

En palabras, y con referencia a números naturales, tenemos:
Dados dos números naturales a y b llamados respectivamente ***dividendo*** *y* ***divisor****, se llama* ***cociente*** *a:b o a/b a un número c,* ***si existe****, tal que da como resultado el dividendo si se lo multiplica por el divisor: a=c·b.*

3.3.2. Algoritmo de la división

Teorema. Sea a, b enteros donde $b > 0$ *entonces existen únicos enteros q y r tal que*

$$a = b \cdot q + r,\ 0 \leq r < b$$

Dem.
Sean a,b enteros fijos con $b \neq 0$. Consideremos todos los enteros de la forma $a - bx$, donde $x \in \mathbb{Z}$. Primero mostraremos que algunos de estos enteros deben ser no negativos.
Hay dos posibilidades:

1. Si $a \geq 0$, entonces $a - b \cdot 0 = a \geq 0$. Así que $a - bx$ es no negativo para $x = 0$ en este caso.

2. Si $a < 0$, entonces $-a > 0$, ya que b es un entero positivo, debemos tener $b \geq 1$. multiplicando esta ultima desigualdad por el número positivo $-a$, muestra que $b(-a) \geq -a$, o equivalente, $a - ba \geq 0$. Así que $a - bx$, es no negativo cuando $x = a$ en este caso.

Luego el conjunto S de todos los enteros no negativos de la forma $a - bx$, con $x \in \mathbb{Z}$, es no vacío.

Por el principio del buen orden, S contiene un elemento mínimo llamemoslo r. Ya que $r \in S$, r es de la forma $a - bx$ para que algún x, digamos $x = q$. Así que hemos encontrado q y r tal que:

$$r = a - bq, \text{ ó equivalentemente, } a = bq + r.$$

Como $r \in S$, sabemos que $r \geq 0$. Ahora mostraremos que $r < b$. Supongamos lo contrario, que $r \geq b$, entonces $r - b \geq 0$, así que:

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

Ya que $a - b(q + 1)$ es no negativo, es un elemento de S por definición. Pero como b es positivo, se tiene que $r - b < r$. Así que

$$a - b(q + 1) = r - b < r$$

La última desigualdad establece que $a - b(q + 1)$ es un elemento de S y menor que r, el menor elemento de S. Esto es una contradicción, así que se puede tener que $r < b$. Luego encontramos enteros q y r tal que $a = bq + r$ y $0 \leq r < b$.

Para completar la prueba, debemos mostrar que q y r son únicos con esta propiedad (Esto es lo que "único´´ significa en la proposición del teorema). Para hacer esto, supongamos que para algunos enteros q_1 y r_1, también tenemos $a = bq_1 + r_1$, con $0 \leq r_1 < b$, entonces probamos que $q = q_1$ y $r = r_1$. Es claro que ó $r \geq r_1$ ó $r_1 \geq r$, sin perder generalidad consideramos $r \geq r_1$. Usando sustracción tenemos:

$$\begin{aligned} a &= bq + r \\ -a &= -bq_1 + (-r_1) \end{aligned}$$

$$\hline$$

$$0 = bq - bq_1 + r - r_1$$

Así tenemos:

$$\begin{aligned} bq_1 - bq &= r - r_1 \\ b(q_1 - q) &= r - r_1 \end{aligned}$$

Esta última ecuación dice que $r - r_1$ es un entero múltiplo de b, pero $b > 0$ y $r - r_1 \geq 0$ (ya que $r \geq r_1$), y así $q_1 - q$ debe ser un entero no negativo . Luego $r - r_1$ es uno de estos: 0b, 1b, 2b, 3b, ..., etc. Pero $0 \leq r_1 \leq r < b$, así que la diferencia $r - r_1$ es también menor estricto que b, ya que $0b < 1b < 2b < 3b < ...$, la única posibilidad es que $r - r_1 = 0b = 0$. Luego $r = r_1$. Finalmente, ya que $b(q_1 - q) = r - r_1 = 0$ y $b > 0$, debemos tener $q - q_1 = 0$, así que $q = q_1$.

Ejercicios:

1. Sea $n \in \mathbb{Z}^+$, probar que a y c dejan el mismo resto cuando son divididos por n si y solo si : $a - c = nk$, $\exists k \in \mathbb{Z}^+$
   Dem. Si a y c dejan el mismo resto cuando son divididos por n entonces tenemos que probar que: $a - c = nk$, $\exists k \in \mathbb{Z}^+$
   En efecto :

   $$\begin{aligned} a &= nq_1 + r_1, && \text{con } 0 \leq r_1 < n; \\ c &= nq_2 + r_2, && \text{con } 0_2 < n; \end{aligned}$$

   Pero por hipótesis $r_1 = r_2$, así que:

   $$r_1 = a - nq_1 \text{ y } r_2 = c - nq_2$$

   luego:

   $$\begin{aligned} a - nq_1 &= c - nq_2 \\ a - c &= nq_1 - nq_2 \\ a - c &= n(q_1 - q_2), && de aqui\ q_1 - q_2 = k \\ a - c &= nk_{\square} \end{aligned}$$

2. Use el algoritmo de la división para probar que todo entero impar de la forma $4k+1$ ó $4k + 3$ para algún entero k.
   Dem. Sea a un entero impar cualquiera y dividamos a entre 4 es decir:
   $a = 4k + r$, $0 \leq r < 4$

$$r = 0, \qquad r = 1, \qquad r = 2, \qquad r = 3$$

Entonces reemplazando tenemos que:
$a = 4k + 0$, no impar, pues es de la forma par $a = 4k$
$a = 4k + 1$,✓
$a = 4k + 2$, $\Rightarrow$, $a = 2(2k + 1)$,no impar, pues es de la forma par $a = 2k$.
$a = 4k + 3$ ✓
Así $a = 4k + 1$ o $a = 4k + 3$

3.3.3. Divisibilidad

Definición:
Sean a y b enteros con $b \neq 0$. Decimos que b divide a a (ó que b es un divisor de a ó que b es un factor de a ó a es múltiplo de b) si $a = bc$ para algún entero c, en símbolos "b divide a a" se escribe $b \mid a$ y "b no divide a a" se escribe $b \nmid a$.
Obs.

i a y $-a$ tienen los mismos divisores.

ii Todo divisor de a es menor o igual a $|a|$

iii Un entero no nulo tiene un número finito de divisores.

3.3.4. Primos y factorización única

Todo entero n $\neq \pm$ 1 tiene por lo menos 4 divisores, los cuales son ± 1, $\pm n$, ahora los enteros que tienen solo estos 4 divisores, constituyen una parte importante dentro de la teoría de números, a estos los llamamos números primos.
Definición.: Un entero P se dice que es primo si y solo si, sus únicos divisores son ± 1 y $\pm p$
Ejemplo:
Si a, b y c son enteros tales que $a \cdot b = c$, entonces se dice que a y b son **factores o divisores** de c, y que c es un **múltiplo** de a y b. Como $3 \cdot 4 = 12$ el número 3 es un factor

de 12, y el 12 es un múltiplo de 3. También 4 es un factor de 12 y 12 es un múltiplo de 4. El número 12 tiene otros factores. Por ejemplo, -2, ya que $(-2) \cdot (-6) = 12$.
Usaremos el símbolo d|c para denotar que d es un factor o divisor de c. Si d no es un factor de c, escribiremos d$\nmid$c.
Consideremos ahora los enteros positivos mayores que 1, esto es, 2, 3, 4, ...Cada uno de estos enteros puede ser clasificado como un *numero primo* o como un *número compuesto*. Un entero positivo p mayor que 1 se dice que es un número **primo** o simplemente un primo, si los únicos enteros positivos factores de p son 1 y p. Un entero positivo mayor que 1 que no es primo se dirá que es un número **compuesto,** o simplemente un compuesto, esto es, un número compuesto es un entero positivo n que posee factores positivos diferentes de 1 y n. El 5 es un número primo, ya que sus únicos factores posibles son 1 y 5. En cambio, 10 es un número compuesto, pues el 2 es un factor de 10 y $2 \neq 1$ y $2 \nmid 10$. Como el 1 no es ni primo ni compuesto, tenemos que cada número del conjunto de los enteros positivos es o un primo o un compuesto, o igual a 1.

Teorema : *Todo entero $n \neq 0, \pm 1$, es un producto de primos*

Dem.:
Supongamos que el teorema es falso; es decir, existe un entero $m \neq 0, \pm 1$ que no es un producto de primos, es decir que no se puede factorizar en producto de primos.
Luego, consideremos el conjunto de todos los enteros no negativos que son producto de primos y llamemoslo S, y por lo anterior $S \neq \varnothing$ pues $m \in S$, pero por el P.B.O. sabemos que S tiene un elemento mínimo, supongamos m_0, es decir $m_0 \leqslant m$, ahora ¿m_0 es primo o no lo es?, pues tenemos m_0 no es primo ya $m_0 \in S$, asi $m_0 = ab$, $0 < a < m_0$ de ahi que a, b no pertenece a S, entonces a es producto de primos y b también. Entonces m_0 es producto de primos es decir m_0 no pertenece a S, pero esto es falso, ya que m_0 es el elemento mas pequeño de S, lo cual es una contradicción.
Luego, el teorema esta probado.

3.3.5. Propiedades de los números primos

El problema de encontrar todos los primos menores que un número dado n se torna muy difícil cuando n es grande. En verdad, para valores extremadamente grandes de n,

el trabajo sería casi imposible desde el punto de vista práctico. Existen varias listas de tales primos para valores de n asta aproximadamente 10^7, que son completas y dignas de confianza.

Una técnica llamada la **criba de Eratóstenes,** en honor al matemático griego eratóstenes (256-194 A.C.), representa un método razonable para obtener una lista completa de primos menores o iguales que n, cuando n es relativamente pequeño. Esta técnica consiste en escribir una lista de los enteros entre 2 y n, para tachar cada segundo número después del 2, es decir4, 6, 8, ..., ya que cada uno de tales números contiene como factor a 2, y por tanto es compuesto. Continuamos eliminando cada tercer número después 3, es decir, 6, 9, 12, ..., ya que ellos son números compuestos; repetimos la operación eliminando cada quinto número después del 5, cada séptimo número después del 7, ... Muchos números son tachados más de una vez. El proceso termina cuando todos los múltiplos de p distintos de p, para todo primo $p \leq \sqrt{n}$ han sido eliminados. Los enteros que quedan después de este tamizado son los primos menores o iguales a n.

La tabla (abajo) muestra el resultado del tamizado para $n = 100$. Los primos menores o iguales que 100 están en los círculos.

La criba de Eratóstenes

PARA $n = 100$

	②	③	4	⑤	6
⑦	8	9	10	⑪	12
⑬	14	15	16	⑰	18
⑲	20	21	22	㉓	24
25	26	27	28	㉙	30
㉛	32	33	34	35	36
㊲	38	39	40	㊶	42
㊸	44	45	46	㊼	48
49	50	51	52	㊸	54
55	56	57	58	㊾	60
㊶	62	63	64	65	66
㊼	68	69	70	㊶	72
㊸	74	75	76	77	78
㊾	80	81	82	㊸	84
85	86	87	88	㊾	90
91	92	93	94	95	96
㊼	98	99	100		

Notar que, excepto por los primos 2 y 3, todo primo en la tabla ocurre en primera o en la quinta columna. Los enteros localizados en esas columnas son de la forma $6k+1$ o $6k-1$, donde k es un entero positivo. Se podría conjeturar que todo primo, distinto de 2 y3, es de la forma $6k+1$ o $6k-1$.

Teorema :*El número de primos es infinito.*

Demostración:
(Por contradicción). Supongamos que existe una cantidad finita de números primos;
es decir: $p_1, p_2, p_3, ..., p_n$ donde p_i es primo; ahora, sin perder generalidad supongamos que: $p_1 < p_2 < p_3 < p_4 < ... < p_{n-1} < p_n$, notemos que p_n es el mas grande primo.

Luego, construyamos el siguiente número:

$$\begin{aligned} A &= p_1 \cdot p_2 \cdot p_3 \cdot \ldots \cdot p_{n-1} \cdot p_n // + 1 \\ A+1 &= (p_1 \cdot p_2 \cdot p_3 \cdot \ldots \cdot p_{n-1} \cdot p_n) + 1 \end{aligned}$$

Ahora A+1 es primo o A+1 es compuesto(no primo);
supongamos que A+1 sea primo entonces vemos que $p_n < A$+1 lo cual es una contradicción ($\Rightarrow\Leftarrow$), pues p_n es el mas grande primo.
Por otro lado si $A+1$ es compuesto tiene mas de 2 divisores, pues los únicos divisores (primos) que tiene $A+1$ diferentes de $A+1$ y 1, son $p_1, p_2, p_3, ..., p_n$, ahora pues notemos que que ninguno de ellos divide exactamente a A+1; pues la division de A+1 entre p_i, con $i = 1, 2, 3, ..., n$, deja resto así llegamos a otra contradicción ($\Rightarrow\Leftarrow$. Por lo tanto llegamos a la conclusión de que el número construido no es primo ni compuesto, con lo que queda demostrado el teorema.

3.4. Máximo Común divisor

En esta sección analizaremos el problema de determinar el mayor de los factores comunes a dos enteros.
Definición Sean a y b enteros no ambos cero, el máximo común divisor (MCD) de a y b es el más grande entero d que divide a a y b, en otras palabras, d es el MCD de a y b, Para demostrar que un entero positivo d es el máximo común divisor de dos enteros a y b, no ambos cero, es suficiente probar que:

(i) $d|a$ y $d|b$
(ii) si $c|a$ y $c|b$, entonces $c \leq d$.

El máximo común divisor de a y b, es usualmente denotado por (a, b)
Por ejemplo, el máximo común divisor de 24 y 78 es 6; esto es,

$$(24, 78) = 6.$$

Notese también que

$$(-24, 78) = (24, -78) = (-24, -78) = 6.$$

Si $a = b = 0$, entonces (a, b) no existe. Si $a \neq 0$ y $b = 0$, entonces (a, b)=$|a|$; si $a = 0$ y $b \neq 0$, entonces (a, b)=$|b|$.
Observaciones:

i $(a, b) \geq 1$

ii $(a, 0) = |a|$

iii Si (a, b)=1 Decimos que a y b son primos relativos o comprimos.

Teorema : *Sean a y b enteros no nulos, y sea d su máximo común divisor, entonces existen (no necesariamente únicos) enteros u y v tal que $d = au + bv$*

Demostración: Sea S el conjunto de todas las combinaciones lineales de a y b, eso es :

$$S = am + bn/m, n \in Z$$

Encontraremos un elemento particular de S y mostraremos que el MCD.
Primero notemos que $a^2 + b^2 = aa + bb$ está en S y $a^2 + b^2 \geq 0$.
Como a y b son ambos no nulos a^2+b^2 debe ser positivo. Luego S contiene enteros positivos y de ahí debe contener un elemento mínimo en S, por el principio del buen orden. Sea t dicho elemento mínimo de S. Por definición de S sabemos que $t = au + bv$ para algunos enteros u y v, afirmamos que t es el MCD de a y b, esto es, $t = d$.

Para probar esto mostraremos que $t|a$. Por el Algoritmo de la División, existen enteros q y r tal que $a = tq + r$, con $0 \leq r < t$. consecuentemente:

$$\begin{aligned} r &= a - tq \\ r &= a - (au + bv)q = a - aqu - bvq \\ r &= a(1 - qu) + b(-vb) \end{aligned}$$

Así que r es una combinación lineal de a y b, y de ahí $r \in S$, ya que $r < t$ (El elemento mínimo positivo de S), sabemos que r es no positivo como $r \geq 0$, la única posibilidad es que $r = 0$.
Luego $a = tq + r = tq + 0 = tq$
Así $t|a$. Un argumento similar muestra que $t|b$. De ahí t es un común divisor de a y b.
Sea c cualquier otro común divisor de a y b, así que $c|a$ y $c|b$ entonces $a = cr$ y $b = cs$, para algunos enteros r y s, consecuentemente

$$t = au + bv = (cr)u + (cs)v = c(ru + sv)$$

La primera y ultima parte de esta ecuación muestra que $c|t$ de donde $c \leq |t|$. Pero t es positivo, así $|t| = t$ y $c \leq t$ esto muestra que t es el Máximo común divisor d

Corolario: Sea a y b enteros no nulos y sea d un entero positivo entonces el MCD de a y b si y sólo si d satisface:

(i) $d|a$ y $d|b$
(ii) si $c|a$ y $c|b$, entonces $c|d$.

Demostración:
Supongamos que $d = (a, b)$.
Entonces $d \geq 1$ y d satisface $i)$ por definición. El ultimo párrafo de la prueba del teorema muestra que (con d en lugar de t) d satisface la condición $ii)$. Recíprocamente supongamos

que d es un entero positivo que satisface las dos condiciones. Entonces d es un divisor común de a y b por i).
Si c es otro divisor común de a y b entonces $c|d$ por ii).
De ahí $c \leq |d|$, pero d es positivo, así $|d| = d$ de donde $c \leq d$, luego d es el máximo común divisor.
Teorema : *El máximo común divisor de dos enteros, no ambos cero, es único.*

Demostración: Si g y g‘ son dos enteros positivos que satisfacen condiciones (i) y (ii) para dos enteros a y b, no ambos cero, entonces $g|g$‘ y g‘$|g$. Por lo tanto, $g = g$‘.

Los dos teoremas anteriores, en conjunto establecen que el máximo común divisor de dos enteros, no ambos nulos, existe y es único; pero ninguno da un procedimiento para determinar el máximo común divisor. Ilustraremos un procedimiento para determinar el máximo común divisor. Ilustraremos un procedimiento en el caso en que ambos enteros sean distintos de 0. Este procedimiento, un *algoritmo*, depende de la propiedad de la division. Un **algoritmo** es un proceso que envuelve el uso repetido de una fórmula o regla u operación tal que la información o resultado obtenido en cada paso es usado en los pasos siguientes hasta que el resultado deseado es obtenido.
Consideremos dos enteros positivos a y b. Sea $a > b$. Entonces, por la propiedad de la división, existen q_i y r_i tales que

$$a = q_1 b + r_1, \text{ donde } 0 < r_1 < b;$$

$$\begin{aligned} b &= q_2 r_1 + r_2, && \text{donde } 0 < r_2 < r_1; \\ r_1 &= q_3 r_2 + r_3, && \text{donde } 0 < r_3 < r_2; \end{aligned}$$

. . . . . .

$$\begin{aligned} r_{k-3} &= q_{k-1}r_{k-2} + r_{k-1}, && \text{donde } 0 < r_{k-1} < r_{k-2}; \\ r_{k-2} &= q_k r_{k-1} + r_k, && \text{donde } 0 < r_k < r_{k-1}; \\ r_{k-1} &= q_{k+1}r_k + 0. \end{aligned}$$

Observar que $r_1, r_2, r_3, ..., r_{k+1}, r_k$ representan una secuencia decreciente de enteros positivos. Como solo existe un número finito de enteros positivos menores que b, el proceso debe terminar; es decir, solo existe un número finito de enteros positivos r_i que satisfacen aquellas condiciones. Este proceso, llamado **algoritmo de Euclides** produce $(a, b) = r_k$. Para demostrar que $(a, b) = r_k$, necesitamos probar que

(i) $r_k|a$ y $r_k|b$
(ii) todo divisor de a y b divide a r_k.

De la ultima ecuación se sigue que $r_k|r_{k-1}$. Sustituyendo $rk - 1$ en la penúltima ecuación,

$$\begin{aligned} r_{k-2} &= q_k q_{k+1} r_k + r_k \\ &= (q_k q_{k+1} + 1) r_k, \end{aligned}$$

Por lo tanto, $r_k|r_{k-2}$. Sustituyendo r_{k-2} y r_{k-1} en la antepenúltima ecuación,

$$\begin{aligned} r_{k-3} &= q_{k-1}(q_k q_{k+1} + 1) r_k + q_{k+1} r_k \\ &= (q_{k-1} q_k q_{k+1} + q_{k-1} + q_{k+1}) r_k \end{aligned}$$

Por lo tanto, $r_k|r_{k-3}$. Continuando en forma análoga, podemos demostrar que $r_k|b$, ya que $r_k|r_1$ y $r_k|r_2$ en la segunda ecuación. Por lo tanto, usando la primera ecuación, $r_k|a$ y entonces la condición (i) es satisfecha; es decir, r_k divide a a y b. Para demostrar que la condición (ii) es satisfecha; sea $d|a$ y $d|b$. Entonces de la primera ecuación se desprende que $d|r_1$; de la segunda ecuación, $d|r_2$; de la tercera ecuación, $d|r_3$; ...; y finalmente, de la penúltima ecuación, $d|r_k$. Por lo tanto, todo divisor de a y b también divide r_k. De aquí que $(a, b) = r_k$.
Si a o b es un número negativo, podemos hacer caso omiso del signo negativo en el algoritmo

de euclides, ya que

$$(a, b) = (a, -b) = (-a, b) = (-a, -b).$$

3.5. Propiedades del máximo común divisor

Se dice que dos enteros a y b, no ambos 0, son **relativamente primos** o primos entre sí, si el máximo común divisor es la unidad; esto es si $(a, b) = 1$. Por ejemplo, 22 y 15 son enteros relativamente primos, aunque ninguno de ellos es primo. En general los $n \geq 2$*enteros* $a_1, a_2, ...,$ y a_n, no todos 0, se dicen **relativamente primos** o primos entre sí, si el máximo común divisor es la unidad; es decir, si $(a_1, a_2, ..., a_n) = 1$. Además, si $(a_i, a_j) = 1$ para cada $i \leq j$ e i, $j = 1, 2, ..., n$, entonces los $n \geq 2$ enteros $a_1, a_2, ...,$ y a_n se dicen **relativamente primos a pares.** Por ejemplo, los tres enteros 5, 10 y 13 son relativamente primos ya que (5, 10, 13)=1; pero ellos no son relativamente primos a pares, puesto que $(5, 10) \leq 1$.
Los siguientes teoremas concernientes a propiedades del máximo común divisor de dos enteros son de cierto interés.

Teorema : *Dos enteros a y b, no ambos 0, son relativamente primos si y solo si existen enteros x e y tales que*

$$1 = xa + yb.$$

Dem.: Si (a, b)=1, entonces por el teorema del MCD existen enteros x e y tales que

$$1 = xa + yb.$$

Si $(a, b) = d$ y $d > 1$, entonces por el teorema del MCD d es el mayor entero positivo que puede ser expresado como función lineal homogénea de a y b. Por lo tanto,

$$1 \leq xa + yb$$

para todo par de enteros x e y. Por lo tanto, el teorema queda demostrado.

Teorema : *Si d=(a, b) entonces* $(\frac{a}{d}, \frac{b}{d}) = 1$.

Dem.: Si $(\frac{a}{d}, \frac{b}{d}) = k$, donde $k \neq 1$, entonces $\frac{a}{d} = ka$‘ y $\frac{b}{d} = kb$‘; esto es, $a = dka$‘ y $b = dkb$‘. Como $dk|a$ y $dk|b$, se tiene $d \neq (a, b)$. De aquí que, si $d = (a, b)$, entonces $(\frac{a}{d}, \frac{b}{d}) = 1$.

Teorema : *Si (a, b)=1 y (a, c)=1, entonces (a, bc)=1.*

Dem.: Si (a, b)=1, entonces, por el teorema del MCD existen enteros x e y tales que

$$1 = xa + yb;$$

si (a, c)=1 entonces existen enteros r y s tales que

$$1 = ra + sc.$$

Entonces

$$\begin{aligned} 1 &= xa + yb(ra + sc) \\ &= (x + ybr)a + (ys)bc. \end{aligned}$$

De aquí que por el teorema de los coprimos, se tiene que (a, bc)=1.

Teorema : *Si* $(a, b_i) = 1$ *para i=1, 2, ..., n, entonces* $(a, b_1b_2...b_n) = 1$. .

Dem.: La demostración es por inducción matemática. Esta dado que $(a, b_1) = 1$. Supongamos ahora que

$$(a, b_1b_2...b_k) = 1.$$

Como $(a, b_{k+1}) = 1$, entonces, por el teorema anterior

$$(a, b_1b_2...b_{k+1}) = 1.$$

Por lo tanto,

$$(a, b_1 b_2 ... b_n) = 1.$$

para cualquier entero positivo n, y el teorema queda demostrado.

Teorema : *Si* $a|bc$ *y* $(a, b) = 1$*, entonces* $a|c$.

Dem.: Si (a, b)=1, entonces, por el teorema del MCD, existen enteros x e y tales que

$$1 = xa + yb$$

Entonces

$$c = xac + ybc.$$

Como $a|bc$ y $a|ac$, se tiene $a|(xac + ybc)$; esto es, $a|c$.

3.6. Criterios de divisibilidad y propiedades elementales de congruencias

Previamente para poder demostrar muchos de los criterios de divisibilidad enunciaremos algunas propiedades de Congruencias que nos podrán ser de mucha ayuda.
La relación de las congruencias módulo m, cuando m es un entero positivo, es una **relación de equivalencia** en el conjunto de los enteros; esto es, la relación de congruencia módulo m es:

1. Reflexiva: $a \equiv a \pmod{m}$ para todo entero a;
2. Simétrica: *sía* $\equiv b \pmod{m}$, entonces $b \equiv a \pmod{m}$ para todo par de enteros a y b;
3. Transitiva: sí $a \equiv b \pmod{m}$ y $b \equiv c \pmod{m}$, entonces $a \equiv c \pmod{m}$ para toda terna de enteros a, b y c.

Algunos teoremas sobre congruencias

1. Sí $a \equiv b \pmod{m}$ y c es un entero, entonces $a + c \equiv b + c \pmod{m}$
2. Sí $a \equiv b \pmod{m}$ y c es un entero, entonces $ac \equiv bc \pmod{m}$
3. Sí $a \equiv b \pmod{m}$ y $c \equiv d \pmod{m}$, entonces $a + c \equiv b + d \pmod{m}$
4. Sí $a \equiv b \pmod{m}$ y $c \equiv d \pmod{m}$, entonces $a - c \equiv b - d \pmod{m}$
5. Sí $a \equiv b \pmod{m}$ y $c \equiv d \pmod{m}$, entonces $ac \equiv bd \pmod{m}$

Para conocer si un número es múltiplo de otro, es decir para averiguar si es divisible por ese otro, no siempre es necesario hacer la división para ver si el cociente es exacto, pues se conocen ciertas características que deben poseer los números para ser múltiplos de otros determinados.

Ahora veremos algunos criterios de divisibilidad. Al conjunto de condiciones que debe cumplir un número cualquiera para ser divisible por otro determinado , se le llama *criterio de divisibilidad* por este último número.

A continuación se enuncian los criterios de divisibilidad más utilizados.

Notación: Para indicar el número tal que : La cifra de las unidades esta representada por a, la cifra de las decenas por b, la cifra de las centenas por c, la cifra de las unidades de mil por d, etc., se utiliza la notación $\underline{dcba}$. El subrayado se efectúa para aclarar que no se trata de un producto, sino de cifras de un número.

Por otro lado:

Sea $n \in N - 0$ y consideremos un $b > 1$, entonces un número n en base b, se representa por el polinomio

$$n = a_k b^k + a_{k-1} b^{k-1} + ... + a_1 b + a_0$$

Donde $0 \leqslant a_i < b$ obsérvese que la precisión es importante

Criterios de divisibilidad por 2. Un entero es divisible por 2 si y sólo si el último dígito de las unidades es par.

Dem: Sea n un entero divisible por 2 es decir: $n = 2 \cdot k$ y

$$n = a_k 10^k + a_{k-1} 10^{k-1} + ... + a_1 10 + a_0$$

Así:

$$2k = a_k 10^k + a_{k-1}10^{k-1} + ... + a_1 10 + a_0$$
$$2k = 10(a_k 10^{k-1} + a_{k-1}10^{k-2} + ... + a_1) + a_0$$
$$2k - 10(\underbrace{a_k 10^{k-1} + a_{k-1}10^{k-2} + ... + a_1}_{\alpha}) = a_0$$
$$2k - 2 \cdot 5(\alpha) = a_0$$
$$2(k - 5(\alpha)) = a_0;$$

Así a_0 es par.

Todo número que termina en cifra par es divisible por 2.
Así, 516, 24, 1968 y 4530, como puede comprobarse son divisibles por 2.
Simbólicamente tenemos:

$$n = \underbrace{\underline{dcba}}_{a \text{ es par}} \Rightarrow n = \mathring{2}$$

Como toda cifra par es múltiplo de , también puede enunciarse:

Un número es divisible por 2 cuando la cifra de sus unidades es múltiplo de 2.

Simbólicamente tenemos:

$$n = \underbrace{\underline{dcba}}_{a=2} \Rightarrow n = \mathring{2}$$

Ejemplos:
Son números divisibles por 2:

- ☞ 1350, pues $0 = \mathring{2}$
- ☞ 278, pues $8 = \mathring{2}$
- ☞ 10002, pues $2 = \mathring{2}$

Criterios de divisibilidad por 5. Un entero es divisible por 5 si y sólo si el dígito de las unidades es 5 o 0.
Dem: Sea n un entero positivo de donde:

$$n = 10q + r; 0 \leq r < 10$$

donde r representa el dígito de las unidades
Luego $n = 5 \cdot 2q + r$
Si n es divisible por 5, entonces $n = 5 \cdot R$ para algún R, así

$$\begin{aligned} 5R &= 5 \cdot 2q + r \\ 5R - 5 \cdot 2q &= r \\ 5(R - 2q) &= r \end{aligned}$$

Así, r es múltiplo de 5, pero los únicos múltiplos de 5 comprendidos entre 0 y 9 son 0 y 5, es decir; $r = 0$ ó $r = 5$ sí el dígito de las unidades es 0 ó 5, entonces $n = 10q + r$ con $r = 0$ ó $r = 5$, así $n = 10q + 0$ ó $n = 10q + 5$, así $n = 5(2q)$ ó $n = 5(2q + 1)$, en cualquier caso n es divisible por 5
Todo número terminado en 0 o en 5 es divisible por 5. Así, 30, 25, 200, 815, como se puede comprobar son divisibles por 5.

$$n = \underbrace{dcba}_{a=5 \text{ o } a=5} \Rightarrow n = \overset{\circ}{5}$$

Ejemplos:
Son numeros divisibles por 5: 1350, 110, 585, 8495, 1020.
Son números divisibles por 5:

- 1350, pues $0 = \overset{\circ}{5}$
- 110, pues $0 = \overset{\circ}{5}$
- 585, pues $5 = \overset{\circ}{5}$

Teniendo en cuenta que 0 y 5 son los únicos números de una cifra múltiplos de 5, el criterio de divisibilidad por 5 también puede enunciarse:

Un número es divisible por 5 si la cifra de las unidades es múltiplo de 5.

Criterios de divisibilidad por 3.
Un número entero es divisible por 3 si y sólo si la suma de sus dígitos es múltiplo de 3.
Dem. : Sea n un entero. Consideremos lo siguiente:
$n = a_k 10^k + a_{k-1} 10^{k-1} + ... + a_1 10 + a_0$; observemos que

$$\begin{aligned}
1 \equiv 1 \pmod 3 // a_0 \Rightarrow \quad & a_0 \equiv a_0 \pmod 3 \\
10 \equiv 1 \pmod 3 // a_1 \Rightarrow \quad & a_1 10 \equiv a_1 \pmod 3 \\
10^2 \equiv 1 \pmod 3 // a_2 \Rightarrow \quad & a_2 10^2 \equiv a_2 \pmod 3 \\
\vdots & \\
10^{k-1} \equiv 1 \pmod 3 // a_{k-1} \Rightarrow \quad & a_{k-1} 10^{k-1} \equiv a_{k-1} \pmod 3 \\
10^k \equiv 1 \pmod 3 // a_k \Rightarrow \quad & a_k 10^k \equiv a_k \pmod 3
\end{aligned}$$

Sumando miembro a miembro :

$$\begin{aligned}
a_0 + a_1 10 + a_2 10^2 + ... + a_{k-1} 10^{k-1} + a_k 10^k \equiv a_0 + a_1 + ... + a_{k-1} + a_k \pmod 3 \\
n \equiv a_0 + a_1 + ... + a_{k-1} + a_k \pmod 3
\end{aligned}$$

Luego si: $3|n \Rightarrow n \equiv 0 \pmod 3$ pero
$n \equiv a_0 + ... + a_k \pmod 3$ de donde
$a_0 + ... + a_k \equiv n \pmod 3$, y por transitividad tenemos
$a_0 + ... + a_k \equiv 0 \pmod 3$
$\therefore 3|a_0 + ... + a_k$, ahora
Si $3|a_0 + ... + a_k \Rightarrow a_0 + ... + a_k \equiv 0 \pmod 3$
y $n \equiv a_0 + ... + a_k \pmod 3$, por transitividad
$n \equiv 0 \pmod 3$ es decir $3|n$
Dado el número 2451 la suma de los valores absolutos de sus cifras es: $2 + 4 + 5 + 1 = 12$.
Este número 12 es $\mathring{3}$, y se observa que el número dado es divisible por 3. En efecto:

$$2451 = 3 \cdot 817 + 0$$

Esta observación es general y se enuncia en el criterio que dice:
Un número es divisible por 3 si la suma de los valores intrínsecos de todas sus cifras es múltiplo de 3.
Es decir:
centerline$n = \underbrace{\underline{dcba}}_{a+b+c+d=\mathring{3}} \Rightarrow n = \mathring{3}$

Ejemplos:
Son números divisibles por 3:

- 513264 es divisible por 3, pues: $5+1+3+2+6+4=21=\mathring{3}$
- 10101 es divisible por 3, pues: $1+1+1=3=\mathring{3}$
- 29700, es divisible por 3, pues: $2+9+7=18=\mathring{3}$

Criterios de divisibilidad por 9.
Un entero expresado en numeración decimal por 9 si y sólo si la suma de todos sus dígitos es divisible por 9
Dem. Sea

$$n = a_k 10^k + a_{k-1}10^{k-1} + ... + a_0 \text{ ; notemos que:}$$

$$\begin{aligned}
1 &\equiv 1 \pmod 9 // a_0 \Rightarrow & a_0 &\equiv a_0 \pmod 9\\
10 &\equiv 1 \pmod 9 // a_1 \Rightarrow & a_1 10 &\equiv a_1 \pmod 9\\
10^2 &\equiv 1 \pmod 9 // a_2 \Rightarrow & a_2 10^2 &\equiv a_2 \pmod 9\\
&\vdots & &\\
10^{k-1} &\equiv 1 \pmod 9 // a_{k-1} \Rightarrow & a_{k-1}10^{k-1} &\equiv a_{k-1} \pmod 9\\
10^k &\equiv 1 \pmod 9 // a_k \Rightarrow & a_k 10^k &\equiv a_k \pmod 9
\end{aligned}$$

De ahí tenemos: $n \equiv a_0 + ... + a_k \pmod 9$
Si $9|n \Rightarrow n \equiv 0 \pmod 9$
$a_0 + ... + a_k \equiv 0 \pmod 9$ es decir $9|a_0 + .. + a_k$
Ahora si $9|a_0 + .. + a_k \Rightarrow a_0 + ... + a_k \equiv 0 \pmod 9$
entonces $n \equiv 0 \pmod 9$ es decir $9|n$
El criterio de divisibilidad por 9 es del todo análogo al criterio de divisibilidad por 3, es decir:
Un número es divisible por 9 si la suma de los valores intrínsecos de todas sus cifras es múltiplo de 9.
Es decir:

$$n = \underbrace{dcba}_{a+b+c+d=\mathring{9}} \Rightarrow n = \mathring{9}$$

Así, en el número 8127 se verifica que:
$8 + 1 + 2 + 7 = 18 = \mathring{9}$
luego dicho número es divisible por 9.
En efecto:

$$8127 = 9 \cdot 903 + 0$$

Ejemplos:
Son números divisibles por 9:

- 74268 es divisible por 9, pues: $7 + 4 + 2 + 6 + 8 = 27 = \mathring{9}$
- 1020321 es divisible por 9, pues: $1 + 2 + 3 + 2 + 1 = 9 = \mathring{9}$

Criterios de divisibilidad por 11.

Sea $n = \sum_{i=0}^{k} a_i 10^i$ la representación de un entero positivo n en base 10. Entonces n es divisible por 11 si y sólo si $\sum_{i=0}^{k}(-1)^i a_i$ es divisible por 11.
El número 818092 es divisible por 11.
Dem.: Sea $n = \sum_{i=0}^{k} a_i 10^i$ es decir
$n = a_0 + a_1 10 + a_2 10^2 + ... + a_{k-1} 10^{k-1} + a_k 10^k$
y $\sum_{i=0}^{k}(-1)^i a_i = a_0 - a_1 + a_2 - a_3 + a_4 - a_5 + a_6 - a_7 + a_8 - ... + (-1)^k a_k$
Notemos que:

$$\begin{aligned}
1 \equiv 1 \pmod{11} // a_0 \Rightarrow \quad & a_0 \equiv a_0 \pmod{11} \\
10 \equiv -1 \pmod{11} // a_1 \Rightarrow \quad & a_1 10 \equiv -a_1 \pmod{11} \\
10^2 \equiv 1 \pmod{11} // a_2 \Rightarrow \quad & a_2 10^2 \equiv a_2 \pmod{11} \\
10^3 \equiv -1 \pmod{11} // a_3 \Rightarrow \quad & a_3 10^3 \equiv -a_3 \pmod{11} \\
10^4 \equiv 1 \pmod{11} // a_4 \Rightarrow \quad & a_4 10^4 \equiv a_4 \pmod{11} \\
\vdots & \\
10^k \equiv (-1)^k \pmod{11} // a_k \Rightarrow \quad & a_k 10^k \equiv a_k (-1)^k \pmod{11}
\end{aligned}$$

Luego por propiedades de congruencia tenemos:

$$a_0 + a_1 10 + ... + a_k 10^k \equiv a_0 - a_1 + a_2 - a_3 + ... + (-1)^k a_k \pmod{11}$$
$$n \equiv a_0 - a_1 + a_2 - a_3 + ... + (-1)^k a_k \pmod{11}$$

Sí $n \equiv 0 \pmod{11} \Rightarrow a_0 - a_1 + a_2 - a_3 + ... + (-1)^k a_k \equiv 0 \pmod{11}$
Ahora sí $a_0 - a_1 + a_2 - a_3 + ... + (-1)^k a_k \equiv 0 \pmod{11}$
Entonces $n \equiv 0(11) \therefore 11|n$

En efecto:

$$818092 = 11 \cdot 74372 + 0$$

Se observa que la suma de las cifras de los lugares pares:

$$9 + 8 + 8 = 25$$

menos la suma de las cifras de los lugares impares, es decir,

$$2 + 0 + 1 = 3$$

da por resultado: $25 - 3 = 22$, que es múltiplo de 11.
Esta observación es general, y se enuncia en el criterio de divisibilidad por 11:
Un número es divisible por 11 si la diferencia entre la suma de los valores intrínsecos de las cifras de los lugares pares y la de las cifras de los lugares impares es múltiplo de 11.
En efecto:

$$n = \underbrace{\underline{dcba}}_{(a+c)-(b+d)=\mathring{1}1} \Rightarrow n = \mathring{1}1$$

Ejemplos:
Son números divisibles por 11:

- 32813 es divisible por 11, pues:
  Suma de cifras, lugares pares: 1+2 = 3 Suma de cifras, lugares impares: 3+8+3 = 14

$$14 - 3 = 11 = \mathring{1}1$$

Después de estudiar algunos criterios de divisibilidad, podemos deducir de esto un patron que es el siguiente:

Criterio de divisibilidad por "m" en el sistema de base 10 utilizando los restos potenciales.

Sea el número n descompuesto polinomicamente tenemos $n = a_k 10^k + a_{k-1}10^{k-1} + ...a_2 10^2 + a_2 10^2 + a_1 10^1 + a_0$ Entonces tenemos:

$$\begin{aligned}
1 &\equiv 1 \pmod{m} // a_0 \Rightarrow & a_0 &\equiv a_0 \pmod{m} \\
10 &\equiv r_1 \pmod{m} // a_1 \Rightarrow & a_1 10 &\equiv r_1 \pmod{m} \\
10^2 &\equiv r_2 \pmod{m} // a_2 \Rightarrow & a_2 10^2 &\equiv r_2 \pmod{m} \\
10^3 &\equiv r_3 \pmod{m} // a_3 \Rightarrow & a_3 10^3 &\equiv r_3 \pmod{m} \\
10^4 &\equiv r_4 \pmod{m} // a_4 \Rightarrow & a_4 10^4 &\equiv r_4 \pmod{m} \\
&\vdots \\
10^k &\equiv \underbrace{r_k}_{\text{Restos potenciales}} \pmod{m} // a_k \Rightarrow & a_k 10^k &\equiv r_k \pmod{m}
\end{aligned}$$

Sumando miembro tenemos:

$$\begin{aligned}
a_0 + a_1 10 + a_2 10^2 + ... + a_{k-1}10^{k-1} + a_k 10^k &\equiv r_0 + r_1 + r_2 + r_3 ... + r_k \pmod{m} \\
n &\equiv r_0 + r_1 + r_2 + r_3 ... + r_k \pmod{m}
\end{aligned}$$

Luego si: $\mathsf{m}|n \Rightarrow n \equiv 0 \pmod{m}$ pero
$n \equiv r_0 + ... + r_k \pmod{m}$ de donde
$r_0 + ... + r_k \equiv n \pmod{m}$, y por transitividad tenemos
$r_0 + ... + r_k \equiv 0 \pmod{m}$
$\therefore \mathsf{m}|r_0 + ... + r_k$, ahora
Si $\mathsf{m}|r_0 + ... + r_k \Rightarrow r_0 + ... + r_k \equiv 0 \pmod{m}$
y $n \equiv r_0 + ... + r_k \pmod{m}$, por transitividad
$n \equiv 0 \pmod{m}$ es decir
$\mathsf{m}|n$

Finalmente el anterior enunciado, que fue demostrado, nos enuncia que, un número n en base 10 es congruente con otro bajo algún módulo m, de esto deducimos que m divide al número n , que es lo que buscábamos en nuestros objetivos preliminares.

Ejemplos:

He aquí unos ejemplos, aplicando la anterior regla:
para desarrollar los subsecuentes ejemplos,
Hallar el criterio de divisibilidad de 13

$$\begin{aligned}
1 &\equiv 1 \\
10 &= \quad \bmod 13-3 \\
10^2 &= (\quad \bmod 13-3)(\quad \bmod 13-3) \\
&= \quad \bmod 13+9 \\
&= \quad \bmod 13+4 \\
10^3 &= (\quad \bmod 13+4)(\quad \bmod 13-3) \\
&= \quad \bmod 13-12 \\
&= \quad \bmod 13-1 \\
10^4 &= (\quad \bmod 13-1)(\quad \bmod 13-3) \\
&= \quad \bmod 13+3 \\
10^5 &= (\quad \bmod 13+3)(\quad \bmod 13-3) \\
&= \quad \bmod 13-9 \\
&= \quad \bmod 13-4 \\
10^6 &= (\quad \bmod 13-4)(\quad \bmod 13-3) \\
&= \quad \bmod 13+12 \\
&= \quad \bmod 13+1 \\
&\vdots
\end{aligned}$$

De ahí tenemos los restos:

$n = r_0(1) + r_1(-3) + r_2(4) + r_3(-1) + r_4(3) + r_5(-4) + r_6(1)...$ (mód 13)

Hallar el criterio de divisibilidad de 17

$$
\begin{aligned}
1 &\equiv 1 \\
10 &= \quad \bmod 17 - 7 \\
10^2 &= (\quad \bmod 17 - 7)(\quad \bmod 17 - 7) \\
&= \quad \bmod 17 + 49 \\
&= \quad \bmod 17 + 13 \\
&= \quad \bmod 17 + 4 \\
10^3 &= (\quad \bmod 17 + 4)(\quad \bmod 17 - 7) \\
&= \quad \bmod 17 - 28 \\
&= \quad \bmod 17 - 10 \\
&= \quad \bmod 17 - 1 \\
10^4 &= (\quad \bmod 17 - 1)(\quad \bmod 17 - 7) \\
&= \quad \bmod 17 + 7 \\
10^5 &= (\quad \bmod 17 + 7)(\quad \bmod 17 - 7) \\
&= \quad \bmod 17 - 49 \\
&= \quad \bmod 17 - 13 \\
&= \quad \bmod 17 - 4 \\
10^6 &= (\quad \bmod 17 - 4)(\quad \bmod 17 - 7) \\
&= \quad \bmod 17 + 28 \\
&= \quad \bmod 17 + 10 \\
&= \quad \bmod 17 + 1 \\
10^7 &= (\quad \bmod 17 + 1)(\quad \bmod 17 - 7) \\
&= \quad \bmod 17 - 7 \\
&\vdots
\end{aligned}
$$

De ahí tenemos los restos:

$n = r_0(1) + r_1(-7) + r_2(4) + r_3(-1) + r_4(7) + r_5(-4) + r_6(1) + r_7(-7)...$ (mód 17)

Hallar el criterio de divisibilidad de 79

$$\begin{aligned}
1 &\equiv 1 \\
10 &= \mod 79 - 69 \\
&= \mod 79 - 15 \\
&= \mod 79 - 6 \\
10^2 &= (\mod 79 - 6)(\mod 79 - 6) \\
&= \mod 79 + 36 \\
&= \mod 79 + 9 \\
10^3 &= (\mod 79 + 9)(\mod 79 - 6) \\
&= \mod 79 - 54 \\
&= \mod 79 - 9 \\
10^4 &= (\mod 79 - 9)(\mod 79 - 6) \\
&= \mod 79 + 54 \\
&= \mod 79 + 9 \\
10^5 &= (\mod 79 + 9)(\mod 79 - 6) \\
&= \mod 79 - 54 \\
&= \mod 79 - 9 \\
&\vdots
\end{aligned}$$

De ahí tenemos los restos:
$n = r_0(1) + r_1(-6) + r_2(9) + r_3(-9) + r_4(9) + r_5(-9)...$ (mód 79)

Hallar el criterio de divisibilidad de 93

$$\begin{aligned}
1 &\equiv 1 \\
10 &= \mod 93 - 83 \\
&= \mod 93 - 11 \\
&= \mod 93 - 2 \\
10^2 &= (\mod 93 - 2)(\mod 93 - 2) \\
&= \mod 93 + 4 \\
10^3 &= (\mod 93 + 4)(\mod 93 - 2) \\
&= \mod 93 - 8 \\
10^4 &= (\mod 93 - 8)(\mod 93 - 2) \\
&= \mod 93 + 16 \\
&= \mod 93 + 7 \\
10^5 &= (\mod 93 + 7)(\mod 93 - 2) \\
&= \mod 93 - 14 \\
&= \mod 93 - 5 \\
10^6 &= (\mod 93 - 5)(\mod 93 - 2) \\
&= \mod 93 + 10 \\
&= \mod 93 + 1 \\
10^7 &= (\mod 93 + 1)(\mod 93 - 2) \\
&= \mod 93 - 2 \\
10^8 &= (\mod 93 - 2)(\mod 93 - 2) \\
&= \mod 93 + 4 \\
&\vdots
\end{aligned}$$

De ahí tenemos los restos:

$$n = r_0(1) + r_1(-2) + r_2(4) + r_3(-8) + r_4(7) + r_5(-5) + r_6(1) + r_7(-2) + r_8(4)... \quad (\text{mód } 93)$$

3.7. Método para determinar la divisibilidad de un número por otro

A continuación describiremos un método que permitirá determinar si un entero positivo es divisible por algún otro o de lo contrario no es divisible por ninguno (primo). Primeramente para poder determinar esto es necesario determinar si el número p dado es primo o es compuesto; en el caso de que sea compuesto se podrá determinar por que números es divisible tal número p.

Por ejemplo, 113. La raíz cuadrada de 113 está entre 10 y 11, ya que $10^2 = 100$ y $11^2 = 121$ entonces $100 < 113 < 121$; esto es

$$10 < \sqrt{113} < 11$$

Ahora podemos notar que lo primos menores o iguales que $\sqrt{113}$ son 2,3,5,7. Ahora veremos que ninguno de estos números es factor de 113:

$$113 = 56 \cdot 2 + 1$$
$$113 = 37 \cdot 3 + 2$$
$$113 = 22 \cdot 5 + 3$$
$$113 = 16 \cdot 7 + 1$$

Por lo tanto,113 es primo, y no tiene más divisores que 1 y 113.

Ejemplo 1: Que número dividen a 1741

La raíz cuadrada de 1741 esta entre 41 y 42 ya que $41^2 = 1681$, $42^2 = 1764$ y:

$$41 < \sqrt{1741} < 42$$

$$1681 < \sqrt{1741} < 1764$$

Los primos menores o iguales a $\sqrt{1741}$ son 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41. Ahora podemos discriminar, a estos primos de la siguiente manera:

los números primos 2 y 5 no podrían ser factores de 1741, porque en ultimo dígito de 1741 es 1, y sabemos que para que un número tenga entre sus factores a 2 y 5 tal número debe terminar en el dígito de la unidad en par, para el 2; y en 0 o 5, para el 5, así que estos números no los tomamos en cuenta, esto para aminorar nuestra tarea.
Así los primos menores a $\sqrt{1741}$ son: 3, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41.

$$1741 = 870 \cdot 2 + 1$$
$$1741 = 580 \cdot 3 + 1$$
$$1741 = 248 \cdot 7 + 5$$
$$1741 = 158 \cdot 11 + 3$$
$$1741 = 133 \cdot 13 + 12$$
$$1741 = 91 \cdot 19 + 12$$
$$1741 = 75 \cdot 23 + 16$$
$$1741 = 60 \cdot 29 + 1$$
$$1741 = 56 \cdot 31 + 5$$
$$1741 = 47 \cdot 37 + 2$$
$$1741 = 42 \cdot 41 + 19$$

Ninguno de estos números es divide de 1741
Por lo tanto 1741 es primo.

Ejemplo 2: Que número dividen a 316
La raíz cuadrada de 316 esta entre 17 y 18 ya que $17^2 = 289$, $18^2 = 324$ y:

$$17 < \sqrt{316} < 18$$

$$289 < \sqrt{316} < 324$$

Los primos menores o iguales a $\sqrt{316}$ son 2, 3, 7, 11, 13, 17.

$$316 = 158 \cdot 2 + 0$$
$$316 = 105 \cdot 3 + 1$$
$$316 = 45 \cdot 7 + 1$$
$$316 = 28 \cdot 11 + 8$$
$$316 = 24 \cdot 13 + 4$$
$$316 = 18 \cdot 17 + 10$$

Ahora notemos que 2 si es un factor de 316 y divide a este número pues al operar $158 \cdot 2 + 0 = 316$ nos da un resto 0, a diferencia de los otros factores primos que claramente no son factores de 316, o en otras palabras no dividen a 316; también podemos notar que el número 316 es un número no primo o sea es un número compuesto.

Así de esta manera podemos encontrar los divisores de un número p por otro número, que no es más que un factor de p. Además que podemos determinar si un número es compuesto o primo.

Capítulo 4

CONCLUSIONES Y RECOMENDACIONES

Para este capítulo final del trabajo de investigación monografica, tenemos las recomendaciones y las conclusiones de este trabajo de investigación monografico.

4.1. Conclusiones

Luego de una descripción matemática de la Divisibilidad en Teoría de Números, se llega a las siguientes conclusiones:
Producto de todo lo tratado en este documento concluimos que es posible desarrollar el algoritmo de la divisibilidad para determinar la divisibilidad de un número por otro.
Nuestros objetivos preliminares mandaban hallar un algoritmo de la divisibilidad, se pudo hallar el Algoritmo de la Divisibilidad en el que se pudo llegar a la forma general de los criterios de divisibilidad por m en el sistema en base 10. Para llegar a este resultado fue necesario estudiar el Algoritmo de la División, además de los los números primos, y las propiedades del MCD, y la mención de lagunas propiedades de las congruencias, propiedades de los cuales era necesario estudiarlas, para finalmente poder llegar al a un criterio general general de la divisibilidad.
Cabe recalcar que el objetivo general del trabajo monográfico, nos pedía hallar un algoritmo general de la divisibilidad, evidentemente se hallo determinado logaritmo, (sección 3.6), el logaritmo es una generalización de la regla de los criterios de divisibilidad, el cual

nos permite descifrar el criterio de divisibilidad de un número.
Por otro lado nuestro objetivos específicos nos demandan cumplir determinados requisitos para desarrollar satisfactoriamente nuestros objetivos generales; es así, que en un trabajo descriptivo como es la monografía, es necesariamente imprescindible poder revisar, estudiar y analizar determinadas teorías para poder enriquecer el presente trabajo y así es que se lo hizo; posteriormente, se describió y se demostró las propiedades de la divisibilidad, (Capitulo 3), asimismo se describió muchas otras propiedades propias de los números enteros, propiedades que sin ellas no se hubiera podido demostrar el criterio general de la divisibilidad de un determinado número.

También pudimos observar que determinar la divisibilidad de un número por otro es posible bajo determinadas reglas del conjunto de los Números Enteros, y que la divisibilidad es una relación definida de los números enteros.
Además podemos extractar que el el estudio de la divisibilidad es importante para poder expresar un número en factores primos, tales que se son estudiados frecuentemente en los primeros cursos de secundaria. Por otro lado, es claro que la matemática es una ciencia exacta, que no sólo merece ser conocida y estudiada superficialmente por alumnos y maestros, sino que merece un mayor estudio y análisis, pues no tiene que limitarse a estudiarla superficialmente, sino más al contrario debería de estudiarse de una manera más profunda, no sólo en las universidades, también que esta forma de estudiarla llegase a los alumnos de secundaria, claro esta con una sólida base de ciertas propiedades que la matemática tiene. Finalmente, es necesario que el maestro de matemáticas de las Unidades Educativas de secundaria, este en permanente renovación y actualización, tal y como lo norma la propia Reforma Educativa en actual vigencia, y no es necesario acudir a ninguna teoría para poder afirmar que el maestro debe saber mucho mas que el alumno sobre su especialidad, pues así, si el maestro esta más preparado se ayuda mejor al alumno.

4.2. Recomendaciones

Hemos visto que la divisibilidad entre números es posible bajo ciertas circunstancias, pues es necesario hallar un criterio de divisibilidad para ese número, esto para saber que tipo de restos potenciales deja. pero para llegar asta esto tuvimos que llegar a desarrollar primero el algoritmo de la Divisibilidad, y mediante este, los números primos y los MCD

de números. Por lo anterior se considera que estudiar La Teoría de la Divisibilidad, es de gran utilidad al estudiante para que pueda desarrollar un números mediante producto de factores primos, además que pueda reconocer los divisores que un número y los números que lo dividen exactamente, que reconozca los divisores comunes de dos números.
Por otro lado, para introducir la divisibilidad en la enseñanza de la Teoría de números en la Educación Secundaria, es necesario realizar las siguientes recomendaciones:

- El estudiante, tiene que ampliar los conceptos matemáticos que a visto en el nivel primario.
- Tal ampliación tiene que estar orientada a que el alumno experimente el trabajo matemático puro, en un contexto netamente matemático.
- A partir de lo anterior, vea el alumno de que manera el conocimiento matemático de la teoría de números tiene sus aplicaciones como un elemento de investigación matemática.
- Desde luego debe tenerse muy en cuenta las propiedades básicas de los enteros.
  - Propiedades de la igualdad
  - Propiedades de la desigualdad
  - Propiedades de la suma
  - Propiedades de la multiplicación
- Una básica noción de conjuntos.
- Números primos y compuestos.
- El MCD
- Criterio de divisibilidad en base 10

Todos estos puntos mencionados, nos serán de mucha ayuda para el estudiante, para que pueda determinar un criterio general de divisibilidad, ya que las propiedades de estos son primordiales para llegar a un criterio general.

Capítulo 5

BIBLIOGRAFÍA

⋆ RUIZ Arango, Isidro; "Teoría de los números primos"; Editorial San Marcos, Lima-Perú; Año 1999.

⋆ HOWARD Eves, "Estudio de las geometrías" Universidad de Maine,Massachusetts - EE.UU,1965.

⋆ PETTOFREZZO Anthony; BYRKIT Donald, "Introducción a la teoría de numero", Editorial Prentice/ hall internacional, Florida - EE.UU, 1972

⋆ DE CASTRO Korgi, Rodrigo; "El universo LaTeX"; Editorial UNIBIBLOS; Bogotá, Colombia, 2001.

⋆ TREJO, Cesar; BOSCH, Jorge; "Matemática Moderna", Editorial Universitaria; Buenos Aires, Argentina, 1982.

⋆ de OLIVEIRA Santos, Jose Plínio; "Introdução á Teoria dos Números", Segunda edición; Rio de Janeiro, Brasil, 2001.

⋆ ZORRILLA Arena, Santiago; "Introducción a la metodología de la investigación"; Editorial Melo S.A.; Mexico D.F. 1996.

⋆ MOLL, Luis c.; "Vygosky y la educación"; Grupo editor Aique; Argentina 1993.

⋆ VOROBIOV, N.N.; "Criterios de divisibilidad"; Editorial MIR; Moscú, URSS; 1975.

⋆ M.E.C.D.; "Nuevo compendio de legislación sobre la Reforma Educativa y leyes conexas"; Edición, BOLIVIA DOS MIL S.R.L.; La Paz; 2001.