CONSTRUCCIÓN DE ANILLOS FINITOS A PARTIR DEL ESTUDIO DE LA RELACIÓN DE DIVISIBILIDAD EN $\mathbb{Z}_m$

FABIO STEVEN JAIMES GÓMEZ

UNIVERSIDAD PEDAGÓGICA NACIONAL

FACULTAD DE CIENCIA Y TECNOLOGÍA

DEPARTAMENTO DE MATEMÁTICAS

LICENCIATURA EN MATEMÁTICAS

BOGOTÁ D.C. 2017

CONSTRUCCIÓN DE ANILLOS FINITOS A PARTIR DEL ESTUDIO DE LA RELACIÓN DE DIVISBILIDAD EN $\mathbb{Z}_m$

FABIO STEVEN JAIMES GÓMEZ

Código: 2013140022

C.C. 1031160248

Trabajo de grado asociado a un grupo de estudio

Trabajo de grado como requisito parcial para optar al título de Licenciado en Matemáticas

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. 2017

AGRADECIMIENTOS

A mis padres, Rafael y Rocío por su constante entrega y apoyo en la construcción de este sueño, por ser el modelo a seguir siempre y por nunca desfallecer, por enseñarme que al luchar, los sueños se alcanzan.

A mis hermanos, por sus consejos, por estar en cada paso que he decidido dar y por la constante compañía y apoyo desde pequeños.

A mis abuelos, Vidal y Cecilia, a él por ser al bastón que no me ha dejado caer, a ella por haber sido el mejor modelo de emprendimiento, responsabilidad, fe, fortaleza y amor sin condiciones.

A mis mejores amigos, Alex y Karen, por su fe en mí, por que creyeron en mí desde el primer momento, porque gran parte de lo que soy hoy es por ellos.

A mis amigos, Yuly, Lizeth, Derly y Santiago por el tiempo y las palabras compartidas.

A Sayda Quiroga, por su paciencia, por hacer el papel de compañera, por su apoyo incondicional desde el primer momento, por estar en los momentos más difíciles y por ser quien me impulsa a seguir a diario.

Al profesor William Jiménez, por la total entrega en el desarrollo de este trabajo, por su paciencia y orientación, pero además por ser persona, por ser amigo, por ser casi como un padre.

A la profesora Luz Libia Pinzón, por ser quien me iniciara en este camino, porque gracias a su consejo hace 5 años hoy estoy aquí, cumpliendo este sueño.

A la Universidad Pedagógica Nacional por ser el espacio en el cual conocí a grandes personas, por brindarme la oportunidad de formarme profesional y personalmente.

En un renglón: Si usted está leyendo esto y se siente identificado, ¡gracias!

Dedicado a:

La memoria de mi vieja escuela, mi amada abuela.

Steven Jaimes

1. Información General	
Tipo de documento	Trabajo de grado
Acceso al documento	Universidad Pedagógica Nacional. Biblioteca Central
Titulo del documento	Construcción de anillos finitos a partir del estudio de la relación de divisibilidad en $\mathbb{Z}_m$.
Autor(es)	Jaimes Gómez, Fabio Steven
Director	Jiménez Gómez, William Alfredo
Publicación	Bogotá, Universidad Pedagógica Nacional, 2017. 88 P.
Unidad Patrocinante	Universidad Pedagógica Nacional.
Palabras Claves	*DIVISIBILIDAD, TEORÍA DE NÚMEROS, TEOREMA FUNDAMENTAL DE LA ARITMÉTICA, ANILLOS, NÚMEROS PRIMOS, CONJUNTOS ZM.*

2. Descripción

Este trabajo se desarrolla en el marco del proyecto curricular de la Licenciatura en Matemáticas y surge como propuesta de estudio desde el Seminario de Álgebra de la universidad con el objetivo general de construir anillos finitos haciendo uso de las características estudiadas a partir del análisis de la relación de divisibilidad en los conjuntos $\mathbb{Z}_m$. Partiendo en primera instancia de un marco de referencia que apoye todo el estudio posterior, pasando por el proceso de analizar la relación de divisibilidad en el conjunto y a partir de esto construir nociones propias de la teoría tales como números primos, unidades, asociados, entre otros, pero orientadas a los elementos del conjunto de partida. El documento concluye con la construcción de anillos finitos tomando como partida los elementos estudiados a *priori* y dejando evidenciar el proceso usado para tal fin.

3. Fuentes

Arrondo, E. (2011). Apuntes de estructuras algebraicas. Madrid: Universidad Complutense de Madrid.

Castro, L., Sánchez, L., & Rojas, S. (2015). La relación de divisibilidad en los enteros de Minkowsky. Tunja: Universidad Pedagógica y Tecnológica de Colombia.

Fraleigh, J. (1988). Algebra Abstracta. Addison-Wesley Publishing Company, Inc., Reading, Massachusetts, E.U.A.

García, M., Giacobbi A., & Ríos, N. (2008). Introducción a la Teoría Algebraica de Números. Universidad Nacional de la Plata. Buenos Aires, Argentina.

Le veque, W. (1968). TEORÍA ELEMENTAL DE LOS NÚMEROS. México: Editorial Herrero hermanos, sucesores, S.A. editores

Luque C., Mora L. & Torres J. (2004). Estructuras análogas a los números reales. Bogotá: Editorial Nomos S.A.

Luque C., Mora L. & Torres J. (2004). Estructuras análogas a los números reales. Bogotá: Editorial Nomos S.A.

Pérez, É. (2005). Estructuras Algebraicas. Bogotá: Universidad Pedagógica Nacional.

Pettofrezzo, J. (1972). Introducción a la Teoría de Números. New Jersey, E.U.A. Editorial Prentice.

Sánchez, Y., & Jiménez, W. (2015). Un estudio de la relación de Divisibilidad en súper conjuntos de Z a partir del estudio en subconjuntos de Z. Tunja: Universidad Pedagógica y Tecnológica de Colombia.

Tabara, J. (2001). Introducción la teoría de anillos. Recuperado de: http://mimosa.pntic.mec.es/jgomez53/matema/docums/tabara-anillos.pdf

Torres, H., Ávila, J., & Rubén, T. (2015). Una caracterización de números primos en el conjunto $\mathbb{Z}(\sqrt{2})$ desde el proceso de analizar. Tunja: Universidad Pedagógica y Tecnológica de Colombia.

4. Contenidos

El presente trabajo de grado se encuentra distribuido en 5 secciones de la siguiente manera

En la sección 1 el lector encontrará un marco de referencia que servirá de apoyo para el desarrollo del trabajo, encontrará elementos en relación a la teoría de números, teoría algebraica de números, teoría de grupos y anillos y algunos teoremas en relación a estos.

En la sección 2 se realiza el análisis completo de la relación de divisibilidad partiendo de su definición, pasando por la definición de elementos tales como unidades, y asociados, posteriormente se estudia la norma de los números y a partir de esta se caracterizan los elementos ya definidos y otros como primos y compuestos, además, se muestran algunos elementos que surgen en el desarrollo del estudio de la norma, tales como subgrupos, clases de equivalencia, diagramas de Hasse, entre otros.

En la sección 3 se realiza una construcción del teorema fundamental de la aritmética en $\mathbb{Z}_m$ tomando como partida el estudio del TFA en la estructura de los enteros y por medio de un análisis realizado a los elementos se construye este TFA en el conjunto $\mathbb{Z}_m$

En la sección 4 finalmente se construyen los anillos haciendo uso de todos los elementos estudiados en las secciones anteriores construyendo inicialmente una tabla de adición de manera cíclica y posteriormente una tabla de multiplicar en base a los elementos mencionados.

En la sección 5 se encontrarán algunas conclusiones en relación a todos los elementos trabajados en las secciones, la metodología y los objetivos planteados.

5. Metodología

En primer lugar, el primer acercamiento que se tuvo con el trabajo fue el de indagación, trabajando en la estructura a partir de los elementos conocidos de otras más cercanas, por ejemplo la estructura de los números enteros y la relación de divisibilidad definida en esta. De esta manera surge la necesidad de realizar una consulta bibliográfica en torno a estos elementos y redefinirlos, es así como surge la definición y caracterización de nociones asociadas al estudio referente, todo esto dio paso para finalmente comenzar a consolidar el estudio general de los conjuntos $\mathbb{Z}_m$ y todas sus propiedades. Se ve la necesidad de construir un programa en Python que sirviera de ayuda para agilizar los cálculos y disminuyera los posibles errores. Adicional también se hizo uso del software Microsoft Excel para generalizar algunos resultados y relacionarlos con los elementos ya trabajados. Además, también se usó el método ensayo – error para la construcción final de las tablas de multiplicación y el uso de ejemplos para apoyar cada construcción.

6. Conclusiones

- El trabajo con los conjuntos $\mathbb{Z}_m$ se hace bastante accesible por ser estructuras finitas y tener gran similitud con otras estructuras incluso infinitas, el hecho de que los estudios principales siempre estén orientados a las propiedades básicas, esto dio paso para el estudio de otros elementos no usuales en el conjunto.

- La norma de los elementos resulta de vital importancia en el estudio, pues es esta la que da paso al estudio de todos los elementos posteriores, permitiendo construir clases de equivalencia y a partir de estas realizar la construcción del teorema fundamental de la aritmética de manera similar a lo realizado en otras estructuras.

- La tecnología jugó un papel importante en el desarrollo del trabajo, pues se diseñó un programa en el software Python que resumiera en gran parte los cálculos e hiciera más progresivo el trabajo, así como el uso del software *Propiedades 3.1* el cual, de igual manera sirvió para concluir con la construcción de los anillos.

- El método aplicado para la construcción final de los anillos no resulta ser el más apropiado, pues no permite evidenciar a groso modo la propiedad distributiva de una operación respecto a otra, así, los caminos que se abren para continuar con el trabajo son bastantes, tanto por los resultados obtenidos, como por los problemas que se abren en el desarrollo

- En cuanto a la formación como docente, este trabajo aporto en torno a cómo podrían abordarse ciertos elementos de la matemática curricular a partir de elementos de la matemática avanzada, esto es, estableciendo las relaciones que existen entre unos con los otros, mostrando así que no son elementos desligados, sino que por el contrario pueden aportar más a la formación de los estudiantes desde su debido abordaje, por ejemplo, la enseñanza de los números primos y el TFA

Elaborado por:	Fabio Steven Jaimes Gómez
Revisado por:	William Alfredo Jiménez Gómez

Fecha de elaboración del Resumen:	31	10	2017

Contenido

Introducción 12

Metodología 14

Objetivos 15

Objetivo General: 15

Objetivos Específicos: 15

1. Marco de Referencia 16

1.1. Teoría de números: 16

1.1.1. Máximo Común Divisor 16

1.1.2. Mínimo Común Múltiplo 16

1.1.3. Conjuntos $\mathbb{Z}\boldsymbol{m}$ 16

1.1.4. Teorema Fundamental de la Aritmética. (TFA) 18

1.1.5. Congruencia 18

1.1.7. Congruencia lineal: 19

1.2. Teoría Algebraica de Números (TAN) 20

1.2.1. Unidades 20

1.2.2. Asociados 20

1.3. Estructuras 20

1.3.1. Grupo 20

1.3.2. Grupo Abeliano 20

1.3.4. Anillo 21

2. Divisibilidad en $\mathbb{Z}\boldsymbol{m}$ 22

2.1. Relación de Divisibilidad en $\mathbb{Z}\boldsymbol{m}$ 22

2.2. Unidades y Asociados 24

2.2.1. Unidades: 24

2.2.2. Asociados 25

2.2.3. La relación de ser asociados es una relación de equivalencia 26

2.3. NORMA 27

2.3.1. Una primera concepción de Norma 28

2.3.2. Definición de Norma 29

2.3.3. Subgrupos a partir de la Norma 32

2.3.4. Norma de una Multiplicación 34
2.4. Números Primos 40
2.4.1. Caracterización de números primos en $\mathbb{Z}\boldsymbol{m}$. 41
2.4.2. Caracterización de los $\mathbb{Z}\boldsymbol{m}$ según la descomposición factorial de $\boldsymbol{m}$. 42
2.5. Diagramas de Hasse 44
2.5.1. Diagramas de Hasse y clasificación de elementos 44
2.5.2. Diagramas de Hasse y subgrupos de $\mathbb{Z}\boldsymbol{m}$ 46
3. Teorema Fundamental de la Aritmética en $\mathbb{Z}\boldsymbol{m}$ 47
3.1. Punto de Partida: Enteros 47
3.2. Conjuntos $\mathbb{Z}\boldsymbol{m}$ 48
3.2.1. Teorema Fundamental de la Aritmética en $\mathbb{Z}\boldsymbol{m}$ 48
4. Construcción de Anillos Finitos 51
4.1. Adición – Multiplicación 51
4.1.1. Tabla de Adición 51
4.1.2. Multiplicación 53
5. Conclusiones: 65
Referencias 68

TABLAS

Tabla 1: Tabla de multiplicación de $\mathbb{Z}4$ 23
Tabla 2: Tabla de adición en $\mathbb{Z}8$ 28
Tabla 3: Normas de $\mathbb{Z}8$ 28
Tabla 4: Normas y elementos de $\mathbb{Z}12$ 33
Tabla 5: Multiplicación de normas en $\mathbb{Z}17$ 35
Tabla 6: Multiplicación de Normas en $\mathbb{Z}14$ 35
Tabla 7: M.C.D entre las Normas de $\mathbb{Z}12$ 36
Tabla 8: Multiplicación de Normas en $\mathbb{Z}12$ 36
Tabla 9: Comparación entre M.C.D de dos normas y Norma de una multiplicación. ..... **¡Error! Marcador no definido.**
Tabla 10: Multiplicación de Normas en $\mathbb{Z}72$ 37
Tabla 11: Características de la Norma de una multiplicación 37
Tabla 12: Tabla de multiplicación de $\mathbb{Z}8$ 40
Tabla 13: Tabla de divisores en $\mathbb{Z}8$ 40
Tabla 14: Construcción tabla de adición para J 52
Tabla 15: Construcción tabla de adición para J 52
Tabla 16: Construcción final tabla de adición para J 53
Tabla 17: Construcción tabla de multiplicación en J (Parte 1) 55
Tabla 18: Construcción tabla de multiplicación para J (Parte 2) 56
Tabla 19: Construcción tabla de multiplicación para J (Parte 3) 57
Tabla 20: Construcción tabla de multiplicación para J (Parte 4) 57
Tabla 21: Construcción tabla de multiplicación para J (Parte 5) 58
Tabla 22: Construcción tabla de multiplicación para J (Parte 6) 59
Tabla 23: Caso 1. Tabla de Multiplicación para J. 60
Tabla 24: Caso 2. Tabla de Multiplicación para J 60
Tabla 25: Caso 3. Tabla de Multiplicación para J 60
Tabla 26: Caso 4. Tabla de Multiplicación para J 60
Tabla 27: Multiplicación 1 $\otimes$ no distributiva respecto a $\oplus$ en J (Caso 1) 61
Tabla 28: Multiplicación 2 $\otimes$ no distributiva respecto a $\oplus$ en J (Caso 1) 61
Tabla 29: Multiplicación 3 $\otimes$ no distributiva respecto a $\oplus$ en J (Caso 2) 62
Tabla 30: Multiplicación 4 $\otimes$ no distributiva respecto a $\oplus$ en J (Caso 2) 62
Tabla 31: Multiplicación 5 $\otimes$ no distributiva respecto a $\oplus$ en J (Caso 4) 62
Tabla 32: Multiplicación 6 $\otimes$ no distributiva respecto a $\oplus$ en J (Caso 4) 63
Tabla 33: Tabla de Multiplicación final para J 63

IMÁGENES

Imagen 1: Diagrama de Hasse para $D(12)$ 44
Imagen 2: Organización de elementos de $\mathbb{Z}12$ 44
Imagen 3: Organización según características en $\mathbb{Z}12$ 45
Imagen 4: Organización de elementos según características en $\mathbb{Z}60$ 46
Imagen 5: Organización de subgrupos de $\mathbb{Z}12$ 46
Imagen 6: Programa en Python para $\mathbb{Z}12$ 49

ANEXOS

Anexo A: Código programa elaborado en Python.....69
Anexo B: Análisis realizado en *Propiedades 3.1* para tablas de multiplicación (caso 1a) 72
Anexo C: Análisis realizado en *Propiedades 3.1* para tablas de multiplicación (caso 1b) 75
Anexo D: Análisis realizado en Propiedades 3.1 para tablas de multiplicación (Caso 2a) 77
Anexo E: Análisis realizado en *Propiedades 3.1* para tablas de multiplicación (Caso 2b).....80
Anexo F: Análisis realizado en *Propiedades 3.1* para tablas de multiplicación (caso 4a).....83
Anexo G: Análisis realizado en *Propiedades 3.1* para tablas de multiplicación (caso 4b).....85
Anexo H: Análisis realizado en *Propiedades 3.1* para tablas de multiplicación (Caso 2) Tabla distributiva.....88

Introducción

El presente trabajo surge como una propuesta del Seminario de Álgebra de la Universidad Pedagógica Nacional en el semestre 2014-2 en marco del estudio de relaciones de divisibilidad en estructuras algebraicas no usuales (extensiones cuadráticas, estructuras finitas…), para este semestre se planteó la idea de estudiar dicha relación en los conjuntos $\mathbb{Z}_m$. El trabajo se comenzó a realizar y finalmente se optó por tomarlo como propuesta para trabajo de grado para optar al título de Licenciado en Matemáticas. El interés particular por estudiar este tipo de estructuras surgió en el curso de Teoría de Números del programa de la licenciatura en matemáticas de la UPN y posteriormente en el Seminario de Algebra ofrecido allí.

El trabajo parte de un marco de referencia obtenido a partir de una consulta bibliográfica con el fin de identificar cuáles elementos teóricos servirían de apoyo para la elaboración del documento, en éste podrán encontrarse elementos referentes a la Teoría de Números, Teoría Algebraica de Números, Teoría de Grupos y Anillos y otros elementos asociados, también se encontrarán algunos teoremas que servirán de base para la construcción de todos los demás elementos.

A partir de todos estos elementos y el estudio que se realiza, en la segunda sección se encuentra todo lo relacionado al estudio de la relación de divisibilidad en $\mathbb{Z}_m$, partiendo de la definición de ésta y sus propiedades, para finalmente construir nociones en relación a las unidades, asociados, primos y compuestos del conjunto, cómo se definen, cómo se identifican y luego, una caracterización de estos a partir de un nuevo elemento de estudio llamado norma, éste último resulta de gran interés para el estudio posterior pues será quién permita definir y caracterizar todos los elementos futuros, así, se encuentra un estudio detallado de este elemento y todo lo que lo caracteriza en sí. La norma permite agrupar los elementos según ciertas características, genera clases de equivalencia, genera subgrupos y además, permite posteriormente tener algunos elementos para la construcción del Teorema Fundamental de la Aritmética (TFA) en $\mathbb{Z}_m$ y construcción de anillos. Adicional a esto se realizó un programa usando el Software Python que permite realizar el análisis de cada conjunto arrojando los resultados importantes de cada uno.

Enseguida, se podrá encontrar una definición de número primo en $\mathbb{Z}_m$ y una caracterización de éstos a partir de la norma, enseguida se hablará del comportamiento de los $\mathbb{Z}_m$ atendiendo a los elementos estudiados y según la descomposición factorial de m, todo esto con el fin de dar paso a la construcción del TFA partiendo de los elementos estudiados y de las nociones clásicas del teorema en las estructuras usuales.

Por último, se encontrará la construcción de los anillos finitos partiendo de los elementos primordiales estudiados, entre estos están las normas, los asociados, las unidades, entre otros, además, esta construcción se hace partiendo de algunos elementos trabajados en las estructuras usuales y realizando una asociación entre todos estos, la construcción se hace partiendo de una operación $\oplus$ adición para construir a partir de esta otra operación $\otimes$ multiplicación.

Metodología

Inicialmente, el primer acercamiento que se tuvo con el trabajo fue el de indagación, trabajando en la estructura a partir de los elementos conocidos de otras más cercanas, por ejemplo la estructura de los números enteros y la relación de divisibilidad definida en esta, aquí se definen algunos elementos como divisores, primos, compuestos; así, el primer paso del estudio fue realizar una "copia" de estos elementos en cuanto a la estructura de los conjuntos $\mathbb{Z}_m$. Allí se definió "divisor" "primos" y "compuesto" de la misma manera que se hace en los enteros, claramente esto no arrojó resultados favorables, pues cada una de estas definiciones se quedaba corta en relación a lo esperado.

De esta manera surge la necesidad de realizar una consulta bibliográfica en torno a estos elementos y redefinirlos, es así como surgen nociones como asociado, unidad, un elemento de gran importancia al que desde el trabajo se le llamó "norma" y otros asociados al estudio referente, todo esto dio paso para finalmente comenzar a consolidar el estudio general de los conjuntos $\mathbb{Z}_m$ y todas sus propiedades. De esta manera, a lo largo del estudio se vio la necesidad de construir un programa en Python que sirviera de ayuda para agilizar los cálculos y disminuyera los posibles errores. Adicional a todo lo mencionado, también se hizo uso del software Microsoft Excel para generalizar algunos resultados y relacionarlos con los elementos ya trabajados. Además, también se usó el método ensayo – error para la construcción final de las tablas de multiplicación y el uso de ejemplos para apoyar cada construcción.

Objetivos

Este trabajo se encuentra fundamentado sobre un objetivo general apoyado en 6 objetivos específicos, estos se describen a continuación:

Objetivo General:

Realizar la construcción de anillos finitos a partir de las propiedades obtenidas del estudio de divisibilidad en $\mathbb{Z}_m$.

Objetivos Específicos:

- Realizar una revisión documental en torno a la teoría de números y teoría algebraica de números que apoyen el trabajo.
- Realizar un estudio de las características de los conjuntos $\mathbb{Z}_m$.
- Construir un programa que apoye el desarrollo del estudio por medio del software Python.
- Realizar un análisis de la relación de divisibilidad en $\mathbb{Z}_m$ y construir un teorema fundamental de la aritmética allí.
- Relacionar los resultados obtenidos con estructuras numéricas usuales.
- Implementar un método de construcción de anillos finitos a partir de las propiedades estudiadas.

1. Marco de Referencia

La teoría de números es una rama importante de la teoría algebraica de números, que estudia la relación de divisibilidad en la estructura de los números enteros. Debido a que el objetivo central de este trabajo estará puesto en el estudio de una estructura algebraica finita, dos operaciones definidas dentro de ésta, las propiedades que cumplen, y la relación de divisibilidad allí establecida, es necesario presentar algunas definiciones preliminares que servirán de apoyo para una comprensión completa del tema a tratar.

1.1. Teoría de números:

En primera instancia, trataremos algunos de los elementos centrales en torno a la teoría de números tales como el máximo común, mínimo común múltiplo, el conjunto $\mathbb{Z}_m$ y algunos teoremas relacionados a éstos, los cuales nos darán un primer acercamiento a los elementos que se estudiarán en capítulos posteriores.

1.1.1. Máximo Común Divisor

Sean $a, b \in \mathbb{Z}$ diferentes de 0. El conjunto de todos los divisores comunes de a y b es un conjunto finito de números enteros, cuyo máximo se denomina el *Máximo Común Divisor* de a y b. Lo notamos $MCD(a, b)$ o simplemente (a, b). Puesto que, si $x \mid a$ entonces $x \mid (-a)$, es fácil observar que $(a, b) = (a, -b) = (-a, b) = (-a, -b)$ (Rubiano, Jiménez y Gordillo, 2004, p.27).

1.1.2. Mínimo Común Múltiplo

El menor múltiplo común positivo de dos enteros a y b diferentes de cero se denomina el *Mínimo Común Múltiplo* de a y b y se denota $MCM(a, b)$ o simplemente $[a, b]$. Puesto que dados a y b enteros cualesquiera diferentes de cero, los números ab y $-ab$ son ambos múltiplos comunes de a y b y uno de ellos es positivos, entonces el PBO[1] garantiza la existencia y unicidad de $[a, b]$. Es inmediato deducir de la definición que $[a, b] = [-a, b] = [a, -b] = [-a, -b]$ (Rubiano *et al*., 2004, p.39).

Teorema: Sean a y b enteros no nulos. Entonces,

$$[a, b] = \frac{|ab|}{(a, b)}$$

1.1.3. Conjuntos $\mathbb{Z}_m$

Los conjuntos $\mathbb{Z}_m$ se definen como:

$$\mathbb{Z}_m = \{n < m \mid n, m \in \mathbb{Z}^+ \ \wedge m \neq 0,1\}$$

[1] Principio de buena ordenación: Todo subconjunto no vacío S de números naturales posee un mínimo.

En estos se establecen las siguientes operaciones y las propiedades que estas cumplen.

Operaciones en $\mathbb{Z}_m$:

Adición:
Sean a y b tal que $a, b \in \mathbb{Z}_m$, se define

$$a \oplus b = res\left(\frac{a+b}{m}\right)$$

Siendo "$\boldsymbol{res}$" el residuo dejado de la división y $\times$ la operación multiplicación usual en $\mathbb{Z}$.

Propiedades:

- Conmutativa:

$$a \oplus b = b \oplus a$$

- Asociativa:

$$(a \oplus b) \oplus c = a \oplus (b \oplus c)$$

- Elemento Neutro:

  Existe 0 tal que $a \oplus 0 = 0 \oplus a = a, \forall a \in \mathbb{Z}_m$

- Elementos inversos:

  $\forall a \in \mathbb{Z}_m$ Existe $-a$ tal que $a \oplus -a = -a \oplus a = 0$

Luego, la pareja $(\mathbb{Z}, \oplus)$ es un grupo abeliano[2].

Multiplicación:

Sean a y b tal que $a, b \in \mathbb{Z}_m$, se define

$$a \otimes b = res\left(\frac{a \times b}{m}\right)$$

Siendo "$\boldsymbol{res}$" el residuo dejado de la división y $\times$ la operación multiplicación usual en $\mathbb{Z}$.

[2] Pág. 5 ***(Estructuras)***.

Propiedades:

- Conmutativa:

$$a \otimes b = b \otimes a$$

- Asociativa:

$$(a \otimes b) \otimes c = a \otimes (b \otimes c)$$

- Elemento Neutro:

Existe 1 tal que $a \otimes 1 = 1 \otimes a = a, \forall a \in \mathbb{Z}_m$

Luego, la pareja $(\mathbb{Z},\otimes)$ es un grupo[3].

Las operaciones $\oplus$ y $\otimes$ se encuentran relacionadas de la siguiente manera:

$$a \otimes (b \oplus c) = a \otimes b \oplus a \otimes c$$
$$(b \oplus c) \otimes a = b \otimes a \oplus c \otimes a$$

Así, podemos observar que la tripla $(\mathbb{Z},\oplus,\otimes)$ tiene estructura de anillo conmutativo con unidad.

Nota: En adelante, se usará la notación $a + b$ para referirnos $a \oplus b$ y ab para referirnos a $a \otimes b$.

1.1.4. Teorema Fundamental de la Aritmética. (TFA)

Un entero $n > 1$ es un primo o puede ser expresado como un producto de primos. Si convenimos que un primo es ya un producto de primos, entonces la factorización prima de cualquier entero $n > 1$ es única, excepto por el orden en que aparecen los factores primos. Esta propiedad de los enteros positivos mayores que 1 es conocida como ***El Teorema Fundamental de la Aritmética (TFA)*** (Pettofrezzo, 1972, p. 51)

1.1.5. Congruencia

Sean a y b enteros cualesquiera y b un entero positivo. Si $m|(a - b)$ decimos que a y b son congruentes módulo m y escribimos $a \equiv b\ (mod\ m)$ (Rubiano et al., 2004, p. 98).

A partir de estas congruencias es posible dar una definición de los $\mathbb{Z}_m$ desde clases residuales, como se muestra a continuación:

[3] Pág. 5 ***(Estructuras)***.

1.1.6. Conjuntos $\mathbb{Z}_m$ como clases residuales

La congruencia es una relación de equivalencia ya que verifica las propiedades reflexiva, simétrica y transitiva. Así, podemos realizar una agrupación del conjunto de los números enteros en familias disyuntas de tal manera que dos números son congruentes modulo m si están en la misma clase.
A estas familias las llamamos clases residuales modulo m y designamos por $\mathbb{Z}_m$ al conjunto formado por ellas.

Así, los elementos $0,1,\dots,m-1$ se encuentran en clases residuales distintas. Y así, como todo número puedes escribirse de manera única de la forma $n = mc + r$ con c entero y $0 \leq r \leq m-1$, entonces todo número entero es congruente con alguno de los números enteros $0,1,\dots,m-1$. De manera general, existen exactamente m clases residuales módulo m.

Si tomamos como representante al menor elemento de cada una de las clases residuales obtenemos el conjunto definido en el ítem 1.1.3.

Además, las congruencias nos permiten generar unas congruencias lineales a partir de un polinomio $f(x)$ de grado 1, a continuación estas se definen y se plantean algunos teoremas importantes para el desarrollo del trabajo.

1.1.7. Congruencia lineal:

La congruencia lineal $f(x) \equiv 0\ (mod\ n)$ se llama lineal cuando $f(x)$ es un polinomio de grado 1. Toda congruencia lineal se puede escribir en la forma $ax \equiv b\ (mod\ n)$ (Rubiano et al., 2004, p. 121).

Teorema: La congruencia lineal $ax \equiv b\ (mod\ n)$ tiene solución si y sólo si $d|b$, donde $d = (a,n)$. Si la congruencia tiene solución, entonces tiene exactamente $(d-1)$ soluciones incongruentes.

Lo que implica:

I. Si $d|b$, hay una solución.
II. Si hay solución, entonces $d|b$.
III. Si x_0 es una solución entonces $x_0 + k\frac{n}{d}$ es solución entera para todo k.
IV. Todas las soluciones se encuentran entre las soluciones mencionadas en 3.
V. Las soluciones incongruentes son precisamente.

$$x_0, x_0 + \frac{n}{d}, x_0 + \frac{2n}{d}, \dots, x_0 + \frac{(d-1)n}{d}.$$

1.2. Teoría Algebraica de Números (TAN)

Dos elementos que serán de gran importancia para el desarrollo del trabajo son las unidades y los asociados, a continuación se da una descripción de ellos desde la TAN.

1.2.1. Unidades

Una unidad en un anillo A es un elemento $a \in A$ que tiene inverso para el producto, es decir que existe a^{-1} tal que $aa^{-1} = a^{-1}a = 1$ (Arrondo, 2011, p.6).

1.2.2. Asociados

Dos elementos a, b en un anillo A son asociados si $a = ub$ donde u es una unidad (Tabara, 2001, p.43).

1.3. Estructuras

A continuación se da una definición de los tipos de estructura que se abordarán a lo largo del trabajo, que además, son el tipo de estructura resultante en los conjuntos $\mathbb{Z}_m$.

1.3.1. Grupo

Un grupo es un conjunto $(G, \oplus)$ con una operación interna $\oplus$ que verifica las siguientes propiedades:

1. $(a \oplus b) \oplus c = a \oplus (b \oplus c)$
2. Existe $e \in G$ (Elemento Neutro) tal que $a \oplus e = e \oplus a = a$ para cualquier $a \in G$
3. Para cada $a \in G$ existe $-a \in G$ (Elemento inverso) tal que $a \oplus -a = -a \oplus a = e$

1.3.2. Grupo Abeliano

Si además: $a \oplus b = b \oplus a$ para cualesquiera $a, b \in G$ (Propiedad conmutativa), entonces se dice que G es un Grupo Abeliano (Arrondo, 2011, p.2).

1.3.3. Subgrupo y Grupos cíclicos

Si G es un grupo $a \in G$, entonces:

$$H = \{a^n | n \in \mathbb{Z}\}$$

es un subgrupo de G. Este grupo es el subgrupo cíclico de G generado por a. Además, dado un grupo G y un elemento $a \in G$, si

$$G = \{a^n | n \in \mathbb{Z}\}$$

Entonces a es un generador de G y el grupo $G =< a >$ es cíclico

Teorema: Todo grupo cíclico es Abeliano (Fraleigh, 1988, pp. 57)

1.3.4. Anillo

Un anillo $(A, +, \cdot)$ es un conjunto A provisto de dos operaciones $+$ y $\cdot$, llamadas adición y multiplicación respectivamente, que satisface los axiomas siguientes.

1) $(A, +)$ es un grupo abeliano
2) La multiplicación es asociativa.
3) Las dos operaciones están relacionadas por las propiedades distributivas

$$a(b + c) = ab + ac = (b + c)a = ba + ca$$

Para todo $a, b, c \in A$

Un anillo donde la multiplicación es conmutativa se dice un anillo conmutativo. Un anillo que tiene una identidad para la multiplicación, que se representa usualmente por 1, es un anillo con identidad (Rubiano *et al*., 2004, p. 109).

2. Divisibilidad en $\mathbb{Z}_m$

Este trabajo parte del estudio de la relación de divisibilidad en los conjuntos $\mathbb{Z}_m$ y a partir de esta se plantean los elementos que serán la base general del trabajo, en primera instancia plantearemos la noción de divisibilidad en esta estructura tomando como referencia la estructura de los $\mathbb{Z}$, esto con el fin de obtener los divisores de un elemento $a \in \mathbb{Z}_m$ y plantear los conceptos que den continuidad al estudio.

2.1. Relación de Divisibilidad en $\mathbb{Z}_m$

Definimos la relación de divisibilidad en $\mathbb{Z}_m$, de manera similar a como se hace en la estructura de los $\mathbb{Z}$, así:

Sean a y b tal que $a, b \in \mathbb{Z}_m$

$$a|b \text{ Si y solo si } \exists c \in \mathbb{Z}_m \text{ tal que } ac = b$$

Esta relación no es de orden, debido a que no es antisimétrica, ya que dados dos números a y b, si $a|b$ y $b|a$ no es estrictamente necesario que $a = b$. Que no se cumpla la propiedad antisimétrica junto con la relación establecida es el resultado que permitirá establecer la relación de ser asociados en la estructura, en la siguiente sección se estudiará esta nueva relación.

Sin embargo, si se cumplen las propiedades:

a) Reflexiva: Para todo $a \in \mathbb{Z}_m$ se cumple $a|a$

Dm//: Por ser el 1 el elemento idéntico de la multiplicación en $\mathbb{Z}_m$ se tiene que para todo $a \in \mathbb{Z}_m$, $a \times 1 = a$, por consiguiente $a|a$.

b) Transitiva: Dados a, b y $c \in \mathbb{Z}_m$ si $a|b$ y $b|c$ entonces $a|c$

Dm//: Si $a|b$ entonces $\exists k \in \mathbb{Z}_m$, tal que $a \times k = b$, y como $b|c$ entonces existe d tal que $b \times d = c$.
Reemplazamos el valor de b en la segunda igualdad y obtenemos $(a \times k) \times d = c$, como la multiplicación en $\mathbb{Z}_m$ es asociativa, entonces $a \times (b \times d) = c$, y dado que $(b \times d) \in \mathbb{Z}_m$, entonces $a|c$.

Inicialmente, bajo esta noción de divisibilidad buscamos los divisores de cada elemento en $\mathbb{Z}_m$, de la siguiente manera:

Para este caso, usaremos a $m = 4$, luego

La tabla de multiplicación de $\mathbb{Z}_4$ es:

×	**0**	**1**	**2**	**3**
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

Tabla 1: *Tabla de multiplicación de* $\mathbb{Z}_4$

La técnica usada para encontrar los divisores de cada elemento de $\mathbb{Z}_4$ es la siguiente:

Sea a un elemento de $\mathbb{Z}_m$, en este caso específico, de $\mathbb{Z}_4$.

Representemos a cada fila con algún i y cada columna como algún j, para $0 \leq i \leq m-1$ y $0 \leq j \leq m-1$. Si a aparece en la casilla (i, j), entonces i, j son divisores de a.

Para este caso, tanto i como j son números entre 0 y 4, de esta manera tenemos que:

- 1 aparece en la casilla (1,1) entonces 1 es divisor de 1.
- 1 aparece en la casilla (3,3) entonces 3 es divisor de 1.
- 2 aparece en la casilla (1,2) entones 1,2 son divisores de 2. (También aparece en la casilla (2,1)).
- 2 aparece en la casilla (2,3) entonces 2,3 son divisores de 2. (También aparece en la casilla (3,2)).
- 3 aparece en la casilla (1,3) entonces 1,3 son divisores de 3. (También aparece en la casilla (3,1)).

Luego:

$$D_1 = \{1,3\}$$
$$D_2 = \{1,2,3\}$$
$$D_3 = \{1,3\}$$

En la siguiente sección buscaremos una posible definición de número primo en la estructura $\mathbb{Z}_m$, para esto es necesario hacer uso de nuevos conceptos que veremos a continuación.

2.2. Unidades y Asociados

Uno de los problemas centrales del trabajo es lograr una particularización de números primos en la estructura y a partir de esto buscar lo que podría llegar a ser el "Teorema Fundamental de la aritmética" en $\mathbb{Z}_m$. Esto intuitivamente nos llevaría a definir *primo* como se define en la estructura de los números enteros, es decir: "Sea $b \in \mathbb{Z}_m$, si b es dividido únicamente por sí mismo y por el módulo, entonces b es primo". Bajo esta definición de lo que sería un primo en $\mathbb{Z}_m$ notamos que no se podría establecer el TFA en la estructura, dicho problema nos condujo a estudiar a fondo algunos de los elementos de la Teoría Algebraica de Números como son las unidades y los asociados, éstos elementos serán la base para todo el estudio posterior.

Inicialmente, tenemos en cuenta las siguientes consideraciones

- Para todo $\mathbb{Z}_m$, se tiene que el elemento 1, para cualquier elemento $a \in \mathbb{Z}_m$ $a \times 1 = a$, luego, 1 es el módulo de $\mathbb{Z}_m$.
- Se observa además que a pesar de que 1 sea el módulo, existen algunos elementos que lo dividen.

2.2.1. Unidades:

Teniendo en cuenta las consideraciones anteriores, entonces definimos:

Unidad: Cualquier elemento $a \in \mathbb{Z}_m$, tal que $a|1$ se llama unidad.

Ahora bien, la definición de unidad desde la Teoría Algebraica de Números es:

> *Una unidad en un anillo A es un elemento $a \in A$ que tiene inverso para el producto, es decir que existe a^{-1} tal que $aa^{-1} = a^{-1}a = 1$.*

A continuación veremos que las dos definiciones resultan ser equivalentes, por tanto podremos usar cualquiera de las dos.

Desde la TAN, a es unidad, si a tiene elemento inverso, esto es:

$$aa^{-1} = 1$$

Como $aa^{-1} = 1$, tenemos por definición de divisibilidad que $a|1$.

De esta manera llegamos desde una definición a la otra, de manera similar podríamos revertir el proceso.

2.2.2. Asociados

Durante el trabajo se establecieron las siguientes definiciones:

Asociados:

- Dos números son asociados si tienen exactamente los mismos divisores.
- Sean $a, b \in \mathbb{Z}_m$, se dice que a y b son asociados si $a|b$ y $b|a$.

A continuación veremos que esta definición resulta ser equivalente con la definición establecida en la TAN:

> *Dos elementos a, b en un anillo A son asociados si $a = ub$ donde u es una unidad.*

Trataremos de llegar desde la definición de asociado nuestra a la definición de asociado de la TAN.

- Sean $a, b \in \mathbb{Z}_m$, si $a|b$ y $b|a$ entonces a y b son asociados:

Por definición de divisibilidad, tenemos que: $ax = b$ Y $by = a$, reemplazando, obtenemos $(ax)y = a$, como la multiplicación en $\mathbb{Z}_m$ es asociativa entonces $a(xy) = a$, por la propiedad del elemento neutro, $xy = 1$.

Por definición de unidad sabemos que si $xy = 1$, entonces x es el inverso de y, y y es el inverso de x con respecto a la multiplicación, luego como x y y, son elementos invertibles entonces x y y son unidades.

Luego $ax = b$ y $by = a$, lo que implica que a y b son asociados, siendo x y y unidades.

Teorema 1: Sea $a \in \mathbb{Z}_m$, si $(a, m) = 1$ entonces a es unidad en $\mathbb{Z}_m$.

Dm//:

Dado que $(a, m) = 1$, por propiedades de M.C.D podemos reescribir este como:

$$ax + my = 1$$

Al llevar esto a congruencias tenemos que $ax + my \equiv 1\ (mod\ m)$, dado que $x \in \mathbb{Z}$, existe algún $b \in \mathbb{Z}_m$ tal que $x \equiv b\ (mod\ m)$

Luego, al realizar los remplazos requeridos llegamos a que

$$ab + 0 \equiv 1\ (mod\ m)$$

Así,

$$ab \equiv 1\ (mod\ m)$$

Llegando a que $ab = 1$ en $\mathbb{Z}_m$, luego, por definición, a es unidad en $\mathbb{Z}_m$

Teorema 2: Dado un $\mathbb{Z}_m$ tal que m es primo, entonces todo elemento $a \in \mathbb{Z}_m$ es unidad.

Dm//: Para cualquier elemento a de $\mathbb{Z}_m$ se cumple que $(a, m) = 1$, debido a que m es primo, luego, a es unidad.

Teorema 3: Los elementos $a \in \mathbb{Z}_m$ que están asociados con 1 son las unidades de $\mathbb{Z}_m$.

Dm//: Si a está asociado con 1, tenemos que $a|1$, luego $ac = 1$.

Por definición, a es unidad.

Teorema 4: Sean $a, b \in \mathbb{Z}_m$, si a y b son unidades, entonces ab es unidad.

Dm//: Dado que a y b son unidades, entonces existe a^{-1} y $b^{-1} \in \mathbb{Z}_m$ tal que $aa^{-1} = 1$, y $bb^{-1} = 1$.

Así, tenemos que $(aa^{-1})(bb^{-1}) = 1$, como la multiplicación en $\mathbb{Z}_m$ es asociativa y conmutativa, entonces $(ab)(a^{-1}b^{-1}) = 1$

Tenemos finalmente que $(ab)(ab)^{-1} = 1$, luego ab es un elemento invertible, luego ab es una unidad.

2.2.3. La relación de ser asociados es una relación de equivalencia

$a\mathbb{R}b$ Si y sólo si a está asociado con b

Para comprobar que efectivamente la relación de ser asociados es una relación de equivalencia debemos comprobar que es:

Reflexiva: Para todo $a \in \mathbb{Z}_m$, a está asociado con a

Dm//: Dado que $ac = a$, siendo $c = 1$ una unidad, entonces a está asociado con a, por definición.

Simétrica: Sean $a, b \in \mathbb{Z}_m$, si a está asociado con b, entonces b está asociado con a

Dm//: Por definición de asociado, $a = ub$ donde u es una unidad, dado, que u es unidad, entonces existe u^{-1}, tal que $uu^{-1} = 1$.

Multiplicamos en ambos lados de la igualdad por u^{-1} y obtenemos $au^{-1} = b$, como u es unidad, entonces u^{-1} también lo será por ser el inverso de u.

Luego $b = au^{-1}$, y por definición de asociado, b está asociado con a.

Transitiva: Sean a, b y $c \in \mathbb{Z}_m$, si a está asociado con b, y b está asociado con c, entonces a está asociado con c

Dm//: Como a está asociado con b, entonces $a = u_1 b$ y como b está asociado con c, entonces $b = u_2 c$, siendo u_1 y u_2 unidades.

Reemplazando obtenemos $a = u_1(u_2 c)$, luego $a = (u_1 u_2)c$, como el producto de unidades es una unidad, entonces $a = u_3 c$, siendo u_3 una unidad, luego, por definición de asociado, a está asociado con c.

De esta manera queda demostrado que la relación de ser asociados, resulta ser una relación de equivalencia, en la cual la clase de un elemento son todos aquellos que estén asociados con él, estas clases quedan definidas como:

$$[\boldsymbol{a}] = \{\boldsymbol{x} \in \mathbb{Z}_{\boldsymbol{m}} | \boldsymbol{a} = \boldsymbol{u_i x}, \text{Siendo } \boldsymbol{u_i} \text{ unidad}\}$$

2.3. NORMA[4]

Ya hemos visto que la relación de asociados genera clases de equivalencia, las cuales podemos re-caracterizar usando la norma.

La norma de un número nos brinda información relevante de éste, esta nos indicará si el número es unidad, si dos números son asociados, si un número es primo (más

[4] Es de resaltar que no nos estamos refiriendo a la noción usual de norma trabajada en la teoría algebraica de números, es solo un nombre que le damos a lo que usualmente se conoce como orden desde la TAN.

adelante veremos qué es ser primo en $\mathbb{Z}_m$) entre otras varias características que veremos más adelante.

2.3.1. Una primera concepción de Norma

En primera instancia, la norma de x, notada como $N(x)$, se define como la menor cantidad de veces que se debe sumar a x consecutivamente (usando la suma en $\mathbb{Z}_m$) hasta que el resultado sea 0. Por definición, la norma de 0 es 1.

A continuación se muestra la obtención de normas para los elementos de $\mathbb{Z}_8$:

$\oplus$	**0**	**1**	**2**	**3**	**4**	**5**	**6**	**7**
0	0	1	2	3	4	5	6	7
1	1	2	3	4	5	6	7	0
2	2	3	4	5	6	7	0	1
3	3	4	5	6	7	0	1	2
4	4	5	6	7	0	1	2	3
5	5	6	7	0	1	2	3	4
6	6	7	0	1	2	3	4	5
7	7	0	1	2	3	4	5	6

Tabla 2: *Tabla de adición en* $\mathbb{Z}_8$

Elemento x	**Sumas reiteradas**	**Conteo de Sumas**	**Norma de x, $N(x)$**
1	$\mathbf{1},\ 1+1=\mathbf{2},\ 2+1=\mathbf{3},\ 3+1=\mathbf{4},\ 4+1=\mathbf{5},\ 5+1=\mathbf{6},\ 6+1=\mathbf{7},\ 7+1=\mathbf{0}$	8	$N(1)=8$
2	$\mathbf{2}, 2+2=\mathbf{4}, 4+2=\mathbf{6}, 6+2=\mathbf{0}$	4	$N(2)=4$
3	$\mathbf{3},\ 3+3=\mathbf{6},\ 6+3=\mathbf{1},\ 6+3=\mathbf{4},\ 4+3=\mathbf{7},\ 7+3=\mathbf{2},\ 2+3=\mathbf{5},\ 5+3=\mathbf{0}$	8	$N(3)=8$
4	$\mathbf{4}, 4+4=\mathbf{0}$	2	$N(4)=2$
5	$\mathbf{5}, 5+5=\mathbf{2}, 2+5=\mathbf{7}, 7+5=\mathbf{4}, 4+5=\mathbf{1}, 1+5=\mathbf{6}, 6+5=\mathbf{3}, 3+5=\mathbf{0}$	8	$N(5)=8$
6	$\mathbf{6}, 6+6=\mathbf{4}, 4+6=\mathbf{2}, 2+6=\mathbf{0}$	4	$N(6)=4$
7	$\mathbf{7}, 7+7=\mathbf{6}, 6+7=\mathbf{5}, 5+7=\mathbf{4}, 4+7=\mathbf{3}, 3+7=\mathbf{2}, 2+7=\mathbf{1}, 1+7=\mathbf{0}$	8	$N(7)=8$

Tabla 3: *Normas de* $\mathbb{Z}_8$

Cada una de estas sumas reiteradas, es equivalente a plantear una congruencia lineal de la siguiente forma: $ax \equiv 0\ (mod\ 8)$ en la cual, la menor solución diferente de 0 será la norma de a.

Ejemplo: Nuevamente, en $\mathbb{Z}_8$, si se plantea la congruencia lineal:

$4x \equiv 0\ (mod\ 8)$, tiene como soluciones a $0, \mathbf{2}, 4$ y 6, luego la norma de 4 será 2. Por ser 2 la menor solución diferente de 0 de la congruencia lineal.

Así, una definición alterna de norma para cualquier $\mathbb{Z}_m$ será:

2.3.2. Definición de Norma

Definición: Sea $a \in \mathbb{Z}_m$, y $ax \equiv 0\ (mod\ m)$ la congruencia lineal generada por a, entonces la norma de a $\big(N(a)\big)$ será la menor solución x_1 diferente de $x_0 = 0$.

Teorema 5: Sea $a \in \mathbb{Z}_m$, entonces $N(a) = \frac{[a,m]}{a}$.

Dm//: Sea $ax \equiv 0\ (mod\ m)$, luego $x_0 = 0$ es la solución trivial de la congruencia.

Ahora, la siguiente solución se obtiene de $x_1 = x_0 + k\frac{m}{d}$, donde $x_0 = 0$, $k = 1$, $d = (a, m)$, esto por el Teorema nombrado en la sección 1.1.6.

Reemplazando tenemos: $x_1 = 0 + \frac{m}{(a,m)}$

Ahora, por teorema 1.1.2 se tiene que $[a, m] = \frac{am}{(a,m)}$, luego $(a, m) = \frac{am}{[a,m]}$, entonces:

$$x_1 = \frac{m}{\frac{am}{[a,m]}} = \frac{[a,m]m}{am} = \frac{[a,m]}{a}$$

$$x_1 = \frac{[a,m]}{a}$$

Así concluimos que $N(a) = \frac{[a,m]}{a}$.

Finalmente, de lo mencionado anteriormente es posible obtener las siguientes posibles formas de la norma de un elemento a.

- Como la cantidad de sumas reiteradas de un elemento a con él mismo en $\mathbb{Z}_m$ hasta obtener 0 como resultado.

- Como solución de una congruencia lineal:

Sea $\mathbb{Z}_m$, y $ax \equiv 0\ (mod\ m)$, y x_0 la menor solución diferente de 0 de la congruencia lineal, entonces x_0 es la norma de $a\ \big(N(a)\big)$.

- En relación al mínimo común múltiplo entre a y m

$$\frac{[a,m]}{a}$$

- En relación al máximo común divisor entre a y m

$$\frac{m}{(a,m)}$$

Teorema 6: El conjunto de normas de $\mathbb{Z}_m$ es igual al conjunto de divisores de m.

Dm//:

- Sea $\mathbb{N}_m$ el conjunto de normas de $\mathbb{Z}_m$. Sea $\frac{[a,m]}{a} = N(a)$ para algún $a \in \mathbb{Z}_m$.

  Tenemos que $\frac{[a,m]}{a} = \frac{m}{(a,m)}$, como $(a,m)|m$ y $m|m$ entonces $\frac{m}{(a,m)}|m$ luego $N(a)|m$.

- Sea $\mathbb{D}_m$ el conjunto de divisores de m

$$\mathbb{D}_m = \{d \in \mathbb{Z}^+ : d|m\}$$

  Como $d|m$ existe un c tal que $dc = m$, al pasar a congruencias módulo m tenemos que, existe c' tal que $c' \equiv c\ (mod\ m)$ y la congruencia obtenida es:

$$dc' \equiv 0\ (mod\ m)$$

  c' Es un elemento que pertenece a $\mathbb{Z}_m$, luego, si d es la incógnita de la congruencia, tenemos que existe alguna solución $d_0 = 0$ y las demás soluciones están dadas por $d = d_0 + k\frac{m}{(c',m)}$, así, si $d_0 = 0$ y $k = 1$, la siguiente solución será $d = \frac{m}{(c',m)}$, luego d es una norma de $\mathbb{Z}_m$.

Teorema 7: La norma de las unidades de $\mathbb{Z}_m$ es m.

Dm//: Sea $a \in \mathbb{Z}_m$, una unidad y $N(a) = \frac{m}{(a,m)}$ cómo a es unidad, entonces $(a,m) = 1$

Así, concluimos que $N(a) = \frac{m}{1} = m$

Teorema 8: Si $ax \equiv 0\ (mod\ m)$, entonces $N(a)|x$.

Dm//: Como $ax \equiv 0\ (mod\ m)$, tenemos $ax = mk$, siendo mk un múltiplo de m

Si $[a, m] = s$, entonces $s|mk$, por consiguiente $s\beta = mk$ y reemplazando obtenemos:

$$ax = mk$$
$$ax = s\beta$$
$$x = \frac{s\beta}{a}$$

Tenemos en cuenta que $\frac{s\beta}{a}$ es un número entero, puesto que $a|s$ por ser s un múltiplo de a.

Como $s = [a, m]$, reemplazamos:

$$x = \frac{[a, b]}{a}\beta$$

Y finalmente, $\frac{[a,b]}{a} = N(a)$ tenemos

$x = N(a)\beta$, lo que implica que $N(a)|x$.

Teorema 9: Sean $a, b \in \mathbb{Z}_m$ si $a|b$ entonces $N(b)|N(a)$

Dm//: Como $a|b$ entonces

$$ac \equiv b \quad (mod\ m)$$
$$N(a)ac \equiv b\ N(a) \quad (mod\ m)$$
$$0c \equiv bN(a) \quad (mod\ m)$$
$$0c \equiv bN(a) \quad (mod\ m)$$

Por el teorema 8, $N(b)|N(a)$

Teorema 10: Dos números están asociados si y solo si tienen la misma norma.

Dm//:

- Sean $a, b \in \mathbb{Z}_m$ tal que a y b son asociados.
  Como a y b están asociados, entonces $a|b$ y $b|a$, por el teorema 9 tenemos que $N(b)|N(a)$ y además $N(a)|N(b)$.
  Como las normas son números enteros positivos, entonces podemos concluir que $N(a) = N(b)$.
- Sean $a, b \in \mathbb{Z}_m$ tal que $N(a) = N(b)$
  Tenemos entonces que $\frac{[a,m]}{a} = \frac{[b,m]}{b} \rightarrow \frac{m}{(a,m)} = \frac{m}{(b,m)}$ así, podemos concluir que $(b, m) = (a, m)$.
  Luego, si $s = (a, m) = (b, m)$ entonces $s|a$, $s|b$ y $s|m$, como $s|b$ y $s|m$ entonces s divide a cualquier combinación lineal de b y m: $s|bw + mz$
  Si $w = 1$,$s|b + mz$ así tenemos que $\alpha s = b + mz$.

  Luego:

  $$\alpha(a, m) = b + mz$$

  Como (a, m) es el menor número que se puedes escribir de la forma $ax + my$ entonces:

  $$\alpha(ax + my) = b + mz$$
  $$\alpha ax + \alpha my = b + mz$$

  Si convertimos a una congruencia $mod\ m$ entonces tenemos

  $$\alpha ax \equiv b\ mod\ m$$

  Luego $a|b\ mod\ m$.

  Similarmente se demuestra que $b|a$.

  Finalmente, como $a|b$ y $b|a$ entonces a y b están asociados.

Teorema 11: Sea $a \in \mathbb{Z}_m$. Si $N(a) = x$ entonces $N(-a) = x$

Dm//: Dado que a y $-a$ son asociados porque $a| -a$ y $-a|a$ se tiene que $N(a) = N(-a) = x$ por el teorema anterior.

2.3.3. Subgrupos a partir de la Norma

Ahora, otro resultado importante que se puede caracterizar a partir de las normas son los subgrupos del grupo $\mathbb{Z}_m$, desde la teoría de grupos y anillos existe un

teorema que dice que el conjunto generado por algún elemento a de $\mathbb{Z}_m$ es un subgrupo de $\mathbb{Z}_m$, de manera más general, esto es:

Sea G un grupo y sea $a \in G$ entonces:

$$H = \{a^n \mid n \in \mathbb{Z}\}$$

Es un subgrupo de G.

Además, se da la siguiente definición:

> ***Definición:*** *El grupo H mencionado es el* ***subgrupo cíclico de G generado por a*** *y se denotará como $< a >$.* (Fraleigh, 1988, p.p. 34)

Este subgrupo se puede generar y redefinir por medio de la norma de un número, veamos a continuación:

Tomemos como ejemplo al conjunto $\mathbb{Z}_{12}$, las normas de $\mathbb{Z}_{12}$ son los divisores de 12, se enlistan a continuación las normas con sus respectivos elementos:

Normas	**1**	**2**	**3**	**4**	**6**	**12**
Elementos	0	6	4 8	3 9	2 10	1 5 7 11

Tabla 4: *Normas y elementos de $\mathbb{Z}_{12}$*

Ahora, veamos los subgrupos generados por cada elemento según el teorema y la definición mencionados anteriormente:

$$< 1 > = \{1,2,3,4,5,6,7,8,9,10,11,0\} = < 5 > = < 7 > = < 11 >$$
$$< 2 > = \{2,4,6,8,10,0\} = < 10 >$$
$$< 3 > = \{3,6,9,0\} = < 9 >$$
$$< 4 > = \{4,8,0\} =< 8 >$$
$$< 6 > = \{6,0\}$$
$$< 0 > = \{0\}$$

Si tomamos cada uno de los subgrupos anteriores y estudiamos sus características en torno a su norma podemos notar lo siguiente:

- En el subgrupo generado por 0 solamente se encuentra el elemento 0, recordemos pues que la norma de 0 es 1.
- En el subgrupo generado por 6 se encuentran los elementos 0 y 6, recordemos:
  - $N(6) = 2$
  - $N(0) = 1$

- En el subgrupo generado por 4, que es el mismo generado por 8 se encuentran los elementos 0, 4 y 8, recordemos:
  - $N(4) = N(8) = 3$
  - $N(0) = 1$

- En el subgrupo generado por 3, que es el mismo generado por 9 se encuentran los elementos 0,3,6 y 9, recordemos:
  - $N(3) = N(9) = 4$
  - $N(6) = 2$
  - $N(0) = 1$
- En el subgrupo generado por 2, que es el mismo generado por 10 se encuentran los elementos 0,2,4,6,8 y 10, recordemos:
  - $N(2) = N(10) = 6$
  - $N(4) = N(8) = 3$
  - $N(6) = 2$
  - $N(0) = 1$

Entonces, la pregunta es ¿Qué relación existe entre las normas de los elementos en un subgrupo con la norma del elemento que lo genera?

La respuesta a esta pregunta es que: ¡todas las normas de los elementos en un subgrupo dividen a la norma del elemento que lo genera! Así, una forma alternativa de subgrupos en $\mathbb{Z}_m$ será la siguiente:

El conjunto $\ll a \gg = \{x \in \mathbb{Z}_m : N(x) | N(a)\}$ es el mismo subgrupo H generado por a.

2.3.4. Norma de una Multiplicación

A lo largo del estudio surge como parte esencial de éste buscar la manera de caracterizar la norma de la multiplicación de dos números, es decir si $a, b \in \mathbb{Z}_m$ ¿cuál es la norma de ab sin tener que realizar dicha multiplicación?

En primera instancia, el trabajo se centró en analizar los $\mathbb{Z}_m$ siendo m un elemento primo, la siguiente tabla muestra la norma de la multiplicación en $\mathbb{Z}_{13}$. Debido a que

las normas en $\mathbb{Z}_{13}$ son únicamente 1 y 13, el producto debe caer en alguna de esas dos normas, específicamente, en el M.C.D entre las dos normas.

		1	13	13	13	13	13	13	13	13	13	13	13	13
	0	0	1	2	3	4	5	6	7	8	9	10	11	12
1	0	1	1	1	1	1	1	1	1	1	1	1	1	1
13	1	1	13	13	13	13	13	13	13	13	13	13	13	13
13	2	1	13	13	13	13	13	13	13	13	13	13	13	13
13	3	1	13	13	13	13	13	13	13	13	13	13	13	13
13	4	1	13	13	13	13	13	13	13	13	13	13	13	13
13	5	1	13	13	13	13	13	13	13	13	13	13	13	13
13	6	1	13	13	13	13	13	13	13	13	13	13	13	13
13	7	1	13	13	13	13	13	13	13	13	13	13	13	13
13	8	1	13	13	13	13	13	13	13	13	13	13	13	13
13	9	1	13	13	13	13	13	13	13	13	13	13	13	13
13	10	1	13	13	13	13	13	13	13	13	13	13	13	13
13	11	1	13	13	13	13	13	13	13	13	13	13	13	13
13	12	1	13	13	13	13	13	13	13	13	13	13	13	13

Tabla 5: *Multiplicación de normas en* $\mathbb{Z}_{17}$

Lo mencionado anteriormente también se cumple si $m = pq$ siendo p y q elementos primos.

Veamos a continuación la tabla de normas de $\mathbb{Z}_{14}$

		1	14	7	14	7	14	7	2	7	14	7	14	7	14
	0	0	1	2	3	4	5	6	7	8	9	10	11	12	13
1	0	1	1	1	1	1	1	1	1	1	1	1	1	1	1
14	1	1	14	7	14	7	14	7	2	7	14	7	14	7	14
7	2	1	7	7	7	7	7	7	1	7	7	7	7	7	7
14	3	1	14	7	14	7	14	7	2	7	14	7	14	7	14
7	4	1	7	7	7	7	7	7	1	7	7	7	7	7	7
14	5	1	14	7	14	7	14	7	2	7	14	7	14	7	14
7	6	1	7	7	7	7	7	7	1	7	7	7	7	7	7
2	7	1	2	1	2	1	2	1	2	1	2	1	2	1	2
7	8	1	7	7	7	7	7	7	1	7	7	7	7	7	7
14	9	1	14	7	14	7	14	7	2	7	14	7	14	7	14
7	10	1	7	7	7	7	7	7	1	7	7	7	7	7	7
14	11	1	14	7	14	7	14	7	2	7	14	7	14	7	14
7	12	1	7	7	7	7	7	7	1	7	7	7	7	7	7
14	13	1	14	7	14	7	14	7	2	7	14	7	14	7	14

Tabla 6: *Multiplicación de Normas en* $\mathbb{Z}_{14}$

La $N(ab)$ para dos cualesquiera elementos a, b de $\mathbb{Z}_{14}$ es el M.C.D entre la $N(a)$ y $N(b)$.

> *En general, sea $\mathbb{Z}_m$ tal que m es primo o es el producto de 2 primos, y $a, b \in \mathbb{Z}_m$, entonces $N(ab) = \big(N(a), N(b)\big)$.*

En este punto se podría pensar entonces que la norma de una multiplicación en cualquier $\mathbb{Z}_m$ siempre será el M.C.D entre las dos normas, sin embargo el estudio se vuelve interesante cuando m es un elemento que resulta ser el producto de 3 o más primos, veamos:

Tomemos como ejemplo a $\mathbb{Z}_{12}$, ya que $12 = 2 \cdot 2 \cdot 3$

En las siguientes tablas se muestran respectivamente (a la izquierda) el M.C.D entre las normas y (a la derecha) la norma de la multiplicación, al comparar los resultados de ambas tablas podemos notar que no se cumple que la norma de la multiplicación coincida en todos los casos con el M.C.D entre las dos normas.

M.C.D

		1	12	6	4	3	12	2	12	3	4	6	12
	0	0	1	2	3	4	5	6	7	8	9	10	11
1	0	1	1	1	1	1	1	1	1	1	1	1	1
12	1	1	12	6	4	3	12	2	12	3	4	6	12
6	2	1	6	**6**	2	3	6	**2**	6	3	2	**6**	6
4	3	1	4	2	4	1	4	2	4	1	4	2	4
3	4	1	3	3	1	3	3	1	3	3	1	3	3
12	5	1	12	6	4	3	12	2	12	3	4	6	12
2	6	1	2	**2**	2	1	2	**2**	2	1	2	**2**	2
12	7	1	12	6	4	3	12	2	12	3	4	6	12
3	8	1	3	3	1	3	3	1	3	3	1	3	3
4	9	1	4	2	4	1	4	2	4	1	4	2	4
6	10	1	6	**6**	2	3	6	**2**	6	3	2	**6**	6
12	11	1	12	6	4	3	12	2	12	3	4	6	12

Tabla 7: *M.C.D entre las Normas de $\mathbb{Z}_{12}$*

NORMA

		1	12	6	4	3	12	2	12	3	4	6	12
	0	0	1	2	3	4	5	6	7	8	9	10	11
1	0	1	1	1	1	1	1	1	1	1	1	1	1
12	1	1	12	6	4	3	12	2	12	3	4	6	12
6	2	1	6	**3**	2	3	6	**1**	6	3	2	**3**	6
4	3	1	4	2	4	1	4	2	4	1	4	2	4
3	4	1	3	3	1	3	3	1	3	3	1	3	3
12	5	1	12	6	4	3	12	2	12	3	4	6	12
2	6	1	2	**1**	2	1	2	**1**	2	1	2	**1**	2
12	7	1	12	6	4	3	12	2	12	3	4	6	12
3	8	1	3	3	1	3	3	1	3	3	1	3	3
4	9	1	4	2	4	1	4	2	4	1	4	2	4
6	10	1	6	**3**	2	3	6	**1**	6	3	2	**3**	6
12	11	1	12	6	4	3	12	2	12	3	4	6	12

Tabla 8: *Multiplicación de Normas en $\mathbb{Z}_{12}$*

En las tablas, los elementos resaltados en rojo corresponden a las no coincidencias entre las dos tablas al realizar la debida comparación.

La relación de las normas en los conjuntos $\mathbb{Z}_m$ tal que m se pueda descomponer como factor de 3 o más primos dio paso al estudio del comportamiento de estas, debido a que el M.C.D no nos condujo a una respuesta general.

Para esto se tomó como partida un conjunto lo suficientemente grande como para tener una cantidad significativa de normas y poder estudiar las propiedades que estas cumplieran, este conjunto fue $\mathbb{Z}_{72}$, obteniendo los siguientes resultados:

En la siguiente tabla, en la primera fila y primera columna se encuentran las normas de $\mathbb{Z}_{72}$, y en la intersección de éstas se encuentra el resultado de la norma que se obtiene al multiplicar dos números con estas normas.

N	**1**	**2**	**3**	**4**	**6**	**8**	**9**	**12**	**18**	**24**	**36**	**72**
1	1	1	1	1	1	1	1	1	1	1	1	1
2	1	2	1	1	1	2	1	1	1	2	1	2
3	1	1	3	1	1	1	3	1	3	1	3	3
4	1	1	1	2	1	4	1	2	1	4	2	4
6	1	1	1	1	1	2	3	1	3	2	3	6
8	1	2	1	4	2	8	1	4	2	8	4	8
9	1	1	3	1	3	1	9	3	9	3	9	9
12	1	1	1	2	1	4	3	2	3	4	6	12
18	1	1	3	1	3	2	9	3	9	6	9	18
24	1	2	1	4	2	8	3	4	6	8	12	24
36	1	1	3	2	3	4	9	6	9	12	18	36
72	1	2	3	4	6	8	9	12	18	24	36	72

Tabla 9: *Multiplicación de Normas en* $\mathbb{Z}_{72}$

En esta tabla se realizó un estudio que arrojó los siguientes resultados:

N	**1**	**2**	**3**	**4**	**6**	**8**	**9**	**12**	**18**	**24**	**36**	**72**
1	1	1	1	1	1	1	1	1	1	1	1	1
2	1	2	1	1	1	2	1	1	1	2	1	2
3	1	1	3	1	1	1	3	1	3	1	3	3
4	1	1	1	2	1	4	1	2	1	4	2	4
6	1	1	1	1	1	2	3	1	3	2	3	6
8	1	2	1	4	2	8	1	4	2	8	4	8
9	1	1	3	1	3	1	9	3	9	3	9	9
12	1	1	1	2	1	4	3	2	3	4	6	12
18	1	1	3	1	3	2	9	3	9	6	9	18
24	1	2	1	4	2	8	3	4	6	8	12	24
36	1	1	3	2	3	4	9	6	9	12	18	36
72	1	2	3	4	6	8	9	12	18	24	36	72

$AB/72$
$AB/36$
$AB/24$
$AB/18$
$AB/9$
$AB/12$
$AB/8$
$AB/6$
$AB/3$
$AB/2$
$AB/4$

Tabla 10: *Características de la Norma de una multiplicación*

En el costado derecho se evidencia a qué corresponde cada color, si A y B son normas.

La forma general de todas estas relaciones es AB/k, pero, la pregunta es ¿Qué valor toma k?

Para darle respuesta a esta pregunta, se hizo uso del software Excel y algunas tablas allí construidas de $\mathbb{Z}_m$ tal que este conjunto tuviera una cantidad significativa de normas y poder realizar una comparación de gran magnitud entre la multiplicación de estás, de esta manera, se pudo llegar a la conclusión de que el valor que toma k, para cualquier valor de m es:

$$k = (AB, m)$$

Por último, en consecuencia, planteamos la siguiente conjetura para la norma de una multiplicación:

Conjetura 1: Sea $\mathbb{Z}_m, a, b \in \mathbb{Z}_m$. La norma de ab es:

$$N(ab) = \frac{N(a)N(b)}{(N(a)N(b), m)}$$

Adicional a todo esto, tenemos otro resultado importante obtenido a partir de las distintas observaciones, de esta manera planteamos la siguiente conjetura:

Conjetura 2: $\forall x, m \in \mathbb{Z}^+$ tal que $x < m$, si $x|m$ entonces:

$$\phi(x) = \#(\{a \in \mathbb{Z}_m : N(a) = x\})$$

O, en otras palabras:

Sea x una norma de $\mathbb{Z}_m$, la cantidad de elementos de norma x es $\phi(x)$.

Ejemplo:

En $\mathbb{Z}_8$ tenemos que las normas son 8,4,2 y 1, así, según lo mencionado

- La cantidad de elementos de norma 8 son $\phi(8) = 4$
  Los elementos de norma 8 son: 1,3,5,7

- La cantidad de elementos de norma 4 son $\phi(4) = 2$
  Los elementos de norma 4 son: 2,6

- La cantidad de elementos de norma 2 son $\phi(2) = 1$

Los elementos de norma 2 son: 4

- La cantidad de elementos de norma 1 son $\phi(1) = 1$
  Los elementos de norma 1 son: 0

2.4. Números Primos

En las secciones anteriores hemos estudiado algunos elementos, que como se había mencionado inicialmente servirían de apoyo para el estudio posterior. En esta sección haremos uso de estos elementos para establecer una definición de *número primo* que nos permita identificar si existe un TFA en $\mathbb{Z}_m$ y la construcción de este. Para esto, partiremos definiendo lo que serían números primos en la estructura, así:

Definición: Un número es primo en $\mathbb{Z}_m$ si y solo si lo dividen únicamente las unidades y sus asociados.

Ejemplo:

×	**0**	**1**	**2**	**3**	**4**	**5**	**6**	**7**
0	0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6	7
2	0	2	4	6	0	2	4	6
3	0	3	6	1	4	7	2	5
4	0	4	0	4	0	4	0	4
5	0	5	2	7	4	1	6	3
6	0	6	4	2	0	6	4	2
7	0	7	6	5	4	3	2	1

Tabla 11: *Tabla de multiplicación de* $\mathbb{Z}_8$

En la tabla, los divisores de un número x son los números de las filas en las cuales aparezca este número x.

En $\mathbb{Z}_8$ tenemos lo siguiente:

Elemento:	**Divisores:**	**Asociados:**
1	1,3,5,7	1,3,5,7
2	1,2,3,5,6,7	2,6
3	1,3,5,7	1,3,5,7
4	1,2,3,4,5,6,7	4
5	1,3,5,7	1,3,5,7
6	1,2,3,5,6,7	2,6
7	1,3,5,7	1,3,5,7

Tabla 12: *Tabla de divisores en* $\mathbb{Z}_8$

Unidades → {1,3,5,7}

Luego, bajo la definición establecida para número primo, en $\mathbb{Z}_8$ los números primos son **2** y **6**, pero recordemos que la relación de ser asociados es de equivalencia, luego la clase de equivalencia del 2, resulta ser una "clase prima".

2.4.1. Caracterización de números primos en $\mathbb{Z}_m$.

2.4.1.1. Divisor propio

Definición: Sea $\mathbb{N}_m$ el conjunto de normas de $\mathbb{Z}_m, N \in \mathbb{N}_m$. Si de los elementos de $\mathbb{N}_m$, N divide únicamente a sí mismo y a m, siendo m la norma mayor, entonces N es un **divisor propio** de $\mathbb{N}_m$.

Como m es la norma mayor y este se puede factorizar como producto de números primos, al dividir a m en alguno de estos factores, el resultado obtenido debe ser un divisor propio de m, así la forma de N será:

$$N = \frac{\prod p_i}{p_j}$$

Ejemplo: En $\mathbb{Z}_8$ el conjunto de normas $\mathbb{N}_8 = \{1,2,4,8\}$.

- 1 Divide a todas las demás normas, luego 1 no es un divisor propio.
- 2 No es un divisor propio dado que divide a 2, 4, 8.
- 4 Divide únicamente a 4 y 8, luego 4 es un divisor propio de $\mathbb{N}_8$.

2.4.1.2. Caracterización

Teorema 13: Para todo $a \in \mathbb{Z}_m$ si $N(a)$ es un divisor propio de m, entonces a es primo en el conjunto $\mathbb{Z}_m$.

Dm//: La $N(a)$ es un divisor propio de $\mathbb{N}_m$, supongamos que a no es primo en $\mathbb{Z}_m$, luego $\exists b \in \mathbb{Z}_m$ tal que $b|a$ y $b \neq u_i$ y $b \neq au_i$, es decir b no es unidad ni asociado de a
Ahora, como $b|a$ entonces $N(a)|N(b)$ por el teorema 9. Como b no es unidad ni asociado de a, entonces $N(b) \neq m \wedge N(b) \neq N(a)$, lo que implica que $N(a)$ divide al menos a una norma diferente a si misma o a la norma mayor, es decir $N(a)$ no es un divisor propio de $\mathbb{N}_m$, lo cual nos lleva a una contradicción.

Luego, si $N(a)$ es un divisor propio de $\mathbb{N}_m$, entonces a es primo.

2.4.2. Caracterización de los $\mathbb{Z}_m$ a partir de la descomposición en factores primos de m, según el TFA.

2.4.2.1. $\mathbb{Z}_m$ Con m primo.

Si tenemos un $\mathbb{Z}_m$ en el cual m es primo, esto implica que para cualquier $x \neq 0 \in \mathbb{Z}_m$, x es una unidad.

Esto sucede debido que a que $\forall x \in \mathbb{Z}_m$ se tiene que $(x, m) = 1$ y por el *teorema 1, x* es unidad.

2.4.2.2. $\mathbb{Z}_m$ Con $m = p \cdot q$ tal que p, q Primos.

Si tenemos un $\mathbb{Z}_m$ en el cual $m = pq$ con p, q primos, esto implica que para cualquier $x \neq 0 \in \mathbb{Z}_m$, x es una unidad o es primo.

Dado que $m = pq$, luego $Div_m = \{1, p, q, pq\}$ que además, es el mismo conjunto $\mathbb{N}_m$ de normas de $\mathbb{Z}_m$.
Ahora, tenemos que en $Div_m = \mathbb{N}_m$ de $\mathbb{Z}_m$, p divide únicamente a pq, que resulta ser la norma mayor, por el teorema 9 tenemos que p es un divisor propio de $\mathbb{N}_m$. Esto implica que $\forall a \in \mathbb{Z}_m$ tal que $N(a) = p$, entonces a es primo.
De la misma manera sucede para q, entonces $\forall a \in \mathbb{Z}_m$ tal que $N(a) = q$, entonces a es primo.
Recordemos que por definición de norma, $N(0) = 1$ y $N(u_i) = m$ para este caso $N(u_i) = pq$, siendo u_i unidad.
Ahora, como todas las normas de $\mathbb{Z}_m$ son $\{1, p, q, pq\}$, entonces tenemos que para todo $x \neq 0 \in \mathbb{Z}_m$, x es una unidad o es primo.

2.4.2.3. $\mathbb{Z}_m$ Con $m = p \cdot q \cdot r \cdot \ldots \cdot z$ tal que $p, q, r \ldots z$ Primos.

Ya observamos que si m es primo, entonces todo $a \in \mathbb{Z}_m$ es unidad, ya que $N(a) = m$. Si m se puede escribir como factor de a lo más 2 números primos p, q, entonces para todo $a \in \mathbb{Z}_m$ se tiene que $N(a)$ es p, q o $pq = m$ (rechazamos el caso de que la norma sea 1 ya que el único elemento de norma 1 es 0), como p y q son divisores propios de m entonces los elementos de norma p o q son primos y los de norma $pq = m$ son unidades.

Ahora, si m se puede escribir como factor de 3 primos o más, podemos afirmar que hay divisores de m que no son divisores propios de m. Supongamos que $m = \prod_{i \in I} p_i$ para algún $I = \{1,2, \ldots, n\}$ donde cada p_i es primo, tenemos que cada p_i es divisor de

m, pero a su vez cada p_i también divide a cualquier $p_i p_j$ para algún j, luego p_i ya no es un divisor propio de m, y cualquier elemento $a \in \mathbb{Z}_m$ cuya norma sea p_i no será primo.

El teorema 9 afirma que si la $N(a)$ es un divisor propio de m entonces a es primo, recíprocamente podemos afirmar que: si a no es primo, entonces $N(a)$ no es un divisor propio de m y a estos elementos los llamamos números compuestos.

En general:

- Si la norma es de la forma $x = \frac{\prod p_i}{p_j}$ para cualquier j, entonces cualquier elemento $a \in \mathbb{Z}_m$ cuya norma sea x, será primo.
- Si la norma es de la forma $x = \prod p_i$, entonces cualquier elemento $a \in \mathbb{Z}_m$ cuya norma sea x, será unidad.
- Si la norma es de la forma $x = \frac{\prod p_i}{\prod p_j}$ para cualquier $1 < j < i$, entonces cualquier elemento $a \in \mathbb{Z}_m$ cuya norma sea x, será un elemento compuesto.

Así, en un $\mathbb{Z}_m$ en el que m se puede expresar como factor de 3 primos o más tenemos unidades, primos y elementos compuestos.

Teorema 14: Sea $a \in \mathbb{Z}_m$, si a es primo en $\mathbb{Z}$ y $(a, m) \neq 1$, entonces a es primo en $\mathbb{Z}_m$.

Dm//: Como a es primo en $\mathbb{Z}$ y $(a, m) \neq 1$, tenemos que $(a, m) = a$, además $a \in \mathbb{Z}_m$, así, $N(a) = \frac{m}{(a,m)}$

Si tenemos que la descomposición factorial de m es $\prod p_j$, entonces:

$$N(a) = \frac{\prod p_j}{a}$$

Como $(a, m) = a$ y a es primo, a hace parte de la descomposición factorial de m, es decir $a = p_j$ para algún j.

Luego, $N(a) = \frac{\prod p_j}{p_j}$ y esta es la norma de un número primo en $\mathbb{Z}_m$, luego, concluimos que a es primo en $\mathbb{Z}_m$.

2.5. Diagramas de Hasse

Hasta el momento, nos hemos dotado de herramientas que han sido la base de este trabajo y a partir de estas hemos construido algunas nociones tales como: Unidades, asociados, números primos, números compuestos, normas, divisor propio, subgrupos, etc. Todos estos elementos podemos "condensarlos" en uno solo: Diagrama de Hasse.

Un diagrama de Hasse es un grafo dirigido cuyos vértices son los elementos de un conjunto X y existe una arista que lleva a x en y, si $x < y$ y no existe un elemento z tal que $x < z < y$.

2.5.1. Diagramas de Hasse y clasificación de elementos

Ahora bien, tomemos un elemento $m \in \mathbb{Z}$ cualquiera, es claro que inmediatamente tendremos a $\mathbb{Z}_m$, realicemos el diagrama de Hasse de los divisores de m.

Sea $m = 12$ los divisores de 12 son $D(12) = \{1,2,3,4,6,12\}$
El diagrama de Hasse de $D(12)$ será:

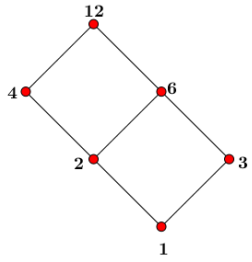

Imagen 1: *Diagrama de Hasse para* $D(12)$

Pero recordemos que ya tenemos un teorema que nos dice que el conjunto de divisores de m es igual al conjunto de normas de $\mathbb{Z}_m$, por tanto, también estamos organizando las normas, lo que de fondo nos permite organizar a los elementos de $\mathbb{Z}_m$ por medio de un diagrama de Hasse así:

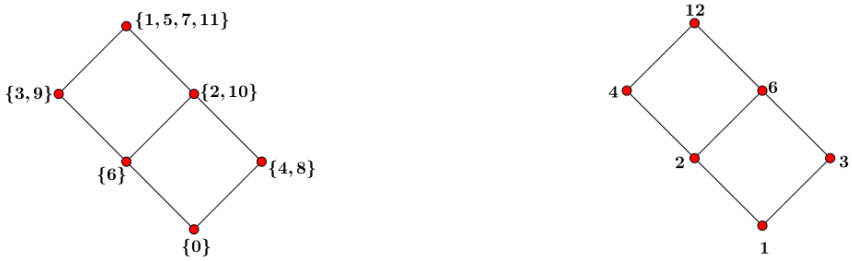

Imagen 2: *Organización de elementos de* $\mathbb{Z}_{12}$

En el primer nivel, se encuentra el único elemento cuya norma es 1 es decir, el 0; en el segundo nivel, se encuentran los elementos de norma 3 (4,8) y los elementos de norma 2 (6); en el tercer nivel se encuentran los elementos de norma 6 (2,10) y los de norma 4 (3,9) y en el último nivel, se encuentran los elementos de norma 12 (1,5,7,11).

Ahora, según las caracterizaciones que se han obtenido tenemos lo siguiente:

- La norma de las unidades es m
- Los elementos cuya norma sea un divisor propio de m, son primos
- Los elementos cuya norma no es un divisor propio de m, ni m, son compuestos
- El único elemento de norma 1 es el cero

Ahora, usando el diagrama de Hasse los números quedan organizados de la siguiente manera según sus características

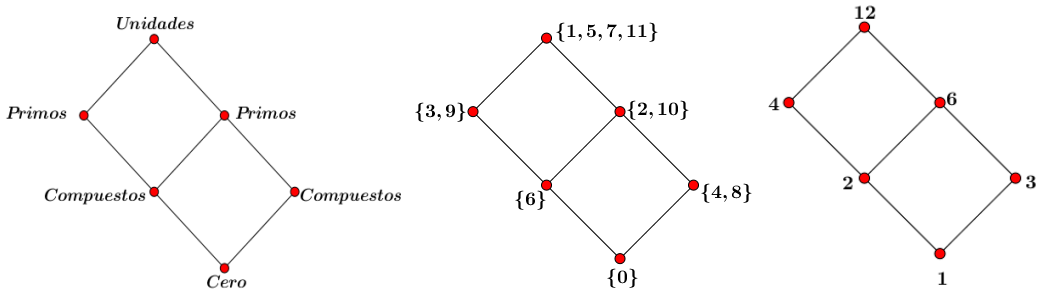

Imagen 3: *Organización según características en* $\mathbb{Z}_{12}$

Es decir, en el primer nivel, siempre se encontrará el elemento 0, en el último nivel se encuentran los elementos que resultan ser unidades, en el penúltimo los elementos que resultan ser primos en $\mathbb{Z}_m$ y en los demás niveles se encuentras los elementos compuestos. Esto se cumple para cualquier valor de m (teniendo en cuenta la clara construcción del diagrama de Hasse).

A continuación se presenta el diagrama de Hasse para $\mathbb{Z}_{60}$

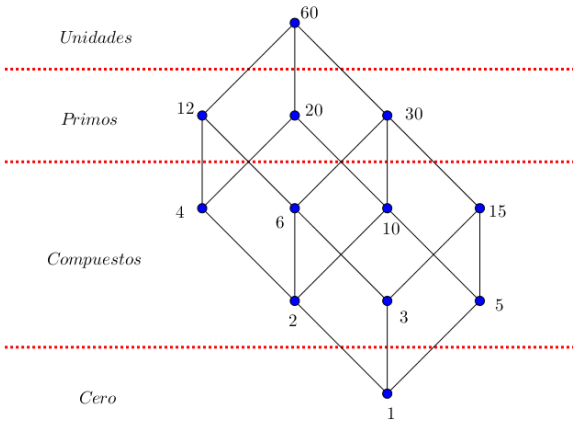

Imagen 4: *Organización de elementos según características en* $\mathbb{Z}_{60}$

Podemos observar que hay 1 clase de unidades, 3 clases primas, 7 clase compuestas y 1 clase del cero.

2.5.2. Diagramas de Hasse y subgrupos de $\mathbb{Z}_m$

En la sección 2.3.3 generamos los subgrupos de $\mathbb{Z}_m$ a partir de las relaciones de divisibilidad de las normas así: El conjunto $\ll a \gg = \{x \in \mathbb{Z}_m : N(x) | N(a)\}$ es un subgrupo de $\mathbb{Z}_m$.

Frente a esto, es claro que los elementos que están asociados entre si generan el mismo subgrupo, dado que tienen la misma norma. Ahora bien, el diagrama de Hasse permite organizar estos subgrupos de la siguiente manera:

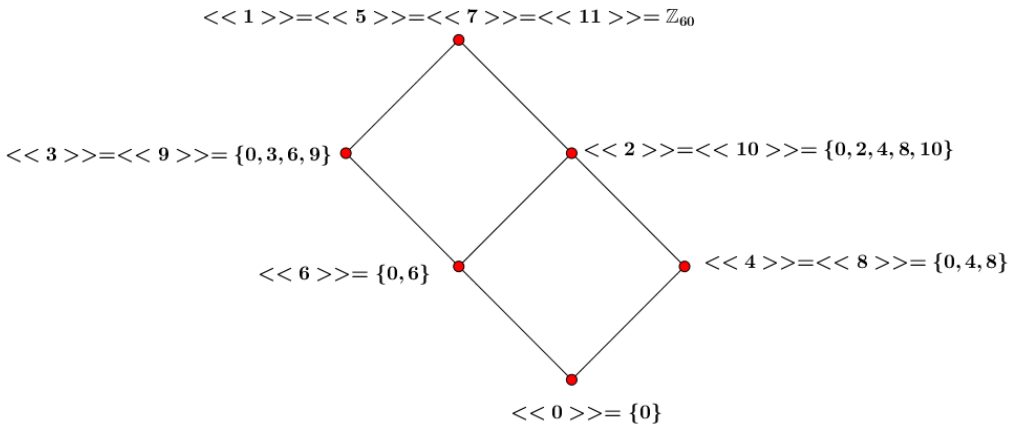

Imagen 5: *Organización de subgrupos de* $\mathbb{Z}_{12}$

Como se puede observar, los subgrupos también se pueden organizar por medio del mismo diagrama de Hasse, esto se debe a la divisibilidad entre las normas (divisores de m) y las relaciones previamente establecidas entre los elementos.

3. Teorema Fundamental de la Aritmética en $\mathbb{Z}_m$

3.1. Punto de Partida: Enteros

En primera instancia, el TFA de la aritmética para la estructura de los números enteros dice que: "Todo entero $n > 1$ o es primo, o se puede factorizar como producto de primos. Este producto es único salvo por el orden de los factores" (Pettofrezzo, 1972, p. 51).

Sin embargo, es de considerar que dicho enunciado aplica incluso si los números son enteros negativos, pues se ha estado considerando los enteros como clases de equivalencia, en las que en cada clase se encuentra un elemento y su inverso aditivo, esto es:

$$\begin{aligned}[1] &= \{1, -1\} \\ [2] &= \{2, -2\} \\ [3] &= \{3, -3\} \\ &\vdots \\ [a] &= \{a - a\}\end{aligned}$$

En esta estructura, se considera al elemento 1 como unidad, luego, su clase de equivalencia será una clase de unidades, es decir, el elemento -1 también será unidad. Los elementos $2, 3, 5, 7, \ldots$ y en general todos los elementos primos considerados están en la misma clase de equivalencia con su elemento inverso, así los elementos $-2, -3, -5, -7, \ldots$ también serán considerados como elementos primos, en general, cada una de estas clases de equivalencia será una clase prima.

La factorización del elemento 30 es

$$30 = 2 \cdot 3 \cdot 5;$$

Pero además, puede ser

$$30 = 2 \cdot -3 \cdot -5$$

Así, se puede afirmar que $[30] = [2] \cdot [3] \cdot [5]$.

Esto nos da un indicio de cómo plantear un posible TFA para los conjuntos $\mathbb{Z}_m$ a partir de las clases de equivalencia allí planteadas, a continuación veremos dicho proceso.

3.2. Conjuntos $\mathbb{Z}_m$

Ahora bien, en los conjuntos $\mathbb{Z}_m$ también tenemos clases de equivalencia las cuales son generadas por las normas, en este sentido, tendremos una clase de unidades, clases de elementos primos, clases de elementos compuestos y una clase que contiene al elemento 0, finalmente queremos verificar si las clases de elementos compuestos se pueden generar a partir de la multiplicación de clases de elementos primos.

Recordemos que si m es de la forma $\prod p_i$ y si una norma N_0 es un divisor propio de m, esta es de la forma:

$$N_0 = \frac{\prod p_i}{p_j}$$

De este modo, el menor elemento de $\mathbb{Z}$ que pertenece a alguna clase residual de $\mathbb{Z}_m$ y tiene norma N_0 es p_j.

Ahora, de manera similar, si N_1 no es un divisor propio de m, esta es de la forma:

$$N_1 = \frac{\prod p_i}{\prod p_j}$$

Para 1<$j < i$

Y el menor elemento de $\mathbb{Z}$ que pertenece a alguna clase residual de $\mathbb{Z}_m$ y tiene norma N_1 es $\prod p_j$.

Esto último se cumple para cualquier norma N_k que no sea un divisor propio de m, además, podemos observar que cualquier $\prod p_j$ con $j < i$ es un divisor de m.

En el teorema 14 demostramos que si un elemento en $\mathbb{Z}$ es primo y no es primo relativo con m entonces el elemento será primo en $\mathbb{Z}_m$. Estos elementos serán precisamente los p_j que hacen parte de la descomposición factorial de m.

Así, podemos tomar como representante de cada clase de asociados a los elementos $\prod p_j$ con $1 \leq j < i$.

3.2.1. Teorema Fundamental de la Aritmética en $\mathbb{Z}_m$

En primera instancia, nuestro interés está puesto en obtener un posible Teorema Fundamental de la Aritmética en $\mathbb{Z}_m$, para esto consideraremos los elementos y las clases de equivalencia a las cuales pertenecen, así como las características de éstos.

Veamos algunos ejemplos de posibles factorizaciones de elementos “compuestos” a partir de elementos “primos” con el fin de postular un posible TFA en los conjuntos $\mathbb{Z}_m$.

A continuación se presentan algunos ejemplos de factorizaciones. En la imagen 6 se puede observar parte de un programa que se diseñó usando el Software Python (Anexo A), el cuál arroja la norma de los números, la clasificación de estos, cuáles son los primos, cuáles unidades y cuáles compuestos. La imagen muestra la clasificación por normas en el conjunto $\mathbb{Z}_{12}$, podemos observar entonces que 2,3,9,10 son números primos en $\mathbb{Z}_{12}$, y con estos debemos generar a los elementos 4,6 y 8, donde 4 y 8 hacen parte de la misma clase, luego:

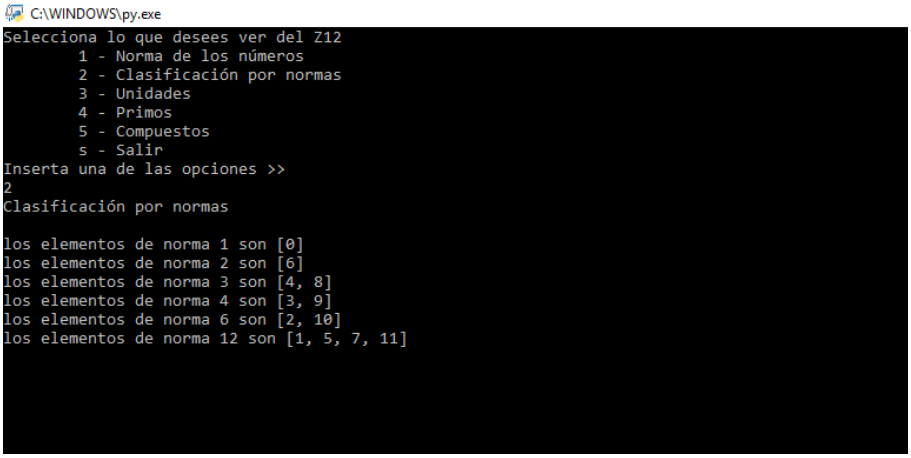

Imagen 6: *Programa en Python para* $\mathbb{Z}_{12}$

Notemos que 2 y 10 hacen parte de la misma clase, 3 y 9 hacen parte de la misma clase y 4 y 8 hacen parte de la misma clase, así:

El elemento 4 se puede factorizar como:

$$4 = 2 \cdot 2$$
$$4 = 10 \cdot 10$$

El elemento 8 se puede factorizar como

$$8 = 2 \cdot 2 \cdot 2$$
$$8 = 2 \cdot 10$$

El elemento 6 se puede factorizar como

$$6 = 2 \cdot 3$$
$$6 = 2 \cdot 9$$

$$6 = 10 \cdot 3$$
$$6 = 10 \cdot 9$$

Si tomamos como representantes a 2,3,4 y 6 de sus respectivas clases, entonces tenemos que:

$$[6] = [2] \cdot [3]$$
$$[4] = [2] \cdot [2] = [2]^2$$

Concluyendo así que cualquier elemento de una clase compuesta se puede factorizar como producto de elementos de clases primas.
Finalmente proponemos un Teorema Fundamental de la Aritmética en $\mathbb{Z}_m$ a partir de los estudios presentados anteriormente, este se enuncia como:

Teorema 15: En $\mathbb{Z}_m$, todo elemento diferente de 0 pertenece a una clase prima o puede expresarse como producto de elementos de clases primas**.**

Al tomar como elementos representantes de cada clase a los $\prod p_j$ con $1 \leq j < i$, tenemos que los elementos representantes de las clases primas son los p_j, en este sentido, como cada elemento $\prod p_j$ es producto de primos, cualquiera de estos elementos se puede factorizar como producto de primos. Sus asociados se obtienen al multiplicar al elemento con cada una de las unidades del conjunto.

Como se observa, la factorización en cierto sentido no es "única", esto se debe a que la unicidad no está dada precisamente por los elementos, sino por sus características y la clase a la cual pertenece, si tomamos a cada clase como un elemento (que contiene a otros), entonces cada clase compuesta puede expresarse como producto de clases primas, de manera única salvo por el orden en que aparecen los factores.

4. Construcción de Anillos Finitos

A lo largo del trabajo se han podido caracterizar algunos elementos que fueron la base para los estudios realizados posteriormente, específicamente, las unidades, asociados, norma y TFA en la estructura.

Ahora, el trabajo estará centrado en la construcción de anillos tomando como base de éste a todos los elementos estudiados a priori, incluyendo algunos teoremas y definiciones.

Recordemos en primer lugar los elementos a tener en cuenta en esta construcción:

Para que obtengamos un anillo bajo dos operaciones necesitamos que el conjunto con la primera operación sea un grupo Abeliano, la segunda operación debe ser asociativa y debe existir una relación entre las dos operaciones de la siguiente manera: $a(b+c) = ab + ac = (b+c)a = ba + ca$.

Un anillo donde la multiplicación es conmutativa se dice un anillo conmutativo. Un anillo que tiene una identidad para la multiplicación, que se representa usualmente por 1, es un anillo con identidad (Rubiano *et al*., 2004, p. 109).

Para realizar la construcción de los anillos, en primer lugar partiremos de la tabla de adición y a partir de esta y la caracterización de las normas, la construcción de una posible tabla de multiplicación.

4.1. Adición – Multiplicación

4.1.1. Tabla de Adición

En primera instancia, debemos tener un conjunto que junto con una operación $\oplus$ sea un grupo Abeliano. Con las propiedades descritas en capítulos anteriores construiremos esta operación de tal manera que obtengamos un grupo Abeliano.

Vamos a tomar un conjunto J con 8 elementos:

$$J = \{0, a, b, c, d, e, f, g\}$$

Vamos a suponer que 0 es el elemento identidad para $\oplus$ y que el elemento a genera a todo J, así, podemos construir a cada elemento de J usando a a y tenemos:

$$a = \boldsymbol{a} \qquad a + a + a = \boldsymbol{e}$$
$$a + a = \boldsymbol{g} \qquad a + a + a + a = \boldsymbol{d}$$

$$a+a+a+a+a=\boldsymbol{c} \qquad a+a+a+a+a+a+a=\boldsymbol{f}$$
$$a+a+a+a+a+a=\boldsymbol{b} \qquad a+a+a+a+a+a+a+a=\mathbf{0}$$

Con esto, podemos comenzar a construir la tabla de $\oplus$ de J:

En primer lugar, como a es un generador de J entonces J es cíclico, como J es cíclico entonces deber ser Abeliano, esto por el teorema mencionado en el ítem 1.3.3.

Como 0, es la identidad para $\oplus$, una primera presentación construible de la tabla de $\oplus$ es la siguiente:

$\oplus$	**0**	***a***	***b***	***c***	***d***	***e***	***f***	***g***
0	0	*a*	*b*	*c*	*d*	*e*	*f*	*g*
a	*a*							
b	*b*							
c	*c*							
d	*d*							
e	*e*							
f	*f*							
g	*g*							

Tabla 13: *Construcción tabla de adición para J*

Ahora, sabemos que $a \oplus a = g$, así que podemos rellenar este espacio con g

$\oplus$	**0**	***a***	***b***	***c***	***d***	***e***	***f***	***g***
0	0	*a*	*b*	*c*	*d*	*e*	*f*	*g*
a	*a*	*g*						
b	*b*							
c	*c*							
d	*d*							
e	*e*							
f	*f*							
g	*g*							

Tabla 14: *Construcción tabla de adición para J*

Ahora, podemos observar que aún no conocemos un valor para $a \oplus g$, sin embargo $g = a \oplus a$, luego $a \oplus g = a \oplus a \oplus a$, y tenemos entonces que $a \oplus g = e$.

O bien por ejemplo no tenemos un valor para $e \oplus d$, escribiendo esto en términos de a, tenemos $(a \oplus a \oplus a) \oplus (a \oplus a \oplus a \oplus a) = a \oplus a \oplus a \oplus a \oplus a \oplus a \oplus a = f$ Finalmente $e \oplus d = f$, realizando este proceso de manera iterada podremos construir finalmente cualquier suma y el resultado obtenido finamente para la operación $\oplus$ será:

$\oplus$	**0**	***a***	***b***	***c***	***d***	***e***	***f***	***g***
0	0	a	b	c	d	e	f	g
a	a	g	f	b	c	d	0	e
b	b	f	d	e	g	a	c	0
c	c	b	e	g	a	0	d	f
d	d	c	g	a	0	f	e	b
e	e	d	a	0	f	b	g	c
f	f	0	c	d	e	g	b	a
g	g	e	0	f	b	c	a	d

Tabla 15: *Construcción final tabla de adición para J*

Por la manera en que construimos la tabla de adición para J podemos afirmar que $(J,\oplus)$ es un grupo Abeliano

Sin embargo, la parte más importante está en la construcción de la tabla de multiplicación, veamos a continuación

4.1.2. Multiplicación

En primer lugar vamos a identificar la norma de cada elemento, notemos que aquí no estamos tratando con números sino con símbolos, por ende no podemos hablar de $M.C.M$ o $M.C.D$ o Congruencia Lineal, sin embargo si podemos hablar de la cantidad de veces que se suma un elemento con él mismo hasta obtener como resultado al módulo, en este caso, el 0.

Si nos ubicamos en la tabla de adición y comenzamos a realizar las sumas sucesivas, obtenemos que:

Los elementos de norma 8 serán: a, e, c, f
Los elementos de norma 4 serán: b, g
El elemento de norma 2 será: d
El elemento de norma 1 será: 0

Recordemos que la norma de una multiplicación es: si x, y son elementos de J la norma de xy es:

$$\frac{N(x)N(y)}{(N(x)N(y),m)}$$

Siendo m en este caso, la cantidad de elementos que tiene el conjunto J.

Así, llenaremos la tabla de multiplicación $\otimes$ según esta regla para multiplicación de números.

Si tomamos un elemento de norma 1 y lo multiplicamos por otro de norma 1 tenemos que la norma de este elemento resultante será:

$$\frac{1 \cdot 1}{(1 \cdot 1{,}8)} = \frac{1}{(1{,}8)} = \frac{1}{1} = 1$$

Así, la multiplicación de dos elementos de norma 1 nos da como resultado uno de norma 1.

Ahora, si multiplicamos un elemento de norma 1 por otro de cualquier norma tenemos que la norma de este elemento resultante será:

$$\frac{1 \cdot k}{(1 \cdot k, 8)} = \frac{k}{(k, 8)}$$

Como k es un divisor de 8, entonces $(k, 8) = k$, así, la norma resultante será:

$$\frac{k}{(k, 8)} = \frac{k}{k} = 1$$

Así, al multiplicar un número de norma 1 con otro cualquiera obtendremos un elemento de norma 1.

Llenemos a continuación una primera parte de la tabla teniendo en cuenta que los elementos de norma 1 son los de la clase de equivalencia del 0

$$\text{Norma } 1 \rightarrow [0]$$

Podemos observar que la esto se cumple incluso si la multiplicación fuera $0 \otimes x$ o $x \otimes 0$

$\otimes$	$\mathbf{0}$	$\boldsymbol{a}$	$\boldsymbol{b}$	$\boldsymbol{c}$	$\boldsymbol{d}$	$\boldsymbol{e}$	$\boldsymbol{f}$	$\boldsymbol{g}$
$\mathbf{0}$	[0]	[0]	[0]	[0]	[0]	[0]	[0]	[0]
$\boldsymbol{a}$	[0]							
$\boldsymbol{b}$	[0]							
$\boldsymbol{c}$	[0]							
$\boldsymbol{d}$	[0]							
$\boldsymbol{e}$	[0]							
$\boldsymbol{f}$	[0]							
$\boldsymbol{g}$	[0]							

Tabla 16: *Construcción tabla de multiplicación en J (Parte 1)*

Ahora, tomemos un elemento de norma 2 por otro elemento de norma 2, la norma de este elemento resultante está dada por:

$$\frac{2 \cdot 2}{(2 \cdot 2{,}8)} = \frac{4}{(4{,}8)} = \frac{4}{4} = 1$$

Como d es el único elemento de norma 2, entonces el elemento obtenido en la multiplicación es un elemento de la clase de equivalencia del 0.

$$d \otimes d = [0]$$

Ahora, tomemos un elemento de norma 2 por un elemento de norma 4, la norma de este elemento resultante está dada por:

$$\frac{2 \cdot 4}{(2 \cdot 4{,}8)} = \frac{8}{(8{,}8)} = \frac{8}{8} = 1$$

Como d es el único elemento de norma 2 y b, g son los elementos de norma 4, entonces tenemos que:

$$d \otimes b = [0]$$
$$d \otimes g = [0]$$

Ahora, tomemos un elemento de norma 2 por un elemento de norma 8, la norma de este elemento resultante está dada por:

$$\frac{2 \cdot 8}{(2 \cdot 8{,}8)} = \frac{16}{(16{,}8)} = \frac{16}{8} = 2$$

Como d es el único elemento de norma 2 y a, e, c, f son los elementos de norma 2, entonces tenemos:

$$d \otimes a = [d]$$
$$d \otimes e = [d]$$
$$d \otimes c = [d]$$
$$d \otimes f = [d]$$

La construcción de la tabla para $\otimes$ hasta el momento se tiene como:

$\otimes$	**0**	***a***	***b***	***c***	***d***	***e***	***f***	***g***
0	[0]	[0]	[0]	[0]	[0]	[0]	[0]	[0]
a	[0]				$[d]$			
b	[0]				[0]			
c	[0]				$[d]$			
d	[0]	$[d]$	[0]	$[d]$	[0]	$[d]$	$[d]$	[0]
e	[0]				$[d]$			
f	[0]				$[d]$			
g	[0]				[0]			

Tabla 17: *Construcción tabla de multiplicación para J (Parte 2)*

Ahora, tomemos un elemento de norma 4 por un elemento de norma 4, la norma de este elemento resultante será:

$$\frac{4 \cdot 4}{(4 \cdot 4{,}8)} = \frac{16}{(16{,}8)} = \frac{16}{8} = 2$$

Como d es el único elemento de norma 2 y b, g son los elementos de norma 4, entonces tenemos que:

$$b \otimes g = [d]$$
$$b \otimes b = [d]$$
$$g \otimes g = [d]$$
$$g \otimes b = [d]$$

Luego, la tabla resultante hasta el momento es:

$\otimes$	**0**	$\boldsymbol{a}$	$\boldsymbol{b}$	$\boldsymbol{c}$	$\boldsymbol{d}$	$\boldsymbol{e}$	$\boldsymbol{f}$	$\boldsymbol{g}$
0	$[0]$	$[0]$	$[0]$	$[0]$	$[0]$	$[0]$	$[0]$	$[0]$
$\boldsymbol{a}$	$[0]$				$[d]$			
$\boldsymbol{b}$	$[0]$		$[d]$		$[0]$			$[d]$
$\boldsymbol{c}$	$[0]$				$[d]$			
$\boldsymbol{d}$	$[0]$	$[d]$	$[0]$	$[d]$	$[0]$	$[d]$	$[d]$	$[0]$
$\boldsymbol{e}$	$[0]$				$[d]$			
$\boldsymbol{f}$	$[0]$				$[d]$			
$\boldsymbol{g}$	$[0]$		$[d]$		$[0]$			$[d]$

Tabla 18: *Construcción tabla de multiplicación para J (Parte 3)*

Notemos que las clases $[0]$ y $[d]$ son clases con un solo elemento, así, en la tabla podemos cambiar esas clases por cada elemento.

$\otimes$	**0**	$\boldsymbol{a}$	$\boldsymbol{b}$	$\boldsymbol{c}$	$\boldsymbol{d}$	$\boldsymbol{e}$	$\boldsymbol{f}$	$\boldsymbol{g}$
0	0	0	0	0	0	0	0	0
$\boldsymbol{a}$	0				d			
$\boldsymbol{b}$	0		d		0			d
$\boldsymbol{c}$	0				d			
$\boldsymbol{d}$	0	d	0	d	0	d	d	0
$\boldsymbol{e}$	0				d			
$\boldsymbol{f}$	0				d			
$\boldsymbol{g}$	0		d		0			d

Tabla 19: *Construcción tabla de multiplicación para J (Parte 4)*

Veamos ahora que resultados obtenemos al tomar un elemento de norma 4 por un elemento de norma 8, la norma de este elemento resultante será:

$$\frac{4 \cdot 8}{(4 \cdot 8{,}8)} = \frac{32}{(32{,}8)} = \frac{32}{8} = 4$$

Como los elementos de norma 4 son b y g, y los de norma 8 son a, e, c, f, tenemos los siguientes casos:

- $b \otimes a = [b]$
- $b \otimes e = [b]$
- $b \otimes c = [b]$
- $b \otimes f = [b]$
- $a \otimes b = [b]$
- $e \otimes b = [b]$
- $c \otimes b = [b]$
- $f \otimes b = [b]$

- $g \otimes a = [b]$
- $g \otimes e = [b]$
- $g \otimes c = [b]$
- $g \otimes f = [b]$
- $a \otimes g = [b]$
- $e \otimes g = [b]$
- $c \otimes g = [b]$
- $f \otimes g = [b]$

Para seguir con la construcción de la tabla vamos a considerar que en cada clase puede incluirse cualquiera de los elementos que pertenecen a ella, la tabla hasta el momento tiene la siguiente forma:

$\otimes$	$\mathbf{0}$	$\boldsymbol{a}$	$\boldsymbol{b}$	$\boldsymbol{c}$	$\boldsymbol{d}$	$\boldsymbol{e}$	$\boldsymbol{f}$	$\boldsymbol{g}$
$\mathbf{0}$	0	0	0	0	0	0	0	0
$\boldsymbol{a}$	0		$[b]$		d			$[b]$
$\boldsymbol{b}$	0	$[b]$	d	$[b]$	0	$[b]$	$[b]$	d
$\boldsymbol{c}$	0		$[b]$		d			$[b]$
$\boldsymbol{d}$	0	d	0	d	0	d	d	0
$\boldsymbol{e}$	0		$[b]$		d			$[b]$
$\boldsymbol{f}$	0		$[b]$		d			$[b]$
$\boldsymbol{g}$	0	$[b]$	d	$[b]$	0	$[b]$	$[b]$	d

Tabla 20: *Construcción tabla de multiplicación para J (Parte 5)*

Por último, tomemos elementos de norma 8 por elementos de norma 8, la norma del elemento resultante será:

$$\frac{8 \cdot 8}{(8 \cdot 8{,}8)} = \frac{64}{(64{,}8)} = \frac{64}{8} = 8$$

Los elementos de norma 8 son a, e, c, f, que además resultan ser las unidades del conjunto J, para construir la multiplicación de estos elementos vamos a partir de lo siguiente:

1. Una de las unidades deber ser el módulo de $\otimes$, vamos a tomar al elemento a como módulo.

Además, vamos a partir del siguiente resultado de la Teoría Algebraica de Números:

2. *"Las unidades de un anillo forman un grupo respecto a la multiplicación"* (Tabara, 2001, pp. 4).

Como nuestro objetivo final es construir anillos, haremos uso de estos resultados para completar la estructuración de la tabla de multiplicación, así:

Para la siguiente parte usaremos el primer resultado, es decir: si a es el módulo de $\otimes$ en J, entonces, la tabla de multiplicación queda construida de la siguiente manera:

$\otimes$	**0**	$\boldsymbol{a}$	$\boldsymbol{b}$	$\boldsymbol{c}$	$\boldsymbol{d}$	$\boldsymbol{e}$	$\boldsymbol{f}$	$\boldsymbol{g}$
0	0	0	0	0	0	0	0	0
$\boldsymbol{a}$	0	a	b	c	d	e	f	$[b]$
$\boldsymbol{b}$	0	b	d	$[b]$	0	$[b]$	$[b]$	d
$\boldsymbol{c}$	0	c	$[b]$		d			$[b]$
$\boldsymbol{d}$	0	d	0	d	0	d	d	0
$\boldsymbol{e}$	0	e	$[b]$		d			$[b]$
$\boldsymbol{f}$	0	f	$[b]$		d			$[b]$
$\boldsymbol{g}$	0	$[b]$	d	$[b]$	0	$[b]$	$[b]$	d

Tabla 21: *Construcción tabla de multiplicación para J (Parte 6)*

Ahora bien, para llenar los espacios en blanco utilizaremos el segundo resultado, considerando que el conjunto de unidades forma un grupo bajo la multiplicación:

Llamemos $U(J)$ al conjunto de unidades de J, como $U(J)$ debe formar un grupo bajo la multiplicación, entonces dicha multiplicación debe ser cancelativa, así, notemos que:

- En la celda $c \otimes c$ los valores permitidos pueden ser e, a ó f
- En la celda $c \otimes e$ los valores permitidos pueden ser a ó f
- En la celda $c \otimes f$ los valores permitidos pueden ser a ó f

Para realizar la construcción vamos a partir de la celda $c \otimes e$ colocando allí el valor a.

Al poner este valor allí, el resto de espacios en blanco inmediatamente quedan determinados de la siguiente manera:

$\otimes$	**0**	***a***	***b***	***c***	***d***	***e***	***f***	***g***
0	0	0	0	0	0	0	0	0
a	0	a	b	c	d	e	f	g
b	0	b	d	$[b]$	0	$[b]$	$[b]$	d
c	0	c	$[b]$	***f***	d	***a***	***e***	$[b]$
d	0	d	0	d	0	d	d	0
e	0	e	$[b]$	***a***	d	***f***	***c***	$[b]$
f	0	f	$[b]$	***e***	d	***c***	***a***	$[b]$
g	0	g	d	$[b]$	0	$[b]$	$[b]$	d

Tabla 22: *Caso 1. Tabla de Multiplicación para J.*

Es de resaltar que el único hecho utilizado para completar esta construcción ha sido que la multiplicación de unidades sea cancelativa, sin embargo, la multiplicación $\otimes$ se sigue obteniendo conmutativa.

Ahora, si el valor a colocar en la celda $c \otimes e$ no es a sino f, obtenemos los siguientes casos:

$\otimes$	**0**	***a***	***b***	***c***	***d***	***e***	***f***	***g***
0	0	0	0	0	0	0	0	0
a	0	a	b	c	d	e	f	g
b	0	b	d	$[b]$	0	$[b]$	$[b]$	d
c	0	c	$[b]$	***e***	d	***f***	***a***	$[b]$
d	0	d	0	d	0	d	d	0
e	0	e	$[b]$	***f***	d	***a***	***c***	$[b]$
f	0	f	$[b]$	***a***	d	***c***	***e***	$[b]$
g	0	g	d	$[b]$	0	$[b]$	$[b]$	d

Tabla 23: *Caso 2. Tabla de Multiplicación para J*

$\otimes$	**0**	***a***	***b***	***c***	***d***	***e***	***f***	***g***
0	0	0	0	0	0	0	0	0
a	0	a	b	c	d	e	f	g
b	0	b	d	$[b]$	0	$[b]$	$[b]$	d
c	0	c	$[b]$	***a***	d	***f***	***e***	$[b]$
d	0	d	0	d	0	d	d	0
e	0	e	$[b]$	***f***	d	***a***	***c***	$[b]$
f	0	f	$[b]$	***e***	d	***c***	***a***	$[b]$
g	0	g	d	$[b]$	0	$[b]$	$[b]$	d

Tabla 24: *Caso 3. Tabla de Multiplicación para J*

$\otimes$	**0**	***a***	***b***	***c***	***d***	***e***	***f***	***g***
0	0	0	0	0	0	0	0	0
a	0	a	b	c	d	e	f	g
b	0	b	d	$[b]$	0	$[b]$	$[b]$	d
c	0	c	$[b]$	***a***	d	***f***	***e***	$[b]$
d	0	d	0	d	0	d	d	0
e	0	e	$[b]$	***f***	d	***c***	**a**	$[b]$
f	0	f	$[b]$	***e***	d	***a***	***c***	$[b]$
g	0	g	d	$[b]$	0	$[b]$	$[b]$	d

Tabla 25: *Caso 4. Tabla de Multiplicación para J*

Si observamos en las tablas, nuestro problema ahora se centra en definir cuáles son los valores que pueden ir en donde aparece [b], en este sentido, estos valores pueden ser b o g para cada casilla.

Haciendo uso del programa *Propiedades 3.1*[5] se analizó cada una de las tablas con cada una de las posibles formas de llenarla, obteniendo como resultado que en las tablas de los casos 1,2 y 4 bajo ninguna asignación de valores es posible obtener una multiplicación que resulte ser distributiva respecto a la suma, a continuación se presentan dos de todas las tablas estudiadas para cada caso que no resultan ser distributivas pero si cumplen todas las demás características

Además, en los debidos anexos se podrán encontrar los estudios realizados a partir del software *Propiedades 3.1.*

Caso 1:

a) (Anexo B)

$\otimes$	**0**	***a***	***b***	***c***	***d***	***e***	***f***	***g***
0	0	0	0	0	0	0	0	0
a	0	*a*	*b*	*c*	*d*	*e*	*f*	*g*
b	0	*b*	*d*	*b*	0	*b*	*b*	*d*
c	0	*c*	*b*	*f*	*d*	*a*	*e*	*b*
d	0	*d*	0	*d*	0	*d*	*d*	0
e	0	*e*	*b*	*a*	*d*	*f*	*c*	*b*
f	0	*f*	*b*	*e*	*d*	*c*	*a*	*b*
g	0	*g*	*d*	*b*	0	*b*	*b*	*d*

Tabla 26: *Multiplicación 1 $\otimes$ no distributiva respecto a $\oplus$ en J (Caso 1)*

b) (Anexo C)

$\otimes$	**0**	***a***	***b***	***c***	***d***	***e***	***f***	***g***
0	0	0	0	0	0	0	0	0
a	0	*a*	*b*	*c*	*d*	*e*	*f*	*g*
b	0	*b*	*d*	*g*	0	*b*	*g*	*d*
c	0	*c*	*g*	*f*	*d*	*a*	*e*	*b*
d	0	*d*	0	*d*	0	*d*	*d*	0
e	0	*e*	*b*	*a*	*d*	*f*	*c*	*g*
f	0	*f*	*g*	*e*	*d*	*c*	*a*	*b*
g	0	*g*	*d*	*b*	0	*g*	*b*	*d*

Tabla 27: *Multiplicación 2 $\otimes$ no distributiva respecto a $\oplus$ en J (Caso 1)*

[5] Diseñado por el profesor José Leonardo Ángel, integrante Grupo de Álgebra, 2011.

Caso 2:

a) (Anexo D)

$\otimes$	**0**	***a***	***b***	***c***	***d***	***e***	***f***	***g***
0	0	0	0	0	0	0	0	0
a	0	*a*	*b*	*c*	*d*	*e*	*f*	*g*
b	0	*b*	*d*	*b*	0	*b*	*b*	*d*
c	0	*c*	*b*	*e*	*d*	*f*	*a*	*b*
d	0	*d*	0	*d*	0	*d*	*d*	0
e	0	*e*	*b*	*f*	*d*	*a*	*c*	*b*
f	0	*f*	*b*	*a*	*d*	*c*	*e*	*b*
g	0	*g*	*d*	*b*	0	*b*	*b*	*d*

Tabla 28: *Multiplicación 3 $\otimes$ no distributiva respecto a $\oplus$ en J (Caso 2)*

b) (Anexo E)

$\otimes$	**0**	***a***	***b***	***c***	***d***	***e***	***f***	***g***
0	0	0	0	0	0	0	0	0
a	0	*a*	*b*	*c*	*d*	*e*	*f*	*g*
b	0	*b*	*d*	*g*	0	*b*	*g*	*d*
c	0	*c*	*g*	*e*	*d*	*f*	*a*	*b*
d	0	*d*	0	*d*	0	*d*	*d*	0
e	0	*e*	*b*	*f*	*d*	*a*	*c*	*g*
f	0	*f*	*g*	*a*	*d*	*c*	*e*	*b*
g	0	*g*	*d*	*b*	0	*g*	*b*	*d*

Tabla 29: *Multiplicación 4 $\otimes$ no distributiva respecto a $\oplus$ en J (Caso 2)*

Caso 4:

a) (Anexo F)

$\otimes$	**0**	***a***	***b***	***c***	***d***	***e***	***f***	***g***
0	0	0	0	0	0	0	0	0
a	0	*a*	*b*	*c*	*d*	*e*	*f*	*g*
b	0	*b*	*d*	*b*	0	*b*	*b*	*d*
c	0	*c*	*b*	*a*	*d*	*f*	*e*	*b*
d	0	*d*	0	*d*	0	*d*	*d*	0
e	0	*e*	*b*	*f*	*d*	*c*	a	*b*
f	0	*f*	*b*	*e*	*d*	*a*	*c*	*b*
g	0	*g*	*d*	*b*	0	*b*	*b*	*d*

Tabla 30: *Multiplicación 5 $\otimes$ no distributiva respecto a $\oplus$ en J (Caso 4)*

b) (Anexo G)

$\otimes$	**0**	***a***	***b***	***c***	***d***	***e***	***f***	***g***
0	0	0	0	0	0	0	0	0
a	0	*a*	*b*	*c*	*d*	*e*	*f*	*g*
b	0	*b*	*d*	*g*	0	*b*	*g*	*d*
c	0	*c*	*g*	*a*	*d*	*f*	*e*	*b*
d	0	*d*	0	*d*	0	*d*	*d*	0
e	0	*e*	*b*	*f*	*d*	*c*	a	*g*
f	0	*f*	*g*	*e*	*d*	*a*	*c*	*b*
g	0	*g*	*d*	*b*	0	*g*	*b*	*d*

Tabla 31: *Multiplicación 6 $\otimes$ no distributiva respecto a $\oplus$ en J (Caso 4)*

Ahora, para las asignaciones en la tabla del caso 3 tampoco resultaban ser distributivas, salvo por una asignación, así, la única multiplicación $\otimes$ en J que resulta ser distributiva (Anexo H) respecto a la adición $\oplus$ es la siguiente:

$\otimes$	**0**	***a***	***b***	***c***	***d***	***e***	***f***	***g***
0	0	0	0	0	0	0	0	0
a	0	*a*	*b*	*c*	*d*	*e*	*f*	*g*
b	0	*b*	*d*	*b*	0	*g*	*g*	*d*
c	0	*c*	*b*	*a*	*d*	*f*	*e*	*g*
d	0	*d*	0	*d*	0	*d*	*d*	0
e	0	*e*	*g*	*f*	*d*	*a*	*c*	*b*
f	0	*f*	*g*	*e*	*d*	*c*	*a*	*b*
g	0	*g*	*d*	*g*	0	*b*	*b*	*d*

Tabla 32: *Tabla de Multiplicación final para J*

Así, damos por finalizada la construcción del anillo $(J,\oplus,\otimes)$ con 8 elementos, partiendo de las propiedades estudiadas en las secciones anteriores de este trabajo.

Sin embargo, surge la pregunta, ¿Es $(J,\oplus,\otimes)$ diferente a $(\mathbb{Z}_8, +,\times)$?

Si realizamos la siguiente asignación:

$0 \to 0$ $\qquad$ $d \to 4$

$a \to 1$ $\qquad$ $c \to 5$

$g \to 2$ $\qquad$ $b \to 6$

$e \to 3$ $\qquad$ $f \to 7$

Podemos ver que $(J,\oplus,\otimes)$ y $(\mathbb{Z}_8,+,\times)$ resultan ser estructuras isomorfas, además, esta afirmación tiene sentido, pues la adición en J la construimos de una manera cíclica y podemos asegurar que existe uno y solo un anillo cíclico de orden n debido a que existe un único grupo cíclico de orden n salvo isomorfismos para cada entero $n \geq 2$ (Rubiano, 2004), y en cada uno de estos se puede construir una única segunda operación distributiva respecto a la otra

Notemos que para esta construcción nuestro mayor problema fue construir una multiplicación $\otimes$ que resultara ser distributiva respecto a la adición $\oplus$, de hecho, para encontrar cuál debería ser distributiva, el estudio fue al estilo Ensayo – Error, hasta obtener cuál de estas debería ser la apropiada, un estudio adicional puede ser tratar de construir dos operaciones que en primera instancia cumplan esta propiedad y a partir de esta intentar construir un anillo, para esto, incluso podría tomarse como partida que el conjunto con la operación resulte ser conmutativo pero no cíclico, incluso estudiar cómo sería el comportamiento allí de lo que nosotros llamamos norma, y si esta permite realizar la misma caracterización realizada en este trabajo.

Ahora, por otro lado, cabe resaltar que la construcción realizada fue hecha a base de 8 elementos y sin embargo la complejidad de esta construcción es evidente a pesar de tener aquí solamente 4 normas, si intentáramos construir un anillo con 12, 16, 24 o incluso muchos más elementos ¿Cómo afectaría esto a la construcción de la tabla de multiplicación? ¿O en definitiva podemos hallar una manera de que las operaciones se relacionen por medio de la distributividad y esto nos limite la construcción por montones? Sin embargo, estos son problemas que no abordaremos en este trabajo, pero que proponemos al lector con el fin de seguir en la construcción del conocimiento, además de todos los que surjan en el camino del estudio.

El objetivo final de este trabajo era construir anillos finitos a partir del estudio de la relación de divisibilidad en $\mathbb{Z}_m$ y aunque lo logramos, es claro que el método de construcción no resulta ser el más apropiado por la cantidad de posibles opciones que este deja a consideración, aun así, los elementos estudiados en secciones anteriores fueron de completa ayuda para la construcción mencionada y de igual manera, hacemos extensa la invitación a continuar con el estudio, o realizar otros similares.

5. Conclusiones:

Los conjuntos $\mathbb{Z}_m$ en esencia son estructuras que permiten trabajar ciertos objetos tanto elementales como avanzados por ser estructuras finitas y a pesar de esto tener similitudes particulares con algunas estructuras infinitas usuales, sin embargo, estos conjuntos son estudiados a menudo solamente desde las propiedades en relación a dos operaciones básicas, adición y multiplicación, sin realizar un análisis profundo de todo lo que esto implica. En este trabajo se estudiaron estas propiedades descritas, así como otras, entorno a una nueva relación, la de divisibilidad y las relaciones establecidas entre estas. Esto da cabida para ampliar los conocimientos básicos y las nociones que se tienen alrededor de este tipo de estructuras, así como una mejor interpretación de elementos propios de los estudios usuales.

El estudio de la norma de los elementos de $\mathbb{Z}_m$ en primera instancia pareció no arrojar muchos resultados, sin embargo con el transcurso del trabajo se evidenció la importancia que ésta toma para el estudio posterior de todos los demás elementos del trabajo: unidades, primos, compuestos, grupos, subgrupos, y demás. A pesar de no ser el tipo de norma usual de la teoría algebraica de números, si permite realizar una caracterización de elementos en el conjunto de la misma manera que se haría en otros diferentes, tomando así vital importancia para concluir con el estudio.

Establecer clases de equivalencia en los conjuntos a partir de ciertas características que éstos cumplan resulta ser la base que consolide la construcción del teorema fundamental de la aritmética, esto pudimos observarlo en los conjuntos $\mathbb{Z}_m$ en los cuales las clases se generaban a partir de la norma de cada número, este hecho también se da en otro tipo de estructuras como el conjunto de los enteros y extensiones cuadráticas de él, dejando así de manifiesto la importancia que toma definir dichas clases en cada conjunto y su importancia en la construcción del teorema.

En todos los estudios que ya se han realizado en torno a los conjuntos $\mathbb{Z}_m$ se han trabajado varios de los elementos que en este documento se mencionan, sin embargo es interesante observar cómo es posible llegar a estos mismos partiendo de un estudio completamente diferente, incluso sin tener idea previa de la existencia de éstos, y además, la construcción de otros que aún no se habían tenido en cuenta.

Además de todos los conocimientos teóricos adquiridos en el desarrollo del trabajo, también se pudo tener un acercamiento a la programación como fuente de apoyo para el estudio, diseñando un programa en Python que resumiera en gran manera

ciertos cálculos y dándole así un papel especial a la tecnología, de igual manera frente al trabajo realizado con el Software *Propiedades 3.1* que aunque no fue diseñado por el autor del trabajo, este fue de ayuda fundamental en la obtención del resultado final, estos elementos resultan ser de gran ayuda y gran importancia finalmente en la construcción de cualquier trabajo.

En la construcción de los anillos convergen todas las consultas realizadas, los elementos estudiados y construidos, así como las diferentes concepciones propias frente a ciertos elementos, es de resaltar que aunque se logró construir un anillo, la forma de hacerlo no fue la mejor, debido a las limitantes que aún presenta el trabajo, como no poder establecer de alguna manera la distributividad de una operación respecto a la otra, esto abre varios caminos para continuar con un estudio que permita de una manera más óptima llegar a una construcción de anillos finitos, así como el estudio de otros elementos en relación.

Este trabajo también aportó en cuanto a la formación como licenciado en matemáticas, frente a cómo se pueden abordar diferentes temáticas desde diferentes perspectivas, cómo se pueden asociar elementos matemáticos avanzados con elementos matemáticos de los currículos tradicionales, es decir, como la matemática avanzada no es algo estrictamente desprendido de las matemáticas curriculares sino que por el contrario se pueden establecer relaciones estrechamente ligadas entre éstas, pudiendo abordar así las diferentes temáticas desde diversos caminos.

El estudio propuesto en este trabajo surgió en primer lugar como una invitación en el seminario de álgebra a comienzos del semestre 2014 – 2 con el fin de analizar y tratar de estructurar las características que cumplen ciertos conjuntos frente a una relación de divisibilidad, el punto de partida de éste fue el mero análisis frente a las concepciones que ya tenía cada participante en torno a ciertos elementos, por ejemplo qué es un divisor, qué es un número primo, el TFA, entre otros varios y tratar de definir estos en la estructura a tratar, esto por supuesto en algún momento se queda corto y es necesario recurrir a consulta bibliográfica de ciertos elementos que den continuidad al trabajo, esto resulta ser una parte fundamental, pues sin dicha consulta la construcción realizada no será del todo eficiente e incluso limitará el estudio.

Por último y no menos importante, es de resaltar que la cantidad de conocimiento teórico adquirido en el desarrollo del trabajo, ya sea porque era necesario para este o en ocasiones por simple curiosidad y amor por estudiar matemáticas, así como la capacidad de comunicación de las ideas lograda en la escritura del mismo, son elementos que no se tienen a consideración de manera profunda, pero que sin

embargo se dan, y se dan de una manera bastante amplia fortaleciendo así el crecimiento intelectual, profesional e incluso personal de quien realiza el trabajo.

Referencias

Arrondo, E. (2011). Apuntes de estructuras algebraicas. Madrid: Universidad Complutense de Madrid.

Castro, L., Sánchez, L., & Rojas, S. (2015). La relación de divisibilidad en los enteros de Minkowsky. Tunja: Universidad Pedagógica y Tecnológica de Colombia.

Fraleigh, J. (1988). Algebra Abstracta. Addison-Wesley Publishing Company, Inc., Reading, Massachusetts, E.U.A.

García, M., Giacobbi A., & Ríos, N. (2008). Introducción a la Teoría Algebraica de Números. Universidad Nacional de la Plata. Buenos Aires, Argentina.

Le veque, W. (1968). TEORÍA ELEMENTAL DE LOS NÚMEROS. México: Editorial Herrero hermanos, sucesores, S.A. editores.

Luque C., Mora L. & Torres J. (2004). Estructuras análogas a los números reales. Bogotá: Editorial Nomos S.A.

Pérez, É. (2005). Estructuras Algebraicas. Bogotá: Universidad Pedagógica Nacional.

Pettofrezzo, J. (1972). Introducción a la Teoría de Números. New Jersey, E.U.A. Editorial Prentice.

Sánchez, Y., & Jiménez, W. (2015). Un estudio de la relación de Divisibilidad en súper conjuntos de Z a partir del estudio en subconjuntos de Z. Tunja: Universidad Pedagógica y Tecnológica de Colombia.

Tabara, J. (2001). Introducción la teoría de anillos. Recuperado de: http://mimosa.pntic.mec.es/jgomez53/matema/docums/tabara-anillos.pdf

Torres, H., Ávila, J., & Rubén, T. (2015). Una caracterización de números primos en el conjunto $\mathbb{Z}(\sqrt{2})$ desde el proceso de analizar. Tunja: Universidad Pedagógica y Tecnológica de Colombia

ANEXOS:

Anexo A: Código programa elaborado en Python

```
    import os

def menu():
    """Función que limpia la pantalla y muestra nuevamente el menú"""

    os.system('cls')
    print("Selecciona lo que desees ver del Z"+str(m))
    print("\t1 - Norma de los números")
    print("\t2 - Clasificación por normas")
    print("\t3 - Unidades")
    print("\t4 - Primos")
    print("\t5 - Compuestos")
    print("\ts - Salir")

"""Función para hallar el máximo común divisor"""
def mcd(num1,num2):
    a=max(num1,num2)
    b=min(num1,num2)
    while b!=0:
        mcd=b
        b=a%b
        a=mcd
    return mcd

"""Función para hallar el mínimo común multiplo"""
def mcm(num1,num2):
    a=max(num1,num2)
    b=min(num1,num2)
    mcm=(a/mcd(a,b))*b
    return mcm

def norma(num):
    norma = mcm(num, m) / num
    return norma

#INGRESO DE DATOS DEL USUARIO
m=int(input("Ingrese el valor de m\n"))
print("\n\n")

b=[]
for k in range(1,m):
    if m % k==0:
        b=b+[k]

while True:
    #mostramos el menu
    menu()

    #solicitamos una opción al usuario
    opcionMenu=input("Inserta una de las opciones >> \n")

    if opcionMenu=="1":
```

```
        print("Norma de los números\n")
        print("La norma de "+str(0)+" es "+str(1))
        for i in range(1, m):
            print("La norma de " + str(int(i)) + " es " +
str(int(norma(i))))
        print("\n")

        input()
    if opcionMenu=="2":
        print("Clasificación por normas\n")
        print("los elementos de norma " + str(1) + " son " + str([0]))
        for h in (b[1:] + [m]):
            t = []
            for k in range(1, m):
                if norma(k) == h:
                    t = t + [k]
            print("los elementos de norma " + str(h) + " son " +
str(t))

        input()
    if opcionMenu=="3":
        print("Unidades\n")
        a = []
        for j in range(1, m):
            if norma(j) == m:
                a = a + [j]
        print(a, "\n"),

        input()
    if opcionMenu=="4":
        print("Primos\n")
        c = []
        d = []
        for q in range(1, m):
            e = 0
            for p in b:
                if p % norma(q) == 0:
                    e = e + 1
            if e == 1:
                c = c + [q]
        print(c, "\n")
        if c==[]:
            print("En este conjunto no existen números primos")
        input()
    if opcionMenu=="5":
        print("Compuestos\n")
        a = []
        for j in range(1, m):
            if norma(j) == m:
                a = a + [j]

        c = []
        d = []
        for q in range(1, m):
            e = 0
            for p in b:
                if p % norma(q) == 0:
```

```
                    e = e + 1
            if e == 1:
                c = c + [q]

        f=[]
        for q in range(1, m):
            if not ((q in c)) and not ((q in a)):
                f = f + [q]
        print(f)
        if f==[]:
            print("En este conjunto no existen números compuestos")


        input()
    elif opcionMenu=="s":
        break
    else:
        print("")
        input("pulsa una tecla para continuar")
```

Anexo B: Análisis realizado en *Propiedades 3.1* para tablas de multiplicación (caso 1a)

Estudio algebraico de la operación

x	0	1	2	3	4	5	6	7
0	0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6	7
2	0	2	4	2	0	2	2	4
3	0	3	2	6	4	1	5	2
4	0	4	0	4	0	4	4	0
5	0	5	2	1	4	6	3	2
6	0	6	2	5	4	3	1	2
7	0	7	4	2	0	2	2	4

2 x (1 + 2) <> 2 x 1 + 2 x 2
2 x (1 + 5) <> 2 x 1 + 2 x 5
2 x (1 + 6) <> 2 x 1 + 2 x 6
2 x (1 + 7) <> 2 x 1 + 2 x 7
2 x (2 + 1) <> 2 x 2 + 2 x 1
2 x (2 + 3) <> 2 x 2 + 2 x 3
2 x (2 + 5) <> 2 x 2 + 2 x 5
2 x (2 + 6) <> 2 x 2 + 2 x 6
2 x (3 + 2) <> 2 x 3 + 2 x 2
2 x (3 + 5) <> 2 x 3 + 2 x 5
2 x (3 + 6) <> 2 x 3 + 2 x 6
2 x (3 + 7) <> 2 x 3 + 2 x 7
2 x (5 + 1) <> 2 x 5 + 2 x 1
2 x (5 + 2) <> 2 x 5 + 2 x 2
2 x (5 + 3) <> 2 x 5 + 2 x 3
2 x (5 + 7) <> 2 x 5 + 2 x 7
2 x (6 + 1) <> 2 x 6 + 2 x 1
2 x (6 + 2) <> 2 x 6 + 2 x 2
2 x (6 + 3) <> 2 x 6 + 2 x 3
2 x (6 + 7) <> 2 x 6 + 2 x 7
2 x (7 + 1) <> 2 x 7 + 2 x 1
2 x (7 + 3) <> 2 x 7 + 2 x 3
2 x (7 + 5) <> 2 x 7 + 2 x 5
2 x (7 + 6) <> 2 x 7 + 2 x 6
3 x (1 + 1) <> 3 x 1 + 3 x 1
3 x (1 + 3) <> 3 x 1 + 3 x 3
3 x (1 + 4) <> 3 x 1 + 3 x 4
3 x (1 + 5) <> 3 x 1 + 3 x 5
3 x (1 + 7) <> 3 x 1 + 3 x 7
3 x (2 + 3) <> 3 x 2 + 3 x 3
3 x (2 + 4) <> 3 x 2 + 3 x 4
3 x (2 + 5) <> 3 x 2 + 3 x 5
3 x (2 + 6) <> 3 x 2 + 3 x 6
3 x (2 + 7) <> 3 x 2 + 3 x 7
3 x (3 + 1) <> 3 x 3 + 3 x 1
3 x (3 + 2) <> 3 x 3 + 3 x 2
3 x (3 + 4) <> 3 x 3 + 3 x 4
3 x (3 + 6) <> 3 x 3 + 3 x 6
3 x (3 + 7) <> 3 x 3 + 3 x 7
3 x (4 + 1) <> 3 x 4 + 3 x 1
3 x (4 + 2) <> 3 x 4 + 3 x 2
3 x (4 + 3) <> 3 x 4 + 3 x 3
3 x (4 + 5) <> 3 x 4 + 3 x 5
3 x (4 + 6) <> 3 x 4 + 3 x 6
3 x (4 + 7) <> 3 x 4 + 3 x 7
3 x (5 + 1) <> 3 x 5 + 3 x 1
3 x (5 + 2) <> 3 x 5 + 3 x 2
3 x (5 + 4) <> 3 x 5 + 3 x 4
3 x (5 + 5) <> 3 x 5 + 3 x 5
3 x (5 + 6) <> 3 x 5 + 3 x 6
3 x (6 + 2) <> 3 x 6 + 3 x 2
3 x (6 + 3) <> 3 x 6 + 3 x 3
3 x (6 + 4) <> 3 x 6 + 3 x 4
3 x (6 + 5) <> 3 x 6 + 3 x 5
3 x (6 + 7) <> 3 x 6 + 3 x 7
3 x (7 + 1) <> 3 x 7 + 3 x 1
3 x (7 + 2) <> 3 x 7 + 3 x 2
3 x (7 + 3) <> 3 x 7 + 3 x 3
3 x (7 + 4) <> 3 x 7 + 3 x 4
3 x (7 + 6) <> 3 x 7 + 3 x 6
5 x (1 + 2) <> 5 x 1 + 5 x 2
5 x (1 + 3) <> 5 x 1 + 5 x 3
5 x (1 + 4) <> 5 x 1 + 5 x 4
5 x (1 + 5) <> 5 x 1 + 5 x 5
5 x (1 + 7) <> 5 x 1 + 5 x 7
5 x (2 + 1) <> 5 x 2 + 5 x 1
5 x (2 + 4) <> 5 x 2 + 5 x 4
5 x (2 + 5) <> 5 x 2 + 5 x 5
5 x (2 + 6) <> 5 x 2 + 5 x 6
5 x (2 + 7) <> 5 x 2 + 5 x 7
5 x (3 + 1) <> 5 x 3 + 5 x 1
5 x (3 + 3) <> 5 x 3 + 5 x 3
5 x (3 + 4) <> 5 x 3 + 5 x 4
5 x (3 + 6) <> 5 x 3 + 5 x 6
5 x (3 + 7) <> 5 x 3 + 5 x 7
5 x (4 + 1) <> 5 x 4 + 5 x 1
5 x (4 + 2) <> 5 x 4 + 5 x 2
5 x (4 + 3) <> 5 x 4 + 5 x 3
5 x (4 + 5) <> 5 x 4 + 5 x 5
5 x (4 + 6) <> 5 x 4 + 5 x 6
5 x (4 + 7) <> 5 x 4 + 5 x 7
5 x (5 + 1) <> 5 x 5 + 5 x 1
5 x (5 + 2) <> 5 x 5 + 5 x 2
5 x (5 + 4) <> 5 x 5 + 5 x 4
5 x (5 + 6) <> 5 x 5 + 5 x 6
5 x (5 + 7) <> 5 x 5 + 5 x 7
5 x (6 + 2) <> 5 x 6 + 5 x 2
5 x (6 + 3) <> 5 x 6 + 5 x 3
5 x (6 + 4) <> 5 x 6 + 5 x 4
5 x (6 + 5) <> 5 x 6 + 5 x 5
5 x (6 + 6) <> 5 x 6 + 5 x 6
5 x (7 + 1) <> 5 x 7 + 5 x 1
5 x (7 + 2) <> 5 x 7 + 5 x 2
5 x (7 + 3) <> 5 x 7 + 5 x 3
5 x (7 + 4) <> 5 x 7 + 5 x 4
5 x (7 + 5) <> 5 x 7 + 5 x 5
6 x (1 + 2) <> 6 x 1 + 6 x 2
6 x (1 + 3) <> 6 x 1 + 6 x 3
6 x (2 + 1) <> 6 x 2 + 6 x 1
6 x (2 + 3) <> 6 x 2 + 6 x 3
6 x (2 + 4) <> 6 x 2 + 6 x 4
6 x (2 + 5) <> 6 x 2 + 6 x 5
6 x (2 + 6) <> 6 x 2 + 6 x 6
6 x (2 + 7) <> 6 x 2 + 6 x 7
6 x (3 + 1) <> 6 x 3 + 6 x 1
6 x (3 + 2) <> 6 x 3 + 6 x 2
6 x (4 + 2) <> 6 x 4 + 6 x 2
6 x (4 + 7) <> 6 x 4 + 6 x 7
6 x (5 + 2) <> 6 x 5 + 6 x 2
6 x (5 + 5) <> 6 x 5 + 6 x 5

6 x (6 + 2) <> 6 x 6 + 6 x 2
6 x (6 + 6) <> 6 x 6 + 6 x 6
6 x (7 + 2) <> 6 x 7 + 6 x 2
6 x (7 + 4) <> 6 x 7 + 6 x 4
7 x (1 + 3) <> 7 x 1 + 7 x 3
7 x (1 + 4) <> 7 x 1 + 7 x 4
7 x (2 + 3) <> 7 x 2 + 7 x 3
7 x (2 + 6) <> 7 x 2 + 7 x 6
7 x (3 + 1) <> 7 x 3 + 7 x 1
7 x (3 + 2) <> 7 x 3 + 7 x 2
7 x (3 + 4) <> 7 x 3 + 7 x 4
7 x (3 + 5) <> 7 x 3 + 7 x 5
7 x (3 + 6) <> 7 x 3 + 7 x 6
7 x (3 + 7) <> 7 x 3 + 7 x 7
7 x (4 + 1) <> 7 x 4 + 7 x 1
7 x (4 + 3) <> 7 x 4 + 7 x 3
7 x (5 + 3) <> 7 x 5 + 7 x 3
7 x (5 + 7) <> 7 x 5 + 7 x 7
7 x (6 + 2) <> 7 x 6 + 7 x 2
7 x (6 + 3) <> 7 x 6 + 7 x 3
7 x (7 + 3) <> 7 x 7 + 7 x 3
7 x (7 + 5) <> 7 x 7 + 7 x 5

Luego la operacion x no es distribuiva a izquierda con respecto a +.

(1 + 1) x 3 <> 1 x 3 + 1 x 3
(1 + 2) x 2 <> 1 x 2 + 2 x 2
(1 + 2) x 5 <> 1 x 5 + 2 x 5
(1 + 2) x 6 <> 1 x 6 + 2 x 6
(1 + 3) x 3 <> 1 x 3 + 3 x 3
(1 + 3) x 5 <> 1 x 5 + 3 x 5
(1 + 3) x 6 <> 1 x 6 + 3 x 6
(1 + 3) x 7 <> 1 x 7 + 3 x 7
(1 + 4) x 3 <> 1 x 3 + 4 x 3
(1 + 4) x 5 <> 1 x 5 + 4 x 5
(1 + 4) x 7 <> 1 x 7 + 4 x 7
(1 + 5) x 2 <> 1 x 2 + 5 x 2
(1 + 5) x 3 <> 1 x 3 + 5 x 3
(1 + 5) x 5 <> 1 x 5 + 5 x 5
(1 + 6) x 2 <> 1 x 2 + 6 x 2
(1 + 7) x 2 <> 1 x 2 + 7 x 2
(1 + 7) x 3 <> 1 x 3 + 7 x 3
(1 + 7) x 5 <> 1 x 5 + 7 x 5
(2 + 1) x 2 <> 2 x 2 + 1 x 2
(2 + 1) x 5 <> 2 x 5 + 1 x 5
(2 + 1) x 6 <> 2 x 6 + 1 x 6
(2 + 3) x 2 <> 2 x 2 + 3 x 2
(2 + 3) x 3 <> 2 x 3 + 3 x 3
(2 + 3) x 6 <> 2 x 6 + 3 x 6
(2 + 3) x 7 <> 2 x 7 + 3 x 7
(2 + 4) x 3 <> 2 x 3 + 4 x 3
(2 + 4) x 5 <> 2 x 5 + 4 x 5
(2 + 4) x 6 <> 2 x 6 + 4 x 6
(2 + 5) x 2 <> 2 x 2 + 5 x 2
(2 + 5) x 3 <> 2 x 3 + 5 x 3
(2 + 5) x 5 <> 2 x 5 + 5 x 5
(2 + 5) x 6 <> 2 x 6 + 5 x 6
(2 + 6) x 2 <> 2 x 2 + 6 x 2
(2 + 6) x 3 <> 2 x 3 + 6 x 3
(2 + 6) x 5 <> 2 x 5 + 6 x 5
(2 + 6) x 6 <> 2 x 6 + 6 x 6
(2 + 6) x 7 <> 2 x 7 + 6 x 7
(2 + 7) x 3 <> 2 x 3 + 7 x 3
(2 + 7) x 5 <> 2 x 5 + 7 x 5
(2 + 7) x 6 <> 2 x 6 + 7 x 6
(3 + 1) x 3 <> 3 x 3 + 1 x 3
(3 + 1) x 5 <> 3 x 5 + 1 x 5
(3 + 1) x 6 <> 3 x 6 + 1 x 6
(3 + 1) x 7 <> 3 x 7 + 1 x 7
(3 + 2) x 2 <> 3 x 2 + 2 x 2
(3 + 2) x 3 <> 3 x 3 + 2 x 3
(3 + 2) x 6 <> 3 x 6 + 2 x 6
(3 + 2) x 7 <> 3 x 7 + 2 x 7
(3 + 3) x 5 <> 3 x 5 + 3 x 5
(3 + 4) x 3 <> 3 x 3 + 4 x 3
(3 + 4) x 5 <> 3 x 5 + 4 x 5
(3 + 4) x 7 <> 3 x 7 + 4 x 7
(3 + 5) x 2 <> 3 x 2 + 5 x 2
(3 + 5) x 7 <> 3 x 7 + 5 x 7
(3 + 6) x 2 <> 3 x 2 + 6 x 2
(3 + 6) x 3 <> 3 x 3 + 6 x 3
(3 + 6) x 5 <> 3 x 5 + 6 x 5
(3 + 6) x 7 <> 3 x 7 + 6 x 7
(3 + 7) x 2 <> 3 x 2 + 7 x 2
(3 + 7) x 3 <> 3 x 3 + 7 x 3
(3 + 7) x 5 <> 3 x 5 + 7 x 5
(3 + 7) x 7 <> 3 x 7 + 7 x 7
(4 + 1) x 3 <> 4 x 3 + 1 x 3
(4 + 1) x 5 <> 4 x 5 + 1 x 5
(4 + 1) x 7 <> 4 x 7 + 1 x 7
(4 + 2) x 3 <> 4 x 3 + 2 x 3
(4 + 2) x 5 <> 4 x 5 + 2 x 5
(4 + 2) x 6 <> 4 x 6 + 2 x 6
(4 + 3) x 3 <> 4 x 3 + 3 x 3
(4 + 3) x 5 <> 4 x 5 + 3 x 5
(4 + 3) x 7 <> 4 x 7 + 3 x 7
(4 + 5) x 3 <> 4 x 3 + 5 x 3
(4 + 5) x 5 <> 4 x 5 + 5 x 5
(4 + 6) x 3 <> 4 x 3 + 6 x 3
(4 + 6) x 5 <> 4 x 5 + 6 x 5
(4 + 7) x 3 <> 4 x 3 + 7 x 3
(4 + 7) x 5 <> 4 x 5 + 7 x 5
(4 + 7) x 6 <> 4 x 6 + 7 x 6
(5 + 1) x 2 <> 5 x 2 + 1 x 2
(5 + 1) x 3 <> 5 x 3 + 1 x 3
(5 + 1) x 5 <> 5 x 5 + 1 x 5
(5 + 2) x 2 <> 5 x 2 + 2 x 2
(5 + 2) x 3 <> 5 x 3 + 2 x 3
(5 + 2) x 5 <> 5 x 5 + 2 x 5
(5 + 2) x 6 <> 5 x 6 + 2 x 6
(5 + 3) x 2 <> 5 x 2 + 3 x 2
(5 + 3) x 7 <> 5 x 7 + 3 x 7
(5 + 4) x 3 <> 5 x 3 + 4 x 3
(5 + 4) x 5 <> 5 x 5 + 4 x 5
(5 + 5) x 3 <> 5 x 3 + 5 x 3
(5 + 5) x 6 <> 5 x 6 + 5 x 6
(5 + 6) x 3 <> 5 x 3 + 6 x 3
(5 + 6) x 5 <> 5 x 5 + 6 x 5
(5 + 7) x 2 <> 5 x 2 + 7 x 2
(5 + 7) x 5 <> 5 x 5 + 7 x 5
(5 + 7) x 7 <> 5 x 7 + 7 x 7
(6 + 1) x 2 <> 6 x 2 + 1 x 2
(6 + 2) x 2 <> 6 x 2 + 2 x 2
(6 + 2) x 3 <> 6 x 3 + 2 x 3
(6 + 2) x 5 <> 6 x 5 + 2 x 5
(6 + 2) x 6 <> 6 x 6 + 2 x 6
(6 + 2) x 7 <> 6 x 7 + 2 x 7
(6 + 3) x 2 <> 6 x 2 + 3 x 2
(6 + 3) x 3 <> 6 x 3 + 3 x 3
(6 + 3) x 5 <> 6 x 5 + 3 x 5
(6 + 3) x 7 <> 6 x 7 + 3 x 7
(6 + 4) x 3 <> 6 x 3 + 4 x 3
(6 + 4) x 5 <> 6 x 5 + 4 x 5
(6 + 5) x 3 <> 6 x 3 + 5 x 3
(6 + 5) x 5 <> 6 x 5 + 5 x 5

(6 + 6) x 5 <> 6 x 5 + 6 x 5
(6 + 6) x 6 <> 6 x 6 + 6 x 6
(6 + 7) x 2 <> 6 x 2 + 7 x 2
(6 + 7) x 3 <> 6 x 3 + 7 x 3
(7 + 1) x 2 <> 7 x 2 + 1 x 2
(7 + 1) x 3 <> 7 x 3 + 1 x 3
(7 + 1) x 5 <> 7 x 5 + 1 x 5
(7 + 2) x 3 <> 7 x 3 + 2 x 3
(7 + 2) x 5 <> 7 x 5 + 2 x 5
(7 + 2) x 6 <> 7 x 6 + 2 x 6
(7 + 3) x 2 <> 7 x 2 + 3 x 2
(7 + 3) x 3 <> 7 x 3 + 3 x 3
(7 + 3) x 5 <> 7 x 5 + 3 x 5
(7 + 3) x 7 <> 7 x 7 + 3 x 7
(7 + 4) x 3 <> 7 x 3 + 4 x 3
(7 + 4) x 5 <> 7 x 5 + 4 x 5
(7 + 4) x 6 <> 7 x 6 + 4 x 6
(7 + 5) x 2 <> 7 x 2 + 5 x 2
(7 + 5) x 5 <> 7 x 5 + 5 x 5
(7 + 5) x 7 <> 7 x 7 + 5 x 7

(7 + 6) x 2 <> 7 x 2 + 6 x 2
(7 + 6) x 3 <> 7 x 3 + 6 x 3
Luego la operacion x no es distribuiva a derecha con respecto a +.
(3 x 5) x 7 <> 3 x (5 x 7)
(5 x 3) x 7 <> 5 x (3 x 7)
(6 x 6) x 7 <> 6 x (6 x 7)
(7 x 3) x 5 <> 7 x (3 x 5)
(7 x 5) x 3 <> 7 x (5 x 3)
(7 x 6) x 6 <> 7 x (6 x 6)
La operación x es asociativa

La operación x es conmutativa

El elemento neutro respecto a x es : 1

El elemento inverso de 1 respecto a x es 1
El elemento inverso de 3 respecto a x es 5
El elemento inverso de 5 respecto a x es 3
El elemento inverso de 6 respecto a x es 6

Anexo C: Análisis realizado en *Propiedades 3.1* para tablas de multiplicación (caso 1b)

Estudio algebraico de la operación

x	0	1	2	3	4	5	6	7
0	0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6	7
2	0	2	4	7	0	2	7	4
3	0	3	7	6	4	1	5	2
4	0	4	0	4	0	4	4	0
5	0	5	2	1	4	6	3	7
6	0	6	7	5	4	3	1	2
7	0	7	4	2	0	7	2	4

2 x (1 + 3) <> 2 x 1 + 2 x 3
2 x (1 + 4) <> 2 x 1 + 2 x 4
2 x (1 + 5) <> 2 x 1 + 2 x 5
2 x (1 + 7) <> 2 x 1 + 2 x 7
2 x (2 + 5) <> 2 x 2 + 2 x 5
2 x (2 + 6) <> 2 x 2 + 2 x 6
2 x (3 + 1) <> 2 x 3 + 2 x 1
2 x (3 + 4) <> 2 x 3 + 2 x 4
2 x (3 + 6) <> 2 x 3 + 2 x 6
2 x (3 + 7) <> 2 x 3 + 2 x 7
2 x (4 + 1) <> 2 x 4 + 2 x 1
2 x (4 + 3) <> 2 x 4 + 2 x 3
2 x (4 + 5) <> 2 x 4 + 2 x 5
2 x (4 + 6) <> 2 x 4 + 2 x 6
2 x (5 + 1) <> 2 x 5 + 2 x 1
2 x (5 + 2) <> 2 x 5 + 2 x 2
2 x (5 + 4) <> 2 x 5 + 2 x 4
2 x (5 + 6) <> 2 x 5 + 2 x 6
2 x (6 + 2) <> 2 x 6 + 2 x 2
2 x (6 + 3) <> 2 x 6 + 2 x 3
2 x (6 + 4) <> 2 x 6 + 2 x 4
2 x (6 + 5) <> 2 x 6 + 2 x 5
2 x (7 + 1) <> 2 x 7 + 2 x 1
2 x (7 + 3) <> 2 x 7 + 2 x 3
3 x (1 + 1) <> 3 x 1 + 3 x 1
3 x (1 + 2) <> 3 x 1 + 3 x 2
3 x (1 + 3) <> 3 x 1 + 3 x 3
3 x (1 + 4) <> 3 x 1 + 3 x 4
3 x (1 + 5) <> 3 x 1 + 3 x 5
3 x (1 + 7) <> 3 x 1 + 3 x 7
3 x (2 + 1) <> 3 x 2 + 3 x 1
3 x (2 + 5) <> 3 x 2 + 3 x 5
3 x (2 + 6) <> 3 x 2 + 3 x 6
3 x (3 + 1) <> 3 x 3 + 3 x 1
3 x (3 + 4) <> 3 x 3 + 3 x 4
3 x (3 + 6) <> 3 x 3 + 3 x 6
3 x (3 + 7) <> 3 x 3 + 3 x 7
3 x (4 + 1) <> 3 x 4 + 3 x 1
3 x (4 + 3) <> 3 x 4 + 3 x 3
3 x (4 + 5) <> 3 x 4 + 3 x 5
3 x (4 + 6) <> 3 x 4 + 3 x 6
3 x (5 + 1) <> 3 x 5 + 3 x 1
3 x (5 + 2) <> 3 x 5 + 3 x 2
3 x (5 + 4) <> 3 x 5 + 3 x 4
3 x (5 + 6) <> 3 x 5 + 3 x 6
3 x (6 + 2) <> 3 x 6 + 3 x 2
3 x (6 + 3) <> 3 x 6 + 3 x 3
3 x (6 + 4) <> 3 x 6 + 3 x 4
3 x (6 + 5) <> 3 x 6 + 3 x 5
3 x (6 + 6) <> 3 x 6 + 3 x 6
3 x (6 + 7) <> 3 x 6 + 3 x 7
3 x (7 + 1) <> 3 x 7 + 3 x 1
3 x (7 + 3) <> 3 x 7 + 3 x 3
3 x (7 + 6) <> 3 x 7 + 3 x 6
5 x (1 + 1) <> 5 x 1 + 5 x 1
5 x (1 + 2) <> 5 x 1 + 5 x 2
5 x (1 + 3) <> 5 x 1 + 5 x 3
5 x (1 + 4) <> 5 x 1 + 5 x 4
5 x (1 + 5) <> 5 x 1 + 5 x 5
5 x (1 + 7) <> 5 x 1 + 5 x 7
5 x (2 + 1) <> 5 x 2 + 5 x 1
5 x (2 + 5) <> 5 x 2 + 5 x 5
5 x (2 + 6) <> 5 x 2 + 5 x 6
5 x (3 + 1) <> 5 x 3 + 5 x 1
5 x (3 + 4) <> 5 x 3 + 5 x 4
5 x (3 + 6) <> 5 x 3 + 5 x 6
5 x (3 + 7) <> 5 x 3 + 5 x 7
5 x (4 + 1) <> 5 x 4 + 5 x 1
5 x (4 + 3) <> 5 x 4 + 5 x 3
5 x (4 + 5) <> 5 x 4 + 5 x 5
5 x (4 + 6) <> 5 x 4 + 5 x 6
5 x (5 + 1) <> 5 x 5 + 5 x 1
5 x (5 + 2) <> 5 x 5 + 5 x 2
5 x (5 + 4) <> 5 x 5 + 5 x 4
5 x (5 + 6) <> 5 x 5 + 5 x 6
5 x (6 + 2) <> 5 x 6 + 5 x 2
5 x (6 + 3) <> 5 x 6 + 5 x 3
5 x (6 + 4) <> 5 x 6 + 5 x 4
5 x (6 + 5) <> 5 x 6 + 5 x 5
5 x (6 + 6) <> 5 x 6 + 5 x 6
5 x (6 + 7) <> 5 x 6 + 5 x 7
5 x (7 + 1) <> 5 x 7 + 5 x 1
5 x (7 + 3) <> 5 x 7 + 5 x 3
5 x (7 + 6) <> 5 x 7 + 5 x 6
7 x (1 + 3) <> 7 x 1 + 7 x 3
7 x (1 + 4) <> 7 x 1 + 7 x 4
7 x (1 + 5) <> 7 x 1 + 7 x 5
7 x (1 + 7) <> 7 x 1 + 7 x 7
7 x (2 + 5) <> 7 x 2 + 7 x 5
7 x (2 + 6) <> 7 x 2 + 7 x 6
7 x (3 + 1) <> 7 x 3 + 7 x 1
7 x (3 + 4) <> 7 x 3 + 7 x 4
7 x (3 + 6) <> 7 x 3 + 7 x 6
7 x (3 + 7) <> 7 x 3 + 7 x 7
7 x (4 + 1) <> 7 x 4 + 7 x 1
7 x (4 + 3) <> 7 x 4 + 7 x 3
7 x (4 + 5) <> 7 x 4 + 7 x 5
7 x (4 + 6) <> 7 x 4 + 7 x 6
7 x (5 + 1) <> 7 x 5 + 7 x 1
7 x (5 + 2) <> 7 x 5 + 7 x 2
7 x (5 + 4) <> 7 x 5 + 7 x 4
7 x (5 + 6) <> 7 x 5 + 7 x 6
7 x (6 + 2) <> 7 x 6 + 7 x 2
7 x (6 + 3) <> 7 x 6 + 7 x 3
7 x (6 + 4) <> 7 x 6 + 7 x 4
7 x (6 + 5) <> 7 x 6 + 7 x 5
7 x (7 + 1) <> 7 x 7 + 7 x 1
7 x (7 + 3) <> 7 x 7 + 7 x 3

Luego la operacion x no es distribuiva a izquierda con respecto a +.

(1 + 1) x 3 <> 1 x 3 + 1 x 3
(1 + 1) x 5 <> 1 x 5 + 1 x 5
(1 + 2) x 3 <> 1 x 3 + 2 x 3
(1 + 2) x 5 <> 1 x 5 + 2 x 5

(1 + 3)x 2 <> 1x2 + 3x2
(1 + 3)x 3 <> 1x3 + 3x3
(1 + 3)x 5 <> 1x5 + 3x5
(1 + 3)x 7 <> 1x7 + 3x7
(1 + 4)x 2 <> 1x2 + 4x2
(1 + 4)x 3 <> 1x3 + 4x3
(1 + 4)x 5 <> 1x5 + 4x5
(1 + 4)x 7 <> 1x7 + 4x7
(1 + 5)x 2 <> 1x2 + 5x2
(1 + 5)x 3 <> 1x3 + 5x3
(1 + 5)x 5 <> 1x5 + 5x5
(1 + 5)x 7 <> 1x7 + 5x7
(1 + 7)x 2 <> 1x2 + 7x2
(1 + 7)x 3 <> 1x3 + 7x3
(1 + 7)x 5 <> 1x5 + 7x5
(1 + 7)x 7 <> 1x7 + 7x7
(2 + 1)x 3 <> 2x3 + 1x3
(2 + 1)x 5 <> 2x5 + 1x5
(2 + 5)x 2 <> 2x2 + 5x2
(2 + 5)x 3 <> 2x3 + 5x3
(2 + 5)x 5 <> 2x5 + 5x5
(2 + 5)x 7 <> 2x7 + 5x7
(2 + 6)x 2 <> 2x2 + 6x2
(2 + 6)x 3 <> 2x3 + 6x3
(2 + 6)x 5 <> 2x5 + 6x5
(2 + 6)x 7 <> 2x7 + 6x7
(3 + 1)x 2 <> 3x2 + 1x2
(3 + 1)x 3 <> 3x3 + 1x3
(3 + 1)x 5 <> 3x5 + 1x5
(3 + 1)x 7 <> 3x7 + 1x7
(3 + 4)x 2 <> 3x2 + 4x2
(3 + 4)x 3 <> 3x3 + 4x3
(3 + 4)x 5 <> 3x5 + 4x5
(3 + 4)x 7 <> 3x7 + 4x7
(3 + 6)x 2 <> 3x2 + 6x2
(3 + 6)x 3 <> 3x3 + 6x3
(3 + 6)x 5 <> 3x5 + 6x5
(3 + 6)x 7 <> 3x7 + 6x7
(3 + 7)x 2 <> 3x2 + 7x2
(3 + 7)x 3 <> 3x3 + 7x3
(3 + 7)x 5 <> 3x5 + 7x5
(3 + 7)x 7 <> 3x7 + 7x7
(4 + 1)x 2 <> 4x2 + 1x2
(4 + 1)x 3 <> 4x3 + 1x3
(4 + 1)x 5 <> 4x5 + 1x5
(4 + 1)x 7 <> 4x7 + 1x7
(4 + 3)x 2 <> 4x2 + 3x2
(4 + 3)x 3 <> 4x3 + 3x3
(4 + 3)x 5 <> 4x5 + 3x5
(4 + 3)x 7 <> 4x7 + 3x7
(4 + 5)x 2 <> 4x2 + 5x2
(4 + 5)x 3 <> 4x3 + 5x3
(4 + 5)x 5 <> 4x5 + 5x5
(4 + 5)x 7 <> 4x7 + 5x7
(4 + 6)x 2 <> 4x2 + 6x2
(4 + 6)x 3 <> 4x3 + 6x3
(4 + 6)x 5 <> 4x5 + 6x5
(4 + 6)x 7 <> 4x7 + 6x7
(5 + 1)x 2 <> 5x2 + 1x2
(5 + 1)x 3 <> 5x3 + 1x3
(5 + 1)x 5 <> 5x5 + 1x5
(5 + 1)x 7 <> 5x7 + 1x7
(5 + 2)x 2 <> 5x2 + 2x2
(5 + 2)x 3 <> 5x3 + 2x3
(5 + 2)x 5 <> 5x5 + 2x5
(5 + 2)x 7 <> 5x7 + 2x7
(5 + 4)x 2 <> 5x2 + 4x2
(5 + 4)x 3 <> 5x3 + 4x3
(5 + 4)x 5 <> 5x5 + 4x5
(5 + 4)x 7 <> 5x7 + 4x7
(5 + 6)x 2 <> 5x2 + 6x2
(5 + 6)x 3 <> 5x3 + 6x3
(5 + 6)x 5 <> 5x5 + 6x5
(5 + 6)x 7 <> 5x7 + 6x7
(6 + 2)x 2 <> 6x2 + 2x2
(6 + 2)x 3 <> 6x3 + 2x3
(6 + 2)x 5 <> 6x5 + 2x5
(6 + 2)x 7 <> 6x7 + 2x7
(6 + 3)x 2 <> 6x2 + 3x2
(6 + 3)x 3 <> 6x3 + 3x3
(6 + 3)x 5 <> 6x5 + 3x5
(6 + 3)x 7 <> 6x7 + 3x7
(6 + 4)x 2 <> 6x2 + 4x2
(6 + 4)x 3 <> 6x3 + 4x3
(6 + 4)x 5 <> 6x5 + 4x5
(6 + 4)x 7 <> 6x7 + 4x7
(6 + 5)x 2 <> 6x2 + 5x2
(6 + 5)x 3 <> 6x3 + 5x3
(6 + 5)x 5 <> 6x5 + 5x5
(6 + 5)x 7 <> 6x7 + 5x7
(6 + 6)x 3 <> 6x3 + 6x3
(6 + 6)x 5 <> 6x5 + 6x5
(6 + 7)x 3 <> 6x3 + 7x3
(6 + 7)x 5 <> 6x5 + 7x5
(7 + 1)x 2 <> 7x2 + 1x2
(7 + 1)x 3 <> 7x3 + 1x3
(7 + 1)x 5 <> 7x5 + 1x5
(7 + 1)x 7 <> 7x7 + 1x7
(7 + 3)x 2 <> 7x2 + 3x2
(7 + 3)x 3 <> 7x3 + 3x3
(7 + 3)x 5 <> 7x5 + 3x5
(7 + 3)x 7 <> 7x7 + 3x7
(7 + 6)x 3 <> 7x3 + 6x3
(7 + 6)x 5 <> 7x5 + 6x5

Luego la operacion x no es distribuiva a derecha con respecto a +.

(2 x 3)x 3 <> 2 x (3 x 3)
(2 x 3)x 5 <> 2 x (3 x 5)
(2 x 5)x 3 <> 2 x (5 x 3)
(2 x 5)x 5 <> 2 x (5 x 5)
(3 x 3)x 2 <> 3 x (3 x 2)
(3 x 3)x 7 <> 3 x (3 x 7)
(3 x 5)x 2 <> 3 x (5 x 2)
(3 x 5)x 7 <> 3 x (5 x 7)
(5 x 3)x 2 <> 5 x (3 x 2)
(5 x 3)x 7 <> 5 x (3 x 7)
(5 x 5)x 2 <> 5 x (5 x 2)
(5 x 5)x 7 <> 5 x (5 x 7)
(7 x 3)x 3 <> 7 x (3 x 3)
(7 x 3)x 5 <> 7 x (3 x 5)
(7 x 5)x 3 <> 7 x (5 x 3)
(7 x 5)x 5 <> 7 x (5 x 5)

La operación x es asociativa

La operación x es conmutativa

El elemento neutro respecto a x es : 1

El elemento inverso de 1 respecto a x es 1
El elemento inverso de 3 respecto a x es 5
El elemento inverso de 5 respecto a x es 3
El elemento inverso de 6 respecto a x es 6

Anexo D: Análisis realizado en Propiedades 3.1 para tablas de multiplicación (Caso 2a)

Estudio algebraico de la operación

x	0	1	2	3	4	5	6	7
0	0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6	7
2	0	2	4	2	0	2	2	4
3	0	3	2	5	4	6	1	2
4	0	4	0	4	0	4	4	0
5	0	5	2	6	4	1	3	2
6	0	6	2	1	4	3	5	2
7	0	7	4	2	0	2	2	4

2 x (1 + 2) <> 2 x 1 + 2 x 2
2 x (1 + 5) <> 2 x 1 + 2 x 5
2 x (1 + 6) <> 2 x 1 + 2 x 6
2 x (1 + 7) <> 2 x 1 + 2 x 7
2 x (2 + 1) <> 2 x 2 + 2 x 1
2 x (2 + 3) <> 2 x 2 + 2 x 3
2 x (2 + 5) <> 2 x 2 + 2 x 5
2 x (2 + 6) <> 2 x 2 + 2 x 6
2 x (3 + 2) <> 2 x 3 + 2 x 2
2 x (3 + 5) <> 2 x 3 + 2 x 5
2 x (3 + 6) <> 2 x 3 + 2 x 6
2 x (3 + 7) <> 2 x 3 + 2 x 7
2 x (5 + 1) <> 2 x 5 + 2 x 1
2 x (5 + 2) <> 2 x 5 + 2 x 2
2 x (5 + 3) <> 2 x 5 + 2 x 3
2 x (5 + 7) <> 2 x 5 + 2 x 7
2 x (6 + 1) <> 2 x 6 + 2 x 1
2 x (6 + 2) <> 2 x 6 + 2 x 2
2 x (6 + 3) <> 2 x 6 + 2 x 3
2 x (6 + 7) <> 2 x 6 + 2 x 7
2 x (7 + 1) <> 2 x 7 + 2 x 1
2 x (7 + 3) <> 2 x 7 + 2 x 3
2 x (7 + 5) <> 2 x 7 + 2 x 5
2 x (7 + 6) <> 2 x 7 + 2 x 6
3 x (1 + 1) <> 3 x 1 + 3 x 1
3 x (1 + 2) <> 3 x 1 + 3 x 2
3 x (1 + 3) <> 3 x 1 + 3 x 3
3 x (1 + 4) <> 3 x 1 + 3 x 4
3 x (1 + 6) <> 3 x 1 + 3 x 6
3 x (1 + 7) <> 3 x 1 + 3 x 7
3 x (2 + 1) <> 3 x 2 + 3 x 1
3 x (2 + 3) <> 3 x 2 + 3 x 3
3 x (2 + 4) <> 3 x 2 + 3 x 4
3 x (2 + 6) <> 3 x 2 + 3 x 6
3 x (2 + 7) <> 3 x 2 + 3 x 7
3 x (3 + 1) <> 3 x 3 + 3 x 1
3 x (3 + 2) <> 3 x 3 + 3 x 2
3 x (3 + 4) <> 3 x 3 + 3 x 4
3 x (3 + 5) <> 3 x 3 + 3 x 5
3 x (4 + 1) <> 3 x 4 + 3 x 1
3 x (4 + 2) <> 3 x 4 + 3 x 2
3 x (4 + 3) <> 3 x 4 + 3 x 3
3 x (4 + 5) <> 3 x 4 + 3 x 5
3 x (4 + 6) <> 3 x 4 + 3 x 6
3 x (4 + 7) <> 3 x 4 + 3 x 7
3 x (5 + 3) <> 3 x 5 + 3 x 3
3 x (5 + 4) <> 3 x 5 + 3 x 4
3 x (5 + 6) <> 3 x 5 + 3 x 6
3 x (5 + 7) <> 3 x 5 + 3 x 7
3 x (6 + 1) <> 3 x 6 + 3 x 1
3 x (6 + 2) <> 3 x 6 + 3 x 2
3 x (6 + 4) <> 3 x 6 + 3 x 4
3 x (6 + 5) <> 3 x 6 + 3 x 5
3 x (6 + 6) <> 3 x 6 + 3 x 6
3 x (6 + 7) <> 3 x 6 + 3 x 7
3 x (7 + 1) <> 3 x 7 + 3 x 1
3 x (7 + 2) <> 3 x 7 + 3 x 2
3 x (7 + 4) <> 3 x 7 + 3 x 4
3 x (7 + 5) <> 3 x 7 + 3 x 5
3 x (7 + 6) <> 3 x 7 + 3 x 6
5 x (1 + 2) <> 5 x 1 + 5 x 2
5 x (1 + 3) <> 5 x 1 + 5 x 3
5 x (2 + 1) <> 5 x 2 + 5 x 1
5 x (2 + 3) <> 5 x 2 + 5 x 3
5 x (2 + 4) <> 5 x 2 + 5 x 4
5 x (2 + 5) <> 5 x 2 + 5 x 5
5 x (2 + 6) <> 5 x 2 + 5 x 6
5 x (2 + 7) <> 5 x 2 + 5 x 7
5 x (3 + 1) <> 5 x 3 + 5 x 1
5 x (3 + 2) <> 5 x 3 + 5 x 2
5 x (4 + 2) <> 5 x 4 + 5 x 2
5 x (4 + 7) <> 5 x 4 + 5 x 7
5 x (5 + 2) <> 5 x 5 + 5 x 2
5 x (5 + 5) <> 5 x 5 + 5 x 5
5 x (6 + 2) <> 5 x 6 + 5 x 2
5 x (6 + 6) <> 5 x 6 + 5 x 6
5 x (7 + 2) <> 5 x 7 + 5 x 2
5 x (7 + 4) <> 5 x 7 + 5 x 4
6 x (1 + 2) <> 6 x 1 + 6 x 2
6 x (1 + 3) <> 6 x 1 + 6 x 3
6 x (1 + 4) <> 6 x 1 + 6 x 4
6 x (1 + 6) <> 6 x 1 + 6 x 6
6 x (2 + 1) <> 6 x 2 + 6 x 1
6 x (2 + 3) <> 6 x 2 + 6 x 3
6 x (2 + 4) <> 6 x 2 + 6 x 4
6 x (2 + 5) <> 6 x 2 + 6 x 5
6 x (2 + 7) <> 6 x 2 + 6 x 7
6 x (3 + 1) <> 6 x 3 + 6 x 1
6 x (3 + 2) <> 6 x 3 + 6 x 2
6 x (3 + 3) <> 6 x 3 + 6 x 3
6 x (3 + 4) <> 6 x 3 + 6 x 4
6 x (3 + 5) <> 6 x 3 + 6 x 5
6 x (3 + 7) <> 6 x 3 + 6 x 7
6 x (4 + 1) <> 6 x 4 + 6 x 1
6 x (4 + 2) <> 6 x 4 + 6 x 2
6 x (4 + 3) <> 6 x 4 + 6 x 3
6 x (4 + 5) <> 6 x 4 + 6 x 5
6 x (4 + 6) <> 6 x 4 + 6 x 6
6 x (4 + 7) <> 6 x 4 + 6 x 7
6 x (5 + 2) <> 6 x 5 + 6 x 2
6 x (5 + 3) <> 6 x 5 + 6 x 3
6 x (5 + 4) <> 6 x 5 + 6 x 4
6 x (5 + 5) <> 6 x 5 + 6 x 5
6 x (5 + 6) <> 6 x 5 + 6 x 6
6 x (5 + 7) <> 6 x 5 + 6 x 7
6 x (6 + 1) <> 6 x 6 + 6 x 1
6 x (6 + 4) <> 6 x 6 + 6 x 4
6 x (6 + 5) <> 6 x 6 + 6 x 5
6 x (6 + 7) <> 6 x 6 + 6 x 7
6 x (7 + 2) <> 6 x 7 + 6 x 2
6 x (7 + 3) <> 6 x 7 + 6 x 3
6 x (7 + 4) <> 6 x 7 + 6 x 4

6 x (7 + 5) <> 6 x 7 + 6 x 5
6 x (7 + 6) <> 6 x 7 + 6 x 6
7 x (1 + 3) <> 7 x 1 + 7 x 3
7 x (1 + 4) <> 7 x 1 + 7 x 4
7 x (2 + 3) <> 7 x 2 + 7 x 3
7 x (2 + 6) <> 7 x 2 + 7 x 6
7 x (3 + 1) <> 7 x 3 + 7 x 1
7 x (3 + 2) <> 7 x 3 + 7 x 2
7 x (3 + 4) <> 7 x 3 + 7 x 4
7 x (3 + 5) <> 7 x 3 + 7 x 5
7 x (3 + 6) <> 7 x 3 + 7 x 6
7 x (3 + 7) <> 7 x 3 + 7 x 7
7 x (4 + 1) <> 7 x 4 + 7 x 1
7 x (4 + 3) <> 7 x 4 + 7 x 3
7 x (5 + 3) <> 7 x 5 + 7 x 3
7 x (5 + 7) <> 7 x 5 + 7 x 7
7 x (6 + 2) <> 7 x 6 + 7 x 2
7 x (6 + 3) <> 7 x 6 + 7 x 3
7 x (7 + 3) <> 7 x 7 + 7 x 3
7 x (7 + 5) <> 7 x 7 + 7 x 5

Luego la operacion x no es distribuiva a izquierda con respecto a +.

(1 + 1) x 3 <> 1 x 3 + 1 x 3
(1 + 2) x 2 <> 1 x 2 + 2 x 2
(1 + 2) x 3 <> 1 x 3 + 2 x 3
(1 + 2) x 5 <> 1 x 5 + 2 x 5
(1 + 2) x 6 <> 1 x 6 + 2 x 6
(1 + 3) x 3 <> 1 x 3 + 3 x 3
(1 + 3) x 5 <> 1 x 5 + 3 x 5
(1 + 3) x 6 <> 1 x 6 + 3 x 6
(1 + 3) x 7 <> 1 x 7 + 3 x 7
(1 + 4) x 3 <> 1 x 3 + 4 x 3
(1 + 4) x 6 <> 1 x 6 + 4 x 6
(1 + 4) x 7 <> 1 x 7 + 4 x 7
(1 + 5) x 2 <> 1 x 2 + 5 x 2
(1 + 6) x 2 <> 1 x 2 + 6 x 2
(1 + 6) x 3 <> 1 x 3 + 6 x 3
(1 + 6) x 6 <> 1 x 6 + 6 x 6
(1 + 7) x 2 <> 1 x 2 + 7 x 2
(1 + 7) x 3 <> 1 x 3 + 7 x 3
(2 + 1) x 2 <> 2 x 2 + 1 x 2
(2 + 1) x 3 <> 2 x 3 + 1 x 3
(2 + 1) x 5 <> 2 x 5 + 1 x 5
(2 + 1) x 6 <> 2 x 6 + 1 x 6
(2 + 3) x 2 <> 2 x 2 + 3 x 2
(2 + 3) x 3 <> 2 x 3 + 3 x 3
(2 + 3) x 5 <> 2 x 5 + 3 x 5
(2 + 3) x 6 <> 2 x 6 + 3 x 6
(2 + 3) x 7 <> 2 x 7 + 3 x 7
(2 + 4) x 3 <> 2 x 3 + 4 x 3
(2 + 4) x 5 <> 2 x 5 + 4 x 5
(2 + 4) x 6 <> 2 x 6 + 4 x 6
(2 + 5) x 2 <> 2 x 2 + 5 x 2
(2 + 5) x 5 <> 2 x 5 + 5 x 5
(2 + 5) x 6 <> 2 x 6 + 5 x 6
(2 + 6) x 2 <> 2 x 2 + 6 x 2
(2 + 6) x 3 <> 2 x 3 + 6 x 3
(2 + 6) x 5 <> 2 x 5 + 6 x 5
(2 + 6) x 7 <> 2 x 7 + 6 x 7
(2 + 7) x 3 <> 2 x 3 + 7 x 3
(2 + 7) x 5 <> 2 x 5 + 7 x 5
(2 + 7) x 6 <> 2 x 6 + 7 x 6
(3 + 1) x 3 <> 3 x 3 + 1 x 3
(3 + 1) x 5 <> 3 x 5 + 1 x 5
(3 + 1) x 6 <> 3 x 6 + 1 x 6
(3 + 1) x 7 <> 3 x 7 + 1 x 7
(3 + 2) x 2 <> 3 x 2 + 2 x 2
(3 + 2) x 3 <> 3 x 3 + 2 x 3
(3 + 2) x 5 <> 3 x 5 + 2 x 5
(3 + 2) x 6 <> 3 x 6 + 2 x 6
(3 + 2) x 7 <> 3 x 7 + 2 x 7
(3 + 3) x 6 <> 3 x 6 + 3 x 6
(3 + 4) x 3 <> 3 x 3 + 4 x 3
(3 + 4) x 6 <> 3 x 6 + 4 x 6
(3 + 4) x 7 <> 3 x 7 + 4 x 7
(3 + 5) x 2 <> 3 x 2 + 5 x 2
(3 + 5) x 3 <> 3 x 3 + 5 x 3
(3 + 5) x 6 <> 3 x 6 + 5 x 6
(3 + 5) x 7 <> 3 x 7 + 5 x 7
(3 + 6) x 2 <> 3 x 2 + 6 x 2
(3 + 6) x 7 <> 3 x 7 + 6 x 7
(3 + 7) x 2 <> 3 x 2 + 7 x 2
(3 + 7) x 6 <> 3 x 6 + 7 x 6
(3 + 7) x 7 <> 3 x 7 + 7 x 7
(4 + 1) x 3 <> 4 x 3 + 1 x 3
(4 + 1) x 6 <> 4 x 6 + 1 x 6
(4 + 1) x 7 <> 4 x 7 + 1 x 7
(4 + 2) x 3 <> 4 x 3 + 2 x 3
(4 + 2) x 5 <> 4 x 5 + 2 x 5
(4 + 2) x 6 <> 4 x 6 + 2 x 6
(4 + 3) x 3 <> 4 x 3 + 3 x 3
(4 + 3) x 6 <> 4 x 6 + 3 x 6
(4 + 3) x 7 <> 4 x 7 + 3 x 7
(4 + 5) x 3 <> 4 x 3 + 5 x 3
(4 + 5) x 6 <> 4 x 6 + 5 x 6
(4 + 6) x 3 <> 4 x 3 + 6 x 3
(4 + 6) x 6 <> 4 x 6 + 6 x 6
(4 + 7) x 3 <> 4 x 3 + 7 x 3
(4 + 7) x 5 <> 4 x 5 + 7 x 5
(4 + 7) x 6 <> 4 x 6 + 7 x 6
(5 + 1) x 2 <> 5 x 2 + 1 x 2
(5 + 2) x 2 <> 5 x 2 + 2 x 2
(5 + 2) x 5 <> 5 x 5 + 2 x 5
(5 + 2) x 6 <> 5 x 6 + 2 x 6
(5 + 3) x 2 <> 5 x 2 + 3 x 2
(5 + 3) x 3 <> 5 x 3 + 3 x 3
(5 + 3) x 6 <> 5 x 6 + 3 x 6
(5 + 3) x 7 <> 5 x 7 + 3 x 7
(5 + 4) x 3 <> 5 x 3 + 4 x 3
(5 + 4) x 6 <> 5 x 6 + 4 x 6
(5 + 5) x 5 <> 5 x 5 + 5 x 5
(5 + 5) x 6 <> 5 x 6 + 5 x 6
(5 + 6) x 3 <> 5 x 3 + 6 x 3
(5 + 6) x 6 <> 5 x 6 + 6 x 6
(5 + 7) x 2 <> 5 x 2 + 7 x 2
(5 + 7) x 3 <> 5 x 3 + 7 x 3
(5 + 7) x 6 <> 5 x 6 + 7 x 6
(5 + 7) x 7 <> 5 x 7 + 7 x 7
(6 + 1) x 2 <> 6 x 2 + 1 x 2
(6 + 1) x 3 <> 6 x 3 + 1 x 3
(6 + 1) x 6 <> 6 x 6 + 1 x 6
(6 + 2) x 2 <> 6 x 2 + 2 x 2
(6 + 2) x 3 <> 6 x 3 + 2 x 3
(6 + 2) x 5 <> 6 x 5 + 2 x 5
(6 + 2) x 7 <> 6 x 7 + 2 x 7
(6 + 3) x 2 <> 6 x 2 + 3 x 2
(6 + 3) x 7 <> 6 x 7 + 3 x 7
(6 + 4) x 3 <> 6 x 3 + 4 x 3
(6 + 4) x 6 <> 6 x 6 + 4 x 6
(6 + 5) x 3 <> 6 x 3 + 5 x 3
(6 + 5) x 6 <> 6 x 6 + 5 x 6
(6 + 6) x 3 <> 6 x 3 + 6 x 3
(6 + 6) x 5 <> 6 x 5 + 6 x 5
(6 + 7) x 2 <> 6 x 2 + 7 x 2

(6 + 7) x 3 <> 6 x 3 + 7 x 3
(6 + 7) x 6 <> 6 x 6 + 7 x 6
(7 + 1) x 2 <> 7 x 2 + 1 x 2
(7 + 1) x 3 <> 7 x 3 + 1 x 3
(7 + 2) x 3 <> 7 x 3 + 2 x 3
(7 + 2) x 5 <> 7 x 5 + 2 x 5
(7 + 2) x 6 <> 7 x 6 + 2 x 6
(7 + 3) x 2 <> 7 x 2 + 3 x 2
(7 + 3) x 6 <> 7 x 6 + 3 x 6
(7 + 3) x 7 <> 7 x 7 + 3 x 7
(7 + 4) x 3 <> 7 x 3 + 4 x 3
(7 + 4) x 5 <> 7 x 5 + 4 x 5
(7 + 4) x 6 <> 7 x 6 + 4 x 6
(7 + 5) x 2 <> 7 x 2 + 5 x 2
(7 + 5) x 3 <> 7 x 3 + 5 x 3
(7 + 5) x 6 <> 7 x 6 + 5 x 6
(7 + 5) x 7 <> 7 x 7 + 5 x 7
(7 + 6) x 2 <> 7 x 2 + 6 x 2
(7 + 6) x 3 <> 7 x 3 + 6 x 3
(7 + 6) x 6 <> 7 x 6 + 6 x 6

Luego la operacion x no es distribuiva a derecha con respecto a +.
(3 x 6) x 7 <> 3 x (6 x 7)
(5 x 5) x 7 <> 5 x (5 x 7)
(6 x 3) x 7 <> 6 x (3 x 7)
(7 x 3) x 6 <> 7 x (3 x 6)
(7 x 5) x 5 <> 7 x (5 x 5)
(7 x 6) x 3 <> 7 x (6 x 3)
La operación x es asociativa

La operación x es conmutativa

El elemento neutro respecto a x es : 1

El elemento inverso de 1 respecto a x es 1
El elemento inverso de 3 respecto a x es 6
El elemento inverso de 5 respecto a x es 5
El elemento inverso de 6 respecto a x es 3

Anexo E: Análisis realizado en *Propiedades 3.1* para tablas de multiplicación (Caso 2b)

Estudio algebraico de la operación

x	0	1	2	3	4	5	6	7
0	0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6	7
2	0	2	4	7	0	2	7	4
3	0	3	7	5	4	6	1	2
4	0	4	0	4	0	4	4	0
5	0	5	2	6	4	1	3	7
6	0	6	7	1	4	3	5	2
7	0	7	4	2	0	7	2	4

2 x (1 + 3) <> 2 x 1 + 2 x 3
2 x (1 + 4) <> 2 x 1 + 2 x 4
2 x (1 + 5) <> 2 x 1 + 2 x 5
2 x (1 + 7) <> 2 x 1 + 2 x 7
2 x (2 + 5) <> 2 x 2 + 2 x 5
2 x (2 + 6) <> 2 x 2 + 2 x 6
2 x (3 + 1) <> 2 x 3 + 2 x 1
2 x (3 + 4) <> 2 x 3 + 2 x 4
2 x (3 + 6) <> 2 x 3 + 2 x 6
2 x (3 + 7) <> 2 x 3 + 2 x 7
2 x (4 + 1) <> 2 x 4 + 2 x 1
2 x (4 + 3) <> 2 x 4 + 2 x 3
2 x (4 + 5) <> 2 x 4 + 2 x 5
2 x (4 + 6) <> 2 x 4 + 2 x 6
2 x (5 + 1) <> 2 x 5 + 2 x 1
2 x (5 + 2) <> 2 x 5 + 2 x 2
2 x (5 + 4) <> 2 x 5 + 2 x 4
2 x (5 + 6) <> 2 x 5 + 2 x 6
2 x (6 + 2) <> 2 x 6 + 2 x 2
2 x (6 + 3) <> 2 x 6 + 2 x 3
2 x (6 + 4) <> 2 x 6 + 2 x 4
2 x (6 + 5) <> 2 x 6 + 2 x 5
2 x (7 + 1) <> 2 x 7 + 2 x 1
2 x (7 + 3) <> 2 x 7 + 2 x 3
3 x (1 + 1) <> 3 x 1 + 3 x 1
3 x (1 + 2) <> 3 x 1 + 3 x 2
3 x (1 + 3) <> 3 x 1 + 3 x 3
3 x (1 + 4) <> 3 x 1 + 3 x 4
3 x (1 + 6) <> 3 x 1 + 3 x 6
3 x (1 + 7) <> 3 x 1 + 3 x 7
3 x (2 + 1) <> 3 x 2 + 3 x 1
3 x (2 + 3) <> 3 x 2 + 3 x 3
3 x (2 + 5) <> 3 x 2 + 3 x 5
3 x (3 + 1) <> 3 x 3 + 3 x 1
3 x (3 + 2) <> 3 x 3 + 3 x 2
3 x (3 + 4) <> 3 x 3 + 3 x 4
3 x (3 + 5) <> 3 x 3 + 3 x 5
3 x (4 + 1) <> 3 x 4 + 3 x 1
3 x (4 + 3) <> 3 x 4 + 3 x 3
3 x (4 + 5) <> 3 x 4 + 3 x 5
3 x (4 + 6) <> 3 x 4 + 3 x 6
3 x (5 + 2) <> 3 x 5 + 3 x 2
3 x (5 + 3) <> 3 x 5 + 3 x 3
3 x (5 + 4) <> 3 x 5 + 3 x 4
3 x (5 + 5) <> 3 x 5 + 3 x 5
3 x (5 + 6) <> 3 x 5 + 3 x 6
3 x (5 + 7) <> 3 x 5 + 3 x 7
3 x (6 + 1) <> 3 x 6 + 3 x 1
3 x (6 + 4) <> 3 x 6 + 3 x 4
3 x (6 + 5) <> 3 x 6 + 3 x 5
3 x (6 + 7) <> 3 x 6 + 3 x 7
3 x (7 + 1) <> 3 x 7 + 3 x 1
3 x (7 + 5) <> 3 x 7 + 3 x 5
3 x (7 + 6) <> 3 x 7 + 3 x 6
5 x (1 + 1) <> 5 x 1 + 5 x 1
5 x (1 + 2) <> 5 x 1 + 5 x 2
5 x (1 + 3) <> 5 x 1 + 5 x 3
5 x (1 + 7) <> 5 x 1 + 5 x 7
5 x (2 + 1) <> 5 x 2 + 5 x 1
5 x (2 + 3) <> 5 x 2 + 5 x 3
5 x (2 + 5) <> 5 x 2 + 5 x 5
5 x (2 + 6) <> 5 x 2 + 5 x 6
5 x (3 + 1) <> 5 x 3 + 5 x 1
5 x (3 + 2) <> 5 x 3 + 5 x 2
5 x (3 + 3) <> 5 x 3 + 5 x 3
5 x (3 + 7) <> 5 x 3 + 5 x 7
5 x (5 + 2) <> 5 x 5 + 5 x 2
5 x (5 + 5) <> 5 x 5 + 5 x 5
5 x (5 + 6) <> 5 x 5 + 5 x 6
5 x (5 + 7) <> 5 x 5 + 5 x 7
5 x (6 + 2) <> 5 x 6 + 5 x 2
5 x (6 + 5) <> 5 x 6 + 5 x 5
5 x (6 + 6) <> 5 x 6 + 5 x 6
5 x (6 + 7) <> 5 x 6 + 5 x 7
5 x (7 + 1) <> 5 x 7 + 5 x 1
5 x (7 + 3) <> 5 x 7 + 5 x 3
5 x (7 + 5) <> 5 x 7 + 5 x 5
5 x (7 + 6) <> 5 x 7 + 5 x 6
6 x (1 + 2) <> 6 x 1 + 6 x 2
6 x (1 + 3) <> 6 x 1 + 6 x 3
6 x (1 + 4) <> 6 x 1 + 6 x 4
6 x (1 + 6) <> 6 x 1 + 6 x 6
6 x (2 + 1) <> 6 x 2 + 6 x 1
6 x (2 + 3) <> 6 x 2 + 6 x 3
6 x (2 + 6) <> 6 x 2 + 6 x 6
6 x (3 + 1) <> 6 x 3 + 6 x 1
6 x (3 + 2) <> 6 x 3 + 6 x 2
6 x (3 + 3) <> 6 x 3 + 6 x 3
6 x (3 + 4) <> 6 x 3 + 6 x 4
6 x (3 + 5) <> 6 x 3 + 6 x 5
6 x (3 + 7) <> 6 x 3 + 6 x 7
6 x (4 + 1) <> 6 x 4 + 6 x 1
6 x (4 + 3) <> 6 x 4 + 6 x 3
6 x (4 + 5) <> 6 x 4 + 6 x 5
6 x (4 + 6) <> 6 x 4 + 6 x 6
6 x (5 + 3) <> 6 x 5 + 6 x 3
6 x (5 + 4) <> 6 x 5 + 6 x 4
6 x (5 + 6) <> 6 x 5 + 6 x 6
6 x (5 + 7) <> 6 x 5 + 6 x 7
6 x (6 + 1) <> 6 x 6 + 6 x 1
6 x (6 + 2) <> 6 x 6 + 6 x 2
6 x (6 + 4) <> 6 x 6 + 6 x 4
6 x (6 + 5) <> 6 x 6 + 6 x 5
6 x (6 + 6) <> 6 x 6 + 6 x 6
6 x (6 + 7) <> 6 x 6 + 6 x 7
6 x (7 + 3) <> 6 x 7 + 6 x 3
6 x (7 + 5) <> 6 x 7 + 6 x 5
6 x (7 + 6) <> 6 x 7 + 6 x 6
7 x (1 + 3) <> 7 x 1 + 7 x 3
7 x (1 + 4) <> 7 x 1 + 7 x 4
7 x (1 + 5) <> 7 x 1 + 7 x 5
7 x (1 + 7) <> 7 x 1 + 7 x 7
7 x (2 + 5) <> 7 x 2 + 7 x 5
7 x (2 + 6) <> 7 x 2 + 7 x 6

7 x (3 + 1) <> 7 x 3 + 7 x 1
7 x (3 + 4) <> 7 x 3 + 7 x 4
7 x (3 + 6) <> 7 x 3 + 7 x 6
7 x (3 + 7) <> 7 x 3 + 7 x 7
7 x (4 + 1) <> 7 x 4 + 7 x 1
7 x (4 + 3) <> 7 x 4 + 7 x 3
7 x (4 + 5) <> 7 x 4 + 7 x 5
7 x (4 + 6) <> 7 x 4 + 7 x 6
7 x (5 + 1) <> 7 x 5 + 7 x 1
7 x (5 + 2) <> 7 x 5 + 7 x 2
7 x (5 + 4) <> 7 x 5 + 7 x 4
7 x (5 + 6) <> 7 x 5 + 7 x 6
7 x (6 + 2) <> 7 x 6 + 7 x 2
7 x (6 + 3) <> 7 x 6 + 7 x 3
7 x (6 + 4) <> 7 x 6 + 7 x 4
7 x (6 + 5) <> 7 x 6 + 7 x 5
7 x (7 + 1) <> 7 x 7 + 7 x 1
7 x (7 + 3) <> 7 x 7 + 7 x 3

Luego la operacion x no es distribuiva a izquierda con respecto a +.

(1 + 1) x 3 <> 1 x 3 + 1 x 3
(1 + 1) x 5 <> 1 x 5 + 1 x 5
(1 + 2) x 3 <> 1 x 3 + 2 x 3
(1 + 2) x 5 <> 1 x 5 + 2 x 5
(1 + 2) x 6 <> 1 x 6 + 2 x 6
(1 + 3) x 2 <> 1 x 2 + 3 x 2
(1 + 3) x 3 <> 1 x 3 + 3 x 3
(1 + 3) x 5 <> 1 x 5 + 3 x 5
(1 + 3) x 6 <> 1 x 6 + 3 x 6
(1 + 3) x 7 <> 1 x 7 + 3 x 7
(1 + 4) x 2 <> 1 x 2 + 4 x 2
(1 + 4) x 3 <> 1 x 3 + 4 x 3
(1 + 4) x 6 <> 1 x 6 + 4 x 6
(1 + 4) x 7 <> 1 x 7 + 4 x 7
(1 + 5) x 2 <> 1 x 2 + 5 x 2
(1 + 5) x 7 <> 1 x 7 + 5 x 7
(1 + 6) x 3 <> 1 x 3 + 6 x 3
(1 + 6) x 6 <> 1 x 6 + 6 x 6
(1 + 7) x 2 <> 1 x 2 + 7 x 2
(1 + 7) x 3 <> 1 x 3 + 7 x 3
(1 + 7) x 5 <> 1 x 5 + 7 x 5
(1 + 7) x 7 <> 1 x 7 + 7 x 7
(2 + 1) x 3 <> 2 x 3 + 1 x 3
(2 + 1) x 5 <> 2 x 5 + 1 x 5
(2 + 1) x 6 <> 2 x 6 + 1 x 6
(2 + 3) x 3 <> 2 x 3 + 3 x 3
(2 + 3) x 5 <> 2 x 5 + 3 x 5
(2 + 3) x 6 <> 2 x 6 + 3 x 6
(2 + 5) x 2 <> 2 x 2 + 5 x 2
(2 + 5) x 3 <> 2 x 3 + 5 x 3
(2 + 5) x 5 <> 2 x 5 + 5 x 5
(2 + 5) x 7 <> 2 x 7 + 5 x 7
(2 + 6) x 2 <> 2 x 2 + 6 x 2
(2 + 6) x 5 <> 2 x 5 + 6 x 5
(2 + 6) x 6 <> 2 x 6 + 6 x 6
(2 + 6) x 7 <> 2 x 7 + 6 x 7
(3 + 1) x 2 <> 3 x 2 + 1 x 2
(3 + 1) x 3 <> 3 x 3 + 1 x 3
(3 + 1) x 5 <> 3 x 5 + 1 x 5
(3 + 1) x 6 <> 3 x 6 + 1 x 6
(3 + 1) x 7 <> 3 x 7 + 1 x 7
(3 + 2) x 3 <> 3 x 3 + 2 x 3
(3 + 2) x 5 <> 3 x 5 + 2 x 5
(3 + 2) x 6 <> 3 x 6 + 2 x 6
(3 + 3) x 5 <> 3 x 5 + 3 x 5
(3 + 3) x 6 <> 3 x 6 + 3 x 6
(3 + 4) x 2 <> 3 x 2 + 4 x 2
(3 + 4) x 3 <> 3 x 3 + 4 x 3
(3 + 4) x 6 <> 3 x 6 + 4 x 6
(3 + 4) x 7 <> 3 x 7 + 4 x 7
(3 + 5) x 3 <> 3 x 3 + 5 x 3
(3 + 5) x 6 <> 3 x 6 + 5 x 6
(3 + 6) x 2 <> 3 x 2 + 6 x 2
(3 + 6) x 7 <> 3 x 7 + 6 x 7
(3 + 7) x 2 <> 3 x 2 + 7 x 2
(3 + 7) x 5 <> 3 x 5 + 7 x 5
(3 + 7) x 6 <> 3 x 6 + 7 x 6
(3 + 7) x 7 <> 3 x 7 + 7 x 7
(4 + 1) x 2 <> 4 x 2 + 1 x 2
(4 + 1) x 3 <> 4 x 3 + 1 x 3
(4 + 1) x 6 <> 4 x 6 + 1 x 6
(4 + 1) x 7 <> 4 x 7 + 1 x 7
(4 + 3) x 2 <> 4 x 2 + 3 x 2
(4 + 3) x 3 <> 4 x 3 + 3 x 3
(4 + 3) x 6 <> 4 x 6 + 3 x 6
(4 + 3) x 7 <> 4 x 7 + 3 x 7
(4 + 5) x 2 <> 4 x 2 + 5 x 2
(4 + 5) x 3 <> 4 x 3 + 5 x 3
(4 + 5) x 6 <> 4 x 6 + 5 x 6
(4 + 5) x 7 <> 4 x 7 + 5 x 7
(4 + 6) x 2 <> 4 x 2 + 6 x 2
(4 + 6) x 3 <> 4 x 3 + 6 x 3
(4 + 6) x 6 <> 4 x 6 + 6 x 6
(4 + 6) x 7 <> 4 x 7 + 6 x 7
(5 + 1) x 2 <> 5 x 2 + 1 x 2
(5 + 1) x 7 <> 5 x 7 + 1 x 7
(5 + 2) x 2 <> 5 x 2 + 2 x 2
(5 + 2) x 3 <> 5 x 3 + 2 x 3
(5 + 2) x 5 <> 5 x 5 + 2 x 5
(5 + 2) x 7 <> 5 x 7 + 2 x 7
(5 + 3) x 3 <> 5 x 3 + 3 x 3
(5 + 3) x 6 <> 5 x 6 + 3 x 6
(5 + 4) x 2 <> 5 x 2 + 4 x 2
(5 + 4) x 3 <> 5 x 3 + 4 x 3
(5 + 4) x 6 <> 5 x 6 + 4 x 6
(5 + 4) x 7 <> 5 x 7 + 4 x 7
(5 + 5) x 3 <> 5 x 3 + 5 x 3
(5 + 5) x 5 <> 5 x 5 + 5 x 5
(5 + 6) x 2 <> 5 x 2 + 6 x 2
(5 + 6) x 3 <> 5 x 3 + 6 x 3
(5 + 6) x 5 <> 5 x 5 + 6 x 5
(5 + 6) x 6 <> 5 x 6 + 6 x 6
(5 + 6) x 7 <> 5 x 7 + 6 x 7
(5 + 7) x 3 <> 5 x 3 + 7 x 3
(5 + 7) x 5 <> 5 x 5 + 7 x 5
(5 + 7) x 6 <> 5 x 6 + 7 x 6
(6 + 1) x 3 <> 6 x 3 + 1 x 3
(6 + 1) x 6 <> 6 x 6 + 1 x 6
(6 + 2) x 2 <> 6 x 2 + 2 x 2
(6 + 2) x 5 <> 6 x 5 + 2 x 5
(6 + 2) x 6 <> 6 x 6 + 2 x 6
(6 + 2) x 7 <> 6 x 7 + 2 x 7
(6 + 3) x 2 <> 6 x 2 + 3 x 2
(6 + 3) x 7 <> 6 x 7 + 3 x 7
(6 + 4) x 2 <> 6 x 2 + 4 x 2
(6 + 4) x 3 <> 6 x 3 + 4 x 3
(6 + 4) x 6 <> 6 x 6 + 4 x 6
(6 + 4) x 7 <> 6 x 7 + 4 x 7
(6 + 5) x 2 <> 6 x 2 + 5 x 2
(6 + 5) x 3 <> 6 x 3 + 5 x 3
(6 + 5) x 5 <> 6 x 5 + 5 x 5
(6 + 5) x 6 <> 6 x 6 + 5 x 6
(6 + 5) x 7 <> 6 x 7 + 5 x 7
(6 + 6) x 5 <> 6 x 5 + 6 x 5

(6 + 6) x 6 <> 6 x 6 + 6 x 6
(6 + 7) x 3 <> 6 x 3 + 7 x 3
(6 + 7) x 5 <> 6 x 5 + 7 x 5
(6 + 7) x 6 <> 6 x 6 + 7 x 6
(7 + 1) x 2 <> 7 x 2 + 1 x 2
(7 + 1) x 3 <> 7 x 3 + 1 x 3
(7 + 1) x 5 <> 7 x 5 + 1 x 5
(7 + 1) x 7 <> 7 x 7 + 1 x 7
(7 + 3) x 2 <> 7 x 2 + 3 x 2
(7 + 3) x 5 <> 7 x 5 + 3 x 5
(7 + 3) x 6 <> 7 x 6 + 3 x 6
(7 + 3) x 7 <> 7 x 7 + 3 x 7
(7 + 5) x 3 <> 7 x 3 + 5 x 3
(7 + 5) x 5 <> 7 x 5 + 5 x 5
(7 + 5) x 6 <> 7 x 6 + 5 x 6

(7 + 6) x 3 <> 7 x 3 + 6 x 3
(7 + 6) x 5 <> 7 x 5 + 6 x 5
(7 + 6) x 6 <> 7 x 6 + 6 x 6
Luego la operacion x no es distribuiva a derecha con respecto a +.
La operación x es asociativa

La operación x es conmutativa

El elemento neutro respecto a x es : 1

El elemento inverso de 1 respecto a x es 1
El elemento inverso de 3 respecto a x es 6
El elemento inverso de 5 respecto a x es 5
El elemento inverso de 6 respecto a x es 3

Anexo F: Análisis realizado en *Propiedades 3.1* para tablas de multiplicación (caso 4a)

Estudio algebraico de la operación

x	0	1	2	3	4	5	6	7
0	0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6	7
2	0	2	4	2	0	2	2	4
3	0	3	2	1	4	6	5	2
4	0	4	0	4	0	4	4	0
5	0	5	2	6	4	3	1	2
6	0	6	2	5	4	1	3	2
7	0	7	4	2	0	2	2	4

2 x (1 + 2) <> 2 x 1 + 2 x 2
2 x (1 + 5) <> 2 x 1 + 2 x 5
2 x (1 + 6) <> 2 x 1 + 2 x 6
2 x (1 + 7) <> 2 x 1 + 2 x 7
2 x (2 + 1) <> 2 x 2 + 2 x 1
2 x (2 + 3) <> 2 x 2 + 2 x 3
2 x (2 + 5) <> 2 x 2 + 2 x 5
2 x (2 + 6) <> 2 x 2 + 2 x 6
2 x (3 + 2) <> 2 x 3 + 2 x 2
2 x (3 + 5) <> 2 x 3 + 2 x 5
2 x (3 + 6) <> 2 x 3 + 2 x 6
2 x (3 + 7) <> 2 x 3 + 2 x 7
2 x (5 + 1) <> 2 x 5 + 2 x 1
2 x (5 + 2) <> 2 x 5 + 2 x 2
2 x (5 + 3) <> 2 x 5 + 2 x 3
2 x (5 + 7) <> 2 x 5 + 2 x 7
2 x (6 + 1) <> 2 x 6 + 2 x 1
2 x (6 + 2) <> 2 x 6 + 2 x 2
2 x (6 + 3) <> 2 x 6 + 2 x 3
2 x (6 + 7) <> 2 x 6 + 2 x 7
2 x (7 + 1) <> 2 x 7 + 2 x 1
2 x (7 + 3) <> 2 x 7 + 2 x 3
2 x (7 + 5) <> 2 x 7 + 2 x 5
2 x (7 + 6) <> 2 x 7 + 2 x 6
3 x (1 + 1) <> 3 x 1 + 3 x 1
3 x (1 + 7) <> 3 x 1 + 3 x 7
3 x (2 + 4) <> 3 x 2 + 3 x 4
3 x (2 + 7) <> 3 x 2 + 3 x 7
3 x (3 + 3) <> 3 x 3 + 3 x 3
3 x (3 + 7) <> 3 x 3 + 3 x 7
3 x (4 + 2) <> 3 x 4 + 3 x 2
3 x (4 + 7) <> 3 x 4 + 3 x 7
3 x (5 + 6) <> 3 x 5 + 3 x 6
3 x (5 + 7) <> 3 x 5 + 3 x 7
3 x (6 + 5) <> 3 x 6 + 3 x 5
3 x (6 + 7) <> 3 x 6 + 3 x 7
3 x (7 + 1) <> 3 x 7 + 3 x 1
3 x (7 + 2) <> 3 x 7 + 3 x 2
3 x (7 + 3) <> 3 x 7 + 3 x 3
3 x (7 + 4) <> 3 x 7 + 3 x 4
3 x (7 + 5) <> 3 x 7 + 3 x 5
3 x (7 + 6) <> 3 x 7 + 3 x 6
5 x (1 + 3) <> 5 x 1 + 5 x 3
5 x (1 + 5) <> 5 x 1 + 5 x 5
5 x (1 + 6) <> 5 x 1 + 5 x 6
5 x (1 + 7) <> 5 x 1 + 5 x 7
5 x (2 + 4) <> 5 x 2 + 5 x 4
5 x (2 + 7) <> 5 x 2 + 5 x 7
5 x (3 + 1) <> 5 x 3 + 5 x 1
5 x (3 + 5) <> 5 x 3 + 5 x 5
5 x (3 + 6) <> 5 x 3 + 5 x 6
5 x (3 + 7) <> 5 x 3 + 5 x 7
5 x (4 + 2) <> 5 x 4 + 5 x 2
5 x (4 + 7) <> 5 x 4 + 5 x 7
5 x (5 + 1) <> 5 x 5 + 5 x 1
5 x (5 + 3) <> 5 x 5 + 5 x 3
5 x (5 + 5) <> 5 x 5 + 5 x 5
5 x (5 + 7) <> 5 x 5 + 5 x 7
5 x (6 + 1) <> 5 x 6 + 5 x 1
5 x (6 + 3) <> 5 x 6 + 5 x 3
5 x (6 + 6) <> 5 x 6 + 5 x 6
5 x (6 + 7) <> 5 x 6 + 5 x 7
5 x (7 + 1) <> 5 x 7 + 5 x 1
5 x (7 + 2) <> 5 x 7 + 5 x 2
5 x (7 + 3) <> 5 x 7 + 5 x 3
5 x (7 + 4) <> 5 x 7 + 5 x 4
5 x (7 + 5) <> 5 x 7 + 5 x 5
5 x (7 + 6) <> 5 x 7 + 5 x 6
6 x (1 + 3) <> 6 x 1 + 6 x 3
6 x (1 + 5) <> 6 x 1 + 6 x 5
6 x (1 + 6) <> 6 x 1 + 6 x 6
6 x (1 + 7) <> 6 x 1 + 6 x 7
6 x (2 + 4) <> 6 x 2 + 6 x 4
6 x (2 + 7) <> 6 x 2 + 6 x 7
6 x (3 + 1) <> 6 x 3 + 6 x 1
6 x (3 + 5) <> 6 x 3 + 6 x 5
6 x (3 + 6) <> 6 x 3 + 6 x 6
6 x (3 + 7) <> 6 x 3 + 6 x 7
6 x (4 + 2) <> 6 x 4 + 6 x 2
6 x (4 + 7) <> 6 x 4 + 6 x 7
6 x (5 + 1) <> 6 x 5 + 6 x 1
6 x (5 + 3) <> 6 x 5 + 6 x 3
6 x (5 + 5) <> 6 x 5 + 6 x 5
6 x (5 + 7) <> 6 x 5 + 6 x 7
6 x (6 + 1) <> 6 x 6 + 6 x 1
6 x (6 + 3) <> 6 x 6 + 6 x 3
6 x (6 + 6) <> 6 x 6 + 6 x 6
6 x (6 + 7) <> 6 x 6 + 6 x 7
6 x (7 + 1) <> 6 x 7 + 6 x 1
6 x (7 + 2) <> 6 x 7 + 6 x 2
6 x (7 + 3) <> 6 x 7 + 6 x 3
6 x (7 + 4) <> 6 x 7 + 6 x 4
6 x (7 + 5) <> 6 x 7 + 6 x 5
6 x (7 + 6) <> 6 x 7 + 6 x 6
7 x (1 + 3) <> 7 x 1 + 7 x 3
7 x (1 + 4) <> 7 x 1 + 7 x 4
7 x (2 + 3) <> 7 x 2 + 7 x 3
7 x (2 + 6) <> 7 x 2 + 7 x 6
7 x (3 + 1) <> 7 x 3 + 7 x 1
7 x (3 + 2) <> 7 x 3 + 7 x 2
7 x (3 + 4) <> 7 x 3 + 7 x 4
7 x (3 + 5) <> 7 x 3 + 7 x 5
7 x (3 + 6) <> 7 x 3 + 7 x 6
7 x (3 + 7) <> 7 x 3 + 7 x 7
7 x (4 + 1) <> 7 x 4 + 7 x 1
7 x (4 + 3) <> 7 x 4 + 7 x 3
7 x (5 + 3) <> 7 x 5 + 7 x 3
7 x (5 + 7) <> 7 x 5 + 7 x 7
7 x (6 + 2) <> 7 x 6 + 7 x 2
7 x (6 + 3) <> 7 x 6 + 7 x 3
7 x (7 + 3) <> 7 x 7 + 7 x 3
7 x (7 + 5) <> 7 x 7 + 7 x 5

Luego la operacion x no es distribuiva a izquierda con respecto a +.

(1 + 1) x 3 <> 1 x 3 + 1 x 3
(1 + 2) x 2 <> 1 x 2 + 2 x 2
(1 + 3) x 5 <> 1 x 5 + 3 x 5
(1 + 3) x 6 <> 1 x 6 + 3 x 6
(1 + 3) x 7 <> 1 x 7 + 3 x 7
(1 + 4) x 7 <> 1 x 7 + 4 x 7
(1 + 5) x 2 <> 1 x 2 + 5 x 2
(1 + 5) x 5 <> 1 x 5 + 5 x 5
(1 + 5) x 6 <> 1 x 6 + 5 x 6
(1 + 6) x 2 <> 1 x 2 + 6 x 2
(1 + 6) x 5 <> 1 x 5 + 6 x 5
(1 + 6) x 6 <> 1 x 6 + 6 x 6
(1 + 7) x 2 <> 1 x 2 + 7 x 2
(1 + 7) x 3 <> 1 x 3 + 7 x 3
(1 + 7) x 5 <> 1 x 5 + 7 x 5
(1 + 7) x 6 <> 1 x 6 + 7 x 6
(2 + 1) x 2 <> 2 x 2 + 1 x 2
(2 + 3) x 2 <> 2 x 2 + 3 x 2
(2 + 3) x 7 <> 2 x 7 + 3 x 7
(2 + 4) x 3 <> 2 x 3 + 4 x 3
(2 + 4) x 5 <> 2 x 5 + 4 x 5
(2 + 4) x 6 <> 2 x 6 + 4 x 6
(2 + 5) x 2 <> 2 x 2 + 5 x 2
(2 + 6) x 2 <> 2 x 2 + 6 x 2
(2 + 6) x 7 <> 2 x 7 + 6 x 7
(2 + 7) x 3 <> 2 x 3 + 7 x 3
(2 + 7) x 5 <> 2 x 5 + 7 x 5
(2 + 7) x 6 <> 2 x 6 + 7 x 6
(3 + 1) x 5 <> 3 x 5 + 1 x 5
(3 + 1) x 6 <> 3 x 6 + 1 x 6
(3 + 1) x 7 <> 3 x 7 + 1 x 7
(3 + 2) x 2 <> 3 x 2 + 2 x 2
(3 + 2) x 7 <> 3 x 7 + 2 x 7
(3 + 3) x 3 <> 3 x 3 + 3 x 3
(3 + 4) x 7 <> 3 x 7 + 4 x 7
(3 + 5) x 2 <> 3 x 2 + 5 x 2
(3 + 5) x 5 <> 3 x 5 + 5 x 5
(3 + 5) x 6 <> 3 x 6 + 5 x 6
(3 + 5) x 7 <> 3 x 7 + 5 x 7
(3 + 6) x 2 <> 3 x 2 + 6 x 2
(3 + 6) x 5 <> 3 x 5 + 6 x 5
(3 + 6) x 6 <> 3 x 6 + 6 x 6
(3 + 6) x 7 <> 3 x 7 + 6 x 7
(3 + 7) x 2 <> 3 x 2 + 7 x 2
(3 + 7) x 3 <> 3 x 3 + 7 x 3
(3 + 7) x 5 <> 3 x 5 + 7 x 5
(3 + 7) x 6 <> 3 x 6 + 7 x 6
(3 + 7) x 7 <> 3 x 7 + 7 x 7
(4 + 1) x 7 <> 4 x 7 + 1 x 7
(4 + 2) x 3 <> 4 x 3 + 2 x 3
(4 + 2) x 5 <> 4 x 5 + 2 x 5
(4 + 2) x 6 <> 4 x 6 + 2 x 6
(4 + 3) x 7 <> 4 x 7 + 3 x 7
(4 + 7) x 3 <> 4 x 3 + 7 x 3
(4 + 7) x 5 <> 4 x 5 + 7 x 5
(4 + 7) x 6 <> 4 x 6 + 7 x 6
(5 + 1) x 2 <> 5 x 2 + 1 x 2
(5 + 1) x 5 <> 5 x 5 + 1 x 5
(5 + 1) x 6 <> 5 x 6 + 1 x 6
(5 + 2) x 2 <> 5 x 2 + 2 x 2
(5 + 3) x 2 <> 5 x 2 + 3 x 2
(5 + 3) x 5 <> 5 x 5 + 3 x 5
(5 + 3) x 6 <> 5 x 6 + 3 x 6
(5 + 3) x 7 <> 5 x 7 + 3 x 7
(5 + 5) x 5 <> 5 x 5 + 5 x 5
(5 + 5) x 6 <> 5 x 6 + 5 x 6
(5 + 6) x 3 <> 5 x 3 + 6 x 3
(5 + 7) x 2 <> 5 x 2 + 7 x 2
(5 + 7) x 3 <> 5 x 3 + 7 x 3
(5 + 7) x 5 <> 5 x 5 + 7 x 5
(5 + 7) x 6 <> 5 x 6 + 7 x 6
(5 + 7) x 7 <> 5 x 7 + 7 x 7
(6 + 1) x 2 <> 6 x 2 + 1 x 2
(6 + 1) x 5 <> 6 x 5 + 1 x 5
(6 + 1) x 6 <> 6 x 6 + 1 x 6
(6 + 2) x 2 <> 6 x 2 + 2 x 2
(6 + 2) x 7 <> 6 x 7 + 2 x 7
(6 + 3) x 2 <> 6 x 2 + 3 x 2
(6 + 3) x 5 <> 6 x 5 + 3 x 5
(6 + 3) x 6 <> 6 x 6 + 3 x 6
(6 + 3) x 7 <> 6 x 7 + 3 x 7
(6 + 5) x 3 <> 6 x 3 + 5 x 3
(6 + 6) x 5 <> 6 x 5 + 6 x 5
(6 + 6) x 6 <> 6 x 6 + 6 x 6
(6 + 7) x 2 <> 6 x 2 + 7 x 2
(6 + 7) x 3 <> 6 x 3 + 7 x 3
(6 + 7) x 5 <> 6 x 5 + 7 x 5
(6 + 7) x 6 <> 6 x 6 + 7 x 6
(7 + 1) x 2 <> 7 x 2 + 1 x 2
(7 + 1) x 3 <> 7 x 3 + 1 x 3
(7 + 1) x 5 <> 7 x 5 + 1 x 5
(7 + 1) x 6 <> 7 x 6 + 1 x 6
(7 + 2) x 3 <> 7 x 3 + 2 x 3
(7 + 2) x 5 <> 7 x 5 + 2 x 5
(7 + 2) x 6 <> 7 x 6 + 2 x 6
(7 + 3) x 2 <> 7 x 2 + 3 x 2
(7 + 3) x 3 <> 7 x 3 + 3 x 3
(7 + 3) x 5 <> 7 x 5 + 3 x 5
(7 + 3) x 6 <> 7 x 6 + 3 x 6
(7 + 3) x 7 <> 7 x 7 + 3 x 7
(7 + 4) x 3 <> 7 x 3 + 4 x 3
(7 + 4) x 5 <> 7 x 5 + 4 x 5
(7 + 4) x 6 <> 7 x 6 + 4 x 6
(7 + 5) x 2 <> 7 x 2 + 5 x 2
(7 + 5) x 3 <> 7 x 3 + 5 x 3
(7 + 5) x 5 <> 7 x 5 + 5 x 5
(7 + 5) x 6 <> 7 x 6 + 5 x 6
(7 + 5) x 7 <> 7 x 7 + 5 x 7
(7 + 6) x 2 <> 7 x 2 + 6 x 2
(7 + 6) x 3 <> 7 x 3 + 6 x 3
(7 + 6) x 5 <> 7 x 5 + 6 x 5
(7 + 6) x 6 <> 7 x 6 + 6 x 6

Luego la operacion x no es distribuiva a derecha con respecto a +.

(3 x 3) x 7 <> 3 x (3 x 7)
(5 x 6) x 7 <> 5 x (6 x 7)
(6 x 5) x 7 <> 6 x (5 x 7)
(7 x 3) x 3 <> 7 x (3 x 3)
(7 x 5) x 6 <> 7 x (5 x 6)
(7 x 6) x 5 <> 7 x (6 x 5)

La operación x es asociativa

La operación x es conmutativa

El elemento neutro respecto a x es : 1

El elemento inverso de 1 respecto a x es 1
El elemento inverso de 3 respecto a x es 3
El elemento inverso de 5 respecto a x es 6
El elemento inverso de 6 respecto a x es 5

Anexo G: Análisis realizado en *Propiedades 3.1* para tablas de multiplicación (caso 4b)

Estudio algebraico de la operación

x	0	1	2	3	4	5	6	7
0	0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6	7
2	0	2	4	7	0	2	7	4
3	0	3	7	1	4	6	5	2
4	0	4	0	4	0	4	4	0
5	0	5	2	6	4	3	1	7
6	0	6	7	5	4	1	3	2
7	0	7	4	2	0	7	2	4

2 x (1 + 3) <> 2 x 1 + 2 x 3
2 x (1 + 4) <> 2 x 1 + 2 x 4
2 x (1 + 5) <> 2 x 1 + 2 x 5
2 x (1 + 7) <> 2 x 1 + 2 x 7
2 x (2 + 5) <> 2 x 2 + 2 x 5
2 x (2 + 6) <> 2 x 2 + 2 x 6
2 x (3 + 1) <> 2 x 3 + 2 x 1
2 x (3 + 4) <> 2 x 3 + 2 x 4
2 x (3 + 6) <> 2 x 3 + 2 x 6
2 x (3 + 7) <> 2 x 3 + 2 x 7
2 x (4 + 1) <> 2 x 4 + 2 x 1
2 x (4 + 3) <> 2 x 4 + 2 x 3
2 x (4 + 5) <> 2 x 4 + 2 x 5
2 x (4 + 6) <> 2 x 4 + 2 x 6
2 x (5 + 1) <> 2 x 5 + 2 x 1
2 x (5 + 2) <> 2 x 5 + 2 x 2
2 x (5 + 4) <> 2 x 5 + 2 x 4
2 x (5 + 6) <> 2 x 5 + 2 x 6
2 x (6 + 2) <> 2 x 6 + 2 x 2
2 x (6 + 3) <> 2 x 6 + 2 x 3
2 x (6 + 4) <> 2 x 6 + 2 x 4
2 x (6 + 5) <> 2 x 6 + 2 x 5
2 x (7 + 1) <> 2 x 7 + 2 x 1
2 x (7 + 3) <> 2 x 7 + 2 x 3
3 x (1 + 1) <> 3 x 1 + 3 x 1
3 x (1 + 2) <> 3 x 1 + 3 x 2
3 x (1 + 3) <> 3 x 1 + 3 x 3
3 x (1 + 7) <> 3 x 1 + 3 x 7
3 x (2 + 1) <> 3 x 2 + 3 x 1
3 x (2 + 3) <> 3 x 2 + 3 x 3
3 x (2 + 5) <> 3 x 2 + 3 x 5
3 x (2 + 6) <> 3 x 2 + 3 x 6
3 x (3 + 1) <> 3 x 3 + 3 x 1
3 x (3 + 2) <> 3 x 3 + 3 x 2
3 x (3 + 3) <> 3 x 3 + 3 x 3
3 x (3 + 7) <> 3 x 3 + 3 x 7
3 x (5 + 2) <> 3 x 5 + 3 x 2
3 x (5 + 5) <> 3 x 5 + 3 x 5
3 x (5 + 6) <> 3 x 5 + 3 x 6
3 x (5 + 7) <> 3 x 5 + 3 x 7
3 x (6 + 2) <> 3 x 6 + 3 x 2
3 x (6 + 5) <> 3 x 6 + 3 x 5
3 x (6 + 6) <> 3 x 6 + 3 x 6
3 x (6 + 7) <> 3 x 6 + 3 x 7
3 x (7 + 1) <> 3 x 7 + 3 x 1
3 x (7 + 3) <> 3 x 7 + 3 x 3
3 x (7 + 5) <> 3 x 7 + 3 x 5
3 x (7 + 6) <> 3 x 7 + 3 x 6
5 x (1 + 1) <> 5 x 1 + 5 x 1
5 x (1 + 3) <> 5 x 1 + 5 x 3
5 x (1 + 5) <> 5 x 1 + 5 x 5
5 x (1 + 6) <> 5 x 1 + 5 x 6
5 x (3 + 1) <> 5 x 3 + 5 x 1
5 x (3 + 3) <> 5 x 3 + 5 x 3
5 x (3 + 5) <> 5 x 3 + 5 x 5
5 x (3 + 6) <> 5 x 3 + 5 x 6
5 x (5 + 1) <> 5 x 5 + 5 x 1
5 x (5 + 3) <> 5 x 5 + 5 x 3
5 x (5 + 5) <> 5 x 5 + 5 x 5
5 x (5 + 6) <> 5 x 5 + 5 x 6
5 x (6 + 1) <> 5 x 6 + 5 x 1
5 x (6 + 3) <> 5 x 6 + 5 x 3
5 x (6 + 5) <> 5 x 6 + 5 x 5
5 x (6 + 6) <> 5 x 6 + 5 x 6
6 x (1 + 2) <> 6 x 1 + 6 x 2
6 x (1 + 5) <> 6 x 1 + 6 x 5
6 x (1 + 6) <> 6 x 1 + 6 x 6
6 x (1 + 7) <> 6 x 1 + 6 x 7
6 x (2 + 1) <> 6 x 2 + 6 x 1
6 x (2 + 3) <> 6 x 2 + 6 x 3
6 x (2 + 5) <> 6 x 2 + 6 x 5
6 x (2 + 6) <> 6 x 2 + 6 x 6
6 x (3 + 2) <> 6 x 3 + 6 x 2
6 x (3 + 5) <> 6 x 3 + 6 x 5
6 x (3 + 6) <> 6 x 3 + 6 x 6
6 x (3 + 7) <> 6 x 3 + 6 x 7
6 x (5 + 1) <> 6 x 5 + 6 x 1
6 x (5 + 2) <> 6 x 5 + 6 x 2
6 x (5 + 3) <> 6 x 5 + 6 x 3
6 x (5 + 7) <> 6 x 5 + 6 x 7
6 x (6 + 1) <> 6 x 6 + 6 x 1
6 x (6 + 2) <> 6 x 6 + 6 x 2
6 x (6 + 3) <> 6 x 6 + 6 x 3
6 x (6 + 7) <> 6 x 6 + 6 x 7
6 x (7 + 1) <> 6 x 7 + 6 x 1
6 x (7 + 3) <> 6 x 7 + 6 x 3
6 x (7 + 5) <> 6 x 7 + 6 x 5
6 x (7 + 6) <> 6 x 7 + 6 x 6
7 x (1 + 3) <> 7 x 1 + 7 x 3
7 x (1 + 4) <> 7 x 1 + 7 x 4
7 x (1 + 5) <> 7 x 1 + 7 x 5
7 x (1 + 7) <> 7 x 1 + 7 x 7
7 x (2 + 5) <> 7 x 2 + 7 x 5
7 x (2 + 6) <> 7 x 2 + 7 x 6
7 x (3 + 1) <> 7 x 3 + 7 x 1
7 x (3 + 4) <> 7 x 3 + 7 x 4
7 x (3 + 6) <> 7 x 3 + 7 x 6
7 x (3 + 7) <> 7 x 3 + 7 x 7
7 x (4 + 1) <> 7 x 4 + 7 x 1
7 x (4 + 3) <> 7 x 4 + 7 x 3
7 x (4 + 5) <> 7 x 4 + 7 x 5
7 x (4 + 6) <> 7 x 4 + 7 x 6
7 x (5 + 1) <> 7 x 5 + 7 x 1
7 x (5 + 2) <> 7 x 5 + 7 x 2
7 x (5 + 4) <> 7 x 5 + 7 x 4
7 x (5 + 6) <> 7 x 5 + 7 x 6
7 x (6 + 2) <> 7 x 6 + 7 x 2
7 x (6 + 3) <> 7 x 6 + 7 x 3
7 x (6 + 4) <> 7 x 6 + 7 x 4
7 x (6 + 5) <> 7 x 6 + 7 x 5
7 x (7 + 1) <> 7 x 7 + 7 x 1

7 x (7 + 3) <> 7 x 7 + 7 x 3

Luego la operacion x no es distribuiva a izquierda con respecto a +.

(1 + 1) x 3 <> 1 x 3 + 1 x 3
(1 + 1) x 5 <> 1 x 5 + 1 x 5
(1 + 2) x 3 <> 1 x 3 + 2 x 3
(1 + 2) x 6 <> 1 x 6 + 2 x 6
(1 + 3) x 2 <> 1 x 2 + 3 x 2
(1 + 3) x 3 <> 1 x 3 + 3 x 3
(1 + 3) x 5 <> 1 x 5 + 3 x 5
(1 + 3) x 7 <> 1 x 7 + 3 x 7
(1 + 4) x 2 <> 1 x 2 + 4 x 2
(1 + 4) x 7 <> 1 x 7 + 4 x 7
(1 + 5) x 2 <> 1 x 2 + 5 x 2
(1 + 5) x 5 <> 1 x 5 + 5 x 5
(1 + 5) x 6 <> 1 x 6 + 5 x 6
(1 + 5) x 7 <> 1 x 7 + 5 x 7
(1 + 6) x 5 <> 1 x 5 + 6 x 5
(1 + 6) x 6 <> 1 x 6 + 6 x 6
(1 + 7) x 2 <> 1 x 2 + 7 x 2
(1 + 7) x 3 <> 1 x 3 + 7 x 3
(1 + 7) x 6 <> 1 x 6 + 7 x 6
(1 + 7) x 7 <> 1 x 7 + 7 x 7
(2 + 1) x 3 <> 2 x 3 + 1 x 3
(2 + 1) x 6 <> 2 x 6 + 1 x 6
(2 + 3) x 3 <> 2 x 3 + 3 x 3
(2 + 3) x 6 <> 2 x 6 + 3 x 6
(2 + 5) x 2 <> 2 x 2 + 5 x 2
(2 + 5) x 3 <> 2 x 3 + 5 x 3
(2 + 5) x 6 <> 2 x 6 + 5 x 6
(2 + 5) x 7 <> 2 x 7 + 5 x 7
(2 + 6) x 2 <> 2 x 2 + 6 x 2
(2 + 6) x 3 <> 2 x 3 + 6 x 3
(2 + 6) x 6 <> 2 x 6 + 6 x 6
(2 + 6) x 7 <> 2 x 7 + 6 x 7
(3 + 1) x 2 <> 3 x 2 + 1 x 2
(3 + 1) x 3 <> 3 x 3 + 1 x 3
(3 + 1) x 5 <> 3 x 5 + 1 x 5
(3 + 1) x 7 <> 3 x 7 + 1 x 7
(3 + 2) x 3 <> 3 x 3 + 2 x 3
(3 + 2) x 6 <> 3 x 6 + 2 x 6
(3 + 3) x 3 <> 3 x 3 + 3 x 3
(3 + 3) x 5 <> 3 x 5 + 3 x 5
(3 + 4) x 2 <> 3 x 2 + 4 x 2
(3 + 4) x 7 <> 3 x 7 + 4 x 7
(3 + 5) x 5 <> 3 x 5 + 5 x 5
(3 + 5) x 6 <> 3 x 6 + 5 x 6
(3 + 6) x 2 <> 3 x 2 + 6 x 2
(3 + 6) x 5 <> 3 x 5 + 6 x 5
(3 + 6) x 6 <> 3 x 6 + 6 x 6
(3 + 6) x 7 <> 3 x 7 + 6 x 7
(3 + 7) x 2 <> 3 x 2 + 7 x 2
(3 + 7) x 3 <> 3 x 3 + 7 x 3
(3 + 7) x 6 <> 3 x 6 + 7 x 6
(3 + 7) x 7 <> 3 x 7 + 7 x 7
(4 + 1) x 2 <> 4 x 2 + 1 x 2
(4 + 1) x 7 <> 4 x 7 + 1 x 7
(4 + 3) x 2 <> 4 x 2 + 3 x 2
(4 + 3) x 7 <> 4 x 7 + 3 x 7
(4 + 5) x 2 <> 4 x 2 + 5 x 2
(4 + 5) x 7 <> 4 x 7 + 5 x 7
(4 + 6) x 2 <> 4 x 2 + 6 x 2
(4 + 6) x 7 <> 4 x 7 + 6 x 7
(5 + 1) x 2 <> 5 x 2 + 1 x 2
(5 + 1) x 5 <> 5 x 5 + 1 x 5
(5 + 1) x 6 <> 5 x 6 + 1 x 6
(5 + 1) x 7 <> 5 x 7 + 1 x 7
(5 + 2) x 2 <> 5 x 2 + 2 x 2
(5 + 2) x 3 <> 5 x 3 + 2 x 3
(5 + 2) x 6 <> 5 x 6 + 2 x 6
(5 + 2) x 7 <> 5 x 7 + 2 x 7
(5 + 3) x 5 <> 5 x 5 + 3 x 5
(5 + 3) x 6 <> 5 x 6 + 3 x 6
(5 + 4) x 2 <> 5 x 2 + 4 x 2
(5 + 4) x 7 <> 5 x 7 + 4 x 7
(5 + 5) x 3 <> 5 x 3 + 5 x 3
(5 + 5) x 5 <> 5 x 5 + 5 x 5
(5 + 6) x 2 <> 5 x 2 + 6 x 2
(5 + 6) x 3 <> 5 x 3 + 6 x 3
(5 + 6) x 5 <> 5 x 5 + 6 x 5
(5 + 6) x 7 <> 5 x 7 + 6 x 7
(5 + 7) x 3 <> 5 x 3 + 7 x 3
(5 + 7) x 6 <> 5 x 6 + 7 x 6
(6 + 1) x 5 <> 6 x 5 + 1 x 5
(6 + 1) x 6 <> 6 x 6 + 1 x 6
(6 + 2) x 2 <> 6 x 2 + 2 x 2
(6 + 2) x 3 <> 6 x 3 + 2 x 3
(6 + 2) x 6 <> 6 x 6 + 2 x 6
(6 + 2) x 7 <> 6 x 7 + 2 x 7
(6 + 3) x 2 <> 6 x 2 + 3 x 2
(6 + 3) x 5 <> 6 x 5 + 3 x 5
(6 + 3) x 6 <> 6 x 6 + 3 x 6
(6 + 3) x 7 <> 6 x 7 + 3 x 7
(6 + 4) x 2 <> 6 x 2 + 4 x 2
(6 + 4) x 7 <> 6 x 7 + 4 x 7
(6 + 5) x 2 <> 6 x 2 + 5 x 2
(6 + 5) x 3 <> 6 x 3 + 5 x 3
(6 + 5) x 5 <> 6 x 5 + 5 x 5
(6 + 5) x 7 <> 6 x 7 + 5 x 7
(6 + 6) x 3 <> 6 x 3 + 6 x 3
(6 + 6) x 5 <> 6 x 5 + 6 x 5
(6 + 7) x 3 <> 6 x 3 + 7 x 3
(6 + 7) x 6 <> 6 x 6 + 7 x 6
(7 + 1) x 2 <> 7 x 2 + 1 x 2
(7 + 1) x 3 <> 7 x 3 + 1 x 3
(7 + 1) x 6 <> 7 x 6 + 1 x 6
(7 + 1) x 7 <> 7 x 7 + 1 x 7
(7 + 3) x 2 <> 7 x 2 + 3 x 2
(7 + 3) x 3 <> 7 x 3 + 3 x 3
(7 + 3) x 6 <> 7 x 6 + 3 x 6
(7 + 3) x 7 <> 7 x 7 + 3 x 7
(7 + 5) x 3 <> 7 x 3 + 5 x 3
(7 + 5) x 6 <> 7 x 6 + 5 x 6
(7 + 6) x 3 <> 7 x 3 + 6 x 3
(7 + 6) x 6 <> 7 x 6 + 6 x 6

Luego la operacion x no es distribuiva a derecha con respecto a +.

(2 x 5) x 5 <> 2 x (5 x 5)
(2 x 5) x 6 <> 2 x (5 x 6)
(2 x 6) x 5 <> 2 x (6 x 5)
(2 x 6) x 6 <> 2 x (6 x 6)
(5 x 5) x 2 <> 5 x (5 x 2)
(5 x 5) x 7 <> 5 x (5 x 7)
(5 x 6) x 2 <> 5 x (6 x 2)
(5 x 6) x 7 <> 5 x (6 x 7)
(6 x 5) x 2 <> 6 x (5 x 2)
(6 x 5) x 7 <> 6 x (5 x 7)
(6 x 6) x 2 <> 6 x (6 x 2)
(6 x 6) x 7 <> 6 x (6 x 7)
(7 x 5) x 5 <> 7 x (5 x 5)
(7 x 5) x 6 <> 7 x (5 x 6)
(7 x 6) x 5 <> 7 x (6 x 5)
(7 x 6) x 6 <> 7 x (6 x 6)

La operación x es asociativa

La operación x es conmutativa
El elemento neutro respecto a x es : 1
El elemento inverso de 1 respecto a x es 1
El elemento inverso de 3 respecto a x es 3
El elemento inverso de 5 respecto a x es 6
El elemento inverso de 6 respecto a x es 5

Anexo H: Análisis realizado en *Propiedades 3.1* para tablas de multiplicación (Caso 2) Tabla distributiva

Estudio algebraico de la operación

x	0	1	2	3	4	5	6	7
0	0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6	7
2	0	2	4	2	0	7	7	4
3	0	3	2	1	4	6	5	7
4	0	4	0	4	0	4	4	0
5	0	5	7	6	4	1	3	2
6	0	6	7	5	4	3	1	2
7	0	7	4	7	0	2	2	4

La operación x es distributiva a izquierda con respecto a la operación +

La operación x es distributiva a derecha con respecto a la operación +

La operación x es asociativa

La operación x es conmutativa

El elemento neutro respecto a x es : 1

El elemento inverso de 1 respecto a x es 1
El elemento inverso de 3 respecto a x es 3
El elemento inverso de 5 respecto a x es 5
El elemento inverso de 6 respecto a x es 6