Un estudio de la relación de divisibilidad en subconjuntos de $\mathbb{Z}$

Jhon Alexander Gómez Aponte

Universidad Pedagógica Nacional
Facultad de Ciencia y Tecnología
Departamento de Matemáticas
Bogotá, Colombia
2016

Un estudio de la relación de divisibilidad en subconjuntos de $\mathbb{Z}$

Jhon Alexander Gómez Aponte

Tesis o trabajo de grado presentada(o) como requisito parcial para optar al título de:
Licenciado en Matemáticas

Asesor:
Juan Carlos Ávila Mahecha

Trabajo de grado asociado al grupo de investigación de Álgebra
de la Universidad Pedagógica Nacional

Universidad Pedagógica Nacional
Facultad de Ciencia y Tecnología
Departamento de Matemáticas
Bogotá, Colombia
2016

Agradecimientos

A mi familia por su apoyo incondicional.
Sin ellos no estaría donde estoy.

Al grupo de Álgebra y en particular al profesor
Yeison Sánchez por su brindarme su asesoría
con tanta dedicación.

UNIVERSIDAD PEDAGÓGICA NACIONAL	FORMATO
	RESUMEN ANALÍTICO EN EDUCACIÓN - RAE
Código: FOR020GIB	Versión: 01
Fecha de Aprobación: 10-10-2012	Página 1 de 3

1. Información General	
Tipo de documento	Trabajo de grado
Acceso al documento	Universidad Pedagógica Nacional. Biblioteca Central
Título del documento	Un estudio de la relación de divisibilidad en subconjuntos de Z
Autor(es)	Gómez Aponte, Jhon Alexander
Director	Ávila Mahecha, Juan Carlos
Publicación	Bogotá, Universidad Pedagógica Nacional, 2016, 65 p.
Unidad Patrocinante	Universidad Pedagógica Nacional
Palabras Claves	ANALIZAR, DIVISIBILIDAD, DESCOMPOSICIÓN, NÚMERO PRIMO, NÚMERO ENTERO

2. Descripción

Este trabajo de grado se propone con la intención de mostrar algunas generalidades relacionadas con el proceso matemático de analizar en una estructura algebraica, entendiendo este como el acto de descomponer los elementos de ella en términos de otros que son especiales: los números primos. Teniendo en cuenta esto, en el trabajo se presentan algunos resultados logrados buscando estudiar dicho proceso en algunas subestructuras de los números enteros tales como sus ideales y los subconjuntos de los números de la forma $ak+1$ lo cual llevó a, entre otras cosas, evidenciar que el hecho de caracterizar dicha descomposición dio lugar a algunos problemas de conteo que no fueron solucionados en el trabajo y que quedaron abiertos dando la posibilidad para la creación de nuevos trabajos de grado. Por otra parte, en el trabajo de grado también se propone un conjunto de actividades que se busca que sirvan para lograr el desarrollo del proceso de analizar en los estudiantes que cursen el espacio académico de Teoría de Números de la Licenciatura en Matemáticas de la Universidad Pedagógica Nacional.

3. Fuentes

- ✓ Ivorra, C. (s.f.). Álgebra. Valencia.
- ✓ Ivorra, C. (s.f.). Teoría de números. Valencia.
- ✓ Jiménez, R., Gordillo, E., & Rubiano, G. (2004). Teoría de números (para principiantes). Bogotá: Universidad Nacional de Colombia.
- ✓ Luque, C., Páez, J., & Mora, L. (2002). Actividades matemáticas para el desarrollo de procesos lógicos. Bogotá: Ediciones Antropos.
- ✓ Luque, C., Sánchez, Y., & Ángel, J. L. (2014). El proceso matemático de analizar en la Teoría de Números: Una aproximación desde la relación de divisibilidad. XII Coloquio regional de Matemáticas y II Simposio de Estadística. San Juan de Pasto: Universidad de Nariño.
- ✓ Ash, R. (2007). Basic Abstract Algebra For Graduate Students and Advanced Undergraduates

4. Contenidos

En el presente trabajo de grado se desarrollaron los siguientes contenidos:

1. El proceso matemático de analizar: En este apartado se hace un acercamiento al proceso matemático de analizar, particularizando en una estructura algebraica, mostrando los ejemplos usuales donde se desarrolla este proceso.
2. Los ideales de los números enteros: Además de lo anterior, se muestra un primer ejemplo donde se logran algunos resultados teóricos en el marco de la búsqueda del desarrollo del proceso matemático de analizar en una estructura algebraica: los ideales de los números enteros.
3. Los conjuntos A_a: También se muestra otro ejemplo de estructura algebraica donde, de igual forma al caso anterior, se lograron algunos resultados teóricos buscando el desarrollo del proceso matemático de analizar: los números de la forma $ak+1$
4. Actividades propuestas: Con base en la exploración realizada, en el trabajo de grado se presenta un conjunto de actividades que busca potenciar el desarrollo del proceso matemático de analizar en una estructura.

5. Metodología

No aplica

6. Conclusiones

Del desarrollo del trabajo de grado se obtuvieron las siguientes conclusiones:

- ✓ Teniendo en cuenta el estudio desarrollado en los ideales de los números enteros se puede concluir que, en primera medida, allí se encuentra una idea pura de elemento especial para la descomposición (elemento irreducible) en la medida que hay números que son imposibles de descomponer en la medida que no tienen divisores. Por otra parte, también se evidenció que no es posible hablar de un teorema análogo al teorema fundamental de la aritmética en esta estructura dado que se tiene la existencia de la descomposición en factores primos, pero no la unicidad de la misma.
- ✓ En lo que tiene que ver con los números de la forma $ak+1$ se definió la relación de descomposición haciendo uso de la multiplicación de los números enteros y a partir de ella se concluyó que se tiene que la existencia de la descomposición en factores primos, pero no se tiene la unicidad de la misma imposibilitando, nuevamente, la formulación de un teorema fundamental de la aritmética en este conjunto.
- ✓ Con base en el estudio desarrollado se puede concluir que la idea de número primo está supeditada, estrechamente, a la búsqueda de la existencia de la descomposición en la medida que, en los casos explorados se dieron definiciones distintas de número primo en aras de garantizar la existencia de la descomposición en términos de elementos que resultan ser, además, irreducibles en la medida que no se pueden escribir como producto de otros elementos del conjunto salvo algunos casos triviales.

Elaborado por:	Jhon Alexander Gómez
Revisado por:	Juan Carlos Ávila Mahecha

Fecha de elaboración del Resumen:	02	05	2016

Contenido

1. Introducción

En el presente trabajo de grado se muestran algunos resultados que tuvieron su origen en el marco de la monitoría de investigación desarrollada por el autor con el grupo de Álgebra de la Universidad Pedagógica Nacional en el proyecto titulado "Actividades matemáticas para el desarrollo de procesos lógicos: El proceso matemático de analizar en el espacio académico Teoría de Números de la Licenciatura en Matemáticas de la UPN-Experimentación y evaluación". Teniendo en cuenta esto, el trabajo aqui mostrado se encuentra fundamentado en la puesta en marcha del proceso matemático de analizar en una estructura, entendiendo este, básicamente, como descomponer un elemento de una estructura algebraica en términos de otros distinguidos o especiales, haciendo uso de una operación, como por ejemplo se hace usualmente en el conjunto de los números naturales y los números enteros cuando se estudia la descomposiciones en factores primos, sirviéndose de la multiplicación y de la definición de una relación de divisibilidad.

Teniendo en cuenta lo anterior, en el presente trabajo de grado se muestran algunos resultados relacionados con la busqueda de llevar a cabo el proceso de descomposición anteriormente mencionado, en algunas subestructuras de los números enteros que cuentan con una operación multiplicación bien definida. Para efectos de desarrollar esto, inicialmente se muestran algunos aspectos generales del proceso matemático de analizar en una estructura como fundamento teórico para los resultados posteriores; luego se presentan algunos resultados logrados alrededor del proceso de analizar en los ideales de los números enteros, particularmente en lo que tiene que ver con las propiedades que cumple la relación de divisibilidad definida en estos conjuntos, el Máximo Común Divisor, una noción de número primo que permite realizar la descomposición, y finalmente se presenta un problema abierto relacionado con el conteo de la cantidad de descomposiciones que tiene un elemento de estos conjuntos.

Adicionalmente, se muestra un desarrollo similar al logrado en los ideales de los números enteros, pero en un subconjunto de los números enteros donde sólo la multiplicación es una operación bien definida, dejando también un problema abierto de conteo para la cantidad de descomposiciones en factores primos de elementos de este conjunto. Finalmente, se propone un conjunto de actividades que buscan potenciar el desarrollo del proceso matemático de analizar en una estructura a través de la exploración guiada hacia los resultados que aquí se presentan.

2. Objetivos

2.1. Objetivo general

Desarrollar y sintetizar un estudio sobre la relación de divisibilidad, la descomposición y otros aspectos tratados usualmente en la Teoría de Números en subestructuras del conjunto de los números enteros tales como sus ideales y subconjuntos donde la multiplicación es una operación bien definida.

2.2. Objetivos específicos

1. Realizar un estudio de aspectos tales como la divisibilidad, Máximo Común Divisor y descomposición en factores primos en los ideales de los números enteros, a partir del estudio de algunos casos particulares y su posterior generalización.

2. Hacer un estudio de la relación de divisibilidad, el Máximo Común Divisor y la descomposición en factores primos en el conjunto $A_a = \{x : x = ak + 1, a, k \in \mathbb{Z}\}$ a partir de la exploración de algunos casos particulares, especialmente el del conjunto A_5 y A_7.

3. Diseñar un conjunto de actividades enfocadas hacia el descubrimiento de los resultados logrados en el estudio de la relación de divisibilidad y los demás conceptos mencionados anteriormente en las estructuras estudiadas, buscando, a partir de ellas, potenciar el desarrollo del proceso matemático de analizar en una estructura, en el espacio académico de Teoría de Números de la Universidad Pedagógica Nacional.

3. Marco teórico

Teniendo en cuenta que la motivación para desarrollar este trabajo de grado está centrada en el estudio de la factorización en algunas estructuras algaebraicas, es necesario resaltar en primera medida que esta es una ejemplificación del proceso matemático de analizar. Desde esta perspectiva, en este capítulo se presenta algunas consideraciones teóricas relacionadas con este proceso, así como algunos constructos matemáticos que se desprenden del desarrollo de este, y que además sirven como base para la exploración matemática que se pretende mostrar en este texto.
Adicionalmente, por la naturaleza del trabajo matemático que en esta monografía se muestra, se hace necesario hacer uso de algunos conceptos matemáticos relacionados con la teoría de números tales como el concepto de número primo, el teorema fundamental de la aritmética, etc., por tal razón, en este capítulo también se busca hacer un acercamiento a estos en aras de tener elementos teóricos que puedan ser utilizados en la exploración que se mostrará posteriormente.

3.1. El proceso matemático de analizar en una estructura

Debido a la naturaleza de la exploración que se pretende mostrar en el presente documento, se hace necesario hablar, como ya se dijo anteriormente, del proceso matemático de analizar como forma de acercamiento a la actividad matemática, que es lo que se mostrará a continuación:

3.1.1. El proceso matemático de analizar

En primera medida, el proceso de analizar es entendido como el hecho de desintegrar o *descomponer* un todo en sus partes para estudiar cada uno de sus elementos, así como las relaciones entre sí y con el todo (Ruiz, 2006), lo cual es transversal en el estudio de cualquier ciencia o teoría, y en especial en matemáticas (Ángel, Luque, y Sánchez, 2014).
Desde esta perspectiva, en el contexto netamente matemático se busca, entre otras cosas, estudiar conjuntos específicos así como las relaciones que se puede establecer entre sus elementos, es decir, *estructuras matemáticas*, (Sánchez, Ángel y Luque, 2014) por ejemplo estructuras algebraicas o topológicas.
En concordancia con lo anterior, un camino para cumplir dicho objetivo es hacer uso del proceso de analizar para hacer el estudio de dichas estructuras, es decir, seleccionar un

todo y descomponerlo en partes constitutivas que den información detallada acerca de la estructura. Para el caso de las estructuras algebraicas en primera medida es necesario decir que, a la hora de hablar de estas, el interés se centra en las operaciones binarias internas que estén definidas en un conjunto, así como las propiedades que estas cumplen (Sánchez, Ángel y Luque, 2014), dado que estas son las relaciones que se establecen entre los elementos del conjunto.

Teniendo en cuenta lo anterior, para hacer un estudio de una estructura algebraica a partir del proceso de analizar hay dos opciones que dependen de lo que se pretenda descomponer, como se muestra a continuación:

3.1.2. Análisis de una estructura algebraica

En concordancia con lo anterior, una primera forma de hacer uso del proceso de analizar para estudiar una estructura algebraica es ver como un todo la estructura misma y descomponerla en partes constitutivas que permitan extraer información, como se hace por ejemplo cuando se realiza una partición de un conjunto a través de una relación de equivalencia (clases de equivalencia disyuntas), o cuando se obtienen dos o mas subestructuras de una estructura algebraica cuya suma directa o producto directo da como resultado la estructura en cuestión, estos son ejemplos de como se descompone una estructura algebraica buscando estudiar sus propiedades a partir de las partes obtenidas.

3.1.3. Análisis en una estructura algebraica

A diferencia del caso anterior, en este caso el todo escogido para llevar a cabo el proceso de analizar son los elementos de la estructura, es decir, lo que se busca es descomponer un elemento de la estructura en términos de otros de la misma, por ejemplo, en un espacio vectorial, un elemento cualquiera se puede *descomponer* como combinación lineal de otros vectores si estos forman un conjunto generador (Takahashi, 1993).

Como se puede ver, en el ejemplo anterior hay dos aspectos importantes que resaltar; primero, la descomposición se logra haciendo uso de la operación que tiene la estructura algebraica, y segundo, los elementos que la componen son *especiales* dentro de la estructura, no todos los vectores forman conjuntos generadores. Por otra parte, otro ejemplo que se puede encontrar para evidenciar este proceso es el de la factorización o la descomposición dentro de la teoría algebraica de números, y allí también se encuentran dos conceptos problemáticos que tienen relación directa con los aspectos mencionados anteriormente: número primo y divisibilidad (Ángel, Luque, y Sánchez, 2014).

Por una parte, la noción de número primo hace referencia a algunos elementos especiales de la estructura algebraica que permiten descomponer todos los demás de la misma y, dentro de la teoría algebraica de números, son aquellos que cumplen con lo siguiente (Ash, 2000):

Definición 3.1 (Definición formal de número primo)**.** *Dada la estructura algebraica* $(A, \cdot)$ *y* $p, a, b \in A$ *se dice que* p *es primo si se cumple la siguiente implicación:*

$$p|ab \rightarrow p|a \vee p|b \ \forall a, b \in A$$

Dado que, primero, estos permiten descomponer a los demas elementos en términos de ellos y segundo bajo esta definición se tiene otro aspecto importante, la unicidad de la descomposición cuando la estructura algebraica es un dominio euclideo, es decir, un dominio de integridad donde se tiene el algoritmo de división (Ash, 2000).

3.1.4. Relación de descomposición

Por otra parte, el concepto de divisibilidad surge como una manera de lograr una descomposición haciendo uso de la operación de la estructura algebraica dado que si $(A, *)$ es una de ellas y $c \in A$ entonces este se podrá descomponer si existen, por lo menos, $a, b \in A$ tal que $a * b = c$, lo cual permite definir una relación en A de la siguiente forma (Sánchez, Ángel y Luque, 2014):

aR_dc si y sólo si la ecuación $a * x = c$ tiene al menos una solución.

O de la siguiente forma:

aR_ic si y sólo si la ecuación $x * a = c$ tiene al menos una solución.

Y si se supone que la operación $*$ es conmutativa, la relación se puede reducir de la siguiente forma:

Definición 3.2 (Relación de descomposición)**.** *Si* $(A, *)$ *es una estructura algebraica y* $a, c \in A$*, se dice que* aRc *si y sólo si la ecuación* $a * x = c$ *tiene al menos una solución.*

Imponiendo algunas propiedades a la operación se tiene lo siguiente (Ángel, Luque, y Sánchez, 2014):

Teorema 3.1. *Si* $(A, *)$ *es un monoide conmutativo, cancelativo y con elemento idéntico, y además este último es el único que tiene inverso, entonces* R *es una relación de orden.*

Prueba.

- R es reflexiva dado que elemento idéntico de la estructura es solución para la ecuación $a * x = a$.
- R es antisimétrica dado que si aRb y bRa entonces existen $x, y \in A$ tal que $a * x = b$ y $b * y = a$, sustituyendo tenemos que $(a * x) * y = a$, y como $*$ es asociativa entonces $a * (x * y) = a$, luego $x * y = e$ donde e es el elemento idéntico de $*$, y como e es el único elemento que tiene inverso, entonces $x = e$ y $y = e$, de donde se tiene que $a = b$.

- R es transitiva ya que si aRb y bRc entonces existen $x, y \in A$ tal que $a * x = b$ y $b * y = c$, sustituyendo tenemos que $(a * x) * y = c$, y como $*$ es asociativa entonces $a * (x * y) = c$ de donde se tiene que $x * y$ es solución de la ecuación $a * z = c$, por lo tanto aRb.

□

Como se puede ver, la relación de descomposición definida para estructuras algebraicas permite, además de buscar una descomposición para los elementos del conjunto, establecer un orden de los mismos, parecido a lo que ocurre con algunas relaciones similares definidas en el siguiente ejemplo:

El conjunto de los números naturales

Desde el punto de vista algebraico, el conjunto de los números naturales cuenta con dos operaciones definidas, suma y multiplicación, en cuanto a la suma, este conjunto cuenta con la estructura de monoide conmutativo con unidad, lo cual permite definir una relación de descomposición de la siguiente forma:

Definición 3.3. *Sean $a, c \in \mathbb{N}$, se dice que aR_+c si y sólo si la ecuación $a + x = c$ tiene al menos una solución.*

La cual, reescrita de otra forma, coincide con la relación de orden usual definida en los números naturales (Luque, Mora y Páez, 2002):

Definición 3.4 (Orden usual en $\mathbb{N}$)**.** *Sean $a, c \in \mathbb{N}$, se dice que $a \leq c$ si y sólo si existe $x \in \mathbb{N}$ tal que $a + x = c$.*

Y el hecho de buscar una descomposición de los elementos del conjunto a partir de esta relación da lugar a la teoría de particiones numéricas (Andrews, 1976).
Por otra parte, para la operación multiplicación que también forma una estructura de monoide conmutativo con identidad, se puede definir la relación de descomposición de la siguiente forma:

Definición 3.5. *Sean $a, c \in \mathbb{N}$, se dice que $aR_\times c$ si y sólo si la ecuación $a \times x = c$ tiene al menos una solución.*

Que, por el teorema 4.1, es una relación de orden, y que además coincide, haciendo un ligero cambio, con la relación conocida como divisibilidad

Definición 3.6 (Divisibilidad en $\mathbb{N}$)**.** *Sean $c, d \in \mathbb{N}$, diremos que $c|d$ si y solo si existe $e \in \mathbb{N}$ tal que $ce = d$.*

A partir de la cual es posible identificar elementos especiales para la descomposición: los números primos, que surgen a partir de la clasificación dada por el hecho de que la relación de descomposición para este caso es un orden, como se muestra a continuación (Sánchez, Ángel y Luque, 2014):

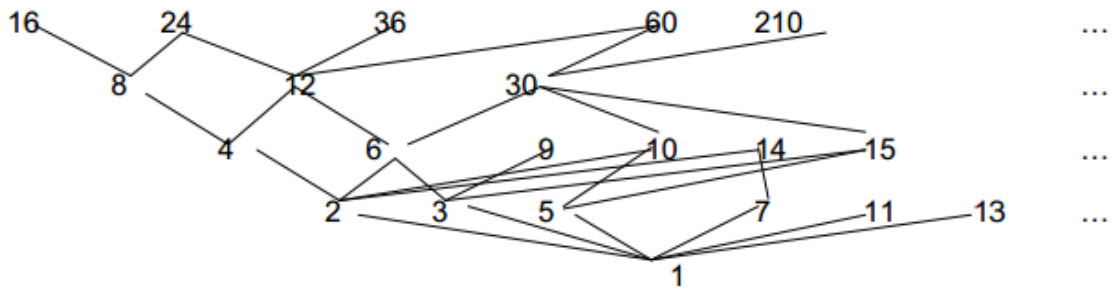

Figura 3-1.: Diagrama de Hasse para la relación de divisibilidad en $\mathbb{N}$

De aquí se puede concluir que los números primos son aquellos que se encuentran en la segunda fila del diagrama, y los demás todos se relacionan con algunos de ellos, por eso tiene sentido pensar que estos son los elementos base para la descomposición, es decir, los números primos que se formalizan, para este caso, de la siguiente forma:

Definición 3.7 (Número primo en $\mathbb{N}$)**.** *Dado $a \in \mathbb{N}$, se dice que a es primo si y sólo si tiene exactamente dos divisores.*

A partir de la cual se puede deducir uno de los resultados más importantes de la teoría de números:

Teorema 3.2 (Teorema fundamental de la aritmética)**.** *Cualquier número compuesto se puede descomponer en factores primos de forma única salvo el orden.*

Y de manera análoga, es posible hacer estudios similares en otras estructuras algebraicas, buscando el cumplimiento del teorema fundamental de la aritmética, así como se suele realizar, por ejemplo en el conjunto de los números enteros, donde se desarrolla un camino similar al mostrado para el conjunto de los números naturales, pero teniendo en cuenta que la relación de descomposición (divisibilidad) no es un orden dado que pierde la propiedad antisimétrica; incluso se puede hablar del estudio generalizado de la relación de divisibilidad y de la descomposición en factores primos para cualquier estructura algebraica que cuente con una operación bien definida o, como se hace desde la teoría algebraica de números, para un conjunto que cuente con la estructura de anillo.

4. Los ideales de los números enteros

En la busqueda de ejemplos en los cuales se pueda estudiar el desarrollo del proceso matemático de analizar, un primer camino puede ser realizar exploraciones alrededor de subestructuras de los números enteros, y recordando que estos cuentan con la estructura de anillo, se puede pensar en desarrollar este trabajo en sus ideales[1] es decir, en la siguiente familia de conjuntos:

$$k\mathbb{Z} = \{x : x = kn, n \in \mathbb{Z}\}$$

Para iniciar este estudio, se propone el estudio del siguiente caso para luego generalizar los resultados:

$$2\mathbb{Z} = \{x : x = 2k, k \in \mathbb{Z}\}$$

Y algunos de sus elementos son:

$$2\mathbb{Z} = \{\ldots, -8, -6, -4, -2, 0, 2, 4, 6, 8, \ldots\}$$

En primera medida es necesario decir que este conjunto cuenta con la particularidad de que no tiene elemento idéntico para la multiplicación, es decir $1 \notin 2\mathbb{Z}$, sin embargo sí cumple el resto de propiedades usuales, como por ejemplo la cancelativa, que se hereda para ambas operaciones por el hecho de ser subanillo.

4.1. Relación de divisibilidad y Máximo Común Divisor

Teniendo en cuenta que en el conjunto en mención se tiene que la multiplicación es cerrada, es posible definir la siguiente relación:

Definición 4.1 (Divisibilidad en $2\mathbb{Z}$)**.** *Sean $c, d \in 2\mathbb{Z}$, diremos que $c|_{2\mathbb{Z}}d$ si y solo si existe $e \in 2\mathbb{Z}$ tal que $ce = d$.*

[1] Es necesario recordar que un ideal es un subconjunto I de un anillo R en el cual se cumplen las siguientes condiciones:

1. Si $a, b \in I$ entonces $a + b \in I$
2. Si $a \in I$ entonces $-a \in I$
3. Si $a \in I$ y $r \in R$ entonces $ra, ar \in I$

Que es análoga a la definición que se tiene para la misma relación en el conjunto de los números naturales y enteros, sin embargo, esta no resulta ser de orden dado que, como ya se dijo $1 \notin 2\mathbb{Z}$, y esto hace que $a \nmid_{2\mathbb{Z}} a$, por lo tanto esta no es reflexiva, pero sí cumple lo siguiente:

Teorema 4.1. *La relación de divisibilidad definida en* $2\mathbb{Z}$ *es asimétrica y transitiva.*

Prueba. Asimétrica: Partamos de que $a|_{2\mathbb{Z}}b$, entonces existe $c \in 2\mathbb{Z}$ tal que $ac = b$, y supongamos que $b|_{2\mathbb{Z}}a$ entonces existe $d \in 2\mathbb{Z}$ tal que $bd = a$ entonces se tiene que $(bd)c = b$ de ahí que $dc = 1$ pero como $1 \notin 2\mathbb{Z}$ se llega a una contradicción, por lo tanto $b \nmid_{2\mathbb{Z}} a$.
Transitiva: Como la estructura en cuestión es un ideal del anillo de los números enteros, la operación multiplicación es asociativa, por lo tanto por el teorema 3.1 se tiene que la relación es transitiva. □

Teniendo en cuenta lo anterior se puede decir que la relación de divisibilidad en $2\mathbb{Z}$ es un orden estricto, de ahí que sea posible construir su respectivo diagrama de Hasse:

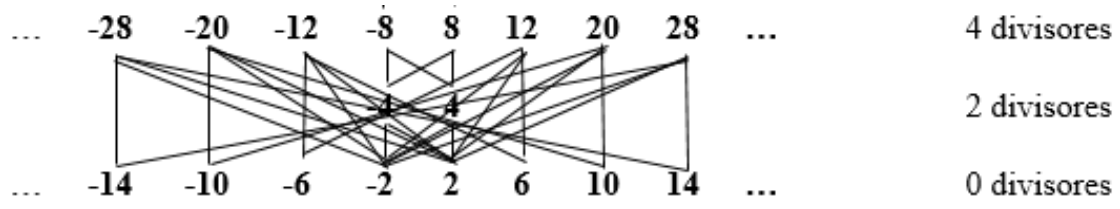

Figura 4-1.: Diagrama de Hasse para la relación de divisibilidad en $2\mathbb{Z}$

A través del cual se puede intuir el siguiente teorema:

Teorema 4.2. *Sea* $c \in 2\mathbb{Z}$,

1. *Si* $c = 4n + 2$ *con* $n \in \mathbb{Z}$ *entonces* c *no tiene divisores en* $2\mathbb{Z}$.
2. *Si* $c = 4n$ *con* n *primo en* $\mathbb{Z}$ *entonces* c *tiene* 4 *divisores.*
3. *Si* $c = 4n^2$ *con* n *primo en* $\mathbb{Z}$ *entonces* c *tiene* 6 *divisores.*
4. *Si* $c = 4mn$ *con* m *y* n *primos en* $\mathbb{Z}$ *entonces* c *tiene* 8 *divisores*

Prueba. 1. Si $c = 4n + 2$, su conjunto de divisores en $\mathbb{Z}$ va a estar dado por:

$$Div(c) = \{1, -1, 4n+2, -(4n+2), 2, 2n+1, -2, -(2n+1)\} \cup Div(2n+1) \cup Div(-(2n+1))$$

Como $1, -1 \notin 2\mathbb{Z}$ y $2n+1, -(2n+1) \notin 2\mathbb{Z}$, entonces no son divisores en este conjunto, así mismo tampoco pueden serlo $2, -2$ y $4n + 2$ y su opuesto porque sus factores son los cuatro primeros, y además todos los divisores de $2n + 1$ y $-(2n + 1)$ son impares, por lo tanto no pertenecen a $2\mathbb{Z}$ entonces c no tiene divisores en este conjunto.

2. Si $c = 4n$ con n primo en $\mathbb{Z}$, entonces cuenta con los siguientes divisores en $\mathbb{Z}$:

$$Div(c) = \{1, -1, 4n, -4n, 2n, -2n, 2, -2, 4, -4, n, -n\}$$

Sin embargo, en $2\mathbb{Z}$ los elementos $1, -1, 4n, -4n$ no son divisores en este conjunto, así como $4, -4, n, -n$ tampoco lo son, por lo tanto el conjunto de divisores se reduce a:

$$Div_{2\mathbb{Z}}(c) = \{2n, -2n, 2, -2\}$$

3. Si $c = 4n^2$ con n primo en $\mathbb{Z}$, entonces cuenta con los siguientes divisores en $\mathbb{Z}$:

$$Div(c) = \{1, -1, 4n^2, -4n^2, 2n, -2n, 2, -2, 4, -4, n, -n, n^2, -n^2, 2n^2, -2n^2\}$$

Sin embargo, en $2\mathbb{Z}$ los elementos $1, -1, 4n^2, -4n^2, 4n, -4n$ no son divisores en este conjunto, así como $4n, -4n, n, -n$ tampoco lo son, por lo tanto el conjunto de divisores se reduce a:

$$Div_{2\mathbb{Z}}(c) = \{2n^2, -2n^2, 2n, -2n, 2, -2\}$$

4. Si $c = 4mn$ con m y n primos en $\mathbb{Z}$ entonces cuenta con los siguientes divisores en este conjunto:

$$Div(c) = \{1, -1, 4mn, -4mn, 2, -2, 2mn, -2mn, 4, -4, mn, -mn, 2m,$$

$$-2m, 2n, -2n, 4m, -4m, n, -n, 4n, -4n, m, -m\}$$

Sin embargo, como $1, -1, m, n \notin 2\mathbb{Z}$ entonces el conjunto de divisores en $2\mathbb{Z}$ se reduce a:

$$Div_{2\mathbb{Z}}(c) = \{2, -2, 2mn, -2mn, 4, -4, mn, -mn, 2m, -2m, 2n, -2n\}$$

Notese que si $m = 2$ se cumple que

$$\pm 2m = \pm 4$$

$$\pm 2n = \pm mn$$

Lo que hace que el conjunto de divisores se reduzca, para este caso, a:

$$Div_{2\mathbb{Z}}(c) = \{2, -2, 2mn, -2mn, 4, -4, mn, -mn\}$$

Y si $m \neq 2$ se puede ver que $mn, -mn \notin 2\mathbb{Z}$ razón por la cual los divisores de c son

$$Div_{2\mathbb{Z}}(c) = \{2, -2, 2mn, -2mn, 2m, -2m, 2n, -2n\}$$

□

Teniendo en cuenta estos comportamientos evidenciados en el diagrama de Hasse, un camino de exploración puede consistir en generalizar el conjunto en cuestión para ver si se mantienen dichas propiedades. Desde esta perspectiva, consideremos el siguiente conjunto:

$$3\mathbb{Z} = \{\ldots, -12, -9, -6, -3, 0, 3, 6, 9, 12, \ldots\}$$

En donde, de manera análoga al caso anterior se tienen teoremas análogos al 5.1 y al 5.3, lo cual permite la construcción del diagrama de Hasse correspondiente:

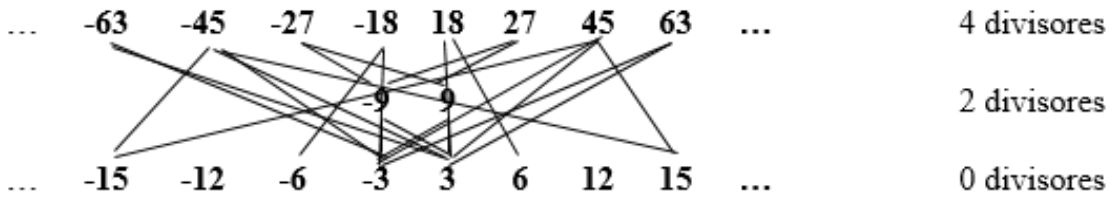

Figura 4-2.: Diagrama de Hasse para la relación de divisibilidad en $2\mathbb{Z}$

Y se pueden hacer observaciones similares al caso anterior, lo cual se materializa en el siguiente teorema:

Teorema 4.3. *Sea $c \in 3\mathbb{Z}$,*

1. *Si $c = 9n + 3$ o $c = 9n + 6$ con $n \in \mathbb{Z}$ entonces c no tiene divisores en $3\mathbb{Z}$.*
2. *Si $c = 9n$ con n primo en $\mathbb{Z}$ entonces c tiene 4 divisores.*
3. *Si $c = 9n^2$ con n primo en $\mathbb{Z}$ entonces c tiene 6 divisores.*
4. *Si $c = 9mn$ con m y n primos en $\mathbb{Z}$ entonces c tiene 8 divisores*

Prueba. 1. Si $c = 9n + 3$, su conjunto de divisores en $\mathbb{Z}$ va a estar dado por:

$$Div(c) = \{1, -1, 9n+3, -(9n+3), 3, 3n+1, -3, -(3n+1)\} \cup Div(3n+1) \cup Div(-(3n+1))$$

Como $1, -1 \notin 3\mathbb{Z}$ y $3n + 1, -(3n + 1) \notin 3\mathbb{Z}$, entonces no son divisores, así mismo tampoco pueden serlo $3, -3$ y $9n + 3$ y su inverso porque sus factores son los cuatro primeros, y además los divisores de $3n+1$ y $-(3n+1)$ no son múltiplos de 3, entonces no pertenecen a $3\mathbb{Z}$, por tanto, c no tiene divisores en este conjunto. Por otra parte, si $c = 9n + 6$, su conjunto de divisores en $\mathbb{Z}$ va a estar dado por:

$$Div(c) = \{1, -1, 9n + 6, -(9n + 6), 3, 3n + 2, -3, -(3n + 2)\}$$

Unido con todos los divisores de los números $3n + 2$ y $-(3n + 2)$, como $1, -1 \notin 3\mathbb{Z}$ y $3n + 2, -(3n + 2) \notin 3\mathbb{Z}$, entonces no son divisores, así mismo tampoco pueden serlo

$3, -3$ y $9n + 6$ y su inverso porque sus factores son los cuatro primeros, y además los divisores de $3n + 2$ y $-(3n + 2)$ no son múltiplos de 3, entonces no pertenecen a $3\mathbb{Z}$, por tanto, c no tiene divisores en este conjunto.

2. Si $c = 9n$ con n primo en $\mathbb{Z}$, entonces cuenta con los siguientes divisores en $\mathbb{Z}$:

$$Div(c) = \{1, -1, 9n, -9n, 3n, -3n, 3, -3, 9, -9, n, -n\}$$

Sin embargo, en $3\mathbb{Z}$ los elementos $1, -1, 9n, -9n$ no son divisores en este conjunto, así como $9, -9, n, -n$ tampoco lo son, por lo tanto el conjunto de divisores se reduce a:

$$Div_{3\mathbb{Z}}(c) = \{3n, -3n, 3, -3\}$$

3. Si $c = 9n^2$ con n primo en $\mathbb{Z}$, entonces cuenta con los siguientes divisores en $\mathbb{Z}$:

$$Div(c) = \{1, -1, 9n^2, -9n^2, 3n, -3n, 3, -3, 9, -9, n, -n, n^2, -n^2, 3n^2, -3n^2\}$$

Sin embargo, en $3\mathbb{Z}$ los elementos $1, -1, 9n^2, -9n^2, 9n, -9n$ no son divisores en este conjunto, así como $9n, -9n, n, -n$ tampoco lo son, por lo tanto el conjunto de divisores se reduce a:

$$Div_{3\mathbb{Z}}(c) = \{3n^2, -3n^2, 3n, -3n, 3, -3\}$$

4. Si $c = 9mn$ con m y n primos en $\mathbb{Z}$ entonces cuenta con los siguientes divisores en este conjunto:

$$Div(c) = \{1, -1, 9mn, -9mn, 3, -3, 3mn, -3mn, 9, -9, mn, -mn, 3m,$$

$$-3m, 3n, -3n, 3m, -3m, n, -n, 3n, -3n, m, -m\}$$

Sin embargo, como $1, -1, m, n \notin 3\mathbb{Z}$ entonces el conjunto de divisores en $3\mathbb{Z}$ se reduce a:

$$Div_{3\mathbb{Z}}(c) = \{3, -3, 3mn, -3mn, 9, -9, mn, -mn, 3m, -3m, 3n, -3n\}$$

Notese que si $m = 3$ se cumple que

$$\pm 3m = \pm 9$$

$$\pm 3n = \pm mn$$

Lo que hace que el conjunto de divisores se reduzca, para este caso, a:

$$Div_{3\mathbb{Z}}(c) = \{3, -3, 3mn, -3mn, 9, -9, mn, -mn\}$$

Y si $m \neq 3$ se puede ver que $mn, -mn \notin 3\mathbb{Z}$ razón por la cual los divisores de c son

$$Div_{3\mathbb{Z}}(c) = \{3, -3, 3mn, -3mn, 3m, -3m, 3n, -3n\}$$

□

Así como se hace importante estudiar la relación de divisibilidad en esta estructura algebraica, también es pertinente considerar otro aspecto propio de la teoría de números: el Máximo Común Divisor, del cual se sabe, desde lo intuitivo, que es el mayor de los divisores comunes entendiendo mayor bajo el orden usual de los números enteros. Desde esta perspectiva, por ejemplo en $2\mathbb{Z}$ para hallar el Máximo Común Divisor entre 24 y 72 veamos los divisores de cada uno de ellos:

$$Div_{2\mathbb{Z}}(24) = \{-12, -6, -4, -2, 2, 4, 6, 12\}$$

$$Div_{2\mathbb{Z}}(72) = \{-36, -18, -12, -6, -4, -2, 2, 4, 6, 12, 18, 36\}$$

De donde se tiene que sus divisores comunes son:

$$Div_{2\mathbb{Z}}(24) \cap Div_{2\mathbb{Z}}(72) = \{-12, -6, -4, -2, 2, 4, 6, 12\}$$

De donde se puede concluir que el Máximo Común Divisor entre 24 y 72 en $2\mathbb{Z}$ es 12.
Teniendo en cuenta esto se define el Máximo Común Divisor de la siguiente forma:

Definición 4.2 (Máximo Común Divisor en $2\mathbb{Z}$)**.** *Sean $a, b \in 2\mathbb{Z}$ se dice que c es el Máximo Común Divisor de a y b si cumple las siguientes condiciones:*

1. $c|_{2\mathbb{Z}}a$ *y* $c|_{2\mathbb{Z}}b$
2. *Si* $d \in 2\mathbb{Z}$ *y* $d|_{2\mathbb{Z}}a$ *y* $d|_{2\mathbb{Z}}b$ *entonces* $c > d$[2]

En primera medida hay que decir que si a es un número que no tiene divisores en $2\mathbb{Z}$, entonces el Máximo Común Divisor entre a y b no existe para cualquier $b \in 2\mathbb{Z}$ debido a que no existe un número que divida a ambos elementos.
En concordancia con lo anterior, ahora hay que ver si existe el Máximo Común Divisor para dos números compuestos, y en caso de que si exista cómo se obtiene, es decir si es posible calcular, según el teorema 4.2 el Máximo Común Divisor de $4m$ y $4n$ con $m, n \in \mathbb{Z}$, para lo cual se tiene el siguiente resultado:

Teorema 4.4. *Si $k, m \in \mathbb{Z}$ entonces se cumple que:*

$$M.C.D_{\mathbb{Z}}(k, m) = d \Leftrightarrow M.C.D_{2\mathbb{Z}}(4k, 4m) = 2d$$

Prueba. Supongamos que $M.C.D_{\mathbb{Z}}(k, m) = d$[3] y probemos que $M.C.D_{2\mathbb{Z}}(4k, 4m) = 2d$[4], entonces primero veamos que $2d$ es un divisor común. En primera medida se sabe que $d|_{\mathbb{Z}}k$ y $d|_{\mathbb{Z}}m$, entonces

$$\begin{array}{rr} ad = k & bd = m \\ (2a)(2d) = 4k & (2b)(2d) = 4m \\ 2d|_{2\mathbb{Z}}4k & 2d|_{2\mathbb{Z}}4m \end{array}$$

[2]Este es el orden usual del conjunto de los números enteros.
[3]Aquí se hace referencia al Máximo Común Divisor en $\mathbb{Z}$
[4]Aquí se hace referencia al Máximo Común Divisor en $2\mathbb{Z}$

Ahora veamos que es el mayor, para esto supongamos que existe $n \in 2\mathbb{Z}$, luego $n = 2h$ y $n \neq 2d$ tal que $n|_{2\mathbb{Z}}4k$ y $n|_{2\mathbb{Z}}4m$, entonces

$$\begin{aligned} n(2t) &= 4k \\ (2h)(2t) &= 4k \\ ht &= k \\ h|_{\mathbb{Z}}k \end{aligned} \qquad \begin{aligned} n(2r) &= 4m \\ (2h)(2r) &= 4m \\ hr &= m \\ h|_{\mathbb{Z}}m \end{aligned}$$

y como $M.C.D_{\mathbb{Z}}(k, m) = d$ entonces

$$h < d$$

de donde se concluye que

$$2h < 2d$$

luego

$$n < 2d$$

entonces se cumple que $M.C.D_{2\mathbb{Z}}(4k, 4m) = 2d$.
Por otra parte, supongamos que $M.C.D_{2\mathbb{Z}}(4k, 4m) = 2d$ y probemos que $M.C.D_{\mathbb{Z}}(k, m) = d$, para esto veamos que d es un divisor común; en primera medida se sabe que $2d|_{2\mathbb{Z}}4k$ y $2d|_{2\mathbb{Z}}4m$ luego:

$$\begin{aligned} (2d)(2t) &= 4k \\ dt &= k \\ d|_{\mathbb{Z}}k \end{aligned} \qquad \begin{aligned} (2d)(2r) &= 4m \\ dr &= m \\ d|_{\mathbb{Z}}m \end{aligned}$$

Ahora, supongamos que existe $r \in \mathbb{Z}$ tal que $r|_{\mathbb{Z}}k$ y $r|_{\mathbb{Z}}m$, entonces por propiedades de la divisibilidad en $\mathbb{Z}$ se tiene que

$$2r|_{\mathbb{Z}}4k \text{ y } 2r|_{\mathbb{Z}}4m$$

y como es cierto que $M.C.D_{2\mathbb{Z}}(4k, 4m) = 2d$ entonces

$$2r < 2d$$

luego

$$r < d$$

entonces se cumple que $M.C.D_{\mathbb{Z}}(k, m) = d$. □

Como se puede ver en esta demostración, no se usa el hecho que el conjunto sea precisamente $2\mathbb{Z}$, por lo tanto se puede generalizar para cualquier conjunto $k\mathbb{Z}$ de la siguiente forma:

Teorema 4.5. *Si $k, m \in \mathbb{Z}$ entonces se cumple que:*

$$M.C.D_{\mathbb{Z}}(n, m) = d \Leftrightarrow M.C.D_{k\mathbb{Z}}(k^2n, k^2m) = kd$$

Prueba. Es totalmente análoga a la del teorema 4.4. □

Una de las propiedades mas importantes que tiene el Máximo Común Divisor definido en el conjunto de los números naturales es que sigue siendo máximo también bajo el orden dado por la relación de divisibilidad, es decir que si c es el máximo común divisor entre a y b entonces se cumple que si d es otro divisor común entre a y b, entonces $d|c$; para ver si en $k\mathbb{Z}$ esto también se tiene analicemos el ejemplo que se mencionó anteriormente en $2\mathbb{Z}$, en el cual los divisores comunes eran:

$$Div_{2\mathbb{Z}}(24) \cap Div_{2\mathbb{Z}}(72) = \{-12, -6, -4, -2, 2, 4, 6, 12\}$$

donde se puede ver, por ejemplo, que 4 es un divisor común y no se cumple que $4|_{2\mathbb{Z}}12$, lo cual muestra que en este conjunto no tiene sentido hablar del máximo común divisor bajo el orden dado por la relación de divisibilidad.

4.2. Un camino de generalización

Como se puede ver, las observaciones realizadas en el diagrama de Hasse en los casos mostrados son totalmente análogas igual que sus demostraciones, así como los resultados mostrados sobre el Máximo Común Divisor, razón por la cual tiene sentido pensar en el estudio del siguiente conjunto:

$$k\mathbb{Z} = \{x : x = km, m \in \mathbb{Z}\}$$

Y, de manera análoga al caso particular de $2\mathbb{Z}$, se puede definir la siguiente relación:

Definición 4.3 (Divisibilidad en $k\mathbb{Z}$)**.** *Sean $c, d \in k\mathbb{Z}$, diremos que $c|d$ si y solo si existe $e \in k\mathbb{Z}$ tal que $ce = d$.*

La cual, también cumple un teorema análogo al teorema 5.3:

Teorema 4.6. *La relación de divisibilidad definida en $k\mathbb{Z}$ es asimétrica y transitiva.*

> *Prueba. Asimétrica*: Partamos de que $a|_{k\mathbb{Z}}b$, entonces existe $c \in k\mathbb{Z}$ tal que $ac = b$, y supongamos que $b|_{k\mathbb{Z}}a$ entonces existe $d \in k\mathbb{Z}$ tal que $bd = a$ entonces se tiene que $(bd)c = b$ de ahí que $dc = 1$ pero como $1 \notin k\mathbb{Z}$ se llega a una contradicción, por lo tanto $b \nmid_{k\mathbb{Z}} a$.
>
> *Transitiva:* Como la estructura en cuestión es un ideal del anillo de los números enteros, la operación multiplicación es asociativa, por lo tanto por el teorema 3.1 se tiene que la relación es transitiva.
>
> □

Y teniendo en cuenta las observaciones realizadas en los diagramas de Hasse para la divisibilidad en $2\mathbb{Z}$ y $3\mathbb{Z}$ se puede enunciar el siguiente teorema:

Teorema 4.7. *Sea $c \in k\mathbb{Z}$,*

1. *Si $c = k^2n + mk$ con $1 \leq m \leq k-1$ y $n \in \mathbb{Z}$ entonces c no tiene divisores en $k\mathbb{Z}$.*
2. *Si $c = k^2$ o $c = -k^2$ entonces c tiene dos divisores.*
3. *Si $c = k^2n$ con n primo en $\mathbb{Z}$ entonces c tiene 4 divisores.*
4. *Si $c = k^2n^2$ con n primo en $\mathbb{Z}$ entonces c tiene 6 divisores.*
5. *Si $c = k^2mn$ con m y n primos en $\mathbb{Z}$ entonces c tiene 8 divisores*

Prueba. 1. Si $c = k^2n + mk$, su conjunto de divisores en $\mathbb{Z}$ va a estar dado por:

$$Div(c) = \{1, -1, k^2n + mk, -(k^2n + mk), k, kn + m, -k, -(kn + m)\}$$
$$\cup Div(kn + m) \cup Div(-(kn + m))$$

Como $1, -1 \notin k\mathbb{Z}$ y $kn + m, -(kn + m) \notin k\mathbb{Z}$, entonces no son divisores, así mismo tampoco pueden serlo $k, -k$ y k^2n+mk y su inverso porque sus factores son los cuatro primeros, y además los divisores de los números $kn+m$ y $-(kn+m)$ no son múltiplos de k, entonces no pertenecen a $k\mathbb{Z}$, por tanto, c no tiene divisores en este conjunto.

2. Si $c = k^2$ o $c = -k^2$ entonces tiene el siguiente conjunto de divisores en $\mathbb{Z}$:

$$Div(c) = \{1, -1, k^2, -k^2, k, -k\} \cup Div(k)$$

Y como $1, -1 \notin k\mathbb{Z}$ y $Div(k) \nsubseteq k\mathbb{Z}$, entonces el conjunto de divisores se reduce a:

$$Div_{k\mathbb{Z}}(c) = \{k, -k\}$$

3. Si $c = k^2n$ con n primo en $\mathbb{Z}$, entonces cuenta con los siguientes divisores en $\mathbb{Z}$:

$$Div(c) = \{1, -1, k^2n, -k^2n, kn, -kn, k, -k, k^2, -k^2, n, -n\} \cup Div(k)$$

Sin embargo, en $k\mathbb{Z}$ los elementos $1, -1, k^2n, -k^2n$ no son divisores en este conjunto, así como $k^2, -k^2, n, -n$ tampoco lo son, y además $Div(k) \nsubseteq k\mathbb{Z}$, por lo tanto el conjunto de divisores se reduce a:

$$Div_{3\mathbb{Z}}(c) = \{kn, -kn, k, -k\}$$

4. Si $c = k^2n^2$ con n primo en $\mathbb{Z}$, entonces cuenta con los siguientes divisores en $\mathbb{Z}$:

$$Div(c) = \{1, -1, k^2n^2, -k^2n^2, kn, -kn, k, -k, k^2, -k^2, n, -n, n^2, -n^2, kn^2, -kn^2\} \cup Div(k)$$

Sin embargo, en $k\mathbb{Z}$ los elementos $1, -1, k^2n^2, -k^2n^2, k^2n, -k^2n$ no son divisores en este conjunto, así como $k^2n, -k^2n, n, -n$ tampoco lo son, y además $Div(k) \nsubseteq k\mathbb{Z}$, entonces el conjunto de divisores se reduce a:

$$Div_{k\mathbb{Z}}(c) = \{kn^2, -kn^2, kn, -kn, k, -k\}$$

5. Si $c = k^2mn$ con m y n primos en $\mathbb{Z}$ entonces cuenta con los siguientes divisores en este conjunto:

$$Div(c) = \{1, -1, k^2mn, -k^2mn, k, -k, kmn, -kmn, k^2, -k^2, mn, -mn, km,$$

$$-km, kn, -kn, km, -km, n, -n, kn, -kn, m, -m\} \cup Div(k)$$

Sin embargo, como $1, -1, m, n \notin k\mathbb{Z}$ y $Div(k) \nsubseteq k\mathbb{Z}$ entonces el conjunto de divisores en $k\mathbb{Z}$ se reduce a:

$$Div_{k\mathbb{Z}}(c) = \{k, -k, kmn, -kmn, k^2, -k^2, mn, -mn, km, -km, kn, -kn\}$$

Notese que si $m = k$ se cumple que

$$\pm km = \pm k^2$$

$$\pm kn = \pm mn$$

Lo que hace que el conjunto de divisores se reduzca, para este caso, a:

$$Div_{k\mathbb{Z}}(c) = \{k, -k, kmn, -kmn, k^2, -k^2, mn, -mn\}$$

Y si $m \neq k$ se puede ver que $mn, -mn \notin k\mathbb{Z}$ razón por la cual los divisores de c son

$$Div_{k\mathbb{Z}}(c) = \{k, -k, kmn, -kmn, km, -km, kn, -kn\}$$

□

4.3. Elementos primos y descomposición en $k\mathbb{Z}$

Teniendo en cuenta las observaciones demostradas en el teorema 4.7 y el hecho que, por ejemplo, en $2\mathbb{Z}$, los números de la forma $4n+2$, es decir, aquellos que no tienen divisores, no se pueden expresar como producto de otros elementos de dicho conjunto, hecho que además ocurre en $k\mathbb{Z}$ para cualquier k, se puede formular la siguiente definición:

Definición 4.4 (Número primo en $k\mathbb{Z}$)**.** *Sea $p \in k\mathbb{Z}$, diremos que p es primo en este conjunto, si p tiene 0 divisores.*

Con base en esta definición, a continuación se muestra un primer resultado que marca una diferencia importante con el comportamiento de los números primos en el conjunto de los números enteros, existe una fórmula para encontrar cualquiera de ellos:

Corolario 4.1. *En $k\mathbb{Z}$, un número es primo si es de la forma $k^2n + mk$ con $1 \leq m \leq k-1$ y $n \in \mathbb{Z}$.*

Prueba. Es consecuencia directa del teorema 4.7 y de la definición de número primo. □

Teniendo en cuenta esta noción de número primo que se adoptó y la forma como se define número primo usualmente en la teoría algebraica de números, veamos sí se cumple, en general, que si p es un:

$$\text{Si } p \text{ es un número primo y } p|_{k\mathbb{Z}}ab \text{ entonces } p|_{k\mathbb{Z}}a \text{ o } p|_{k\mathbb{Z}}b$$

O, en otras palabras, es necesario preguntarse, ¿existe algún número primo en $k\mathbb{Z}$ que cumpla esta propiedad? Un primer candidato natural es el número 2 en $2\mathbb{Z}$, sin embargo este es un número primo que no cumple esta propiedad dado que, por ejemplo, $2|_{2\mathbb{Z}}100$, pero $2 \nmid_{2\mathbb{Z}} 10$. Teniendo en cuenta esto, se puede decir que, en general, no existen números primos que cumplen esta condición dado que, si existiera, supongamos que $p|_{k\mathbb{Z}}ab$ y si a y b son números primos bajo la definición adoptada en este trabajo, es decir, que no tienen divisores, evidentemente no se tiene que $p|_{k\mathbb{Z}}a$ o $p|_{k\mathbb{Z}}b$.
Teniendo en cuenta la definición adoptada de número primo, así como el comportamiento de los elementos de $k\mathbb{Z}$, el propósito ahora consiste en caracterizar la descomposición en factores primos en este conjunto de la cual se puede decir, inicialmente, que no es única dado que, por ejemplo en $2\mathbb{Z}$:

$$100 = 10 \times 10$$

Pero también

$$100 = 2 \times 50$$

Las cuales vistas de otra forma son:

$$100 = (2 \times 5)(2 \times 5)$$

$$100 = 2(2 \times 5^2)$$

Lo cual muestra que estas se deducen de la descomposición de 100 vista como $100 = 2^2(5\times5)$, es decir que, si de manera general, la descomposición en factores primos en $\mathbb{Z}$ de un elemento de este conjunto es:

$$2^k(p_1p_2\cdots p_r)$$

Para obtener cualquier descomposición en factores primos del elemento en $2\mathbb{Z}$ se hace necesario formar entre 1 y k grupos de elementos primos con los números $p_1p_2\cdots p_r$, para multiplicar cada uno de ellos por un 2 y así obtener la descomposición, razón por la cual la cantidad de factorizaciones va a estar dada por:

$$\sum_{i=1}^{k} S(r,i)$$

donde $S(r,i)$ es la cantidad de i grupos no vacios que se pueden formar con r elementos, de donde se puede concluir que la cantidad va a estar dada por (Fernandez, P. y Fernandez, J., 2008):

$$\sum_{i=1}^{k}\left(\frac{1}{i!}\sum_{j=0}^{i}(-1)^j\begin{pmatrix} k \\ j \end{pmatrix}(i-j)^r\right)$$

Esto siempre y cuando $r > k$, sin embargo, si $r < k$, entonces la cantidad de descomposiciones va a ser:

$$\sum_{i=1}^{r} S(r,i) = \sum_{i=1}^{r} \left(\frac{1}{i!} \sum_{j=0}^{i} (-1)^j \begin{pmatrix} r \\ j \end{pmatrix} (i-j)^r \right)$$

Cabe resaltar que esta fórmula es cierta en el caso en que los factores primos presentes en la descomposición sean todos diferentes, sin embargo si alguno de ellos se repite una determinada cantidad de veces, se puede ver que algunas de ellas se repiten, por ejemplo, para el número 7700 se tiene que su descomposición en factores primos en $\mathbb{Z}$ es:

$$7700 = 2^2 \times (5^2 \times 7 \times 11)$$

Y como la cantidad de descomposiciones, bajo la fórmula mencionada anteriormente, se está contando a partir de la cantidad de grupos que se puede formar con los elementos $\mathbf{5}, 5, 7, 11$, las factorizaciones, contadas por la fórmula van a ser, entre otras, las siguientes:

$$2 \times [2 \times (\mathbf{5} \times 5 \times 7 \times 11)]$$

$$(2 \times \mathbf{5} \times 5) \times (2 \times 7 \times 11)$$

$$(2 \times \mathbf{5} \times 7) \times (2 \times 5 \times 11)$$

$$(2 \times 5 \times 7) \times (2 \times \mathbf{5} \times 11)$$

Donde claramente se ve que se están repitiendo descomposiciones, por lo tanto el problema para caracterizar las descomposiciones se convierte en uno de conteo en el cual se hace necesario ver de cuantas maneras se pueden formar entre 1 y k grupos con r elementos, teniendo en cuenta que algunos de ellos se repiten.

Como se puede ver, esta generalización surge de la descomposición en factores primos en $\mathbb{Z}$ del elemento, y particularmente del hecho que 2 es un número primo en dicho conjunto. Debido a esto, el resultado puede generalizarse al conjunto $k\mathbb{Z}$ donde k es primo, como sigue: Sea $c \in k\mathbb{Z}$, luego $c = k^n(p_1 p_2 \cdots p_r)$, entonces la cantidad de descomposiciones en factores primos en $k\mathbb{Z}$ de c va a estar dada por:

$$\sum_{i=1}^{n} \left(\frac{1}{i!} \sum_{j=0}^{i} (-1)^j \begin{pmatrix} n \\ j \end{pmatrix} (i-j)^r \right)$$

Siempre y cuando $r > n$, y si $r < n$ se tendrá que:

$$\sum_{i=1}^{r} \left(\frac{1}{i!} \sum_{j=0}^{i} (-1)^j \begin{pmatrix} r \\ j \end{pmatrix} (i-j)^r \right)$$

Sin embargo esto solo ocurre si los números primos de la descomposición del elemento en $\mathbb{Z}$ son diferentes entre sí, en caso contrario se reduce al mismo problema del caso anterior.

5. Un nuevo ejemplo: Los números de la forma $ak + 1$

Teniendo en cuenta que una de las estructuras algebraicas en las cuales se ha logrado un mayor desarrollo en relación con el estudio del proceso matemático de analizar, y particularmente con el cumplimiento del teorema fundamental de la aritmética, es la del conjunto de los números enteros con la operación multiplicación, tiene sentido pensar que, si se quiere buscar nuevos ejemplos donde se ponga de manifiesto el proceso, hay que hacerlo de manera tal que sea útil el desarrollo teórico existente para dicha estructura algebraica.
Desde esta perspectiva, y recordando que la estructura algebraica mencionada anteriormente es un monoide conmutativo con unidad, una manera de buscar nuevos ejemplos es encontrar subconjuntos de los números enteros donde, con la operación multiplicación, se tenga la misma estructura del conjunto original, es decir, un submonoide de la estructura inicial, en otras palabras, un subconjunto donde la multiplicación sea cerrada.
Teniendo en cuenta este propósito, uno de los ejemplos encontrados para realizar el estudio del proceso de analizar es el siguiente:

$$A_a = \{x : x = ak + 1, a, k \in \mathbb{Z}\}$$

Donde a es un número entero fijo pero arbitrario.
Dado que, en primera medida, este es un submonoide de los números enteros debido a que se cumple el siguiente teorema:

Teorema 5.1 (Cerradura de la multiplicación)**.** *Si $c, d \in A_a$ entonces $cd \in A_a$*

Prueba. Sean $b, c \in A_a$, luego $b = ak_1 + 1$ y $c = ak_2 + 1$, luego $bc = (ak_1 + 1)(ak_2 + 1)$ y por propiedades de la suma y el producto en los números enteros, tenemos que $bc = a(ak_1k_2 + k_1 + k_2) + 1$, por lo que $bc \in A_a$ □

Adicionalmente, como este conjunto es un submonoide de los números enteros, se tiene que en él la operación multiplicación sigue siendo asociativa, conmutativa, cancelativa, etc., además se hace evidente que sigue teniendo elemento idéntico dado que $1 \in A_a$ porque se puede considerar el caso en que $k = 0$:

$$ak + 1 = a(0) + 1 = 1$$

Con lo cual se puede concluir que este conjunto con la operación multiplicación es un monoide conmutativo con unidad igual que el conjunto de los números enteros con dicha operación, lo cual hace que, en esta estructura valga la pena realizar un estudio de la relación de divisibilidad, la noción de número primo, la descomposición en factores primos y otros conceptos relacionados con el proceso de analizar, en aras de que, como se dijo anteriormente, se pueda hacer uso de los desarrollos teóricos que se tienen para el conjunto de los números enteros. Adicionalmente, una de las propiedades más importantes que cumple la multiplicación entre números enteros, es la propiedad cancelativa, es decir:

$$\text{Si } ab = ac \text{ entonces } b = c, \text{ si } a \neq 0$$

Para ver si esta propiedad se mantiene en A_a, en primera medida es necesario ver que si $ab \in A_a$ entonces, por ejemplo, $b \in A_a$ lo cual se confirma con el siguiente teorema:

Teorema 5.2. *Dados $c, d \in \mathbb{Z}$, si $c \in A_a$ y $cd \in A_a$, entonces $d \in A_a$*

Prueba. Como $c \in A_a$ entonces $c = ak + 1$ de ahí que $ak = c - 1$ luego $a|c - 1$ y de ahí se concluye que

$$c \cong 1(\text{mod a}) \tag{5-1}$$

Por otra parte, como $cd \in A_a$, de forma análoga se concluye que

$$cd \cong 1(\text{mod a}) \tag{5-2}$$

Y por (1), (2), la simetría y la transitividad de la congruencia se tiene que

$$c \cong cd(\text{mod a})$$

Y como $c - ak = 1$, entonces por el lema de Bezout se tiene que $(c, a) = 1$ de donde se puede concluir que

$$1 \cong d(\text{mod a})$$

De donde se puede afirmar que

$$d \cong 1(\text{mod a})$$

Luego $a|d-1$, de ahí que $am = d-1$, entonces $d = am+1$, llegando a concluir que $d \in A_a$. □

Por otra parte, como lo ideal sería que esta estructura sea un subanillo de los números enteros, este conjunto debería ser, por lo menos, cerrado para la suma, pero esto no se cumple dado que:

$$(5k + 1) + (5k' + 1) = 5(k + k') + 2$$

A pesar de lo anterior, a continuación se muestra una exploración relacionada con la caracterización de algunas propiedades de este conjunto, estudiando casos particulares. Para estos efectos, aquí se presenta el caso de $a = 2$:

$$A_2 = \{\ldots, -9, -7, -5, -3, -1, 1, 3, 5, 7, 9, \ldots\}$$

En el cual se puede ver que si $a \in A_2$ entonces $-a \in A_2$, sin embargo se puede ver que en otros casos:

$$A_3 = \{\ldots, -14, -11, -8, -5, -2, 1, 4, 7, 10, 13, \ldots\}$$
$$A_4 = \{\ldots, -19, -15, -11, -7, -3, 1, 5, 9, 13, 17, \ldots\}$$
$$A_5 = \{\ldots, -24, -19, -14, -9, -4, 1, 6, 11, 16, 21, \ldots\}$$
$$\vdots$$

Esto no se cumple, y particularmente en ninguno de los casos el número -1 pertenece al conjunto, razón por la cual se puede ver que se cumple el siguiente teorema que marca una diferenciación importante entre este conjunto y el de los números enteros:

Teorema 5.3. *Sean $c, d \in A_a$. Si $cd = 1$ y $a > 2$, entonces $c = 1$ y $d = 1$*

Prueba. Por hipótesis, tenemos que $cd = 1$, donde $c = ak_1 + 1$ y $d = ak_2 + 1$, y como $c, d \in \mathbb{Z}$ por ser $A_a \subseteq \mathbb{Z}$ podemos suponer que si $c \neq 1$ entonces necesariamente debe cumplirse que $c = -1$, luego $ak_1 = -2$ de ahí que $a \leq 2$ lo que contradice que $a > 2$ luego $c = 1$, de manera análoga tenemos que $d = 1$. □

5.1. Relación de divisibilidad y Máximo Común Divisor en A_a

Como es sabido, a la hora de estudiar el desarrollo del proceso de analizar en una estructura se hace necesaria la existencia de una operación y una relación definidas en el conjunto, y como en este ejemplo ya se tiene que la operación multiplicación de los números enteros junto con todas sus propiedades usuales, se define lo siguiente:

Definición 5.1 (Divisibilidad)**.** *Sean $c, d \in A_a$, diremos que $c|_a d$ si y solo si existe $e \in A_a$ tal que $ce = d$*

Que coincide con la definición que se tiene en el conjunto de los números enteros.
A pesar de las similitudes presentes para la multiplicación en comparación con $\mathbb{Z}$, para el caso de la relación si existe una diferencia muy importante, que hace que esta relación tenga un parecido a la que se define usualmente en el conjunto de los números naturales:

Teorema 5.4. *Si $a > 2$, la relación de divisibilidad definida en A_a es una relación de orden.*

Prueba. En primer lugar, como $1 \in A_a$, entonces $b|_a b$ para todo $b \in A_a$, por lo tanto, $|_a$ es **reflexiva**. Ahora, si $c|_a b$ y $b|_a d$, entonces existen $f, e \in A_a$ tal que $cf = b$ y $be = d$, luego $(cf)e = d$, y por propiedades del producto en A_a, tenemos que $c(fe) = d$, luego $c|_a d$, esto

hace que $|_a$ sea **transitiva**, y por último si $c|_a b$ y $b|_a c$, tenemos que existen $h, d \in A_a$ tal que $cd = b$ y $bf = c$, luego $(cd)f = c$, de donde tenemos, por propiedades de la multiplicación en A_a, que $df = 1$, y como $a \neq 2$, por el teorema 5.3 tenemos $d = 1$ y $f = 1$, y sustituyendo, tenemos que $c = b$, luego $|_a$ es **antisimétrica**, con lo cual queda demostrado el teorema. □

Corolario 5.1. *Si $a = 2$ la relación de divisibilidad es un preorden[1].*

Prueba. Como en este caso no se cumple el teorema 5.3, no se tiene la antisimetría, pero se sigue cumpliendo la reflexividad y la transitividad, por lo tanto en A_2 la divisibilidad es un preorden. □

Teniendo en cuenta la relación de divisibilidad definida en A_a, se define otro concepto importante en la teoría de números, el Máximo Común Divisor de la siguiente forma:

Definición 5.2 (Máximo Común Divisor en A_a)**.** *Sean $b, d \in A_a$ se dice que $c \in A_a$ es el Máximo Común Divisor entre b y d si y solo sí cumple las siguientes condiciones:*

I. *$c|b$ y $c|d$*

II. *Si $e \in A_a$ y además $e|b$ y $e|d$, entonces $e < c$*[2]

De donde se puede ver que, por ejemplo, en A_5 para los números 21 y 6 es posible hallar el Máximo Común Divisor entre ellos de la siguiente forma:

$$Div_{A_5}(21) = \{1, 21\}$$

$$Div_{A_5}(6) = \{1, 6\}$$

de donde se puede concluir que el máximo común divisor es 1 que resulta ser diferente al que tienen en el conjunto de los números enteros que es 3, de donde se puede concluir que, en general, no es cierto que:

$$M.C.D_{A_5}(a, b) = M.C.D_{\mathbb{Z}}(a, b)$$

Por otra parte, de manera análoga al estudio realizado en los ideales de los números enteros, se puede ver si se cumple el hecho que el Máximo Común Divisor siga siendo máximo bajo el orden dado por la relación de divisibilidad, pero esto no se cumple ya que por ejemplo en A_7 se tiene que los divisores de -48 y 120 son:

$$Div(-48) = \{1, -6, 8, -48\}$$

$$Div(120) = \{1, -6, 8, 15, -20, 120\}$$

De donde se puede concluir que su máximo común divisor es 8, sin embargo facilmente se ve que -6 también es un divisor común, sin embargo $-6 \nmid 8$, lo cual muestra que, en general, para este caso tampoco tiene sentido hablar del Máximo Común Divisor bajo el orden dado por la divisibilidad.

[1] En este caso la relación tiene un comportamiento similar a la definida en el conjunto de los números enteros.

[2] Este es el orden usual del conjunto de los números enteros.

5.2. Elementos primos en A_a

Teniendo en cuenta las propiedades que cumple la relación de divisibilidad definida en A_a, y el parecido que esta tiene, en la mayoría de los casos, con la que se tiene en el conjunto de los números naturales, a continuación se introduce la siguiente definición:

Definición 5.3 (Número primo)**.** *Sea $b \in A_a (a > 2)$ y $b \neq 1$, diremos que b es primo en A_a si y solo si tiene exactamente 2 divisores en A_a. Si b no es primo, diremos que b es compuesto.*

A partir de esta definición surgen de manera inmediata algunas preguntas: ¿todo primo en $\mathbb{Z}$ será primo en A_a y viceversa?, y además ¿cómo afecta esto la descomposición? Para darle respuesta a una de estas preguntas, veamos primero que si p es primo en $\mathbb{Z}$ y $p \in A_a$, sabemos que sus únicos divisores van a ser 1 y p, por ende todo primo en $\mathbb{Z}$ que pertenezca a A_a, va a ser primo también en este último conjunto.
Por otra parte, otra de las preguntas naturales que surgen a raiz de esta definición es que si un número es primo en A_a, ¿será primo em $\mathbb{Z}$?, es decir, ¿existirán nuevos primos en A_a en comparación con $\mathbb{Z}$? Para dar respuesta a esta pregunta, se puede observar algunos ejemplos:

$$A_3 = \{\ldots, -14, \textbf{-11}, -8, \textbf{-5}, \textbf{-2}, 1, 4, \textbf{7}, 10, \textbf{13}, \ldots\}$$

En este conjunto se puede evidenciar (tal como se resaltó) que los números primos que aparecen, por lo menos en esta lista, coinciden con primos en los números enteros, y los demás son compuestos, como por ejemplo el número -14 que tiene como divisores en A_3 a $1, -2$ y a 7 por lo tanto es compuesto. Por tal razón, aparentemente, aquí no habrá nuevos primos, por ende veamos el siguiente ejemplo:

$$A_4 = \{\ldots, -15, \textbf{-11}, \textbf{-7}, \textbf{-3}, 1, \textbf{5}, 9, \textbf{13}, \ldots\}$$

De donde se puede conjeturar que tiene un comportamiento similar al que se sospecha que tiene A_3 dado que, como está resaltado, aparecen primos que también son primos en $\mathbb{Z}$ y los demás son compuestos, como por ejemplo el número -15 que tiene como divisores en A_4 a $1, -3$ y a 5, de ahí que sea necesario buscar otro ejemplo para poder encontrar, posiblemente, comportamientos distintos en la descomposición:

5.3. Un primer caso: $A_5 = \{x : x = 5k + 1, k \in \mathbb{Z}\}$

Para dar inicio a la exploración en este conjunto veamos algunos de sus elementos, en aras de tratar de caracterizar a los mismos:

$$A_5 = \{\ldots, -24, \textbf{-19}, \textbf{-14}, \textbf{-9}, \textbf{-4}, 1, \textbf{6}, \textbf{11}, 16, \textbf{21}, \ldots\}$$

Inicialmente, aqui se puede ver que, a diferencia de los otros ejemplos mostrados, en este si se encuentran nuevos primos, como por ejemplo el número 6 dado que tiene como divisores en $\mathbb{Z}$ a:

$$Div(6) = \{-6, -3, -2, -1, 1, 2, 3, 6\}$$

Y como $-6, -3, -2, -1, 2, 3 \notin A_5$ los únicos divisores de 6 en dicho conjunto son 1 y 6, por lo tanto este número es primo en esta estructura. Como consecuencia de lo anterior, en este conjunto vale la pena iniciar un estudio en relación con la descomposición en factores primos en aras de verificar si se cumple o no el teorema fundamental de la aritmética, por lo tanto:

5.3.1. Hacia una caracterización de la descomposición

Teniendo en cuenta lo dicho anteriormente, el interés ahora va a ser ver si para cualquier elemento de A_5 existe una descomposición en factores primos, y además si (de existir) esta es única, es decir, ver si se puede establecer una versión para este conjunto del teorema fundamental de la aritmética, para estos efectos se puede iniciar una exploración a través de ejemplos como los siguientes:

Número compuesto en A_5	Descomposiciones en $\mathbb{Z}$ (Salvo los signos)	Descomposiciones en A_5
-484	$2^2 \cdot 11^2$	$(-4) \cdot 11^2$
-424	$2^3 \cdot 53$	$(-4) \cdot 106$
116	$2^2 \cdot 29$	$(-4) \cdot (-29)$
-494	$2 \cdot 13 \cdot 19$	$26 \cdot (-19)$
-474	$2 \cdot 3 \cdot 79$	$6 \cdot (-79)$
-444	$2^2 \cdot 3 \cdot 37$	$(-4) \cdot 111$ $6 \cdot (-74)$
-434	$2 \cdot 7 \cdot 31$	$(-14) \cdot 31$
-414	$2 \cdot 3^2 \cdot 23$	$(-9) \cdot 46$ $6 \cdot (-74)$
-399	$3 \cdot 7 \cdot 19$	$(-19) \cdot 21$
156	$2^2 \cdot 3 \cdot 13$	$(-4) \cdot (-39)$ $6 \cdot 26$
186	$2 \cdot 3 \cdot 31$	$6 \cdot 31$

Número compuesto en A_5	Descomposiciones en $\mathbb{Z}$ (Salvo los signos)	Descomposiciones en A_5
-4914	$2 \cdot 3^3 \cdot 7 \cdot 13$	$6 \cdot 21 \cdot (-39)$ $6 \cdot (-9) \cdot 91$ $26 \cdot 21 \cdot (-9)$
-4884	$2^2 \cdot 3 \cdot 11 \cdot 37$	$6 \cdot 11 \cdot (-74)$ $(-4) \cdot 11 \cdot 111$
8736	$2^5 \cdot 3 \cdot 7 \cdot 13$	$(-4) \cdot 6 \cdot (-14) \cdot 26$ $(-4)^2 \cdot (-39) \cdot (-14)$ $(-4)^2 \cdot 26 \cdot 21$ $(-4)^2 \cdot 6 \cdot 91$

Tabla 5-1.: Algunas descomposiciones en factores primos de elementos de A_5

De la cual se puede ver, inicialmente, que no es posible hablar del teorema fundamental de la aritmética debido a que es posible encontrar, para algunos elementos del conjunto, más de una descomposición en factores primos, sin embargo, si se puede, a partir de la exploración, ver que cualquier descomposición en factores primos de los elementos del conjunto, puede ser obtenida a partir de realizar productos en la descomposición del mismo en $\mathbb{Z}$, por ejemplo: El número -4884 pertenece a A_5 y su descomposición factores primos en $\mathbb{Z}$ es $2\times2\times3\times11\times37$ (salvo los signos) y esta se puede ver de la siguiente forma:

$$-(2 \times 2) \times 11 \times (3 \times 37) = (-4) \times 11 \times 111$$

$$(2 \times 3) \times 11 \times -(2 \times 37) = 6 \times 11 \times (-74)$$

Teniendo en cuenta esto, el siguiente paso en la exploración consiste en tratar de caracterizar el producto entre números primos en el conjunto de los números enteros dado que, como ya se vió, las diferentes descomposiciones de un elemento en A_5 surgen de operaciones de este tipo. En concordancia con lo anterior, se introducirá un teorema muy famoso en la teoría de números que será útil en la caracterización mencionada anteriormente:

Teorema 5.5 (Teorema de Dirichlet)**.** *Si $(a, b) = 1$ con a y b enteros positivos, entonces hay un número infinito de primos de la forma $a + kb$.*

Para dar inicio al estudio de regularidades en el producto entre números primos en $\mathbb{Z}$ en relación con el conjunto A_5, tiene sentido pensar, en primera medida, en los comportamientos resultantes de elevar un número primo al cuadrado. en este sentido, se obtiene el siguiente resultado:

Teorema 5.6. *Sea $p \in \mathbb{Z}$. Si p es primo en este conjunto y $p \notin A_5$, entonces $p^2 \in A_5$ o $-p^2 \in A_5$.*

Prueba. Los primos que no están en A_5, por el teorema 4.4, van a tener la forma $5k+2, 5k+3$ o $5k+4$, y si elevamos estas formas al cuadrado tenemos que:

$$(5k+2)^2 = 25k^2 + 20k + 4 = 5(5k^2 + 4k) + 4$$

$$(5k+3)^2 = 25k^2 + 30k + 9 = 5(5k^2 + 6k + 1) + 4$$

$$(5k+4)^2 = 25k^2 + 40k + 16 = 5(5k^2 + 8k + 3) + 1$$

Y como se sabe, adicionalmente, que si un número es de la forma $5k+4$, su inverso es de la forma $5k+1$, se puede afirmar que:

$$-(5k+2)^2 \in A_5$$

$$-(5k+3)^2 \in A_5$$

$$(5k+4)^2 \in A_5$$

Lo cual demuestra que cualquier primo elevado al cuadrado o su inverso pertenece a A_5. □

Tomando como base el teorema anterior se puede inferir un resultado más general, el cual nos servirá como base para caracterizar la descomposición en factores primos de los elementos de A_5:

Teorema 5.7. *Sean $p, q \in \mathbb{Z}$. Si p, q son primos en $\mathbb{Z}$ y $p, q \notin A_5$ entonces $pq \in A_5$ o $-pq \in A_5$.*

Prueba. Por el teorema 5.5 se sabe que los primos en $\mathbb{Z}$ tienen la forma $5k+2$ o $5k+3$ y si se hacen todas las posibles multiplicaciones de primos que no estén en A_5 se tiene que:

$$(5k+2)(5k+3) = 5(5k^2 + 5k + 1) + 1$$

Lo cual demuestra, de forma similar al resultado anterior, que cualquier producto de dos números primos en $\mathbb{Z}$, o su inverso, pertenece a A_5. □

Teniendo en cuenta los resultados hasta aqui mostrados, se puede ver que si la descomposición en factores primos en $\mathbb{Z}$ de un elemento de A_5 es:

$$a = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_n^{\alpha_n}$$

y si se supone que $p_1, p_2, \cdots, p_n \notin A_5$, para encontrar la cantidad de descomposiciones en factores primos con que cuenta el elemento en A_5 se hace necesario encontrar la cantidad de maneras es posible organizar en parejas los factores teniendo en cuenta que, primero, algunos de ellos se repiten, y segundo que no importa el orden de las parejas ni al interior de cada una de las parejas; resolviendo este problema de conteo será posible obtener la cantidad de descomposiciones en factores primos de un elemento cualquiera de A_5, por ejemplo, para algunos casos particulares se tienen los siguientes resultados:

Caso 1. $a = p_1^{\alpha_1}$			
$\alpha_1 = 2n$	Una descomposición $p_1^2 p_1^2 \cdots p_1^2$		
$\alpha_1 = 2n + 1$	No hay elementos de esta forma en A_5		
Caso 2. $a = p_1^{\alpha_1} p_2^{\alpha_2}$ **si** $\alpha_1 \leq \alpha_2$			
$\alpha_1 = 2k$		$\alpha_2 = 2n$	$k + 1$ descomposiciones
$\alpha_1 = 2k + 1$		$\alpha_2 = 2n + 1$	$k + 1$ descomposiciones
$\alpha_1 = 2k$ o $\alpha_1 = 2k + 1$		$\alpha_2 = 2n + 1$ o $\alpha_2 = 2n$	No hay elementos de esta forma en A_5
Caso 3. $a = p_1^{\alpha_1} p_2^{\alpha_2} p_3^{\alpha_3}$ **si** $\alpha_1 \leq \alpha_2 \leq \alpha_3$			
α_1	α_2	α_3	*Descomposiciones*
1	1	1	No hay elementos de esta forma en A_5
	1	2	$(p_1p_2)p_3^2$ $(p_1p_3)(p_2p_3)$
	1	3	No hay elementos de esta forma en A_5
	1	4	$(p_1p_2)p_3^2p_3^2$ $(p_1p_3)(p_2p_3)p_3^2$
1	1	$2n + 1$	No hay elementos de esta forma en A_5
1	1	$2n$	2 descomposiciones
1	2	2	No hay elementos de esta forma en A_5
	2	3	$(p_1p_2)(p_2p_3)p_3^2$ $(p_1p_3)p_2^2p_3^2$ $(p_1p_3)(p_2p_3)(p_2p_3)$
	2	4	No hay elementos de esta forma en A_5
	2	5	$(p_1p_2)(p_2p_3)p_3^2p_3^2$ $(p_1p_3)p_2^2p_3^2p_3^2$ $(p_1p_3)(p_2p_3)(p_2p_3)p_3^2$
1	2	$2n + 1$	3 descomposiciones
1	2	$2n$	No hay elementos de esta forma en A_5
1	3	4	$(p_1p_2)p_2^2p_3^2p_3^2$ $(p_1p_3)(p_2p_3)(p_2p_3)p_3^2$ $(p_1p_3)(p_2p_3)p_2^2p_3^2$ $(p_1p_3)(p_2p_3)(p_2p_3)(p_2p_3)$
1	4	5	5 descomposiciones
1	$2n + 1$	$2k$	$2n + 2$ descomposiciones
1	$2n$	$2k + 1$	$2n + 1$ descomposiciones

α_1	α_2	α_3	*Descomposiciones*
2	2	2	5 descomposiciones
2	2	$2k$, $k>1$	6 descomposiciones
2	3	3	6 descomposiciones
2	3	$2k+1$, $k>2$	7 descomposiciones
2	4	4	7 descomposiciones
2	4	$2k$, $k>2$	8 descomposiciones

Tabla 5-2.: Algunas generalizaciones de la cantidad de factorizaciones de elementos de A_5

Teniendo en cuenta esta exploración, lo que falta por hacer es generalizar para hallar la cantidad de descomposiciones para el caso n donde $a = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_n^{\alpha_n}$, lo cual lleva al problema de conteo descrito anteriormente.

5.4. Algunos casos más: A_7 y A_{11}

De manera similar al caso anterior, en A_7 se puede evidenciar que existen nuevos números primos:

$$A_7 = \{\ldots, \textbf{-27, -20, -13, -6, 1, 8, 15, 22, 29,}36, \ldots\}$$

y a diferencia de lo que ocurre en A_7, no se cumple en general que si p y q son primos en $\mathbb{Z}$ entonces $pq \in A_7$, sin embargo si es parcialmente cierto dependiendo de la forma del número primo, por ejemplo:

Teorema 5.8. *Si $p, q \in \mathbb{Z}$ y además $p = 7k+2$ y $q = 7m+4$ entonces $pq \in A_7$*

Prueba. Como $p = 7k+2$ y $q = 7m+4$ entonces

$$pq = (7k+2)(7m+4) = 7(7mk + 4k + 2m + 1) + 1$$

y como $7mk + 4k + 2m + 1 \in \mathbb{Z}$ entonces $pq \in A_7$. □

Además, de la misma forma que en A_5, los productos de números primos que entran en el conjunto A_7, resultan ser primos en este conjunto. Adicional a lo anterior, y a diferencia de lo que ocurre en A_5 se cumple que algunos productos de tres números primos en $\mathbb{Z}$ pertenecen a A_7, por ejemplo:

Teorema 5.9. *Si $p, q, r \in \mathbb{Z}$ y $p = 7m+3$, $q = 7n+3$ y $r = 7k+4$ entonces $pqr \in A_7$.*

Prueba. Como $p = 7m+3$, $q = 7n+3$ y $r = 7k+4$ entonces

$$pqr = 7(49kmn + 21km + 21kn + 9k + 28mn + 12m + 12n + 5) + 1$$

y como $49kmn + 21km + 21kn + 9k + 28mn + 12m + 12n + 5 \in \mathbb{Z}$ entonces $pqr \in A_7$. □

Teniendo en cuenta esto, en la siguiente tabla se muestran los productos de elementos de $\mathbb{Z}$ que dan como resultado un elemento de A_7:

$7k+2$	$7k+3$	$7k+4$	$7k+5$
√	√		
√		√	
	√		√
		√	√
√√√			
√√			√
√			√√
			√√√
	√√√		
	√√	√	
	√	√√	
		√√√	

Tabla 5-3.: Productos que dan como resultado elementos de A_7

Con base en lo anterior, la cantidad de descomposiciones en factores primos de un elemento de A_7 va a estar dada por la relación entre los factores primos del número en $\mathbb{Z}$ y la tabla anterior, teniendo en cuenta que, para algunos casos, quien está en el conjunto es el inverso del número, este es el problema de conteo que permite establecer la cantidad de factorizaciones en A_7.

Habiendo visto el problema de caracterizar la cantidad de descomposiciones para los casos de A_5 y A_7, se puede analizar otro caso donde también aparecen nuevos números primos: A_{11}, en el cual, de forma similar al caso anterior, hay algunos productos de números enteros que caen dentro del conjunto:

$11k+2$	$11k+3$	$11k+4$	$11k+5$	$11k+6$	$11k+7$	$11k+8$	$11k+9$
√			√				
√				√			
	√	√					
	√				√		
		√				√	
			√				√

$11k+2$	$11k+3$	$11k+4$	$11k+5$	$11k+6$	$11k+7$	$11k+8$	$11k+9$
				$\surd$			$\surd$
					$\surd$	$\surd$	
					$\surd$	$\surd$	

Tabla 5-4.: Productos que dan como resultado elementos de A_{11}

Y de manera análoga al caso de A_7, hay algunos productos de tres números enteros que caen en el conjunto, lo cual hace que el problema de determinar la cantidad de descomposiciones de un elemento de A_{11} se configure en un problema de conteo similar al de A_7, que dependerá de la forma de los números primos que estan en la descomposición en $\mathbb{Z}$ del elemento.

6. Actividades propuestas

Teniendo en cuenta los objetivos propuestos para este trabajo de grado, en este capítulo se presentan algunas actividades con las que se pretende buscar que los estudiantes del espacio académico Teoría de Números de la Licenciatura en Matemáticas de la Universidad Pedagógica Nacional, desarrollen el proceso matemático de analizar a través del descubrimiento, a partir de la exploración, de los resultados presentados en las estructuras algebraicas estudiadas en este trabajo.

6.1. Los ideales de los números enteros

En concordancia con lo anterior, a continuación se muestra una actividad en la cual se involucran los resultados logrados alrededor de esta estructura algebraica, particularmente en lo que tiene que ver con los siguientes aspectos:

- **Comportamiento de las operaciones en $k\mathbb{Z}$:** En esta primera sección se busca que los estudiantes evidencien que la suma y la multiplicación definidas usualmente en el conjunto de los números enteros, son también operaciones bien definidas en este subconjunto, y adicionalmente, se pretende que ellos hagan un reconocimiento de dicha estructura algebraica a través de la observación de algunos elementos y el desarrollo de operaciones entre ellas:

- **Relación de divisibilidad en $k\mathbb{Z}$:** Teniendo en cuenta la cerradura de las operaciones ya evidenciada, en esta sección se introducirá la relación de divisibilidad de la misma forma que se define en el conjunto de los números enteros, y con base en esta definición se proponen preguntas que lleven a los estudiantes a ver las propiedades que cumple esta relación en este conjunto, en particular en lo que tiene que ver con el hecho que esta es un orden estricto.

- **Caracterización de los elementos del conjunto a partir de sus divisores:** Teniendo en cuenta que la relación de divisibilidad definida en $k\mathbb{Z}$ es un orden estricto, en esta sección se propone hacer uso del diagrama de Hasse como herramienta para identificar la cantidad de divisores de los elementos del conjunto, y a partir de ello caracterizarlos.

- **Definición de número primo en $k\mathbb{Z}$:** A partir de la caracterización hecha, se busca además que los estudiantes construyan una definición de número primo adecuada para

esta estructura algebraica, teniendo en cuenta que esta debe servir para garantizar que existe una desomposición de los demás elementos del conjunto como producto de ellos, y además que esta, en la medida de lo posible, sea única.

- **Descomposición de factores primos:** Teniendo en cuenta la definición de número primo acordada, se busca que los estudiantes exploren en relación con la existencia y la unicidad de la descomposición en factores primos buscando, si es posible, el cumplimiento de una proposición análoga al teorema fundamental de la aritmética en $k\mathbb{Z}$.

Teniendo en cuenta esto, a continuación se muestra las secciones de la actividad asociadas a cada uno de los objetivos mencionados:

La relación de divisibilidad en los conjuntos $k\mathbb{Z}$

Teniendo en cuenta que una de las maneras de estudiar el proceso de analizar es a través de definir una relación de divisibilidad en una estructura algebraica, en este taller se propone que se desarrolle esto en algunos conjuntos numéricos: Los ideales de los números enteros; los cuales, recordemos, son la siguiente familia de conjuntos:

$$k\mathbb{Z} = \{x \in \mathbb{Z} | x = km, m \in \mathbb{Z}\}$$

donde k es un entero cualquiera. Con base en esto, responda las siguientes preguntas:

1. Haga un listado de algunos elementos de $2\mathbb{Z}$ y responda:
   a. ¿La suma de elementos de $2\mathbb{Z}$ pertenece a $2\mathbb{Z}$? Justifique.
   b. ¿La multiplicación de elementos de $2\mathbb{Z}$ pertenece a $2\mathbb{Z}$? Justifique.
2. Responda las mismas preguntas del punto anterior pero con $3\mathbb{Z}$
3. Si $x, y \in k\mathbb{Z}$, ¿se cumple que $x + y \in k\mathbb{Z}$? Demuestre se respuesta.
4. Si $x, y \in k\mathbb{Z}$, ¿se cumple que $xy \in k\mathbb{Z}$? Demuestre se respuesta.
5. ¿Para cuales valores de k se cumple que $1 \in k\mathbb{Z}$?
6. ¿Para cuales valores de k se cumple que $-1 \in k\mathbb{Z}$?

Con este primer grupo de preguntas se busca que los estudiantes evidencien la cerradura de la suma y la multiplicación en los conjuntos en mención ya que esto, como se vió a través de este trabajo, es muy importante para poder hablar de la relación de divisibilidad como una herramienta para el desarrollo del proceso matemático de analizar en una estructura; adicionalmente, se pretende que evidencien el hecho que no se cuenta con el 1 y el -1, es decir las unidades en el conjunto de los números enteros, lo cual hará que, mas adelante, se presenten novedades en lo que tiene que ver con el comportamiento de la relación de

divisibilidad.

Teniendo en cuenta que la multiplicación se puede definir, igual que en los casos usuales, la relación de divisibilidad en la siguiente forma:

Definición: Sea $x, y \in k\mathbb{Z}$ se dice que $a|b$ si y solo si existe $c \in k\mathbb{Z}$ tal que $ac = b$.

7. Teniendo en cuenta la definición, para cada una de las siguientes preguntas, si la respuesta es afirmativa demuestre su respuesta, en caso contrario, explique:
   a. ¿La relación de divisibilidad es reflexiva en $k\mathbb{Z}$?
   b. ¿La relación de divisibilidad es asimétrica en $k\mathbb{Z}$?
   c. ¿La relación de divisibilidad es transitiva en $k\mathbb{Z}$?

Con estas preguntas se busca que el estudiante descubra el hecho que la relación de divisibilidad no cuenta con la propiedad reflexiva debido a la ausencia del elemento 1 en estos conjuntos, pero que sin embargo si es asimétrica y transitiva, lo que hace que esta sea un orden estricto.

8. Teniendo en cuenta la definición de la relación de divisibilidad, contruya el diagrama de Hasse de la misma para el caso $2\mathbb{Z}$ y con base en él, responda, justificando sus respuestas:
   a. ¿Existen elementos que no tengan divisores? Si es así, de una fórmula para encontrarlos.
   b. ¿Cuáles elementos tienen dos divisores?
   c. ¿Existe alguna fórmula que permita encontrar los números que tengan cuatro divisores? ¿Qué tengan 6? ¿Qué tengan 8?
   d. ¿Existe algún número con una cantidad impar de divisores?
9. Construya el diagrama de Hasse y responda preguntas similares para los casos de $3\mathbb{Z}$ y $4\mathbb{Z}$. Procure generalizar para cualquier $k\mathbb{Z}$ los resultados obtenidos.
10. Con base en los resultados vistos hasta ahora, ¿como definiría número primo en $k\mathbb{Z}$? Con base en esta definición, ¿existe una fórmula que permita encontrar números primos en este conjunto.
11. ¿Existe algún número que sea primo en $k\mathbb{Z}$ que también sea primo en $\mathbb{Z}$. Justifique su respuesta

Estas preguntas tiene como intención que los estudiantes exploren desde el diagrama de Hasse y den una caracterización de los elementos de $k\mathbb{Z}$ a partir de sus divisores. Por otra parte

se busca que los estudiantes lleguen a hablar de número primo en este conjunto como aquel que no tiene divisores y evidencie que, a diferencia de los números enteros, aquí es posible encontrar una fórmula que permita encontrar cualquier número primo. En lo que tiene que ver con las respuestas dadas por los estudiantes, se espera que ellos busquen, con la ayuda del profesor que dirija la actividad, una definición que sirva como herramienta para, como se dijo anteriormente, lograr obtener una descomposición de los elementos que, en la medida de lo posible, sea única; sin embargo, puede ocurrir, por ejemplo, que los estudiantes opten por copiar la definición de primo de los números naturales o de los números enteros, pero basta con hacerlos ver que estas no son útiles debido a que existirán elementos que no se podrán descomponer en términos de ellos, justamente los elementos que no tienen divisores, dejando así a estos como candidatos naturales para ser los números primos además porque es facilmente verificable que los demás elementos del conjunto se pueden descompone en términos de ellos, dejando entrever una manera clara de llevar a cabo el proceso de analizar en una estructura.

12. Teniendo en cuenta la definición que dió, haga un listado algunos números primos en $2\mathbb{Z}$ y descomponga los siguientes números como producto de ellos:

Elemento de $2\mathbb{Z}$	**Descomposición**
-8	
28	
242	
-18	
60	
-140	

¿Hay una sola forma de lograr dicha descomposición? Justifique su respuesta.

13. Complete la siguiente tabla:

Elemento de $2\mathbb{Z}$	**Descomposición en $2\mathbb{Z}$**	**Cantidad de factores**	**Descomposición en $\mathbb{Z}$**	**Cantidad de factores**
-8				
28				
242				
-18				
60				
-140				

Y con base en ella responda:

a. Con base en lo visto, ¿es posible decir que cualquier elemento de $2\mathbb{Z}$ tiene descomposición en factores primos?

b. ¿Hay casos en los que esta sea única?

Justifique sus respuestas

Con estas preguntas se busca que los estudiantes evidencien que siempre se tiene la existencia de la descomposición en factores primos para cualquier elemento de $2\mathbb{Z}$ pero que esta no es única, y que vean además que esto depende de la descomposición del número en el conjunto de los números enteros.

6.2. Los números de la forma $ak + 1$

De manera similar al caso de los ideales del conjunto de los números enteros, a continuación se muestran dos actividades que buscan que los estudiantes descubran los resultados que aquí se mostraron sobre el conjunto de los números de la forma $ak+1$. Cabe resaltar que estas fueron diseñadas con el apoyo del grupo de Álgebra de la Universidad Pedagógica Nacional como insumo para el espacio académico Teoría de Números, y además como producto del proyecto de investigación titulado .ªctividades Matemáticas para el desarrollo de procesos lógicos: el proceso matemático de analizar en el espacio académico teoría de Números de la Licenciatura en Matemáticas de la UPN-experimentación y evaluación"; también es necesario resaltar que la construcción de la actividad respondió a los siguientes objetivos:

- **Caracterización del conjunto y cerradura de las operaciones:** De forma similar al caso anterior, en esta primera parte de la actividad se busca que los estudiantes evidencien algunas características propias del conjunto, particularmente en lo que tiene que ver con la caracterización de los elementos del conjunto y con la cerradura de la multiplicación en este conjunto. Adicionalmente, se busca que vean que la suma no es una operación bien definida, lo cual marca una diferencia importante entre esta estructura y el conjunto de los números naturales y los npumeros enteros.
- **Relación de divisibilidad en A_a:** Con esta actividad también se busca que los estudiantes vean que el hecho de tener una multiplicación permite definir una relación de divisibilidad de forma similar a los casos usuales, y además se busca que exploren alrededor de las propiedades que esta cumple definida en A_a.
- **Número primo en A_a:** Además de lo anterior, también se busca que con esta actividad los estudiantes construyan una definición de número primo haciendo uso del parecido que tiene la divisibilidad definida en este conjunto, respecto a la definida en el conjunto de los números naturales, así como del hecho de estudiar la caracterización de los elementos de este conjunto a partir de sus divisores. Adicionalmente se busca que los estudiantes identifiquen la diferencia entre ser primo en esta estructura algebraica y en el conjunto de los números naturales.

Actividad 1: La relación de divisibilidad en subconjuntos de $\mathbb{Z}$

Con el ánimo de *analizar* matemáticamente la relación de *divisibilidad* y sus implicaciones, proponemos estudiar tal relación en conjuntos diferentes a los usuales pero tomándolos como referencia, esto es, la divisibilidad tanto en los número naturales como en los enteros. En este primer taller y con el fin de no ir a conjuntos muy abstractos, consideraremos tal estudio en subconjuntos de los números enteros.

Los conjuntos sobre los cuales trabajaremos son de la forma:

$$A_a = \{x \in \mathbb{Z} \mid x = ak + 1 \wedge k \in \mathbb{Z}\},$$

donde a es un entero cualquiera. A continuación, responda las preguntas que se formulan.

1. Determine la veracidad de las siguientes afirmaciones:

   (a) $7 \in A_3$ (b) $6 \in A_5$ (c) $-1 \in A_3$ (d) $7 \in A_6$ (e) $79 \in A_3$
   (f) $9 \in A_7$ (g) $-6 \in A_5$ (h) $-1 \in A_2$ (i) $99 \in A_8$ (j) $347 \in A_8$

2. Considere el conjunto A_3 y responda lo siguiente:
   a) Haga un listado de elementos de A_3.
   b) ¿La multiplicación de elementos de A_3 pertenece a A_3? Explique.
   c) ¿Se puede caracterizar los elementos de A_3 a través de sus cifras? Explique.

3. Responda a las mismas preguntas del ítem anterior pero ahora en A_5.

4. Sean x, y elementos de A_a, ¿está xy en A_a? Demuestre su respuesta.

5. Sean x, y elementos de A_a, ¿está $x + y$ en A_a? Justifique su respuesta.

6. Responda las siguientes preguntas:
   a) ¿Para cuáles valores de a, $1 \in A_a$? Explique.
   b) ¿Para cuáles valores de a, $13 \in A_a$? Explique.
   c) ¿Para cuáles valores de a, $15 \in A_a$? Explique.
   d) ¿Para cuáles valores de a, $-1 \in A_a$? Explique.
   e) ¿Para cuáles valores de a, $-8 \in A_a$? Explique.
   f) Con base en los ítemes anteriores, dado un entero m ¿para cuáles valores de a, $m \in A_a$? Justifique su respuesta.

7. Sea m un entero, ¿para cuáles valores de a, tanto m como $-m$ están en A_a? Explique y procure una demostración.

Atendiendo a los objetivos anteriormente propuestos, con estas preguntas se prentende que los estudiantes hagan un reconocimiento de las características propias del conjunto, en particular con lo que tiene que ver con el comportamiento de sus elementos y la manera de caracterizarlos, ya que esto les brindará herramientas para la exploración que se propondrá posteriormente. Adicionalmente, se busca que los estudiantes evidencien que la suma no es cerrada, mientras que la multiplicación si, lo cual permitirá continuar con la siguiente parte

del taller:

Como en los casos usuales, definimos la relación de *divisibilidad* entre elementos de A_a de la siguiente manera:

`Definición.` *Sea a un entero fijo. Para todo $x, y \in A_a$ se dice que x* ***divide*** *a y, y lo notamos $x \mid y$, si y solo si, existe $z \in A_a$ tal que $xz = y$.*

1. Con base en esta definición responda, justificando sus respuestas, a las siguientes preguntas.
   a) ¿La relación de divisibilidad es reflexiva en A_a?
   b) ¿La relación de divisibilidad es transitiva en A_a?
   c) ¿La relación de divisibilidad es antisimétrica en A_a?
   d) Compare sus demostraciones o contraejemplos a las preguntas anteriores, según el caso, con las propiedades de divisibilidad en $\mathbb{N}$ y $\mathbb{Z}$.

Con estas preguntas se pretende que el estudiante evidencie las propiedades que cumple la relación de divisibilidad definida en este conjunto, y así mismo establezca semejanzas y diferencias entre estas y las que cumple la misma relación definida en el conjunto de los números naturales y de los números enteros, teniendo en cuenta las propiedades de la multiplicación en A_a que se heredan de la multiplicación en $\mathbb{Z}$.

2. Con el fin de analizar la cantidad de divisores de elementos de A_5, complete una tabla como la siguiente

n	Divisores de n
6	
-4	
16	
121	
-24	
56	

3. Con base en lo encontrado en el punto anterior, complete la siguiente tabla:

No. de Divisores	Elementos de A_5
1	
2	
3	
4	

Ahora bien, teniendo en cuenta los resultados anteriores, ¿cómo definiría número primo en A_5?

4. Haga un estudio similar para A_8 y para otros casos particulares. Con base en lo que ha visto proponga una definición de número primo en A_a. ¿Servirá la misma definición para todos los valores de a? ¿Existe algún(os) valor(es) de a en los que es necesaria una definición distinta? Explique.

5. Desde la definición dada de número primo en A_5:

   a) Si un elemento que pertenece a A_5 es primo en $\mathbb{Z}$, ¿será primo en A_5? Explore algunos casos particulares.

   b) ¿Existe algún número primo en A_5 que no sea primo en $\mathbb{Z}$? Explique.

Como ya se dijo anteriormente, uno de los propósitos de la actividad es construir una definición de número primo para esta estructura algebraica, para lo cual se propone que los estudiantes hagan una exploración alrededor de la cantidad de divisores de los elementos del conjunto para, tomando como referencia el conjunto de los números naturales, llegar a definir número primo como aquellos que tienen la segunda menor cantidad de divisores, es decir, dos divisores, aludiendo además al hecho que uno no se considera número primo por no ser útil para la descomposición.

Además de la actividad anteriormente descrita, a continuación se muestra otra actividad que tiene como propósito, esencialmente, explorar la descomposición en factores primos en A_5 en aras de evidenciar que no se tiene, en esta estructura, la unicidad de la misma, pero en general si se tiene su existencia. Adicionalmente se pretende que los estudiantes evidencien que la existencia de diccha descomposición, así como la cantidad de ellas depende de la factorización del elemento en $\mathbb{Z}$ tal como se mostró en capítulos anteriores de este trabajo:

Actividad 2: La relación de descomposición en subconjuntos de $\mathbb{Z}$

Teniendo en cuenta que ya se inició un trabajo relacionado con el estudio de la relación de divisibilidad y de la noción de número primo en el subconjunto de los enteros A_5, el presente taller tiene como objetivo hacer algunas exploraciones relacionadas con la descomposición en factores primos en dicho conjunto, en lo que tiene que ver con la existencia y la unicidad de la misma para los diferentes elementos del conjunto. Con base en la definición de número primo que se tiene para A_5 algunos de ellos son los siguientes:

$$P = \{\ldots, -34, -29, -19, -14, -9, -4, 6, 11, 21, 26, 31, 41, \ldots\}$$

1. Descomponga los siguientes números, si es posible, como producto de números primos en A_5.

Elemento de A_5	**Descomposición**
66	
-44	
-209	
341	
156	
-31104	

¿Cuáles números de A_5 tienen la misma descomposición que en $\mathbb{Z}$? Justifique.

2. Complete la tabla siguiente:

Elemento de A_5	**Descomposición en A_5**	**Cantidad de factores**	**Descomposición en $\mathbb{Z}$**	**Cantidad de factores**
66				
-44				
-209				
341				
156				
-31104				

Con base en los datos de la tabla responda:

a. ¿Existe algún número en A_5 que tenga la misma cantidad de factores primos en A_5 en su descomposición que en la de $\mathbb{Z}$? Explique.

b. ¿Existe algún número en A_5 que tenga un mayor número de factores primos en A_5 en su descomposición que en la de $\mathbb{Z}$? Explique.

c. ¿Existe algún número en A_5 que tenga un menor número de factores primos en A_5 en su descomposición que en la de $\mathbb{Z}$? Explique.

d. De lo anterior, ¿es posible concluir que todo número en A_5 se puede descomponer en factores primos de A_5? Justifique su respuesta.

Con estas primeras preguntas se busca que los estudiantes hagan un reconocimiento de los números primos en A_5 con base en la definición obtenida durante la solución de la actividad anterior, y adicionalmente sospechen que, en general, se tiene la existencia de por lo menos una descomposición en factores primos para cada uno de los elementos del conjunto, y además que empiecen a evidenciar quue existe relación entre esta y la factorización del elemento en el conjunto de los números enteros.

3. Considere el número 186 que pertenece a A_5 y su descomposición en factores primos en $\mathbb{Z}$ es:

$$186 = 2 \times 3 \times 31$$

y esta puede verse como:

$$186 = 6 \times 31$$

$$186 = 62 \times 3$$

$$186 = 93 \times 2$$

¿En alguno de estos productos hay elementos de A_5? De ser así, ¿son primos en este conjunto?

4. Haga el mismo procedimiento del punto anterior, pero para el número -31104. ¿Cuantas descomposiciones en factores primos tiene este número en A_5?

5. Teniendo en cuenta el razonamiento de los dos puntos anteriores, si $a \in A_5$ y $a = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_n^{\alpha_n}$ la descomposición en factores primos de a en $\mathbb{Z}$ con la condición de que $p_1, p_2, p_3, \ldots, p_n \in A_5$, ¿cuántas descomposiciones de este elemento se puede encontrar en A_5? Explique.

Con este grupo de preguntas se busca que los estudiantes evidencien que las descomposiciones en factores primos de elementos de A_5 surgen a partir de la factorización del número en

los números enteros, y adicionalmente se propone, como un primer caso, el hecho que en el caso que la descomposición en $\mathbb{Z}$ sirva en A_5 (los primos en $\mathbb{Z}$ esten en A_5) hacen que esta sea única.

6. Si p es un número primo en $\mathbb{Z}$ tal que $p \notin A_5$, verifique, con algunos ejemplos, si:
   a. $p^2 \in A_5$
   b. $p^3 \in A_5$
   c. $p^4 \in A_5$
   d. $p^5 \in A_5$

   Si algunas de las anteriores afirmaciones son ciertas, ¿el elemento en cuestión será primo en este conjunto? Procure generalizar.

7. Teniendo en cuenta el razonamiento hecho en los puntos anteriores, si p y q son primos en $\mathbb{Z}$ y $p, q \notin A_5$, ¿se puede concluir que $pq \in A_5$, y si es así, ¿este será primo en este conjunto? Justifique su respuesta.

8. Con base en la respuesta dada en los dos últimos puntos, si $a \in A_5$ y la descomposición de él en $\mathbb{Z}$ es $a = p_1^6 p_2^8$ y $p_1, p_2 \notin A_5$, ¿cuántas descomposiciones tendrá este elemento en A_5? Justifique su respuesta.

9. Responda la pregunta del punto anterior para los siguientes elementos:
   a. $a = p_1^4 p_2^{10}$
   b. $a = p_1^2 p_2^6$

   Procure una generalización.

10. Siguiendo el mismo razonamiento, proponga la cantidad de descomposiciones que tendrá un número de la forma $a = p_1^{\alpha_1} p_2^{\alpha_2}$ con α_1 y α_2 números impares.

11. Ahora, busque la cantidad de descomposiciones de los siguientes elementos de A_5:
    a. $a = p_1^7 p_2^{10}$
    b. $a = p_1^9 p_2^5$

    Bajo el supuesto de que $p_1 \in A_5$ y $p_2 \notin A_5$. Procure una generalización.

12. Finalmente, con base en el punto anterior, proponga una conjetura con respecto a la cantidad de descomposiciones de $a \in A_5$ cuya descomposición en $\mathbb{Z}$ es $a = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_n^{\alpha_n}$ y solo $p_n^{\alpha_n} \notin A_5$

Con estas preguntas se busca que los estudiantes evidencien el hecho que multiplicar dos números primos en $\mathbb{Z}$ da como resultado un elemento de A_5, y además que vean esto como

una herramienta para obtener variadas descomposiciones en A_5 y así mismo lo usen como una herramienta para obtener la cantidad de factorizaciones en algunos casos particulares.

7. Conclusiones, reflexiones y recomendaciones

Teniendo en cuenta lo desarrollado en el transcurso del presente trabajo de grado se pueden hacer las siguientes afirmaciones a manera de conclusión:

1. Teniendo en cuenta el estudio desarrollado en los ideales de los números enteros se puede concluir que, en primera medida, allí se encuentra una idea pura de elemento especial para la descomposición (elemento irreducible) en la medida que hay números que son imposibles de descomponer en la medida que no tienen divisores. Por otra parte, también se evidenció que no es posible hablar de un teorema análogo al teorema fundamental de la aritmética en esta estructura dado que se tiene la existencia de la descomposición en factores primos, pero no la unicidad de la misma.

2. En lo que tiene que ver con los números de la forma $ak + 1$ se definió la relación de descomposición haciendo uso de la multiplicación de los números enteros y a partir de ella se concluyó que se tiene que la existencia de la descomposición en factores primos, pero no se tiene la unicidad de la misma imposibilitando, nuevamente, la formulación de un teorema fundamental de la aritmética en este conjunto.

3. Con base en el estudio desarrollado se puede concluir que la idea de número primo está supeditada, estrechamente, a la búsqueda de la existencia de la descomposición en la medida que, en los casos explorados se dieron definiciones distintas de número primo en aras de garantizar la existencia de la descomposición en términos de elementos que resultan ser, además, irreducibles en la medida que no se pueden escribir como producto de otros elementos del conjunto salvo algunos casos triviales.

Por otra parte, como producto del desarrollo del presente trabajo de grado se puede decir que sirvió como una manera de ver que toma una gran importancia el desarrollo de actividad matemática por parte de futuros licenciados en Matemáticas en la medida que, primero, esto brinda herramientas para obtener un mayor conocimiento matemático que se configura en una herramienta esencial para el buen desarrollo de la labor docente; y segundo, porque brinda herramientas para generar cuestionamientos que pueden llevar a los estudiantes al desarrollo de actividad matemática en el aula, es decir, a la formulación y demostración de resultados, apuntando a que se desarrolle una microsociedad científica en el aula como herramienta para la construcción de conocimiento de forma tanto individual como colectiva.

Finalmente, también se vió en el desarrollo de este trabajo de grado que surgieron una serie de problemas de conteo a la hora de intentar caracterizar la cantidad de descomposiciones de los elementos de cada uno de los conjuntos estudiados, por lo tanto, una manera de darle continuidad al mismo es buscar una solución para estos. Adicionalmente, también se vió que para los conjuntos A_a solo se estudiaron algunos casos, de ahí que aún hay infinitos conjuntos por estudiar para darle continuidad al trabajo aqui iniciado.

8. Bibliografía

- Apostol, T. (1984). *Introducción a la teoría analítica de números.* España: Editorial Reverté S.A.
- Ash, R. (2007) *Basic Abstract Algebra. For Graduate Students and Advanced Undergraduates* United States of America: Dover Publications Inc.
- Fernandez P. y Fernandez J. (2008). *El discreto encanto de la Matemática.* España: Universidad Autonoma de Madrid.
- Ivorra, C. (s.f.). *Álgebra.* Valencia.
- Ivorra, C. (s.f.). *Teoría de números.* Valencia.
- Jiménez, R., Gordillo , E., y Rubiano, G. (2004). *Teoría de números (para principiantes).* Bogotá: Universidad Nacional de Colombia.
- Le Veque, W. (1962). *Teoría elemental de números.* Massachusetts: Addison-Wesley.
- Luque , C., Paez, J., y Mora , L. (2002). *Actividades matemáticas para el desarrollo de procesos lógicos.* Bogotá: Ediciones Antropos.
- Luque Arias, C. J., Mora Mendieta, L. C., y Torres Diaz, J. A. (2006). *Estructuras análogas a los números reales.* Bogotá: Universidad Pedagógica Nacional.
- Luque, C., Jimenez, H., y Angel, J. L. (2013). *Actividades matemáticas para el desarrollo de procesos lógicos: Representar estructuras algebraicas finitas y enumerables.* Bogotá: Universidad Pedagógica Nacional.
- Luque, C., Mora, L., y Torres, J. (2005). *Actividades matemáticas para el desarrollo de procesos lógicos: Clasificar, medir e invertir.* Bogotá: Universidad Pedagógica Nacional.
- Luque, C., Sánchez, Y., y Ángel, J. L. (2014). El proceso matemático de analizar en la Teoría de Números: Una aproximación desde la relación de divisibilidad. *XII Coloquio regional de Matemáticas y II Simposio de Estadística.* San Juan de Pasto: Universidad de Nariño.

A. Anexo 1: Actividad relación de divisibilidad y descomposición en los ideales de $\mathbb{Z}$

La relación de divisibilidad en los conjuntos $k\mathbb{Z}$

Teniendo en cuenta que una de las maneras de estudiar el proceso de analizar es a través de definir una relación de divisibilidad en una estructura algebraica, en este taller se propone que se desarrolle esto en algunos conjuntos numéricos: Los ideales de los números enteros; los cuales, recordemos, son la siguiente familia de conjuntos:

$$k\mathbb{Z} = \{x \in \mathbb{Z} | x = km, m \in \mathbb{Z}\}$$

donde k es un entero cualquiera. Con base en esto, responda las siguientes preguntas:

1. Haga un listado de algunos elementos de $2\mathbb{Z}$ y responda:
   a. ¿La suma de elementos de $2\mathbb{Z}$ pertenece a $2\mathbb{Z}$? Justifique.
   b. ¿La multiplicación de elementos de $2\mathbb{Z}$ pertenece a $2\mathbb{Z}$? Justifique.
2. Responda las mismas preguntas del punto anterior pero con $3\mathbb{Z}$
3. Si $x, y \in k\mathbb{Z}$, ¿se cumple que $x + y \in k\mathbb{Z}$? Demuestre se respuesta.
4. Si $x, y \in k\mathbb{Z}$, ¿se cumple que $xy \in k\mathbb{Z}$? Demuestre se respuesta.
5. ¿Para cuales valores de k se cumple que $1 \in k\mathbb{Z}$?
6. ¿Para cuales valores de k se cumple que $-1 \in k\mathbb{Z}$?

Teniendo en cuenta que la multiplicación se puede definir, igual que en los casos usuales, la relación de divisibilidad en la siguiente forma:

Definición: Sea $x, y \in k\mathbb{Z}$ se dice que $a|b$ si y solo si existe $c \in k\mathbb{Z}$ tal que $ac = b$.

14. Teniendo en cuenta la definición, para cada una de las siguientes preguntas, si la respuesta es afirmativa demuestre su respuesta, en caso contrario, explique:

a. ¿La relación de divisibilidad es reflexiva en $k\mathbb{Z}$?

b. ¿La relación de divisibilidad es asimétrica en $k\mathbb{Z}$?

c. ¿La relación de divisibilidad es transitiva en $k\mathbb{Z}$?

15. Teniendo en cuenta la definición de la relación de divisibilidad, contruya el diagrama de Hasse de la misma para el caso $2\mathbb{Z}$ y con base en él, responda, justificando sus respuestas:

    a. ¿Existen elementos que no tengan divisores? Si es así, de una fórmula para encontrarlos.

    b. ¿Cuáles elementos tienen dos divisores?

    c. ¿Existe alguna fórmula que permita encontrar los números que tengan cuatro divisores? ¿Qué tengan 6? ¿Qué tengan 8?

    d. ¿Existe algún número con una cantidad impar de divisores?

16. Construya el diagrama de Hasse y responda preguntas similares para los casos de $3\mathbb{Z}$ y $4\mathbb{Z}$. Procure generalizar para cualquier $k\mathbb{Z}$ los resultados obtenidos.

17. Con base en los resultados vistos hasta ahora, ¿como definiría número primo en $k\mathbb{Z}$? Con base en esta definición, ¿existe una fórmula que permita encontrar números primos en este conjunto.

18. ¿Existe algún número que sea primo en $k\mathbb{Z}$ que también sea primo en $\mathbb{Z}$. Justifique su respuesta

B. Anexo 2: Actividades relación de divisibilidad y descomposición en los números de la forma $ak + 1$

Actividad 1: La relación de divisibilidad en subconjuntos de $\mathbb{Z}$

Con el ánimo de *analizar* matemáticamente la relación de *divisibilidad* y sus implicaciones, proponemos estudiar tal relación en conjuntos diferentes a los usuales pero tomándolos como referencia, esto es, la divisibilidad tanto en los número naturales como en los enteros. En este primer taller y con el fin de no ir a conjuntos muy abstractos, consideraremos tal estudio en subconjuntos de los números enteros.

Los conjuntos sobre los cuales trabajaremos son de la forma:

$$A_a = \{x \in \mathbb{Z} \mid x = ak + 1 \wedge k \in \mathbb{Z}\},$$

donde a es un entero cualquiera. A continuación, responda las preguntas que se formulan.

1. Determine la veracidad de las siguientes afirmaciones:

   (a) $7 \in A_3$ (b) $6 \in A_5$ (c) $-1 \in A_3$ (d) $7 \in A_6$ (e) $79 \in A_3$
   (f) $9 \in A_7$ (g) $-6 \in A_5$ (h) $-1 \in A_2$ (i) $99 \in A_8$ (j) $347 \in A_8$

2. Considere el conjunto A_3 y responda lo siguiente:
   a) Haga un listado de elementos de A_3.
   b) ¿La multiplicación de elementos de A_3 pertenece a A_3? Explique.
   c) ¿Se puede caracterizar los elementos de A_3 a través de sus cifras? Explique.

3. Responda a las mismas preguntas del ítem anterior pero ahora en A_5.

4. Sean x, y elementos de A_a, ¿está xy en A_a? Demuestre su respuesta.

5. Sean x, y elementos de A_a, ¿está $x + y$ en A_a? Justifique su respuesta.

6. Responda las siguientes preguntas:
   a) ¿Para cuáles valores de a, $1 \in A_a$? Explique.
   b) ¿Para cuáles valores de a, $13 \in A_a$? Explique.
   c) ¿Para cuáles valores de a, $15 \in A_a$? Explique.
   d) ¿Para cuáles valores de a, $-1 \in A_a$? Explique.
   e) ¿Para cuáles valores de a, $-8 \in A_a$? Explique.
   f) Con base en los ítemes anteriores, dado un entero m ¿para cuáles valores de a, $m \in A_a$? Justifique su respuesta.

7. Sea m un entero, ¿para cuáles valores de a, tanto m como $-m$ están en A_a? Explique y procure una demostración.

Con estas preguntas se prentende que los estudiantes hagan un reconocimiento de las características propias del conjunto, en particular con lo que tiene que ver con el comportamiento de sus elementos y la manera de caracterizarlos. Adicionalmente, se busca que los estudiantes evidencien que la suma no es cerrada, mientras que la multiplicación si, lo cual permitirá continuar con la siguiente parte del taller:

Como en los casos usuales, definimos la relación de *divisibilidad* entre elementos de A_a de la siguiente manera:

`Definición.` *Sea a un entero fijo. Para todo $x, y \in A_a$ se dice que x* ***divide*** *a y, y lo notamos $x \mid y$, si y solo si, existe $z \in A_a$ tal que $xz = y$.*

1. Con base en esta definición responda, justificando sus respuestas, a las siguientes preguntas.
   a) ¿La relación de divisibilidad es reflexiva en A_a?
   b) ¿La relación de divisibilidad es transitiva en A_a?
   c) ¿La relación de divisibilidad es antisimétrica en A_a?
   d) Compare sus demostraciones o contraejemplos a las preguntas anteriores, según el caso, con las propiedades de divisibilidad en $\mathbb{N}$ y $\mathbb{Z}$.

Con estas preguntas se pretende que el estudiante evidencie las propiedades que cumple la relación de divisibilidad definida en este conjunto, y así mismo establezca semejanzas y diferencias entre estas y las que cumple la misma relación definida en el conjunto de los números naturales y de los números enteros.

2. Con el fin de analizar la cantidad de divisores de elementos de A_5, complete una tabla como la siguiente

n	Divisores de n
6	
-4	
16	
121	
-24	
56	

3. Con base en lo encontrado en el punto anterior, complete la siguiente tabla:

No. de Divisores	Elementos de A_5
1	
2	
3	
4	

   Ahora bien, teniendo en cuanta los resultados anteriores, ¿cómo definiría número primo en A_5?

4. Haga un estudio similar para A_8 y para otros casos particulares. Con base en lo que ha visto proponga una definición de número primo en A_a. ¿Servirá la misma definición para todos los valores de a? ¿Existe algún(os) valor(es) de a en los que es necesaria una definición distinta? Explique.

5. Desde la definición dada de número primo en A_5:
   a) Si un elemento que pertenece a A_5 es primo en $\mathbb{Z}$, ¿será primo en A_5? Explore algunos casos particulares.
   b) ¿Existe algún número primo en A_5 que no sea primo en $\mathbb{Z}$? Explique.

Actividad 2: La relación de descomposición en subconjuntos de $\mathbb{Z}$

Teniendo en cuenta que ya se inició un trabajo relacionado con el estudio de la relación de divisibilidad y de la noción de número primo en el subconjunto de los enteros A_5, el presente taller tiene como objetivo hacer algunas exploraciones relacionadas con la descomposición en factores primos en dicho conjunto, en lo que tiene que ver con la existencia y la unicidad de la misma para los diferentes elementos del conjunto. Con base en la definición de número primo que se tiene para A_5 algunos de ellos son los siguientes:

$$P = \{\ldots, -34, -29, -19, -14, -9, -4, 6, 11, 21, 26, 31, 41, \ldots\}$$

1. Descomponga los siguientes números, si es posible, como producto de números primos en A_5.

Elemento de A_5	**Descomposición**
66	
-44	
-209	
341	
156	
-31104	

¿Cuáles números de A_5 tienen la misma descomposición que en $\mathbb{Z}$? Justifique.

2. Complete la tabla siguiente:

Elemento de A_5	**Descomposición en A_5**	**Cantidad de factores**	**Descomposición en $\mathbb{Z}$**	**Cantidad de factores**
66				
-44				
-209				
341				
156				
-31104				

Con base en los datos de la tabla responda:

a. ¿Existe algún número en A_5 que tenga la misma cantidad de factores primos en A_5 en su descomposición que en la de $\mathbb{Z}$? Explique.

b. ¿Existe algún número en A_5 que tenga un mayor número de factores primos en A_5 en su descomposición que en la de $\mathbb{Z}$? Explique.

c. ¿Existe algún número en A_5 que tenga un menor número de factores primos en A_5 en su descomposición que en la de $\mathbb{Z}$? Explique.

d. De lo anterior, ¿es posible concluir que todo número en A_5 se puede descomponer en factores primos de A_5? Justifique su respuesta.

3. Considere el número 186 que pertenece a A_5 y su descomposición en factores primos en $\mathbb{Z}$ es:

$$186 = 2 \times 3 \times 31$$

y esta puede verse como:

$$186 = 6 \times 31$$

$$186 = 62 \times 3$$

$$186 = 93 \times 2$$

¿En alguno de estos productos hay elementos de A_5? De ser así, ¿son primos en este conjunto?

4. Haga el mismo procedimiento del punto anterior, pero para el número -31104. ¿Cuantas descomposiciones en factores primos tiene este número en A_5?

5. Teniendo en cuenta el razonamiento de los dos puntos anteriores, si $a \in A_5$ y $a = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_n^{\alpha_n}$ la descomposición en factores primos de a en $\mathbb{Z}$ con la condición de que $p_1, p_2, p_3, \ldots, p_n \in A_5$, ¿cuántas descomposiciones de este elemento se puede encontrar en A_5? Explique.

6. Si p es un número primo en $\mathbb{Z}$ tal que $p \notin A_5$, verifique, con algunos ejemplos, si:

a. $p^2 \in A_5$

b. $p^3 \in A_5$

c. $p^4 \in A_5$

d. $p^5 \in A_5$

Si algunas de las anteriores afirmaciones son ciertas, ¿el elemento en cuestión será primo en este conjunto? Procure generalizar.

7. Teniendo en cuenta el razonamiento hecho en los puntos anteriores, si p y q son primos en $\mathbb{Z}$ y $p, q \notin A_5$, ¿se puede concluir que $pq \in A_5$, y si es así, ¿este será primo en este conjunto? Justifique su respuesta.

8. Con base en la respuesta dada en los dos últimos puntos, si $a \in A_5$ y la descomposición de él en $\mathbb{Z}$ es $a = p_1^6 p_2^8$ y $p_1, p_2 \notin A_5$, ¿cuántas descomposiciones tendrá este elemento en A_5? Justifique su respuesta.

9. Responda la pregunta del punto anterior para los siguientes elementos:

   a. $a = p_1^4 p_2^{10}$

   b. $a = p_1^2 p_2^6$

   Procure una generalización.

10. Siguiendo el mismo razonamiento, proponga la cantidad de descomposiciones que tendrá un número de la forma $a = p_1^{\alpha_1} p_2^{\alpha_2}$ con α_1 y α_2 números impares.

11. Ahora, busque la cantidad de descomposiciones de los siguientes elementos de A_5:

    a. $a = p_1^7 p_2^{10}$

    b. $a = p_1^9 p_2^5$

    Bajo el supuesto de que $p_1 \in A_5$ y $p_2 \notin A_5$. Procure una generalización.

12. Finalmente, con base en el punto anterior, proponga una conjetura con respecto a la cantidad de descomposiciones de $a \in A_5$ cuya descomposición en $\mathbb{Z}$ es $a = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_n^{\alpha_n}$ y solo $p_n^{\alpha_n} \notin A_5$

Este es un trabajo apenas iniciado, aún hay un gran camino por explorar.