# Estudio de divisibilidad en estructuras análogas a los números de Minkowski

**Julián Alfonso Tibavizco Boada**

**CC: 1022383743**

**Código: 2011140071**

**Trabajo de grado presentado como requisito parcial para optar por el título de licenciado en matemáticas**

**Modalidad: Asociado a un grupo de investigación**

**Asesor**

**William Jiménez Gómez**

**Docente Universidad Pedagógica Nacional**

**Firma del Asesor**

_____

**Universidad Pedagógica Nacional**

**Facultad de Ciencia y Tecnología**

**Departamento de Matemáticas**

**Bogotá D.C, Julio de 2016**

## RESUMEN ANALÍTICO EN EDUCACIÓN - RAE

| 1. Información General | |
|---|---|
| **Tipo de documento** | Trabajo de grado para optar por el título de licenciado en matemáticas |
| **Acceso al documento** | Universidad Pedagógica Nacional. Biblioteca Central |
| **Titulo del documento** | Estudio de divisibilidad en estructuras análogas a los números de Minkowski |
| **Autor(es)** | Tibavizco Boada, Julián Alfonso |
| **Director** | Jiménez Gómez, William |
| **Publicación** | Bogotá. Universidad Pedagógica Nacional, 2016.177 p. |
| **Unidad Patrocinante** | Universidad Pedagógica Nacional |
| **Palabras Claves** | TEORIA DE NÚMEROS; NÚMEROS DE MINKOWSKI;DIVISIBILIDAD EN ANILLOS, |

| 2. Descripción |
|---|
| Trabajo de grado que se propone ser una herramienta de referencia y estudio para los estudiantes de teoría de números en la Universidad Pedagógica Nacional, surge del trabajo del grupo de Algebra de la universidad en los seminarios de algebra. El conjunto de los números de Minkowski $M = \{a + bi : i^2 = 1, a, b \in \mathbb{Z}, i \neq \pm 1\}$ es un conjunto similar a los enteros gaussianos en su definición que cumple una propiedad especial, existen raíces de $i^2$ en los enteros. De forma similar a como se define este conjunto, se define en este trabajo una familia de conjuntos que cumplen la misma propiedad $M(i^2) = \{a + bi : i^2 = c^2, a, b, c \in \mathbb{Z}, i \neq \pm c\}$, en base a esto se estudian las propiedades en generales que se pueden deducir de estos conjuntos y principalmente se estudia la relación de divisibilidad y sus elementos, esto para intentar responder a la pregunta ¿Hay un teorema análogo al teorema fundamental de la aritmética en la teoría sobre estos conjuntos?. |

| 3. Fuentes |
|---|
| Arrondo, E. (2009). *Apuntes de Teoría de Números.* Universidad Complutense de Madrid, Madrid. Recuperado el Mayo de 2016, de http://www.mat.ucm.es/~arrondo/ten.pdf |

Brausín, M., & Pérez, A. (2012). *Estudio de Congruencias en Números Gussianos Duales.* Trabajo de grado, Universidad Pedagógica Nacional.

Busqué, C., Saorín, M., & Simón, J. (2011-2012). *Curso de Conjuntos y números.Guiones de clase.* Recuperado el 4 de Junio de 2016, de http://www.um.es/docencia/jsimon/depmat/2011-2012/CyN/GuionesdeClase.pdf

*CALCULUS, One Variable- Calculus, with an introduction to Linear Algebra* (Vol. 1). (1984). Barcelona-España: REVERTÉ, S.A.

Gonzáles, F. (2004). *Apuntes de Matemática Discreta-11.Teorema Fundamental de la Aritmética.* Andalucía. Recuperado el Noviembre de 2015, de http://www2.uca.es/matematicas/Docencia/ESI/1710003/Apuntes/Leccion11.pdf

Ivorra, C. (2011). *Teoría de Números.* Valencia, España. Recuperado el Septiembre de 2015, de https://www.uv.es/ivorra/Libros/Numeros.pdf

LeVeque, W. (1968). *Teoría Elemental de los Números.* Universidad de Michigan . México: Herrero Hermanos, Sucs, S.A.

Rubiano, G., Jiménez, L., & Rubiano, G. (2004). *Teoría de Números para principìantes* (2 ed.). (B. Jiménez, & J. Gordillo, Edits.) Bogotá D.C, Colombia : Universidad Nacional de Colombia. Recuperado el Diciembre de 2015, de http://ciencias.uis.edu.co/conjuntos/doc/Tmerospaprinci.pdf

Sanchez, Y., Angel, L., & Luque, C. (2013). *¿Son necesarios los enteros para demostrar el Teorema Fundamental de la Aritmetica?* Bogotá D.C.

Urbina, L. (2006). *Notas en Desigualdades.* Asociación Venezolana de Competencias en Matemáticas(ACM), Venezuela. Recuperado el 16 de Abril de 2016, de http://www.acm.ciens.ucv.ve/main/entrenamiento/material/desigualdades_urbina.pdf

## 4. Contenidos

El presente trabajo consta de 6 capítulos: el capítulo 1 denota los objetivos y la justificación del trabajo además de una breve descripción del surgimiento de la idea de estudiar teoría de números en conjuntos poco usuales, el capítulo 2 organiza varios resultados de la teoría de números enteros que dan validez y sustento al estudio realizado y además se referencia un camino seguido para la construcción del TFA en los números naturales, en el capítulo 3 se abordan por primera vez las estructuras no usuales definidas similarmente a los números de Minkowski, el capítulo trata de las propiedades algebraicas de estas estructuras, en el capítulo 4 se define la relación de divisibilidad y se hace una exploración de sus propiedades y de las ideas de primo y compuesto en estos conjuntos, en el capítulo 5 se compara el camino referenciado en el capítulo 2 con teoremas homólogos en estas estructuras, se trata de contrastar entre estos

teoremas y finalmente en el capítulo 6 se encuentra el código fuente y las descripciones de varios programas en Matlab que fueron útiles para la deducción de propiedades de los números dentro de las estructuras de estudio.

## 5. Metodología

Se realizaron 1-2 horas de trabajo semanal con el profesor asesor William Jiménez Gómez, se llevó a cabo trabajo independiente semanal por parte del autor y en las sesiones de asesoría se presentaron avances periódicamente, se discutieron semana a semana los resultados encontrados con el fin de mejorarlos o refutarlos y se eligieron los más relevantes para la elaboración de este documento. Se revisaron documentos relativos a teoría de números enteros, teoría de números naturales, teoría de números algebraicos, teoría de números gaussianos duales, teoría de números de Minkowski, relaciones de orden en el cálculo y teoría de conjuntos. Se eligieron dentro de los elementos de la bibliografía, los más trascendentes para contribuir a un estudio de la divisibilidad en nuevas estructuras y el autor interpreto cada elemento adaptándolo a los conjuntos $M(i^2)$.

## 6. Conclusiones

En los conjuntos $M(i^2)$ se tienen divisores de (0,0), lo cual provoca que varios teoremas que se tienen en los dominios de integridad no se cumplan en estos conjuntos, como el Teorema de Bézout y el Lema de Euclides necesarios para demostrar el TFA-unicidad.

En $M(i^2)$ se se cumple una versión del TFA(existencia) pero no del TFA(unicidad).

No se pueden definir relaciones de orden total definiendo números $M(i^2)$ −positivos, y no es posible definir una relación de orden que cumpla la tricotomía usar y sea total.

Las relaciones ‘menor que’ y de divisibilidad son preordenes y determinan en el conjunto relaciones de equivalencia que cuando se hace el paso al conjunto cociente determinan dos conjuntos isomorfos a números naturales y enteros respectivamente.

Aunque se cumplen la mayoría de los teoremas necesarios para construir el TFA en $M(i^2)$, la existencia de divisores de (0,0) no permite concluir el resto de ellos, uno de los mayores problemas de esto fueron aquellos que dependen del residuo del algoritmo de la división de $M(i^2)$.

Se lograron varios métodos de descomposición de números, uno que determina descomposiciones válidas para cualquier conjunto sin depender del valor de $i^2$ y otras que requieren un análisis de la norma del número.

Como definimos los conjuntos $M(i^2)$, con $i^2 = r^2, r \in \mathbb{Z}, i \neq \pm r$ nos lleva a implícitamente aceptar para que se cumpla $i \neq \pm r$ que existe un nuevo elemento $x$ tal que $x^2 = 1, x \neq \pm 1$, confirmamos que se desarrolló en este trabajo teoría de números en conjuntos isomorfos a los números de Minkowski, es decir todo conjunto $M(i^2), i^2 \neq 0,$ es en realidad una representación de $M(1)$.

| | |
|---|---|
| **Elaborado por:** | Tibavizco Boada, Julián Alfonso |
| **Revisado por:** | Jiménez Gómez, William |

| | | | |
|---|---|---|---|
| **Fecha de elaboración del Resumen:** | 22 | 07 | 2016 |

# Contenido

# 1. Preliminares

## 1.1Introducción

Este trabajo surge en los Seminarios de Algebra de la Licenciatura en Matemáticas en la Universidad Pedagógica Nacional, en ellos se intentaba dar respuesta a cuestiones como ¿Qué es la divisibilidad?, ¿Qué es un numero primo?, ¿Esta idea se mantiene en todos los conjuntos?, ¿Qué elementos nuevos surgen en el estudio de la divisibilidad en varios conjuntos?, ¿Qué son unidades?, ¿Qué son asociados?;para intentar dar una respuesta general a estas preguntas se reunieron elementos de varios trabajos, diversos conjuntos y definiciones y conjeturas ; lo que se muestra en este trabajo es el resultado de una de estas investigaciones correspondiente a conjuntos que siguen la misma idea con que se definen los números gaussianos, es decir con números de la forma $a + bi, a, b \in$ con cada valor de $i^2$ posible, se puede definir una nueva estructura de números, por ejemplo para $i^2 = -1$ los números gaussianos, para $i^2 = 1$ con $i \neq \pm 1$ los números de Minkowski, para $i^2 = 2$, $i^2 = 3, i^2 = 4$ con $i \neq \pm 2$ …etc; en este trabajo se abordan los casos para $i^2 = 1$ con $i \neq \pm 1$, para $i^2 = 4$ con $i \neq \pm 2$, $i^2 = 9$ con $i \neq \pm 3$ y en general cuando $i^2 = c$ con $i \neq \pm \sqrt{c}$ donde $c$ es un número cuadrado perfecto.

Inicialmente como marco referencia, se presentara el ejemplo de estudio de teoría de números en $\mathbb{Z}$, se presentaran varios de los elementos básicos del estudio de la divisibilidad en esta estructura y un camino por el cual se llega a deducir la versión del Teorema Fundamental de la aritmética para esta estructura, la primera sección se tomará como un compilado de elementos que fundamentan el trabajo realizado sobre los nuevos conjuntos numéricos, estos se toman como hechos de la teoría de números enteros por lo cual no se incluyen demostraciones.

En continuación, se presentará el estudio de teoría de números en conjuntos definidos de la forma $a + bi$, iniciando por la definición de estos y un breve estudio de su estructura algebraica, luego se abordara el estudio de la divisibilidad y una exploración para dar

respuesta a la pregunta ¿Se cumple un Teorema análogo al Teorema Fundamental de la Aritmética en estos conjuntos?; se espera que este trabajo sea de utilidad al lector para analizar y resolver problemas similares a los que se enfrentan en un curso usual de teoría de números, que intente buscar similitudes entre lo leído y los ejemplos usuales y que así ideas más completas obre los conceptos básicos del estudio de la divisibilidad.

## 1.2Justificación

Este trabajo de grado se realiza con el fin de elaborar una herramienta de consulta y estudio para estudiantes de teoría de números que les permita abordar conceptos como la divisibilidad desde una perspectiva más amplia a la que se aborda en cursos de introducción a la teoría de números, con ejemplos distintos a los usuales, enfocando el desarrollo de tales conceptos con el proceso de analizar en matemáticas, entendido como descomponer un elemento en términos de otros que lo configuran también tiene como objetivo, además de un documento para optar por el título de licenciado en matemáticas, poner en juego los conocimientos adquiridos en la carrera con énfasis en los cursos de la línea de algebra de la Universidad Pedagógica Nacional, asumiendo el papel de un matemático y explorar, descubrir y argumentar ideas y hechos respecto a la divisibilidad y con este ejercicio contribuir a mi formación continua en matemáticas.

Fue mi interés el abordar la teoría de números y más específicamente la teoría de la divisibilidad a partir de la experiencia que adquirí en los seminarios de Algebra de la Licenciatura en Matemáticas, a partir de la actividad de problematizarse, conjeturar, probar y demostrar varios de los teoremas famosos de la teoría de números, y preguntarme ¿cuál es el significado de estos hechos y conceptos?, ¿por qué funcionan los algoritmos que utilizamos cotidianamente?, ¿que sustenta estos algoritmos? y ¿por qué funcionan de esta manera?, el querer reflexionar sobre todo esto me impulso a trabajar en algunas de las preguntas abiertas que surgían en las sesiones de los seminarios, en particular profundice en la cuestión ¿existirán conjuntos diferentes a los usuales en los cuales se cumpla el teorema fundamental de la aritmética?, ¿Cómo funcionarán los teoremas que estudiamos usualmente en $\mathbb{Z}$ dentro de estos conjuntos?; con base en esto y en mi experiencia en trabajar sobre estas preguntas con el conjunto de los números de Minkowski surgió este trabajo de grado.

Se espera que esta herramienta sirva como punto de referencia para la reflexión de los estudiantes sobre algunos conceptos clásicos de la teoría de números y para incentivarlos a hacer y aprender teoría de números en cualquier conjunto y a crear sus propias ideas y conjeturas y versiones de los teoremas clásicos para contribuir a su comprensión sobre el mundo de las matemáticas.

Los números a tratar en este trabajo se definen de una forma muy similar a la cual se definen los números complejos, son de la forma $a + bi$, con $i^2 = c$, con $i \neq \pm \sqrt{c}, a, b, c \in \mathbb{Z}$ y $c$ un número cuadrado, de esta manera en este documento se trabajará sobre los resultados generales que se pueden obtener sobre varios de los conceptos más famosos de la teoría de números dentro de una familia de conjuntos, un conjunto por cada $c$, y cuando sea necesario se especificara sobre los resultados que son particulares en algún conjunto de la familia, como en los números duales o los números de Minkowski.

Otro caso interesante que se podría sería los conjuntos de números $a + bi$, con $i^2 = c$, con $i \neq \pm \sqrt{c}$, y $c$ un número que no tiene raíz cuadrada en $\mathbb{Z}$, como por ejemplo 2 , 3 o 5, sin embargo estos conjuntos tienen estructura de dominio de integridad y el estudio de teoremas de teoría de números en estos se asemeja mucho más al caso de los números enteros, no obstante se propone al lector que explore para algún valor de $c$ la teoría de números en tal conjunto y haga sus propias suposiciones y conjeturas para ampliar sus esquemas conceptuales en este campo.

## 1.3Objetivos

**General:** Hacer un estudio de varios de los conceptos clave en la teoría de divisibilidad en conjuntos distintos a los números enteros.

**Específicos:**

- Elaborar un documento como requisito para optar por el título de Licenciado en Matemáticas en la Universidad Pedagógica Nacional
- Poner en juego los conocimientos adquiridos en la carrera Licenciatura en matemáticas, para hacer una investigación en el campo de la Teoría de Números, y

asumir el papel de un matemático al descubrir, explorar, conjeturar y demostrar en matemáticas.

- Definir un esquema para poder definir la relación de divisibilidad que sea funcional para cada estructura determinada por un número cuadrado.
- Estudiar la relación de divisibilidad en conjuntos no usuales, deducir las propiedades de sus elementos y determinar cuáles de ellas son generales y cuales dependientes del conjunto
- Determinar si en los conjuntos dados se cumple un análogo al Teorema Fundamental de la Aritmética, de lo contrario determinar las razones por las cuales no se da.

## 2. Marco Teórico: Los números enteros ($\mathbb{Z}$)

En esta sección, como sustento para el estudio de teoría de números en distintos de los usuales se presenta en el conjunto de estudio más referenciado, los números enteros, los hechos que fundamentan la construcción de teoría de números en otros conjuntos, si el lector ya está familiarizado con la teoría de números en $\mathbb{Z}$, (de ser el caso la lectura de esta sección no es estrictamente necesaria para el entendimiento de este trabajo), quizás no encuentre algo desconocido en esta primera parte, pues presentaremos varios de los teoremas y definiciones más conocidas en el estudio de la divisibilidad y una axiomática de $\mathbb{Z}$, se hará mención de tales teoremas sin demostración, pues no es objetivo de este trabajo realizar una exploración de los resultados que se cumplen en los números enteros.

Comenzaremos definiendo el conjunto y listaremos algunas propiedades algebraicas que posee como estructura con 2 operaciones binarias internas, tomaremos como dados algunos resultados de la teoría de conjuntos y abordaremos una relación de orden, se listaran algunos elementos calves que permite la relación de orden, como el principio del buen orden y el algoritmo de la división, los máximos y los mínimos , además se abordaran las propiedades de la norma que se define en los números enteros (el valor absoluto).

En segunda instancia se presentará la relación de divisibilidad y sus propiedades en $\mathbb{Z}$, se mencionará el comportamiento de los elementos importantes en ella, unidades, asociados, numero primo, compuesto, primos relativos entre otros, y la influencia que tiene la norma de $\mathbb{Z}$ en esta relación de divisibilidad, una manera en que se pueden clasificar los números con esta relación como primos, compuestos y unidades, sus propiedades y el Teorema Fundamental de la Aritmética en su versión de los números enteros.

Por último, como introducción al estudio de teoría de números en casos poco conocidos, se referencia un camino que se siguió en el seminario de Algebra (Sanchez, Angel, & Luque, 2013) de la Licenciatura en Matemáticas en la Universidad Pedagógica Nacional, para la construcción de una demostración para el Teorema Fundamental de la Aritmética en los números naturales, en esta sección encontraremos las primeras propiedades homologas a las

de los enteros y luego de ello comenzaremos el estudio de otros conjuntos numéricos menos conocidos.

## 2.1. El conjunto de los números enteros y sus propiedades

Para hacer distinción entre los teoremas y definiciones referenciados de $\mathbb{Z}$ y los que son producto de este trabajo, se llamará a los teoremas y definiciones del marco teórico, Definición $n$ –z y Hecho $n$ –z, respectivamente donde $n$ corresponde al número de resultado que abordamos, cabe aclarar que en ocasiones se incluirán dentro de las definiciones los axiomas que sustentan la existencia de los elementos a utilizar, como para la suma, así las definiciones en esta primera sección además de cumplir el papel de describir elementos que existen, también afirmarán su existencia. Iniciemos con la caracterización del conjunto:

**Definición 1 -z:** $(\mathbb{Z}, +)$ es un conjunto con una operación binaria que cumple las siguientes condiciones (Axiomas de Padoa[1] (Brausín & Pérez, 2012)):

I. $\forall x \in \mathbb{Z}, \exists! \, y \in \mathbb{Z}: x^+ = y$, a tal $y$ lo llamaremos sucesor de $x$ y se notará $x^+$

II. $\forall x \in \mathbb{Z}, \exists! \, y \in \mathbb{Z}: \ -x = y$ a tal $y$ lo llamaremos inverso aditivo de $y$ y se notará $-x$

III. $\forall x \in \mathbb{Z}: - \ -x \ = x$

IV. $\forall x \in \mathbb{Z}: \ - \ x^+ \ ^+ = -x$

V. $\exists! \, 0 \ \in \ \mathbb{Z}: 0 = -0$

VI. $\forall x \in \mathbb{Z}: x \neq 0 \rightarrow x \neq -x$

VII. $\forall x, y \in \mathbb{Z}: x + y \in \mathbb{Z}$

VIII. $\forall x, y \in \mathbb{Z}: x + 0 = x, \ x + y^+ = (x + y)^+$

IX. $\forall x, y, z, c \in \mathbb{Z}: \ z = y^+ \ \rightarrow x + y = c, \ c^+ = x + z$

X. $\forall A \subseteq \mathbb{Z}, A \neq \phi$, tal que:

   i. $x \in A \rightarrow x^+ \in A$

   ii. $x \in A \wedge x = y^+ \rightarrow y \in A$

[1] Los axiomas de Padoa se utilizan para definir el conjunto de los enteros de manera similar a los axiomas de Peano.

Entonces $A = \mathbb{Z}$(principio de inducción).

**Teorema 1-z:** $\forall x \in \mathbb{Z}, \exists! \, y \in \mathbb{Z}: y^+ = x$, a tal $y$ lo llamaremos antecesor de $x$ y se notará $x^-$.

**Teorema 2-z:** $\forall x, y \in \mathbb{Z}: \ x + y^- = (x + y)^-$

**Definición 2-z:** La estructura $(\mathbb{Z}, +, *)$ cumple las siguientes condiciones:

I. $\forall x, y \in \mathbb{Z}: x * y \in \mathbb{Z}$

II. $\forall x \in \mathbb{Z}: x * 0 = 0$

III. $\forall x, y \in \mathbb{Z}: x * y^+ = x * y + x$

IV. $\forall x, y \in \mathbb{Z}: x * y^- = x * y + (-x)$

V. $\exists! \, 1, -1 \in \mathbb{Z}: \ -1 \ \ -1 \ = 1, 0^+ = 1, 0^- = -1$

VI. $\forall x \in \mathbb{Z}: x * 1 = x$

**Teorema 3-z:** $(\mathbb{Z}, +, *)$ es un dominio de integridad, esto significa que:

I. $(\mathbb{Z}, +)$ es un grupo abeliano, esto significa:

a. $\forall x, y, z \in \mathbb{Z}: x + (y + z) = (x + y) + z$, la operación es asociativa

b. $\exists! \, y \in \mathbb{Z}, \forall x \in \mathbb{Z}, : x + y = x$, en este caso $y = 0$, la operación tiene elemento neutro

c. $\forall x \in \mathbb{Z}, \exists! \, y \in \mathbb{Z} : x + y = 0$, en este caso $y = -x$, la operación tiene inversos

d. $\forall x, y \in \mathbb{Z}: x + y = y + x$, la operación es conmutativa

II. $(\mathbb{Z}, *)$ es monoide conmutativo con unidad, esto significa:

e. $\forall x, y, z \in \mathbb{Z}: x * \ y * z \ = \ x * y \ * z$, la operación es asociativa

f. $\exists! \, y \in \mathbb{Z}, \forall x \in \mathbb{Z} : x * y = x$, en este caso $y = 1$, la operación tiene elemento neutro

g. $\forall x, y \in \mathbb{Z}: x * y = y * x$, la operación es conmutativa

III. $\forall x, y, z \in \mathbb{Z}, x \neq 0: \ x * y = x * z \ \rightarrow y = z$, se cumple la propiedad cancelativa para la segunda operación.

IV. $\forall x, y, z \in \mathbb{Z}: x \ y + z \ = xy + xz$, la segunda operación distribuye respecto a la primera operación.

Cuando $x * y = z$, podemos escribir $x = \frac{z}{y}$ como referencia a la aplicación de la propiedad cancelativa en esta igualdad.

**Teorema 4-z:** $\forall x, y, z \in \mathbb{Z}, :\ \ x + y = x + z\ \ \rightarrow y = z$

**Teorema 5-z:** $\mathbb{Z}$ tiene $\aleph_0$[2] (Busqué, Saorín, & Simón, 2011-2012) elementos (un número infinito contable de elementos) y de la misma forma el conjunto de parejas ordenadas $\mathbb{Z}$x $\mathbb{Z}$ tiene el mismo número de elementos.

Aunque este último teorema no se demuestra con elementos externos a los anteriormente presentados, será clave para la caracterización de los conjuntos que se estudiarán en este documento, por ello se incluye como parte de los teoremas de propiedades del conjunto.

Dados estos resultados, desde a lo largo del documento se usará la notación usual para los elementos del conjunto $\mathbb{Z}$ para ejemplificar los teoremas, verificar su funcionamiento y se usaran representaciones isomorfas a esta para visibilizar mejor las propiedades a demostrar, se utilizan para representar los símbolos {0,1,2,3,4,5,6,7,8,9} y las combinaciones entre ellos para la representación en base 10, de esta manera se elige el orden lexicográfico usual para los sucesores, 0-1-2-3-4-5-6-7-8-9-10-11… donde $a$-$b$ indica que $b$ es sucesor de $a$ y que $a$ es antecesor de $b$, de manera análoga, la cadena de números antecesores se representa con los símbolos ... $(-10)$- $(-9)$- $(8)$- $(-7)$… $(-1)$-0.

**Teorema 6-z:** $\forall a, b \in \mathbb{Z}, \exists!\, x \in \mathbb{Z}: a + x = b$, esto es, todas las ecuaciones en $(\mathbb{Z}, +)$, tienen solución única.

**Teorema 7-z:** $\forall a, b \in \mathbb{Z}: ab = 0 \rightarrow a = 0 \vee b = 0$

Este teorema es muy importante en el estudio de la divisibilidad ya que indica que no hay dos números distintos de 0 que multiplicados sean 0, es decir no hay divisores de 0, en los conjuntos que se estudian usualmente en teoría de números, los dominios de integridad,

[2] $\aleph_0$ o aleph-0 se denomina como el cardinal de los números naturales, aceptando la hipótesis del continuo, no hay ningún conjunto que tenga cardinal mayor al de los naturales y menor que el de los reales o aleph -1

esta propiedad es muy deseada para que se cumplan ciertos resultados que tienen que ver con la unicidad de las descomposiciones de un número, sin embargo en contraste a esto como se verá más adelante, en los conjuntos que estudiaremos si existirán elementos distintos del neutro de la suma, un equivalente al 0, cuyo producto es ese neutro.

**Definición 3-z:** $\forall a, b \in \mathbb{Z} : a - b = a + (-b)$, a $a - b$ se le denominará resta entre $a$ y $b$

**Teorema 8-z:** $(\mathbb{Z}, -)$ cumple:

I. $\exists!\, 0 \in \mathbb{Z}, \forall x \in \mathbb{Z}: x - 0 = x$
II. $\forall x \in \mathbb{Z}, \exists!\, y \in \mathbb{Z}: x - y = 0$

**Teorema 9-z:** $\forall a, b \in \mathbb{Z}$ se cumple:

I. $-\ a + b\ = -a - b$
II. $-\ a - b\ = -a + b = b - a$
III. $-ab = \ -a\ \ b\ = \ -a\ \ b$
IV. $\ a - b\ +\ b - c\ = a - c$

Con estas propiedades algebraicas del conjunto, se prosigue a listar las propiedades de $\mathbb{Z}$ como conjunto ordenado primero se debe definir un conjunto al que llamaremos enteros positivos (Brausín & Pérez, 2012):

**Definición 4-z:** $\exists P \subset \mathbb{Z}$ tal que:

I. $\forall x, y \in P: x + y \in P \wedge x * y \in P$
II. $\forall x \in \mathbb{Z}: x \neq 0 \rightarrow (x \in P \veebar -x \in P)$

**Teorema 10-z:** $(P, +, *) \approx (\mathbb{N}, +, *)$

Este teorema, al establecer que el conjunto de enteros positivos es isomorfo a los números naturales, nos permitirá usar indistintamente las dos representaciones de este conjunto indistintamente, esto es importante puesto que en el documento las estructuras de estudio se definen a partir de los números enteros, sin embargo en algunos casos se usaran sin distinción propiedades de $\mathbb{N}$ cuando hablamos enteros positivos.

**Definición 5-z:** $\forall x, y \in \mathbb{Z}: x < y \leftrightarrow \exists n \in P: x + n = y, x \leq y$ significa que $x < y \vee x = y$, y a $x > y$ se le dará el significado $y < x$.

Con la definición de la relación $\leq$ en $\mathbb{Z}$ procedemos a demostrar las propiedades (Urbina, 2006):

**Teorema 11-z:** $\leq$ es una relación de orden, esto significa que$\forall x, y, z \in \mathbb{Z}$:

I. $x \leq x$, la relación es reflexiva
II. $(x \leq y \wedge y \leq x) \rightarrow x = y$, la relación es antisimétrica
III. $x \leq x \wedge y \leq z \rightarrow x \leq z$, la relación es transitiva

**Teorema 12-z:** $(\mathbb{Z}, \leq)$ es un conjunto totalmente ordenado, esto es, se cumple una y solo una de las siguientes condiciones $\forall x, y \in \mathbb{Z}$:

$$x < y \vee y < x \vee y = x$$

**Teorema 13-z:** $\forall a, b, c, d \in \mathbb{Z}, \forall x, y \in P$:

I. $a \leq b \wedge c \leq d \rightarrow a + c \leq b + d$
II. $a \leq b \rightarrow ax \leq bx$
III. $ax \leq bx \rightarrow a \leq b$
IV. $a \leq b \rightarrow a - x \geq b(-x)$
V. $a < b \rightarrow -a > -b$
VI. $-(x - y) \in P$
VII. $(a > 0 \leftrightarrow a \in P) \wedge (a < 0 \vee a = 0 \leftrightarrow a \notin P)$
VIII. $ab < 0 \rightarrow (a > 0 \wedge b < 0) \vee (a < 0 \wedge b > 0)$
IX. $a \neq 0 \rightarrow a * a > 0$
X. $a > b \leftrightarrow a - b \in P$
XI. $a^2 + b^2 \geq 0 \wedge (a^2 + b^2 > 0 \leftrightarrow ab \neq 0)$
XII. $a^+ > a$
XIII. $a < b \rightarrow a^+ \leq b$

Habiendo definido algunos aspectos del comportamiento de la relación de orden respecto al conjunto y a las operaciones y relaciones que se tenían procedemos a definir su comportamiento en subconjuntos de los números enteros (Apostol, 1984):

**Definición 6-z:** Sea $S \subseteq \mathbb{Z}, S \neq \emptyset$:

$x \in \mathbb{Z}$ es una cota superior de $S$ si y solamente si $\forall y \in S, y \leq x$.

$x \in \mathbb{Z}$ es una cota inferior de $S$ si y solamente si $\forall y \in S, x \leq y$.

Si hay en $\mathbb{Z}$ cotas superiores de $S$ se dice que $S$ está acotado superiormente, análogamente, si hay en $\mathbb{Z}$ cotas inferiores de $S$ se dice que $S$ está acotado inferiormente.

Si $x$ es una cota superior de $S$ y $x \in S$, se dice que $x$ es máximo de $S$, esto se nota $x = \max S$; análogamente si $x$ es una cota inferior de $S$ y $x \in S$, se dice que $x$ es un mínimo de $S$ y se nota $x = \min S$.

**Teorema 14-z:** $\forall S \subseteq \mathbb{Z}, S \neq \emptyset, (x = \max S\,, y = \max S \rightarrow x = y) \wedge (x = \min S\,, y = \min S \rightarrow x = y)$

Aunque el máximo y el mínimo de un conjunto, en los números enteros cuando existen son únicos, hay conjuntos que no tienen máximos y hay conjuntos sin mínimos, y como se verá más adelante en otras estructuras hay conjuntos que tienen varios máximos y mínimos.

**Teorema 15-z:** $\forall S \subseteq \mathbb{Z}, S \neq \emptyset$, si $S$ está acotado superiormente entonces tiene máximo, y si está acotado inferiormente entonces tiene mínimo.

**Teorema 16-z:** $\forall S \subseteq P, S \neq \emptyset, S$ es finito$\rightarrow S$ tiene mínimo y máximo.

**Teorema 17-z:** $\forall S \subseteq P, S \neq \emptyset, S$ tiene mínimo.

Al teorema anterior se le conoce como Principio de Buen Orden o (PBO), junto al principio de inducción y las propiedades del conjunto, se da lugar al siguiente teorema:

**Teorema 18-z:** $\forall a, b \in \mathbb{Z}, b > 0, \exists!\, q, r \in \mathbb{Z}: a = br + r, con\ 0 \leq r < b$ (Algoritmo de la división para $b \in P$).

El algoritmo de la división en esta primera forma está restringido a un número entero que será dividido y un número enteros positivo; la definición de la siguiente relación, la norma de $\mathbb{Z}$, permite declarar de forma más completa el algoritmo de la división y para complementar las propiedades que derivan de esta incluiremos un elemento asociado a la reiteración de la segunda operación del conjunto.

**Definición 7-z:** Se define la función valor absoluto en los números enteros como sigue:

$$: \mathbb{Z}\text{x}\ \mathbb{Z} \to P \text{ tal que}$$

$$a \geq 0 \to \ |a| = a$$

$$a < 0 \to \ |a| = -a$$

Se define también la potencia enésima de un número con $n \in \mathbb{N}$, por recurrencia como sigue como $a \in \mathbb{Z}$:

$$a^0 = 1$$

$$a^1 = a$$

$$a^n = a^{n-1} * a$$

La idea de norma es una generalización de las funciones que indican la distancia al origen de los elementos del conjunto, aunque usualmente se definen normas sobre espacios vectoriales, $\mathbb{Z}$ cumple por sí mismo varias propiedades clásicas referente a esta:

**Teorema 19-z:** $\forall x, y \in \mathbb{Z}, :\ \ \forall a \in P$ se cumple:

I. $|x| \geq 0$
II. $|-x| = |x|$
III. $|x| = 0 \to x = 0$
IV. $|x * y| = |x| * |y|$
V. $|x + y| \leq |x| + |y|$

VI. $x^{n} = x^{n}$

VII. $x = a \rightarrow (x = a \vee x = -a)$

VIII. $x \leq a \rightarrow (-a \leq x \leq a)$

IX. $x \geq a \rightarrow (x \geq a \vee x \leq -a)$

X. $-x \leq x \leq x$

Con esta nueva relación, se puede extender el algoritmo de la división para cualquier par de números enteros de la siguiente forma:

**Teorema 20-z: :** $\forall a, b \in \mathbb{Z}, b \neq 0, \exists! q, r \in \mathbb{Z}: a = bq + r, con\ 0 \leq r < b$ (Algoritmo de la división para cualquier entero)

Sobre las propiedades de las potencias se contribuirán al trabajo los siguientes resultados:

**Teorema 21-z: :** $\forall x, y \in \mathbb{Z},:\ \forall m, n \in P$ se cumple:

I. $(x * y)^n = x^n * y^n$

II. $x^{m+n} = x^m x^n$

III. $(x^m)^n = x^{mn}$

IV. $(a+b)^n = \sum_{k=1}^{k=n} \binom{n}{k} a^k b^{n-k}$, donde $\binom{n}{k} = \frac{n!}{k! * (n-k)!}$ (Binomio de Newton)

## 2.2. La relación de divisibilidad de $\mathbb{Z}$

De manera similar a como se definió la relación < en la sección anterior, procederemos a definir la relación de divisibilidad | , esta vez utilizando la segunda operación de $\mathbb{Z}$ (Rubiano, Jiménez, & Rubiano, 2004) , (Rafael & Isaacs, 2005), (LeVeque, 1968):

**Definición 8-z: :** $\forall x, y \in \mathbb{Z}: x|y \leftrightarrow \exists k \in \mathbb{Z}: x * k = y$, cuando $x|y$ diremos que $x$ divide a $y$ o $x$ es un divisor de $y$, también decimos cuando se cumple $x * k = y$ que $y$ es múltiplo de $x$.

El primer resultado que se obtiene, directamente de la definición, en cuanto a las propiedades que cumple | es:

**Teorema 22-z: :** $|$ es una relación de pre-orden en $\mathbb{Z}$ esto significa que $\forall x, y \in \mathbb{Z}$:

I. $x|x$, la relación es reflexiva

II. $(x|y \wedge y|x) \rightarrow (x = y \vee x = -y)$ , La relación no es antisimétrica

III. $x|x \wedge y|z \rightarrow x|z$, la relación es transitiva

Algunas otras propiedades de la relación de divisibilidad son:

**Teorema 23-z: :** $\forall x, y, z, a, b \in \mathbb{Z}$ se cumple:

I. $1|x \wedge x|0$, esto significa que 1 es un mínimo(hay más de uno)de esta relación y 0 es el máximo

II. 0 no es divisor de ningún número distinto de sí mismo.

III. $x\ y \rightarrow (x\ -y \wedge -x|y)$

IV. $(x|y \wedge x|z) \rightarrow x|ay + bz$, a $ay + bz$ se le llama combinación lineal con coeficientes enteros de $y$ y $z$; cuando se da $x|y \wedge x|z$ decimos que $x$ es un divisor común de $y$ y $z$.

Corolario: $(x\ y \rightarrow x\ ay) \wedge ((x|y \wedge x|z) \rightarrow x|y + z)$

V. $(x|a + b \wedge x|a) \rightarrow x|b$

VI. $(x|y \wedge y \neq 0) \rightarrow x \leq y$

VII. $((x|a \wedge y|b) \wedge (x \neq 0 \wedge y \neq 0)) \rightarrow xy|ab$

VIII. $(x \neq 0 \wedge y \neq 0) \rightarrow (y|a \leftrightarrow yx|ax)$

La situación $(x|y \wedge y|x) \rightarrow x = \pm y$ da la oportunidad de definir una nueva relación para comparar los elementos que se dividen entre sí:

**Definición 9-z:** $\forall x, y \in \mathbb{Z}$: $x \sim y \leftrightarrow x|y \wedge y|x$, cuando $x \sim y$ se dé diremos que $x$ e $y$ están asociados.

Por el teorema 22-z ya sabemos que los números asociados a $x$ son $x$ y $-x$, por lo que en el caso de $\mathbb{Z}$, una definición equivalente a la anterior es:

$$x \sim y \leftrightarrow x = y \wedge x = -y$$

Sin embargo, solo se cumple en algunos conjuntos similares a $\mathbb{Z}$, por ejemplo en $\mathbb{N}$, no existen tales elementos como números asociados, en la exploración dentro de este documento se responderá porque y se hará una generalización en el capítulo de 4; sin embargo la definición anterior es necesaria para establecer una versión del Teorema Fundamental de la Aritmética en los números enteros, para ahondar un poco en esta, veamos sus propiedades:

**Teorema 24-z:** $\sim$ es una relación de equivalencia, esto significa que $\forall x, y \in \mathbb{Z}$:

I. $x \sim x$, la relación es reflexiva
II. $(x \sim y \rightarrow y \sim x)$, la relación es simétrica
III. $x \sim x \wedge y \sim z \rightarrow x \sim z$, la relación es transitiva

Como dato curioso por si el lector quiere profundizar sobre esta relación se deja el siguiente teorema:

**Teorema 25-z:** El conjunto cociente $(\mathbb{Z}/\sim)$ con las operaciones inducidas por la relación equivalencia en $[+]$ y $[*]$ es isomorfo a $(\mathbb{N}, +, *)$

Retomando en el teorema 23-z se definió que significa ser un divisor común de dos números enteros, usualmente nos preocupamos por saber cuál es el más grande, ordenando con alguna de las relaciones de orden encontradas, usualmente se usa la de divisibilidad pero en ocasiones < definida coincide con esta como sucederá aquí, el concepto al que nos referimos se denomina máximo común divisor; este es un concepto muy importante en la teoría de números para definir los conceptos de supremo e ínfimo, confirmar varias propiedades de las relaciones de divisibilidad, demostrar el lema de Euclides, y trabajar con el algoritmo de la división; este ostenta varias propiedades útiles en el estudio a desarrolla :

**Definición 10-z:** $\forall a, b \in \mathbb{Z}, a \neq 0 \wedge b \neq 0$ definimos el conjunto $D = \{x \in P : x|a \wedge x|b\}$, a $\max D$ se le llama máximo común divisor y se nota $mcd\ a, b$ . En el caso $a = 0 = b, mcd = 0$.

En la literatura al máximo común divisor entre dos números se le suele escribir simplemente como $a, b$ , pero para evitar confusiones con las notaciones que se utilizaran más adelante se notara en este documento de la manera indicada.

Se puede afirmar que el conjunto $D$ no es vacío, efectivamente existe el máximo común divisor pues al menos $1 \in D$.Cabe mencionar que utilizamos la función $\max D$ sin indicar a cuál de las relaciones de orden encontradas hace referencia, esto no es necesario debido a que el utilizar $|$ o $<$ , para este caso tienen los mismos resultados, este máximo es el máximo desde dos puntos de vista diferentes, sin embargo se acordara usar $<$ ya que es una relación de orden y además es total, a diferencia de $|$ que es un pre orden, pero es valioso que el lector recuerde este hecho cuando estudie como definimos máximo común divisor al final del capítulo 4. Teniendo en cuenta las consideraciones anteriores, una versión más cómoda de la definición anterior es:

**Definición 10'-z:** $\forall a, b \in \mathbb{Z}, m$ es el máximo común divisor entre $a$ y $b$ si y solo si:

i. $m \in P$
ii. $m|a \wedge m|b$
iii. $\forall k \in \mathbb{Z}: (k|a \wedge k|b) \rightarrow k|m$

Algunas de las propiedades relevantes de $mcd$ son:

**Teorema 26-z:** $\forall a, b, c \in \mathbb{Z}, (a \neq 0 \vee b \neq 0) \wedge c \neq 0$, se cumple que:

I. $mcd\ a, b = x \wedge mcd\ a, b = y \rightarrow x = y$
II. $mcd\ a, 0 = a$
III. $mcd\ a, b = mcd(a, b)$
IV. $mcd\ mcd\ a, b, c = mcd(a, mcd(b, c))$
V. $mcd\ a, b = mcd(b, a)$
VI. $mcd\ a, a = a$
VII. $mcd\ a, b = mcd\ a, -b = mcd\ -a, b = mcd\ -a, -b$

VIII. $(\exists! x, y \in \mathbb{Z}: mcd\ a,b\ = ax + by) \wedge (\forall x', y' \in \mathbb{Z}, \forall\, z \in P:\ z = ax' + by'\ \rightarrow mcd\ a,b\ < z)$, esto es, el máximo común divisor es el menor entero positivo que puede ser escrito como combinación lineal de $a$ y $b$. (Teorema de Bézout)

IX. $\forall a, b, q, r \in \mathbb{Z},:\ a = bq + r\ \rightarrow mcd\ a,b\ = mcd\ \ b,r$

Recapitulando hasta el momento hemos listado en $\mathbb{Z}$ propiedades algebraicas, de orden, de equivalencia y hemos definido algunas funciones en este conjunto, teniendo este los elementos $(\mathbb{Z}, +, 0, *, 1, -, ', \wedge, \leq, \sim, \quad , , \mathrm{mcd}$ , elementos que a lo largo de este trabajo deberemos identificar sus homólogos en otros conjuntos, sin embargo aún no hemos profundizado mucho en los elementos en si del conjunto de los números enteros, de los elementos que tienen propiedades especiales solo hemos abordado un tipo, los números neutros para ambas operaciones, a continuación comenzaremos a identificar los elementos que son de especial interés en el estudio a realizar.

**Definición 11-z:** Un número entero $x$ es una unidad si y solamente si es divisor de todo número entero, o en lenguaje alfanumérico del algebra: ($x \in \mathbb{Z}$ es unidad) $\leftrightarrow$ $(\forall y \in \mathbb{Z}: x|y)$

En los números enteros solo hay dos unidades, 1 y -1, esta definición nos da posibilidad de reformular la definición de $\sim$ si se deseara en una equivalente de la siguiente forma:

**Definición 9'-z:** $\forall x, y \in \mathbb{Z}:\ x \sim y \leftrightarrow x = y * u, u$ unidad

Cualquiera de las dos formas es válida para definir números asociados, de hecho, al definir una la otra es un resultado inmediato o teorema, quizás para el entendimiento de la lectura posterior sea más conveniente esta segunda forma, pero se deja como criterio al lector la elección de esta definición al practicar estos conceptos.

Los dos elementos anteriores, unidades y asociados nos permiten caracterizar completamente los elementos del conjunto en varios conjuntos por las propiedades de la relación de divisibilidad en números primos, compuestos, unidades y primos relativos:

**Definición 12-z:** Sea $p \in \mathbb{Z}, p \neq u,$ para toda $u$ que sea unidad, diremos que $p$ es un número primo si y solo si sus únicos divisores son las unidades y sus asociados. Si $p$ no es un número primo diremos que es un número compuesto.

**Definición 13-z:** $\forall x, y \in \mathbb{Z}$: $mcd\ x, y = 1 \leftrightarrow x\ e\ y$ son primos relativos.

Abordaremos primero algunas propiedades importantes de los primos relativos

**Teorema 27-z:** $\forall a, b, c \in \mathbb{Z}, (a \neq 0 \vee b \neq 0) \wedge c \neq 0$, se cumple que:

I. $mcd\ a, b = 1 \leftrightarrow (\exists x, y \in \mathbb{Z}: 1 = ax + by)$

II. $mcd\ a, b = c \rightarrow mcd\ \frac{a}{c}, \frac{b}{c} = 1$

III. $(a|bc \wedge mcd\ a, b = 1) \rightarrow a|c$

IV. $(mcd\ a, b = 1 \wedge mcd\ a, c = 1) \rightarrow mcd\ a, b * c = 1$

Corolario: $mcd\ a, b_i\ , i = 1,2 \ldots n \rightarrow mcd\ a, b_1 * b_2 * \ldots * b_n = 1$

V. $(a\ b \wedge b\ c \wedge mcd\ a, b = 1) \rightarrow ab|c$

VI. $mcd\ ac, bc = c\ mcd\ a, b$

VII. $(b|c \wedge mcd\ a, c = 1) \rightarrow mcd\ a, b = 1$

VIII. $b|c \rightarrow mcd\ a, b = mcd\ a + c, b$

IX. $mcd\ a, c = 1 \rightarrow mcd\ a, b = mcd\ a, bc$

X. $mcd\ a, b = 1 \rightarrow mcd\ a, bc = mcd\ a, b * mcd\ a, c$

XI. $mcd\ a, b = 1 \rightarrow mcd\ a^k, b^n = 1, \forall k, n \in \mathbb{N}$

XII. $mcd\ a, b = 1 \rightarrow mcd\ a + b, a - b = 1$ ó $mcd\ a + b, a - b = 2$

XIII. $mcd\ a, bc = 1 \rightarrow mcd\ a, b = 1 \wedge mcd\ a, c$ =1

XIV. Una ecuación $ax + by = c$ tiene solución en $\mathbb{Z}$ si y solo si $mcd\ a, b\ |c$.

XV. $mcd\ a, b = m, m|c$ y $x_0, y_0$ es una solución particular a la ecuación $ax + by = c$ entonces todas las soluciones a la ecuación están determinadas por :

$$x = x_0 + \frac{b}{g}\ k, y = y_0 - \frac{a}{g}\ k$$

Retomemos con esto la definición de número primo y compuesto, varias de las propiedades más importantes se organizan en:

**Teorema 28-z:** $\forall p, c, a, b \in \mathbb{Z}, p$ primo, $c$ compuesto se cumple que:

I. $c$ tiene al menos un divisor primo
II. Hay infinitos números primos
III. $p\ ab \rightarrow p\ a \vee p|b$
IV. $p\ a_1 * a_2 * \ldots * a_n \rightarrow p\ a_i$ para algún $i, 1 \leq i \leq n$
V. Todo número puede escribirse de manera única como producto de factores primos salvo por el orden y asociados.

## 2.3. Un primer caso: construcción del teorema fundamental de la aritmética en $\mathbb{N}$

En la sección anterior se definieron varios conceptos clave para el desarrollo de la teoría de números, uno de ellos fue números primos, las propiedades que estos tienen en los números enteros nos permite aplicar el proceso de analizar a todo número del conjunto, no obstante con lo que los primeros teoremas establecen ya podemos afirmar que todo número entero puede ser escrito como suma de otros dos, sin embargo el estudio de este primer tipo de descomposición no es de mucho interés $\mathbb{Z}$ y en general para cualquier grupo abeliano aditivo todas las ecuaciones tienen solución, esto significa que no solo todo número puede descomponerse como suma de otros dos, sino que todo número puede descomponerse como suma utilizando cualquier número, por ejemplo $5 = 2 + 3$, pero $5 = 4 + 1 = -2 + 7$ y en general, $\forall a \in \mathbb{Z}, 5 = a + (5 - a)$, esto es resultado directo de la existencia de inversos para la operación +.

Si hablamos de la segunda operación,* no permite inversos en $\mathbb{Z}$**,** lo cual agrega más interés a estudiar, ¿Cuándo es posible que un número pueda ser escrito como producto de otro?, esto es estudiar la relación de divisibilidad, si de lo contrario como sucede en $\mathbb{R}$, existieran inversos multiplicativos con la operación *, no tendría mucho sentido estudiar la relación de divisibilidad pues todo elemento $a$ no nulo es divisor de todo elemento $x, = a * \frac{1}{a}$.

Teniendo lo anterior en cuenta, la descomposición por producto y el análisis de las partes que componen un número, y en general con operaciones que no permitan inversos multiplicativos, es la forma del proceso de analizar en la que nos fijaremos, como punto más cercano a $\mathbb{Z}$, se comenzará mostrando un camino se mostrará en el Seminario de Algebra (2013) de la Universidad Pedagógica Nacional para llegar al resultado que nos permite escribir todo número natural como producto de otros que lo configuran, además de manera única, esto es, un camino para demostrar el Teorema Fundamental de la Aritmética en $\mathbb{N}$, el lector distinguirá en esta sección en ocasiones para demostrar un teorema presentado, se hace uso de otro que no se haya demostrado aun, esto se debe a que el documento el cual referenciaremos es producto de una construcción social de conocimientos, los teoremas fueron surgiendo como ideas para resolver los problemas que surgieran al afirmar que un número natural tiene descomposición única en términos de factores primos.

Esta sección es un resumen del documento resultado del seminario de Algebra (2013), (Sanchez, Angel, & Luque, 2013) modificado de cierta manera para que su lenguaje coincida con el utilizado en este documento e incluyendo algunos datos útiles en el con fines de que sean comparables los elementos de este con los resultados del estudio que llevaremos a cabo, y un sustento como esquema del camino que tomaremos para intentar una demostración del Teorema Fundamental de la Aritmética para otros conjuntos, incluiremos demostraciones y más adelante contrastaremos sus elementos con los de la sección 5.

Se toma como marco de referencia la Axiomática de Peano cuyos parámetros se enfocan en la idea de sucesor, las definiciones por recurrencia y el principio de inducción y se acepta que la operación suma en los números naturales definidos con este esquema da una estructura de monoide conmutativo con unidad, no hay en inversos aditivos, y se define a partir de la primera operación una relación de orden total definiendo la resta entre dos números, de manera muy similar a como se vio en la sección 2.1.

Como se explicó anteriormente, aunque en los números naturales no todas las ecuaciones tienen solución y se podría hacer un estudio por descomposiciones de sumas de un número, siendo un punto común entre los enteros, los naturales y los conjuntos que estudiaremos el que la segunda operación no tenga inversos, es esta (*) la de mayor interés por lo cual se inicia con esta definición:

**Definición 1-n:** $\forall a, b \in \mathbb{N}$ se define la operación de multiplicación tal que:

i. $a * 0 = 0$
ii. $a * b^{+} = a * b + a$

Con base en el siguiente teorema se acepta que se puede probar que $(\mathbb{Z},*)$ es un monoide conmutativo con unidad que además cumple la propiedad distributiva respecto a la suma, es decir $(\mathbb{Z}, +, *)$ es un anillo conmutativo con unidad:

**Teorema 1-n:** $0 * a = 0, \forall a \in \mathbb{N}$
Demostración:
$b * a + 0 = b * a = \ b + 0 \ * a = b * a + 0 * a$ y por cancelativa de la adición $0 = 0 * a$

Se prosigue a definir la relación a estudiar, la divisibilidad:

**Definición 2-n:** $\forall a, b \in \mathbb{N}: a|b \ \leftrightarrow \exists c \in \mathbb{N}: a * c = b$

Y se explicitan las propiedades de esta relación en cuanto a su tipo:

**Teorema 2-n:** La relación $|$ en el conjunto de los números naturales es una relación de orden.

Demostración:
La relación es reflexiva gracias al elemento neutro de la multiplicación, $\exists 1 \in \mathbb{N}: a * 1 = a$ por tanto $a|a$.

Es transitiva dado que: $a|c$ y $b|$c, por la Definición 2-n, $\exists k, h \in \mathbb{N}: a * k = b \wedge b * h = c$, al reemplazar $b$ en la segunda ecuación se tiene $(a * k) * h = c$, y por la propiedad asociativa de * , $a * (k * h) = c$, luego por la Definición 2-n $a|c$.

Es antisimétrica dado que: Si $a|b$ y $b|$a, por la Definición 2-n, $\exists c, d \in \mathbb{N}: a * c = b \wedge b * d = a$, si $a = 0$ se tiene que $0 * c = b$, por Teorema 1-n $b = 0$, y por lo tanto $a = b$. Con $a \neq 0,$ al reemplazar $b$ en la segunda ecuación se obtiene $(a * c) * d = a$ y por la propiedad asociativa de * se tiene que $a * (c * d) = a$ , si tuviéramos la propiedad cancelativa se tendría $c * d = 1$ y estando en $\mathbb{N}$ no queda otra opción que $c = 1 \wedge d = 1$, y al reemplazar en las ecuaciones iniciales se concluye que $a = b$. Por lo cual se concluye que la relación $|$ es de orden.

En el documento, ya que hacen falta la propiedad cancelativa y $c * d = 1 \rightarrow c = 1 \wedge d = 1$, estas dos propiedades se toman como hechos sin demostración, sin embargo al ser trascendente para este trabajo estos dos teoremas, se incluye la demostración a continuación, en el caso del primero de ellos utilizamos propiedades del orden e iniciamos para demostrarlo un hecho importante que diferencia algunas estructuras de otras, este hecho equivale a la propiedad cancelativa, aquí lo mostraremos como lema:

**Teorema 3-n:** $\forall a, b, c \in \mathbb{N},$ Si $a \neq 0$ y $a * b = a * c$ entonces $b = c$

Lema: $\forall a, b \in \mathbb{N},$ Si $ab = 0$ entonces $a = 0$ o $b = 0$

Demostración Lema:

Supongamos por contradicción que existen $a, b \in \mathbb{N}$ tales que $ab = 0$ y $a \neq 0$ o $b \neq 0$, si $a = 1$, de manera directa se obtiene $b = 0$ y llegaríamos a una contradicción pues tomamos suponemos $b \neq 0$. Entonces $a > 1$ necesariamente, por lo que por definición de $>$, $a - 1 > 0$, y como $b \neq 0$ debe suceder $b > 0$, por lo cual por propiedades de la relación de orden $a - 1\ b > 0,$ y por la propiedad distributiva de la multiplicación respecto a la resta $ab - b > 0$, por lo que se deduce $ab > b$, y reemplazando $ab$ se llega a que $0 > b$, situación que en los números naturales es una contradicción ya que 0 es el mínimo del conjunto.

Por lo cual no queda otra opción más que $a = 0$ o $b = 0$.

Demostración Teorema 3-z:

Tomaremos como hipótesis que $a * b = a * c, a \neq 0$, ahora si $b = 0$, se tiene que $0 = a * c, a \neq 0$ y por el lema anterior solo se puede dar $c = 0$ y en consecuencia $b = c$, por lo cual se tiene el teorema. Análogamente suponer $c = 0$ nos lleva a concluir que $b = c = 0$. Para el otro caso $b > 0$ y $c > 0$, se pueden tener tres posibilidades, ya que en $\mathbb{N}$ se cumple la tricotomía, $b > c$ o $c > b$, o $b = c$. Supongamos que se cumple $b > c$, por definición de $>$ se tiene que $b - c > 0$, y como $a \neq 0$, la desigualdad se mantiene al multiplicarlo, $a(b - c) > 0$ por la propiedad distributiva se tiene que $ab - ac > 0$ y por la definición de $>$ se concluye que $ab > ac$, pero llegamos a una contradicción con la tricotomía en los naturales puesto que supusimos $a * b = a * c$. De manera análoga se llega a una contradicción si suponemos $c > b$, por lo cual no queda otra opción más que $a = b$.

**Teorema 4-n:** $\forall a, b \in \mathbb{N}$, Si $ab = 1$ entonces $a = 1$ y $b = 1$

Lema: No hay un número natural que cumpla $0 < n < 1$

Demostración del Lema:

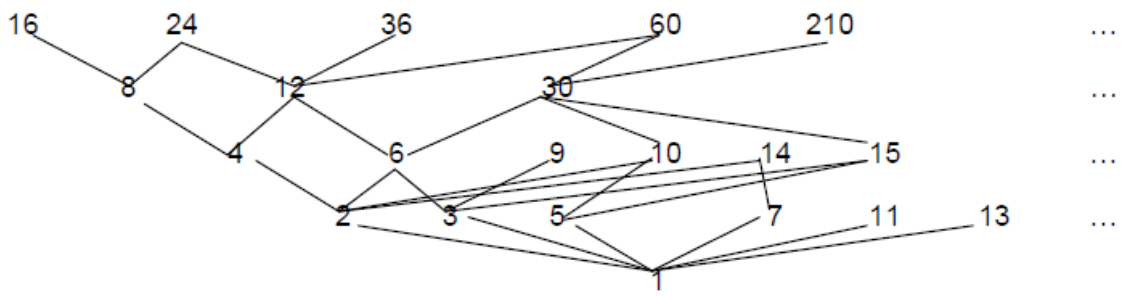
Supongamos por contradicción que existe tal $n$ natural que cumple $n > 0, 1 > n$, multiplicando por $n$ a ambos lados de la desigualdad ya que $n \neq 0$, se tiene que $n > n^2$ lo cual es una contradicción pues en $\mathbb{N}, n \neq 0, n^2 > n$.

Demostración de Teorema 4-n:

Tomaremos como hipótesis $ab = 1$ y supongamos por contradicción $a \neq 1 \vee b \neq 1$, en el caso de que $a \neq 1$, puede darse $a = 0$ o $a > 1$ por el lema anterior, si $a = 0$, reemplazando en nuestra hipótesis se tiene que $0 * b = 1, 1 = 0$ , por el Teorema 1-n y esto es una contradicción, por un proceso similar se llega a qué $b \neq 0$ . Por lo cual se debe cumplir que $a > 1, b > 0$ y por definición de $>$ se tiene que $a - 1 > 0$, multiplicando a ambos lados de la desigualdad por $b$ se tiene que $a - 1\ b > 0$ y por la propiedad distributiva de la multiplicación respecto a la resta $ab - b > 0$, luego por definición de $>$, $ab > b$ y

reemplazando por nuestra hipótesis $ab = 1$, $1 > b$, por lo que tenemos que $1 > b > 0$, y esto contradice el lema anterior, por lo cual $a = 1$ necesariamente. Análogamente si suponemos que es $b \neq 1$, se deduce que esto conduce a una contradicción y se debe cumplir $b = 1$, por tanto se tiene el teorema.

En el documento se muestra el siguiente esquema para indicar que la relación de divisibilidad no es un orden total, puesto que hay pares de elementos que no son comparables, esto es existen $a, b \in \mathbb{N}$ tales que no se cumple $a|b$ ni $b|a$, los números en el diagrama de Hasse están ordenados de forma que en las filas inferiores se encuentran los números primos y las flechas en sentido ascendente indican que el número de abajo divide al de arriba:




Además el documento nos ofrece la siguiente tabla con los resultados encontraron para los números que se encuentran en cada fila:

| Numero de divisores distintos a si mismo | Números | Forma general |
|---|---|---|
| 0 | 1 | |
| 1 | 2,3,5,7,11,13 ... | $p$ que llamaremos primos |
| 2 | 4,6,9,10,14,15 ... | $p^2, pq$ con $p, q$ primos |
| 3 | 8,12,30 ... | $p^3,\ p^2q, pqr$ con $p, q, r$ primos |

| | | |
|---|---|---|
| 4 | 16,24,36,60,210 … | $p^4, p^3q,\ p^2qr, p^2q^2, pqrt$ con $p, q, r, t$ primos |
| … | … | … |
| $n$ | --- | "todo producto de primos cuyos exponentes sumen $n$" |

Tabla 1- Observaciones del Diagrama de Hasse del Orden Multiplicativo (|)

Con esta información se procede a definir los números con la propiedad de que solo tienen un divisor distinto a sí mismos, el 1 y en total solo tienen dos divisores, a estos se les denomina números primos:

**Definición 3-n:** $\forall p \in \mathbb{N}, p > 1: p$ es primo si y solo si sus únicos divisores son 1 y $p$. Si $p$ no es primo, entonces decimos que $p$ es un número compuesto.

Con la definición de números primos y ya comprobado que efectivamente si hay números primos, como el 2, 5 ,7, 11, se responde a las cuestiones ¿Cuántos números primos hay? y ¿Cómo saber si un número es primo o compuesto?, a la primera se le da respuesta con el siguiente teorema:

**Teorema 5-n:** Existen infinitos números primos.

Demostración:

Por contradicción se supone que hay finitos números primos, además se sabe que como < es una relación de orden total en $\mathbb{N}$, se pueden ordenar como $p_1 < p_2 < \cdots p_n$, para algún $n$ natural, se define el producto $q = p_1 * p_2 * \ldots * p_n$ y $p = q^+$, se sabe que cada primo es diferente de 0, por lo tanto $q = p_1 * p_2 * \ldots * p_n > p_{n,}\ \forall n,$ y como $p > q$ pues todo número es menor a su sucesor, $p > p_{n,} \forall n,$ siendo $p_n$ el máximo del conjunto de los primos, $p$ debe ser compuesto, $q$ también es compuesto pues todo $p_i$, $1 \leq i \leq n$ es divisor suyo.

(A partir de este punto de la demostración se utilizan teoremas que se consideran ciertos en el documento, se incluirá la demostración de la misma manera que para los Teoremas 3-n y 4-n.)

Como $p$ es compuesto, debe existir al menos un $p_i$ primo que lo divida, así $p_i|\mathrm{p}$ y $p_i|\mathrm{q}$, por lo anterior se deduce que $p_i|\mathrm{p}+\mathrm{q}$ y reemplazando $p$, $p_i|1+\ \mathrm{q}+\mathrm{q}$ , $p_i|1+2\mathrm{q}$, como $p_i|\mathrm{q}$ también es divisor de $kq, \forall k \in \mathbb{N},$ por lo cual $p_i|2\mathrm{q}$ y en consecuencia $p_i|1$, y en conclusión $p_i = 1$, pues 1 solo tiene un divisor, pero como $p_i$ es primo, se llega a una contradicción, por tanto se tiene el teorema.

Hay cuatro teoremas que se necesitaron para poder demostrar el teorema anterior y que aún no se habían demostrado, estos fueron:

**Teorema 6-n:** $\forall a, b \in \mathbb{N}$: Si $a|b$ y $b \neq 0$ entonces $a \leq b$

Demostración:

Por definición de divisibilidad, si $a|b$ con $b \neq 0$, entonces $\exists c \in \mathbb{N}, c \neq 0: a * c = b$, ahora como $a \leq ac$ pues $c \neq 0$, reemplazando por $b$ se tiene el resultado $a \leq b$.

**Teorema 7-n:** Todo número compuesto tiene al menos un divisor primo.

La demostración de este teorema no se llega a mostrar en el documento, aunque se indica que para demostrar este, son necesarios otros dos que abordaremos y después de ellos, demostraremos este teorema.

**Teorema 8-n:** $\forall a, b, c \in \mathbb{N}$: Si $a|b+c$ y $a|b$ entonces $a|c$

Demostración: Si $a = 0$ se tiene el teorema pues se debe dar que $b = 0$ y $c = 0$, pues 0 solo es divisor de sí mismo.

Para $a > 0$, tenemos que $a|b+c$ y $a|b$ luego por la Definición 2-n $\exists p, q \in \mathbb{N}: a * p = b + c \wedge a * q = b$, luego sustituyendo la segunda ecuación en la primera obtenemos que $a * p = a * q + c$, como todos estos números son naturales se debe dar $a * p \geq a * q$ pues en caso contrario si $a * p < a * q$, sumando $c$ a ambos lados se tiene que $a * p + c < a *$

$q + c$ y reemplazando nuestra ecuación que $a * p = a * q + c$ se tiene $a * p + c < a * p$, lo cual es contradictorio pues $\forall x, y \in \mathbb{N}, x \leq x + y$.

Como $a * p \geq a * q$ debe darse necesariamente, la resta $a * p * -a * q$ se puede hacer, es un número natural, además se tiene que $a * p * -a * q = c$ y por la propiedad distributiva de la multiplicación respecto a la resta $a * (p - q) = c$, luego por la Definición 2-n, $a|c$ y se tiene el teorema.

**Teorema 9-n:** $\forall a \in \mathbb{N}$ si $a|1$ entonces $a = 1$

Demostración:

Tenemos $a|1$ por lo cual por el Teorema 6-n $a \leq 1$, si $a = 1$ se tiene el teorema, si $a < 1$ por el Lema utilizado en el Teorema 4-n, no queda otra posibilidad más que $a = 0$, pero esto es una contradicción ya que 0 solo es divisor de sí mismo, por lo cual se tiene el teorema.

Como mencionábamos antes, se establece que el Teorema 7-n, requiere del siguiente resultado para demostrarse, se trata del principio del buen orden:

**Teorema 10-n:** $\forall A \subseteq \mathbb{N}, A \neq \emptyset \rightarrow \exists m \in A: m = \min A$

Demostración:

Supongamos $S \subseteq \mathbb{N}, S \neq \emptyset$, tal que $S$ no tiene mínimo, sea el conjunto $A = \{x \in \mathbb{N}: x \notin S \wedge \forall b \in S, x < b\}$, sabemos que $A$ no es vacío pues 0 es cota inferior de $\mathbb{N}$ y por tanto lo es de todo subconjunto de él, si $0 \in S$ se tiene que 0 es mínimo en $S$, por lo cual $0 \notin S$ y en consecuencia $0 \in A$, si $n \in A$ por la definición de $A$, $n \notin S$, $\forall n$ y también por definición de $A$, $n$ es cota inferior de $S$, ahora si $n^+ \in S$, como $S$ no tiene mínimo, $\exists b \in S: b < n^+$, además $n < b$, y en conclusión $n < b < n^+$, lo cual en $\mathbb{N}$ no es posible, llegando así a una contradicción, luego $n^+ \notin S$, por lo tanto $n^+ \in A$, luego por el principio de inducción $A = \mathbb{N}$, siendo $A$ un conjunto de números que no pertenecen a $S$, se tiene que $S = \emptyset$, pero habíamos supuesto que $S \neq \emptyset$, por lo cual se llega a una contradicción, por tanto se debe cumplir $\exists m \in A: m = \min A$.

Para demostrar el teorema anterior se necesitó de que no existe un número natural entre $a$ y $a^+$, este resultado también debe demostrarse si se quiere que el Teorema 10-n y el Teorema 7-n sean válidos:

**Teorema 11-n:** $\nexists x, n \in \mathbb{N}: n < x < n^+$

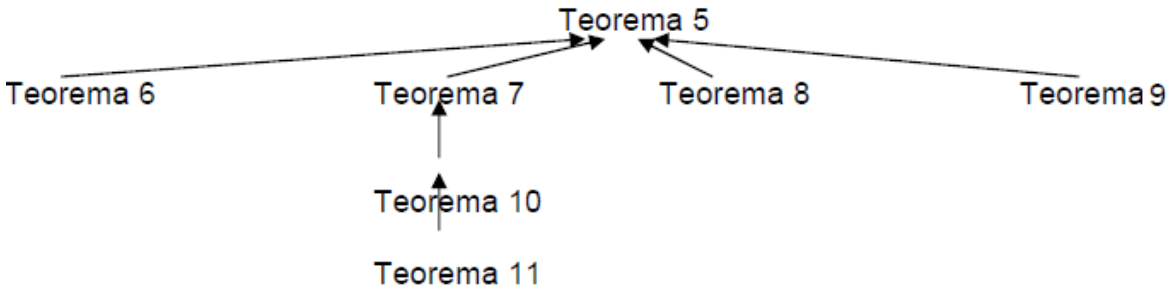
Demostración:

Dado $n < x < n^+$, si se resta $n$ en las desigualdades se tiene $0 < x - n < 1$, pero por el lema utilizado en el Teorema 4-n esto es una contradicción por lo cual se tiene que tales $n, x$ no pueden existir en los naturales.

Demostración Teorema 7-n:

Sea $c > 1$ un número compuesto, definiremos $C = \{x \in \mathbb{N}: x\ es\ compuesto\ \wedge x|c\}$, por el Teorema 10-n, se tiene que $C$ tiene mínimo, llamemos a este $m$, por supuesto ya que $m \in C$, me es compuesto y $m|c$, ahora sea $n$ un divisor de $m, n \neq 1, n \neq m$, tal $n$ existe ya que $m$ es compuesto y por ello tiene más de dos divisores, como $n|m$ se concluye que $n|c$ por la propiedad transitiva de $|$, ahora si $n$ es primo se tiene el teorema, supongamos que $n$ es compuesto y por tanto $n \in C$, pero como $n|m$ se tiene por el Teorema 6-n que $n \leq m$, pero como $m = \min C$ se tiene que $m \leq n$ y por lo tanto $m = n$ lo cual es una contradicción pues tomamos , $n \neq m$, por tanto $n$ debe ser primo y se tiene el teorema.

Habiendo sustentado completamente el Teorema 7-n, la lectura nos da el siguiente esquema que indica el proceso que se siguió para validar el Teorema 5:



Y así se confirma que el resultado es verdadero, existen infinitos números primos.

A continuación se plantea un procedimiento para saber cuándo un número es primo o cuándo es compuesto, la primera idea que surge, usando la experiencia que tenemos trabajando en matemáticas, es dividir por los posibles candidatos de divisores el número primo, si efectivamente alguno diferente de 1 y de el mismo lo divide entonces el número no es compuesto, si de lo contrario ninguno lo divide se concluye que el número es primo; así hace falta tal herramienta para dar una respuesta, esto es, definir como dividir:

**Teorema 12-n:** Dados $a, b \in \mathbb{N}, b \neq 0$ existen $q, r$ únicos tal que $a = bq + r$ con $r < b$

Demostración:

Se tienen tres posibilidades para $a, b$ ya que se cumple la tricotomia en $\mathbb{N}$,

$$a < b \veebar a = b \veebar b < a$$

Si $a < b, a = b\ 0\ + a$.

Si $a = b, a = b\ 1\ + 0$.

Puede suceder $b|$a o $b \nmid a$, para el primer caso por Definición 2-n, $bx + 0 = a$, para algún $x$ natural, por tanto se tiene el teorema, en caso contrario $b \nmid a$, se define $B = \{bk \in \mathbb{N}: bk < a\}$, este conjunto tiene un maximo que llamaremos $bq$ pues $a$ es cota inferior de el, se cumple que $bq < a < b(q + 1)$ pues $b \nmid a$ y $bq$ es el máximo de los múltiplos de $b$ menores que $a$, por definición de $<$ , $a = bq + r$ y reemplazando esta igualdad en la desigualdad anterior $bq + r < bq + b$, luego por la propiedad de monotonia de $<$ respecto a la suma $r < b$.

Ahora demostremos que $q, r$ son únicos, por contradicción supongamos que hay dos, sean $q' y\ r'$ el otro par de números que satisfacen $a = bq' + r'$ con $r' < b$ por ambas igualdades se tiene que $bq' + r' = bq + r$, se tienen tres posibilidades para $q$ y $q'$:

$$q < q' \veebar q = q' \veebar q' < q$$

Si $q = q'$, reemplazando en la ecuación anterior se obtiene $bq + r' = bq + r$, y como en $\mathbb{N}$, la suma es cancelativa$r' = r$ y se tendría el teorema.

Consideraremos por ejemplo $q' < q$ y el proceso para deducir la unicidad para el otro caso es análogo al siguiente, $0 < q - q'$ ya que por la condición anterior esta resta se puede hacer, además $q' < q$ implica que $r < r'$, si los residuos fueran iguales $bq' + r = bq + r, bq = bq', q = q'$ ya que $b \neq 0$ se tendría el teorema, y si se diera $r' < r, a - r' > a - r$, por lo cual $bq' > bq$ y por la monotonía de la multiplicación respecto a la relación de orden en $\mathbb{N}$ se tendria que $q' > q$, lo cual es una contradicción con nuestra hipótesis, como $r < r'$ la resta $r' - r$ puede hacerse, de esta manera $bq - bq' = r' - r$ y por la propiedad distributiva de la multiplicación respecto a la resta se tiene que $b(q - q') = r' - r$, por la Definición 2-n $b|r' - r$, y por el Teorema 6-n $b \leq r' - r$, pero como $r' < b \wedge r < b$ se tiene que $r' - r < b$, llegándose así a una contradicción, análogamente suponer por tanto tales $q < q'$ nos lleva a una contradicción por lo cual tales $q' y\, r'$ no pueden existir y se tiene el teorema.

Dado este teorema el documento prosigue con enunciar el teorema fundamental de la aritmética para los números naturales, cuya demostración depende de un teorema posterior:

**Teorema Fundamental de la aritmética.** Todo número natural $n$ mayor que 1, se puede representar como $n = p_1 p_2 p_3 \dots p_k$ donde $p_1 p_2 p_3 \dots p_k$ son números primos y esta representación es única salvo el orden de los factores.

El teorema que da pie a que se demuestre este es el siguiente:

**Teorema 13-n:** Dado $p$ primo, Si $p|a * b$ entonces $p|a$ ó $p|b$

Demostración Teorema 13-n:

Si $p|a$ se tiene el resultado, por tanto supongamos $p \nmid a$, para $a \neq 0$ se define $A = \{x \in \mathbb{N}: p|xb \wedge p \nmid x\}$, este conjunto no es vacío pues $a \in A$, si $1 \in A$ se tiene el teorema, por lo cual consideraremos lo contrario, por el Teorema 10-n $A$ tiene un mínimo al que llamaremos $s$. Ahora por el algoritmo de la división, existen dos naturales $q, r$ tales que

$p = sq + r$ con $r < s$, ya que $s \in A$ por definición de este conjunto se tiene que $p|sb$ y por la Definición 2-n existe un $d \in \mathbb{N}$ tal que $pd = sb$, por otro lado de nuestra primera ecuación tenemos que multiplicando por $b$ a ambos lados $pb = sbq + rb$, y reemplazando $pd = sb$ en esta se obtiene $pb = pdq + rb$ y por el Teorema 8-n $p|rb$.

Se pueden dar dos casos $p|r \ \veebar \ p \nmid r$ supongamos que se cumple lo segundo $p \nmid r$, por definición del conjunto $A$, $r \in A$ pero como $r < s$, esto contradice el hecho de que $s$ sea el mínimo de $A$.

Se debe dar $p|r$ , ahora por el Teorema 6-n $p \leq r$ ó $r = 0$. Si $r = 0$, se tendrá que $p = sq$ y como $p$ es primo, $s = p \vee s = 1$, como $p \nmid s, s = 1$, pero si esto pasa como $p|sb$ se concluye que $p|b$ y se tendría el teorema.

Por otro lado, si $p \leq r$ como $p = sq + r$, $p \geq r$, por lo que se concluye $p = r$, pero esto nos llevaría a que $p < s$, en este punto de la demostración hace falta algún resultado que nos indique que esto no es cierto, en este punto el documento es inconcluso ya que afirma $p \in A$ y esto conlleva a $r \in A$ , reduciendo así al caso anterior y entrando en una contradicción, sin embargo en sí mismo suponer $p \in A$ es contradictorio puesto que $p|p$.

En los números enteros se tiene el Teorema de Bézout que permite obtener este resultado más directamente, usando una propiedad del máximo común divisor, para completar la demostración de este teorema, aunque no se tenga el Teorema de Bézout en $\mathbb{N}$, aceptaremos como cierta una propiedad del máximo común divisor, que se cumple en $\mathbb{N}$, tuvimos oportunidad de enunciarla en el Teorema 27-z:

Lema: $\forall a, b \in \mathbb{N}: (mcd\ a, b = 1 \wedge mcd\ a, c = 1) \rightarrow mcd\ a, b * c = 1$

Demostración Teorema 13-n:

Tomaremos como hipótesis que $p|a * b$ , supongamos por contradicción que $p \nmid a \wedge p \nmid b$, se tiene que $mcd\ p, a = 1$ puesto que por la Definición 2-n como $p$ es primo solo tiene dos divisores $1, p$ y si $mcd\ p, a = p$, por definición de máximo común divisor $p$ sería un divisor de $a$ y se llegaría a una contradicción. De la misma manera se concluye que

$mcd\ p, b\ = 1$, y por nuestro lema tenemos que $mcd\ p, a * b\ = 1$, esto es una contradicción ya que $p$ es divisor de $a * b$ por nuestra hipótesis y $p > 1$, por tanto se tiene el teorema.

Corolario: Dado $p$ primo, Si $p|a_1 * a_2 * ... * a_n$ entonces $p|a_i$, para algún $i, 1 \leq i \leq n$

Con el este teorema que usualmente se le denota como Lema de Euclides, se puede proseguir a dar una demostración del Teorema Fundamental de la Aritmética en $\mathbb{N}$:

Demostración TFA- $\mathbb{N}$ (existencia):

Demostraremos inicialmente que si $a \in \mathbb{N}, a > 1$, existe una descomposición en factores primos para $a$.

Sea $a \in \mathbb{N}, a > 1$ si $a$ es un numero primo puede escribirse de manera única como producto de el mismo, por tanto se tendría el teorema.

Si $a$ es compuesto por el Teorema 7-n se tiene que tiene al menos un divisor primo, notemos a este $p_1$, por la Definición 2-n $\exists a_1 \in \mathbb{N}: a_1 * p_1 = a$ y $a_1 < a$.

Si $a_1$ es primo se tiene el teorema, en caso contrario $a_1$ es compuesto, repetimos el proceso que seguimos para $a$ encontrando $a_2 * p_2 = a_1$, con $p_2$ primo, $a_2 < a_1$ ,y sucesivamente repetimos el proceso para los siguientes $a_i$, con $1 \leq i$obteniendo números primos $p_i$ tales que $a_i = a_{i+1} * p_{i+1}$, y se tiene la cadena de desigualdades , $a_i < \cdots < a_2 < a_1 < a$, llamemos al conjunto de todos los $a_i$ compuestos obtenidos por este proceso $A$, $A \neq \emptyset$ por tanto aplicando el Teorema 10-n, $A$ tiene un mínimo que notaremos $a_n$.

Si $a_n$ es primo se tiene el teorema pues la descomposición que se obtiene es $a = p_1 * p_2 * p_3 * ... * p_n$ y si es 1, se tiene $a = p_1 * p_2 * p_3 * ... * p_{n-1} * 1 = p_1 * p_2 * p_3 * ... * p_{n-1}$, por lo cual consideremos el caso contrario en que $a_n$ es compuesto, por el Teorema 7-n y la Definición 2-n este tiene al menos un divisor primo $p_{n+1}$ tal que $p_{n+1} * a_{n+1} = a_n$, $a_{n+1} < a_n$, se debe cumplir que $a_{n+1}$ es primo, pues si fuera compuesto se daría que $a_{n+1} \in A$ lo que es una contradicción ya que $a_n$ es el mínimo de $A$, por tanto se obtiene la descomposición $a = p_1 * p_2 * p_3 * ... * p_n * p_{n+1}$ y se cumple el teorema.

Demostración TFA- ℕ (unicidad):

Supongamos por contradicción que existen dos descomposiciones en factores primos de $a$, por lo cual:

$$a = p_1 * p_2 * p_3 * ... * p_n \text{ con } p_i \text{ primos } 1 \leq i \leq n$$

$$a = q_1 * q_2 * q_3 * ... * q_m \text{ con } q_j \text{ primos } 1 \leq j \leq m$$

Supongamos que $m \neq n$, y sin pérdida de generalidad que $m > n$. Como:

$$a = p_1 * (p_2 * p_3 * ... * p_n)$$

Por la Definición 2-n, se tiene que $p_1|$a, por lo tanto $p_1|q_1 * q_2 * q_3 * ... * q_m$. Ahora por el corolario del Teorema 13-n, $\exists j, 1 \leq j \leq m$ tal que $p_1|q_j$, pero como $p_1$ y $q_j$ son primos, no queda otra opción más que $p_1 = q_j$, podemos suponer que $j = 1$, pues si no lo fuera, podemos cambiar el orden de los factores en la descomposición para que se cumpla, de esta manera $p_1 = q_1$.

Reemplazando la igualdad anterior en las dadas se tiene entonces que:

$$p_1 * p_2 * p_3 * ... * p_n = p_1 * q_2 * q_3 * ... * q_m$$

Y aplicando la propiedad cancelativa de la multiplicación en ℕ ya que $p_1 > 0$:

$$p_2 * p_3 * ... * p_n = q_2 * q_3 * ... * q_m = a_1$$

Obtenemos que $a_1 < a$ y repitiendo el proceso anterior para $a_1$:

$$a_1 = p_2 * (p_3 * ... * p_n)$$

Por la Definición 2-n, se tiene que $p_2|$a$_1$, por lo tanto $p_2|q_2 * q_3 * ... * q_m$. Por el corolario del Teorema 13-n, $\exists j, 2 \leq j \leq m$ tal que $p_2|q_j$, pero como $p_2$ y $q_j$ son primos, no queda otra opción más que $p_2 = q_j$, podemos suponer que $j = 2$, de manera similar al paso anterior y concluimos $p_2 = q_2$, de esto obtenemos que:

$$p_2 * p_3 * \dots * p_n = p_2 * q_3 * \dots * q_m$$

$$p_3 * \dots * p_n = q_3 * \dots * q_m = a_2$$

Obtenemos que $a_2 < a_1 < a$, con $m > n$ al repetir el proceso $n - 1$ veces se llega a:

$$a_{n-1} = p_n = q_n * q_{n+1} * q_{n+2} * \dots * q_m$$

Con $a_n < a_{n-1} < \dots < a_2 < a_1 < a_0 = a$, y repitiendo el proceso una vez más:

Por la Definición 2-n y el Teorema 2-n se tiene que $p_n | a_{n-1}$, por lo tanto:

$$p_n | q_n * q_{n+1} * q_{n+2} * \dots * q_m$$

Por el corolario del Teorema 13-n, $\exists j, n \leq j \leq m$ tal que $p_n | q_j$, pero como $p_n$ y $q_j$ son primos, se debe dar $p_n = q_j$, podemos suponer que $j = n$ y concluimos $p_n = q_n$, de esto obtenemos que:

$$p_n = p_n * q_{n+1} * q_{n+2} * \dots * q_m$$

$$1 = q_{n+1} * q_{n+2} * \dots * q_m$$

Del Teorema 4-n se deduce que:

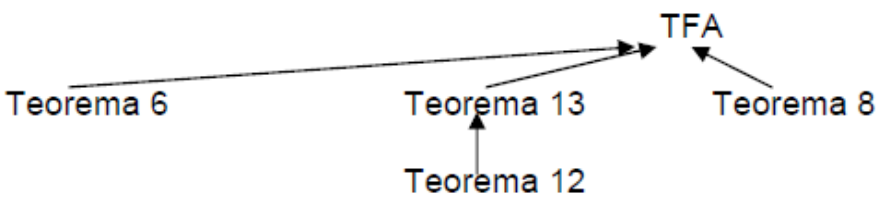
$$1 = q_{n+1} = q_{n+2} = q_m$$

Lo cual es una contradicción pues $q_j$ son primos y por tanto $q_j > 1$, por esto se debe cumplir $m = n$, con el proceso además demostramos que $\forall n, q_n = p_n$, por lo cual:

$$a = p_1 * p_2 * p_3 * \dots * p_n$$

Es una descomposición única.

El documento producto del seminario de algebra, como último inzumo nos ofrece el siguiente esquema que resume el camino que hemos seguido para la demostración de un TFA en $\mathbb{N}$:




A lo largo del documento al trabajar con teoremas similares a los que se presentan en este camino, iremos notando cuales propiedades se pierden o cuales se ganan respecto a este primer ejemplo de estudio de teoría de números no usual. Buscamos que este proceso para demostrar el TFA en $\mathbb{N}$ nos de herramientas para que con los que se siguieron en los nuevos conjuntos se pueda comprobar o refutar un TFA, se busca, ¿qué elementos hay diferentes?, ¿cuáles se conservan? , ¿cuáles se pierden?, ¿qué elementos distintos hay en cada camino para llegar al TFA?

Comenzaremos el trabajo sentando las bases necesarias para estudiar la relación de divisibilidad, esto es, definiendo los elementos más básicos de los nuevos conjuntos que llamaremos $M(i^2)$ y mostrando varias de sus propiedades para familiarizar al lector con estos, tal y como lo hicimos al principio de esta sección.

# 3. Conjuntos $\mathbf{M(i^2)}$ y las operaciones para trabajar divisibilidad

## 3.1 Propiedades algebraicas

Cuando se habla de teoría de números en un determinado conjunto, usualmente dominios de integridad como en el caso de $\mathbb{Z}$, es inevitable preguntarse por ciertos elementos básicos para el desarrollo de esta, algunos son claves como los números primos, unidades, los teoremas de descomposición, las propiedades de las operaciones (en especial de la multiplicación), la divisibilidad, las relaciones entre números y entre otros que, según el significado que se les atribuya, permiten el desarrollo de la teoría y conseguir o refutar la existencia de otros elementos importantes como el algoritmo de Euclides, el teorema fundamental de la aritmética, el teorema del residuo y el teorema del factor, análogos a los que se tienen en la teoría de números en conjuntos usuales, en el caso de este trabajo, serán de nuestro interés los conceptos mencionados y los conjuntos sobre los cuales se construirá la teoría son muy similares al conjunto de los números gaussianos (Brausín & Pérez, 2012), esto es, dentro del conjunto de los números enteros consideraremos la existencia de un elemento adicional $i$ siendo la raíz de un número que no tiene raíz cuadrada en los números enteros, en este caso $-1$, surgiendo así la forma general $a + bi$ que caracterizan todo elemento del conjunto, una parte real y una imaginaria, la diferencia será que en este trabajo el elemento $i$ cumple una condición diferente pero análoga a que su cuadrado sea $-1$, inicialmente definamos los conjuntos cuyo cuadrado es cualquier entero:

**Definición 1**: Sean los conjuntos de la forma

$$A = \{a + bi : a, b \in \mathbb{Z} \ \wedge i^2 = r^2, r \ \in \mathbb{Z}, i \neq \pm r\}$$

Una de los elementos básicos para trabajar antes de definir las operaciones es la igualdad entre números, la definición componente a componente sirve para estos casos:

**Definición 2, igualdad entre números (μ):**

$$\forall a+bi, c+di \in A, a+bi = c+di \leftrightarrow a = c \wedge b = d$$

La primera definición nos será útil para referirnos a resultados los cuales son válidos para cualquier valor de $i^2$, esto puede ser útil para el lector si está realizando estudios sobre números Gaussianos, de Minkowski o algún conjunto que siga el mismo esquema para ser definido, es la intención de este trabajo abordar el caso en el cual el número obtenido con $i^2$ es algún número entero al cuadrado, aunque como podremos demostrar después de pasar por la cuarta sección de este trabajo cuando $i^2$ no es un número cuadrado la estructura del conjunto determina un dominio de integridad y por lo tanto el estudio de teoría de números sobre estos conjuntos $A$ se hace muy similar al de los números enteros, nuestro objetivo será un estudio diferente, de manera que la definición de las estructuras de interés en este trabajo será:

**Definición 3**, **conjuntos con $r^2$:** $M(i^2) = \{a+bi : a, b \in \mathbb{Z} \wedge i^2 = r^2, r \in \mathbb{Z}, i \neq \pm r\}$

Como ejemplo de estas estructuras, como casos usuales se tiene a $M\ 0$ , $M\ 1$ los números duales y de Minkowski respectivamente, se presenta la generalización de las operaciones básicas de este tipo de conjuntos:

**Definición 4**, **operaciones (μ):**

$$+: \forall a+bi \in M(i^2), (a+bi) + (c+di) = (a+c) + (b+d)i$$

$$*: \forall a+bi \in M(i^2),\ a+bi * (c+di) = (ac+bdr^2) + (bc+ad)i$$

Cabe notar que en cada estructura las operaciones + y * están bien definidas, es decir la suma de dos números en $M(i^2)$ es un numero en el conjunto, y la multiplicación de dos números del conjunto también pertenecerá a $M(i^2)$, ya que la suma y el producto en $\mathbb{Z}$ están bien definidas, por lo cual $a+c$ , $b+d$ , $ac+bdr^2$ , $(bc+ad)$ son números enteros, lo que implica que $a+bi + c+di$ y $a+bi * (c+di)$ son elementos de $M(i^2)$.

### 3.2 Otra representación para los números $M(i^2)$

**Teorema 1**, **isomorfismo $a + bi$ y $(a, b)$ (μ):** La estructura $(M(i^2), +, *)$ es isomorfa a la estructura $(A_{r^2}, +', *')$ definida de la siguiente manera

$$A_{r^2} = \{a, b : a, b \in \mathbb{Z}\}$$

$$+' : \forall a, b \in A_{r^2}, (a, b) + (c, d) = (a + c, b + d)$$

$$*' : \forall a, b \in A_{r^2}, \ (a, b) *' (c, d) = (ac + bdr^2, ad + bc)$$

**Demostración:**

Dada la función $f : (M(i^2), +, *) \rightarrow (A_{r^2}, +', *')$ tal que $f(a + bi) = (a, b)$, demostraremos que es un isomorfismo entre las estructuras, demostremos inicialmente que la función es biyectiva:

a) $f$ es inyectiva $(\forall x, y \in M(i^2))(f(x) = f(y) \rightarrow x = y)$:

$a + bi$ , $c + di$ dos elementos cualesquiera de $M(i^2)$.

$f(a + bi) = (a, b) \wedge f(c + di) = (c, d)$ son las imágenes de $a + bi$ y $c + di$ por la definición de la función $f$.

$(a, b) = (c, d)$, es la hipótesis de nuestro teorema[3]

$a = c \wedge b = d$, por la definición de igualdad en parejas ordenadas

$a + bi = c + di$, por D2

$f$ es inyectiva, por definición de función inyectiva.

b) $f$ es sobreyectiva $(\forall x \in A_{r^2})(\exists y \in M(i^2))(f(y) = x)$:

Sea un elemento cualquiera $(a, b)$ de $A_{r^2}$, para este existe $a + bi$ en $M(i^2)$ tal que $f(a + bi) = (a, b)$, por lo tanto la función es sobreyectiva.

[3] Recordemos que la igualdad entre parejas ordenadas (a,b)=(c,d) se da si y solamente si a=b y c=d.

Por lo anterior la función $f$ es biyectiva.

Ya demostramos que la función $f$ es biyectiva, para que esta sea isomorfismo (para las dos operaciones) falta demostrar que $f$ es un homomorfismo para cada una:

a) El homomorfismo entre sumas:

$$f\ \ a+bi\ +\ c+di\ \ = f\ \ a+c\ +\ b+d\ i\ \text{, por D4}$$

$$f\ \ a+c\ +\ b+d\ i\ \ = (a+c, b+d)\text{, por la definición de } f$$

$$a+c, b+d\ \ = (a,b)\ +'(b,d)\text{, por la definición de } +'$$

$$a,b\ +'\ b,d\ \ = f(a+bi)+'f(c+di)\text{, por la definición de } f$$

$$f\ \ a+bi\ \ +(c+di)\ \ = f(a+bi)+'f(c+di)\text{, por propiedad transitiva de la igualdad.}$$

b) El homomorfismo entre multiplicaciones:

$$f\ \ a+bi\ *\ c+di\ \ = f\ ac+bdr^2+\ \ ad+bc\ i\ \text{, por D4}$$

$$f\ ac+bdr^2+\ \ ad+bc\ i\ =\ ac+bdr^2,\ ad+bc\ \text{, por la definición de } f$$

$$ac+bdr^2, ad+bc\ =\ a,b\ *'\ (c,d)\text{, por la definición de } *'$$

$$a,b\ *'\ b,d\ \ = f(a+bi)*'f(c+di)\text{ , por la definición de } f$$

$$f\ \ a+bi\ *(c+di)\ \ = f(a+bi)*'f(c+di)\text{, por propiedad transitiva de la igualdad.}$$

Ya que la función $f$ es un homomorfismo (para ambas operaciones) biyectivo, se concluye que es un isomorfismo entre $(M(r^2),+,*)$ y $(M(r^2),+',*')$.

Con el teorema anterior, hemos ganado una nueva representación para nuestra estructura de números $(M(i^2),+,*)$, esta nueva representación resulta más conveniente para hacer cálculos y simplificar la escritura de la mayoría de demostraciones y en algunas ocasiones esta representación nos enseña propiedades que en la original no son tan simples de notar,

por ello, llegamos a los siguientes acuerdos para trabajar de forma eficiente con ambas representaciones en el presente trabajo:

- ✓ Se usara principalmente la representación $(A_{r^2}, +', *')$ en este trabajo
- ✓ Usaremos indiscriminadamente el símbolo $+$ en vez de $+'$, y $*$ en vez de $*'$, para que no se presenten ambigüedades y teniendo en cuenta que en la representación de parejas ordenadas el significado de igualdad, suma y multiplicación es el mismo que se tiene para los números $a + bi$.
- ✓ Se usará la notación $(M(i^2), +, *)$ para hablar de la estructura de números en ambas representaciones.
- ✓ Para simplificar la escritura de las operaciones se introduce la notación $(a, b)(c, d)$ significando esto el producto $(a, b) * (c, d)$.
- ✓ Se debe tener en cuenta que la definición de igualdad entre parejas ordenadas es equivalente a la definición 2 que establecimos para los $M(i^2)$.
- ✓ Los Teoremas y definiciones válidas para cualquier valor de $i^2$ incluso sin ser este un número cuadrado, tendrán un símbolo **(μ)** para distinguirlos.

Ya establecidas las operaciones con las cuales se trabajará , es de interés conocer cómo funcionan estas operaciones, como hacen interactuar a los números definidos entre sí, en otras palabras, que propiedades cumplen, algunas de las encontradas se presentan en el siguiente teorema:

**Teorema 2(μ):** $(M(i^2), +)$ es un grupo abeliano, $(M(i^2), *)$ un monoide conmutativo y $(M(i^2), +, *)$, es un anillo conmutativo con unidad.

**Demostración:**

Inicialmente probaremos las propiedades de la suma, que $(M(i^2), +)$ sea un grupo abeliano significa:

1) *+ es asociativa*:

$$a, b \ + \ c, d \ \ + \ e, f \ = \ \ a + c, b + d \ \ + (e, f), \text{ por T1}$$

$$a+c, b+d \quad + (e,f) = ((a+c)+e, (b+d)+f), \text{ por T1}$$

$$a+c \ +e, \ b+d \ +f \ = (a+(c+e), b+(d+f)), \text{ por la propiedad asociativa de la suma en } \mathbb{Z}$$

$$a+ \ c+e \ , b+ \ d+f \ = \ a,b \ + \ c+e, d+f \ , \text{ por T1}$$

$$a,b \ + \ c+e, d+f \ = \ a,b \ + (\ c,d \ + (e,f)), \text{ por T1}$$

$$a,b \ + \ c,d \ + \ e,f \ = \ a,b \ + (\ c,d \ + (e,f)), \text{ por propiedad transitiva de la igualdad.}$$

2) *+ es conmutativa*:

$$a,b \ + \ c,d \ = (a+c, b+d), \text{ por T1}$$

$$a+c, b+d \ = (c+a, d+b), \text{ por la propiedad conmutativa de la suma en } \mathbb{Z}$$

$$c+a, d+b \ = \ c,d \ + (a,b), \text{ por T1}$$

$$a,b \ + \ c,d \ = \ c,d \ + (a,b), \text{ por propiedad transitiva de la igualdad.}$$

3) *+ tiene un elemento neutro*:

Para cualquier $a,b \ \in M(i^2)$ se tiene $(0,0)$ tal que $a,b \ + \ 0,0 \ = (a,b)$ pues $a,b \ + \ 0,0 \ = (a+0, b+0)$ y ya que en $\mathbb{Z}$, 0 es elemento neutro, se tiene que esto último es $a+0, b+0 \ = (a,b)$

4) *+ tiene elementos inversos:*

Para cualquier $a,b \ \in M(i^2)$ se tiene $(-a,-b)$ tal que $a,b \ + \ -a,-b \ = (0,0)$ pues $a,b \ + \ -a,-b \ = (a+(-a), b+(-b))$ y ya que en $\mathbb{Z}$ el elemento inverso de $a$ es $-a$, se tiene que esto último es $a+(-a), b+(-b) \ = (0,0)$.

Para que $(M(i^2), +, *)$ sea anillo se necesita que * sea una operación asociativa y distributiva respecto a la suma, además demostraremos que * es conmutativa y tiene un elemento neutro para comprobar que $(M(i^2), *)$ es un monoide conmutativo, probaremos que $\forall \ a,b \ , \ c,d \ , (e,f) \in M(i^2)$:

1) * *es asociativa*:

$$a,b \quad c,d \quad e,f \;=\; ac+bdr^2, ad+bc \quad (e,f), \text{ por T1}$$

$$ac+bdr^2, ad+bc \quad e,f \;=\; ac+bdr^2\ e+\ ad+bc\ fr^2,\ ac+bdr^2\ f+ ad+bc\ e\ , \text{ por T1}$$

$$ac+bdr^2\ e+\ ad+bc\ fr^2,\ ac+bdr^2\ f+\ ad+bc\ e \;=\; ace+ bdr^2e\ +\ adfr^2+bcfr^2\ ,\ acf+bdr^2f\ +\ ade+bce\ , \text{ por la propiedad distributiva de la multiplicación respecto a la suma en } \mathbb{Z}$$

$$ace+bdr^2e\ +\ adfr^2+bcfr^2\ ,\ acf+bdr^2f\ +\ ade+bce \;= ace+bdr^2e+adfr^2+bcfr^2, acf+bdr^2f+ade+bce\ , \text{ por la propiedad asociativa de la multiplicación en } \mathbb{Z}$$

$$ace+bdr^2e+adfr^2+bcfr^2, acf+bdr^2f+ade+bce\ = (a\ ce+dfr^2\ + b\ dr^2e+cfr^2\ , a\ de+cf\ +b(ce+dfr^2)), \text{ por la propiedad distributiva de la multiplicación respecto a la suma en } \mathbb{Z} \text{ y la propiedad conmutativa de la suma en } \mathbb{Z}$$

$$a\ ce+dfr^2\ +b\ dr^2e+cfr^2\ , a\ de+cf\ +b\ ce+dfr^2\ = (a,b)(ce+ dfr^2, cf+de), \text{ por T1}$$

$$a,b \quad ce+dfr^2, cf+de\ = (a,b)(\ c,d \quad e,f\ ), \text{ por T1}$$

$$a,b \quad c,d \quad e,f\ = (a,b)(\ c,d \quad e,f\ ), \text{ propiedad transitiva de la igualdad.}$$

2) * *es conmutativa*:

$$a,b \quad c,d\ = (ac+bdr^2, ad+bc), \text{ por T1}$$

$(ac + bdr^2, ad + bc) = (ca + dbr^2, da + cb)$, propiedad conmutativa de la multiplicación en $\mathbb{Z}$

$(ca + dbr^2, da + cb) = \ c, d \ (a, b)$, por T1

$a, b \quad c, d \ = \ c, d \ (a, b)$, por propiedad transitiva de la igualdad.

3) * *tiene un elemento neutro*:

En particular, es interesante exponer aquí el proceso de exploración para encontrar el elemento neutro de la multiplicación, ya que, este proceso nos indica la existencia de elementos diferentes a el que tienen una propiedad similar, la cual retomaremos más adelante, esta deducción se presenta haciendo uso del método analítico:

$a, b \quad x, y \ = (a, b)$, es nuestra hipótesis

$ax + byr^2, ay + bx \ = \ a, b$ , por T1

$ax + byr^2 = a \wedge ay + bx = b$, por T1 y D2

$a(x - 1) + byr^2 = 0 \wedge ay + b(x - 1) = 0$, sumando $-a$ a ambos lados en la primera ecuación, $-b$ a ambos lados en la segunda y usando la propiedad distributiva en $\mathbb{Z}$

$ab(x - 1) + b^2yr^2 = 0 \wedge a^2y + ab(x - 1) = 0$, multiplicando la primera ecuación por $b$ y la segunda por $a$

$a^2y - b^2yr^2 = 0$, restando la primera ecuación de la segunda

$(a^2 - b^2r^2)y = 0$, usando la propiedad distributiva de la multiplicación respecto a la suma en $\mathbb{Z}$

$a^2 - b^2r^2 \ = 0 \ \vee \ y = 0$, Propiedad del módulo de la suma

$(ab = 0 \rightarrow a = 0 \vee b = 0)$, es equivalente a la propiedad cancelativa en los números enteros.

$a^2 = b^2r^2 \vee (\ a,b\ \ x,0\ =\ a,b\ \rightarrow (ax = a \wedge bx = b))$, en la primera igualdad se suma a ambos lados el inverso de $-b^2r^2$, si $y = 0$ para deducir la segunda implicación, donde $x = 1$, por definición de multiplicación y de igualdad en parejas ordenadas.

$a^2 = b^2r^2 \vee x = 1,\ x,y\ = (1,0)$, se deduce por T2 usando la propiedad del elemento neutro de ser único.

$a = \pm\ \overline{b^2r^2} \vee\ x,y\ = (1,0)$, usando la definición de raíz cuadrada en $\mathbb{Z}$, ya que$b^2r^2$ es un número cuadrado esta se puede hallar.

$$a = \pm br \vee\ x,y\ = (1,0)$$

Confirmemos que para cualquier $a,b \in M(i^2)$ $1,0$ es elemento neutro, $a,b\ \ 1,0\ =\ a,b$ pues $a,b\ \ 1,0\ =\ a\ 1\ +b\ 0\ r^2, b\ 1\ +a\ 0$ y ya que en $\mathbb{Z}$, $1$ es elemento neutro de la multiplicación y $a\ 0\ = 0\ \forall a \in \mathbb{Z}$, $a\ 1\ + b\ 0\ r^2, b\ 1\ +a\ 0\ =\ a+0, b+0\ =\ a,b$ por ultimo por transitividad de la igualdad se tiene que $a,b\ \ 1,0\ =\ a,b\ , \forall (a,b) \in M(i^2)$. Como hemos dicho antes hay otro tipo de solución a la ecuación $a,b\ \ x,y\ = (a,b)$, sin embargo esta no es genérica, es dependiente de los valores de $a,b$ y $r$ por lo cual estos números aunque cumplen esta propiedad dependiendo de con quien se multipliquen, en general no son neutros, se retomaran más adelante.

4) * *distribuye respecto a* +, Debemos demostrar que para tres elementos cualesquiera $a,b\ ,\ c,d\ , (e,f) \in M(i^2)$ se tiene que $a,b\ (\ c,d\ +\ e,f\ ) =\ a,b\ \ c,d\ +\ (a,b)\ \ e,f\ :$

$$a,b\ \ \ c,d\ +\ e,f\ \ = (a,b)(c+e, d+f), \text{ por T1}$$

$$a,b\ \ c+e, d+f\ = (a\ c+e\ +b\ d+f\ r^2, a\ d+f\ +b(c+e)), \text{ por T1}$$

$$a\ c+e\ +b\ d+f\ r^2, a\ d+f\ +b\ c+e\ = (ac+ae+bdr^2+bfr^2, ad+af+bc+be), \text{ por la propiedad distributiva de la multiplicación respecto a la suma en } \mathbb{Z} \text{ y también por la propiedad asociativa de la suma}$$

$$ac + ae + bdr^2 + bfr^2, ad + af + bc + be \;=\; ac + bdr^2, ad + bc \;+ (ae + bfr^2, af + be)$$, por T1

$$ac + bdr^2, ad + bc \;+\; ae + bfr^2, af + be \;=\; a, b \;\; c, d \;+ (a, b)(e, f)$$, por T1

$$a, b \;(\; c, d \;+\; e, f \;) = \; a, b \;\; c, d \;+ (a, b) \; e, f$$ , por propiedad transitiva de la igualdad.

El compilado de los resultados anteriores respecto a las propiedades de los conjuntos $M(i^2)$(independiente de quien sea $i^2$)con sus operaciones nos indican que $(M(i^2), +,\; 0{,}0\; ,*,\; 1{,}0\;)$ es un anillo conmutativo con unidad; una característica que es deseable en una estructura algebraica con una segunda operación de la cual no se ha hecho mención hasta ahora es la existencia de elementos inversos para esa segunda operación, lamentablemente, o por suerte para los fines de este trabajo, nuestras estructuras no cumplen esta propiedad, es decir en general no se tendrán elementos inversos para la multiplicación, tal como ocurre en $\mathbb{Z}$, esto da interés para estudiar una idea amplia de la teoría de números en estas estructuras como la que se estudia en los números enteros, parece ser que como varias de las propiedades revisadas, esta se 'hereda' por nuestra definición de $M(i^2)$ .

### 3.3El producto por escalar

Teniendo en cuenta el objetivo principal de este trabajo, el estudiar teoría de números y en específico la divisibilidad en las estructuras $(M(i^2), +,\; 0{,}0\; ,*,\; 1{,}0\;)$, explorando las propiedades de estas se puede encontrar una herramienta muy útil para determinar divisores de un número, sobre esto se profundizara más adelante al definir la relación de divisibilidad, no obstante tal herramienta le da una nueva identidad a nuestras estructuras, por la cual se incluye en esta primera sección:

**Definición 5 (μ):** $\forall\; a, b \;\in M(i^2)\; \forall x \in \mathbb{Z},$ se define el producto por escalar $.: \mathbb{Z} * M(i^2) \to M(i^2)$ como $x\;\; a, b \;\; = (xa, xb)$.

Ya que $a, b, x$ son números enteros, el número $(xa, xb)$ será siempre un elemento de $M(i^2)$ por lo cual el producto por escalar está bien definido, también se cumple para este que el un segundo producto por escalar $.: M(i^2) * \mathbb{Z} \to M(i^2)$ generará el mismo número para cualesquiera $a, b, x$, es decir $x\ a, b\ = (a, b)x$, acordamos escribirlo de esta manera sin riesgo a que hayan confusiones con la multiplicación entre números de $M(i^2)$; hemos definido una operación externa cerrada sobre el conjunto, en el siguiente teorema se enuncian algunas propiedades significativas para nuestro trabajo del producto por escalar respecto a la estructura de $M(i^2)$:

**Teorema 3 (μ):** Para el producto por escalar se comprueban las 6 propiedades $\forall\ a, b\ , (c, d) \in\ M(i^2)\ \forall x, y \in \mathbb{Z}$:

1. $x\ \ y\ \ a, b\ \ = (xy)(a, b)$

2. $1\ \ a, b\ \ = (a, b)$

3. $x\ \ \ a, b\ \ +\ \ c, d\ \ \ = x\ \ a, b\ \ + x(c, d)$

4. $\ x + y\ \ \ a, b\ \ = x\ \ a, b\ \ + y(a, b)$

5. $\ x\ \ a, b\ \ \ \ c, d\ \ = x\ \ \ a, b\ \ \ c, d\ \ \ = (a, b)(x(c, d))$

6. $x \neq 0\ \wedge x\ \ a, b\ \ = x(c, d) \to (a, b) = (c, d)$

**Demostración:**

1) $\ x\ \ y\ \ a, b\ \ \ =\ \ xy\ \ \ a, b$

$x\ \ y\ \ a, b\ \ \ = x(ya, yb)$, por D5

$x\ \ ya, yb\ \ = (x\ \ ya\ \ , x(yb))$, por D5

$x\ \ ya\ \ , x\ \ yb\ \ \ = (\ \ xy\ \ a, (xy)b)$, por la propiedad asociativa de la multiplicación en $\mathbb{Z}$

$xy\ \ a,\ \ xy\ \ b\ \ = (xy)(a, b)$, por D5

$x\ \ y\ \ a, b\ \ \ = (xy)(a, b)$, por la propiedad transitiva de la igualdad

2) $1\ a,b\ = (a,b)$

$$1\ a,b\ = (1(a),1(b)), \text{ por D5}$$

$$1\ a\ ,1\ b\ = (a,b), \text{ 1 es elemento neutro en } \mathbb{Z}$$

$$1\ a,b\ = (a,b), \text{ por propiedad transitiva de la igualdad}$$

3) $x\ \ a,b\ +\ c,d\ = x\ a,b\ + x(c,d)$

$$x\ \ a,b\ +\ c,d\ = x(a+c,b+d), \text{ por T1}$$

$$x\ a+c,b+d\ = (x\ a+c\ ,x(b+d)), \text{ por D5}$$

$$x\ a+c\ ,x\ b+d\ = (xa+xc,xb+xd), \text{ por la propiedad distributiva de la multiplicación respecto a la suma en } \mathbb{Z}$$

$$xa+xc,xb+xd\ =\ xa,xb\ + (xc,xd), \text{ por T1}$$

$$xa,xb\ +\ xc,xd\ = x\ a,b\ + x(c,d), \text{ por D5}$$

$$x\ \ a,b\ +\ c,d\ = x\ a,b\ + x(c,d), \text{ por la propiedad transitiva de la igualdad}$$

4) $x+y\ \ a,b\ = x\ a,b\ + y(a,b)$

$$x+y\ \ a,b\ = (\ x+y\ a,(x+y)b), \text{ por D5}$$

$$x+y\ a,\ x+y\ b\ = (xa+ya,xb+yb), \text{ por la propiedad distributiva de la multiplicación respecto a la suma en } \mathbb{Z}$$

$$xa+ya,xb+yb\ =\ xa,xb\ + (ya,yb), \text{ por T1}$$

$$xa,xb\ +\ ya,yb\ = x\ a,b\ + y(a,b), \text{ por D5}$$

$$x+y\ \ a,b\ = x\ a,b\ + y(a,b), \text{ por la propiedad transitiva de la igualdad}$$

5) $x\ a,b\ \ c,d\ = x\ \ a,b\ \ c,d\ = (a,b)(x(c,d))$

$$x\ a,b\ \ c,d\ = (xa,xb)(c,d), \text{ por D5}$$

$$xa,xb\ \ c,d\ = (xac+xbdr^2,xad+xbc), \text{ por T1}$$

$$xac+xbdr^2,xad+xbc\ = x(ac+bdr^2,ad+bc), \text{ por D5}$$

$$x\ ac+bdr^2,ad+bc\ = x((a,b)(c,d)), \text{ por T1}$$

$x\ a,b\quad c,d\ = x\quad a,b\quad c,d\quad$ , por propiedad transitiva de la igualdad

Ahora $a,b\quad x\ c,d\quad = (a,b)(xc,xd)$, por D5

$a,b\quad xc,xd\ =\ axc + bxdr^2, axd + bxc\ $ , por D5

$axc + bxdr^2, axd + bxc\ = x\ ac + bdr^2, ad + bc\ = x(\ a,b\quad c,d\ $ , por la propiedad transitiva de la igualdad

6) $x \neq 0\ \wedge x\ a,b\ = x(c,d) \rightarrow (a,b) = (c,d)$

$x\ a,b\ = x\ c,d\ $ Hipótesis

$xa,xb\ = (xc,xd)$, por D5

$xa = xc\ \wedge xb = xd$, por D2 y T1

$a = c\ \wedge b = d$, por la propiedad cancelativa de la multiplicación en $\mathbb{Z}$ puesto que $x \neq 0$

$a,b\ = (c,d)$, por D2 y T1

Usualmente con las primeras 4 propiedades del producto por escalar, y llamando a $(M(i^2),+)$ conjunto de vectores y a $(\mathbb{Z},+,*)$ conjunto de escalares se llama a $M(i^2)$ un módulo sobre $\mathbb{Z}$ , muy similar a la idea de espacio vectorial, la quinta propiedad además le da a la estructura la identidad de algebra asociativa y adicional a esto notemos que aparecen dos propiedades más que involucran la multiplicación de $M(i^2)$ con la operación producto por escalar, esto nos será muy útil a la hora de hacer operaciones en cualquier estructura $M(i^2)$.

Al igual que en los números reales, el producto por escalar, relacionado con las operaciones suma y multiplicación puede hacer que en notaciones que tienen distintos sentidos, estos se confundan, por ejemplo para indicar el inverso aditivo de $(a,b)$, escribimos $-(a,b)$, que por definición es $(-a,-b)$, pero además esto es equivalente a $((-1)a,(-1)b)$, y esto último es $(-1)(a,b)$, por transitividad de la igualdad diríamos $-\ a,b\ = (-1)(a,b)$, sin embargo en un lado de la igualdad estamos trabajando con solo elementos del conjunto, en el segundo estamos trabajando con un escalar y con un vector del conjunto, esperamos que

este sentido no se pierda al trabajar con el producto por escalar, ya que aunque parece que estuviésemos "factorizando" un número, en esta representación no es así.

Además de las propiedades de las operaciones, hay ciertos elementos en estas estructuras que cumplen propiedades especiales, ejemplo de esto son los elementos neutros de cada operación, mientras seguimos el proceso de deducción de la existencia del neutro para la multiplicación, en este se dedujo la existencia de elementos con una propiedad similar a esta y que cobran un papel importante en el estudio de la divisibilidad en estos conjuntos ya que gracias a la existencia de estos, no se puede afirmar que se cumple la propiedad cancelativa en todo un conjunto $M(i^2)$ y además tienen la propiedad de que estos números se pueden descomponer como multiplicaciones de infinitas maneras, si retomamos con las soluciones a la ecuación $a,b\ \ x,y\ = (a,b)$ son $a = \pm br,\ x,y\ = (1,0)$, la segunda solución a la ecuación nos indicó el elemento neutro usual $x,y\ =\ 1,0$ , por eso para ella el valor de $a,b$ es cualquiera y se cumple $a,b\ \ 1,0\ =\ a,b$ , por otro lado la primera solución es dependiente de $b$ y $r$ estos elementos son menos que neutros, están condicionados a con quien se multipliquen, cumplen una propiedad conocida como absorción, en este caso tanto a izquierda como a derecha ya que nuestra multiplicación es conmutativa, encontremos entonces los $(x,y)$ que hacen que se cumpla la igualdad:

$$\pm br,b\ \ x,y\ = (\pm br,b)$$

Con las propiedades, en específico las 5,6 de T3, del producto por escalar se comprueba que esto equivale a solucionar:

$$b\ \pm r,1\ \ x,y\ = b(\pm r,1), \text{ por D5}$$

$$\pm r,1\ \ x,y\ = (\pm r,1), \text{ por las propiedades 5, 6 de T3}$$

Por ejemplo para el primer caso:

$$r,1\ \ x,y\ =\ r,1\ , \text{ Hipótesis.}$$

$$rx + r^2y, ry + x \ = (r, 1), \text{ por T1}$$

$$r\ x + ry \ = r \ \wedge ry + x = 1, \text{ por la definición de igualdad en parejas ordenadas y aplicando la propiedad distributiva en la primera ecuación}$$

$$x + ry = 1 \ \wedge ry + x = 1, \text{ una ecuación es múltiplo de la otra}$$

$$x = 1 - ry, \text{ se deduce como condición total de las ecuaciones anteriores, sumando a ambos lados de la igualdad el inverso de } ry$$

$$r, 1 \quad 1 - ry, y \ = (r, 1), \text{ adjuntando la solución a la hipótesis}$$

La expresión $1 - ry, y$ nos da infinitas soluciones a la ecuación $r, 1 \quad x, y \ = \ r, 1$ , una por cada valor posible de $y$, por ello estos valores fungen como elementos "neutros" condicionados solo al valor $r, 1$ , o en otros términos encontramos infinitas descomposiciones para los números de la forma $r, 1$ , además multiplicando a ambos lados la ecuación por el escalar $a$:

$$a\ r, 1 \quad 1 - ry, y \ = a(r, 1)$$

$$ar, a \quad 1 - ry, y \ = (ar, a)$$

Y de manera similar para el segundo caso se encuentra:

$$-ar, a \quad 1 + ry, y \ = (-ar, a)$$

Juntando nuestras soluciones se encuentra:

$$\pm ar, a \quad 1 \mp ry, y \ = (\pm ar, a)$$

Obteniendo que cualquier número de la forma $\pm ar, a$ puede ser descompuesto[4] de infinitas maneras en $M(i^2)$, por ejemplo revisemos en $M(4)$ la descomposición de $(6(2),6) = (12,6)$ siguiendo nuestro resultado sería:

$$12,6 \ = (12,6)(1 - 2 \ y \ , y)$$

Considerando $a = 6, r = 2$:

Para $y = 1$

$$12,6 \ = \ 12,6 \ -1,1 \ = (-12 + 6 \ 4 \ , 12 - 6)$$

Para $y = 2$

$$12,6 \ = \ 12,6 \ -3,2 \ = (-36 + 12 \ 4 \ , 24 - 18)$$

Para $y = 3$

$$12,6 \ = \ 12,6 \ -5,3 \ = (-60 + 18 \ 4 \ , 36 - 30)$$

Y sucesivamente se tendrá una descomposición para cada valor de $y$.

Como un elemento $(\pm ar, a)$ puede descomponerse de infinitas formas en $\pm ar, a \ \ 1 \mp ry, y$ , al tener $\pm ar, a \ \ c, d \ = (\pm ar, a)(e, f)$, no se puede afirmar que $c, d \ = (e, f)$, comprobemos esto en el ejemplo anterior:

$$12,6 \ = \ 12,6 \ -5,3 \ = \ 12,6 \ -3,2 \ = \ 12,6 \ -1,1 \ = (12,6)(1,0)$$

La propiedad cancelativa de la multiplicación se cumple para los números no divisores de 0, como demostraremos más adelante, empleándola tendríamos cancelando $12,6$ :

$$-5,3 \ = \ -3,2 \ = \ -1,1 \ = (1,0)$$

[4]Que un número pueda ser descompuesto significa que puede ser escrito usando las operaciones usando otros números, $a, b \ = (x, y)(m, n)$ indica que $(a, b)$ puede ser descompuesto en términos de $(x, y)$ y $(m, n)$.

Y tal cadena de igualdades se extendería para todo valor posible de $y$; como veremos más adelante estos elementos guardan una relación con el elemento neutro de la suma $(0,0)$ tan cercana que se podría decir que son como los ceros de nuestras estructuras, al aplicar la propiedad cancelativa en estas estructuras sobre estos elementos estaríamos haciendo algo similar a dividir por 0.

Nótese que los números $\pm ar, a$ , dependen del valor de $\pm r$, o más específicamente dependen de la existencia de ese $\pm r,$ tal se obtiene en nuestras estructuras gracias a que $i^2 = r^2$, es decir en las estructuras en las cuales $i^2$ no sea un numero cuadrado, estos números problemáticos no existirán; por otro lado los números $1 - ry, y$ , pueden ser obtenidos a partir de los $\pm ar, a$ , como $1 \mp ry, y = 1,0 + (\mp ry, y)$, tomando $a = y$, esta relación no es nueva en las matemáticas, de hecho a estos elementos usualmente se les relaciona cuando $\pm ar, a$ es nilpotente , sin embargo como se demostrara más adelante estos números solo cumplen tal condición en el conjunto de los números duales $M(0)$.

El hecho de que no se cumpla la propiedad cancelativa en los conjuntos $M(i^2)$, para los números distintos a (0,0), es un equivalente a establecer decir existen números cuyo producto es (0,0), hagamos entonces una exploración similar a la anterior para encontrar tales números:

$$a, b \quad x, y = (0,0), \text{ será nuestra hipótesis}$$

$$ax + byr^2, ay + bx = (0,0), \text{ por T1}$$

$$ax + byr^2 = 0 \ \wedge \ ay + bx = 0, \text{ por definición de igualdad en parejas ordenadas}$$

$$axy + by^2r^2 = 0 \ \wedge \ axy + bx^2 = 0, \text{ multiplicando la primera igualdad por } y \text{ y la segunda por } x$$

$$b \ x^2 - y^2r^2 = 0, \text{ restando la primera ecuación de la segunda}$$

$$b = 0 \ \vee \ x^2 - y^2r^2 = 0, \text{ Propiedad del módulo de la suma } (ab = 0 \rightarrow a = 0 \vee b = 0)$$

$b = 0 \rightarrow a = 0 \ \vee (x^2 - y^2 r^2 \rightarrow x = \pm yr) = 0$, usando el mismo razonamiento para el par de ecuaciones del caso anterior

Es decir se tienen de nuevo los números de la forma $(\pm yr, y)$, tomando el primer caso:

$a, b \ y \ r, 1 \ = (0,0)$, será nuestra hipótesis, usando la propiedad 5 del producto por escalar y la definición de este

$y \ ar + br^2, a + br \ = (0,0)$, por la definición de multiplicación

$ar + br^2 = 0 \ \wedge \ a + br = 0$ , por la definición de igualdad en parejas ordenadas ya que el caso $y = 0$ no tiene sentido analizarlo

$a + br = 0$, ya que la primera ecuación es linealmente dependiente de la segunda

$a = -br$, sumando el inverso de $br$ a ambos lados de la igualdad.

En conclusión, $yr, y \ -br, b \ = (0,0)$, por lo cual se hace innecesario verificar el segundo caso .Como síntesis de los resultados de esta exploración se presenta el siguiente teorema: $a, b \ \ x, y \ = \ a, b \ , \ a, b \ \ x, y \ = \ 0,0$

**Teorema 4(μ):** En $M(i^2)$, con $i^2 = r^2, i \neq \pm r$

$\forall a, y, b \in \mathbb{Z}, \ \pm ar, a \ \ 1 \mp ry, y \ = \ \pm ar, a \ \ y \ \ br, b \ \ -ar, a \ = (0,0)$ donde $a, b$ no son necesariamente números diferentes.

**Corolario:** $a^2 - b^2 r^2 \ = 0 \leftrightarrow \ a, b$ es un divisor de $(0,0)$.

### 3.4 Potencias de números M$(i^2)$

Respecto a la potenciación, esta puede ser definida similarmente a como se hace en $\mathbb{N}$, para nuestros conjuntos $M(i^2)$:

**Definición 6(μ):** $\forall n \in \mathbb{Z} \forall \ a, b \ \in M \ i^2 \ , \ a, b \ ^0 = (1,0) \wedge \ a, b \ ^n = (a, b) \ a, b \ ^{n-1}$

Como consecuencia de esta definición, se logra un sentido de la potenciación como una reiteración de la multiplicación de $(a, b)$ $n$ veces, si representamos esta situación en la

forma $a + bi$, se puede determinar fácilmente la potencia $n - sima$ de un número $(a, b)$, esto es, viendo este número como un binomio, con la identidad del binomio de Newton, lo aplicamos teniendo en cuenta las potencias de $i$ y también que $(0,1)^0 = (1,0)$ es decir $i^0 = 1$.

En cuanto a hallar las potencias de un número, hay un método muy similar al que se usa para hallar potencias de términos binomiales, polinomios, recordando que para $a + bx$ tenemos el binomio de Newton:

$$a + bx\ ^n = \sum_{k=0}^{k=n} \binom{n}{k}\ a^k (bx)^{n-k}$$

De lo anterior, como trabajamos con polinomios, el sentido de la variable nos da pie a extender esta propiedad a cualquier conjunto que cumpla el mismo sentido de la multiplicación, y por ende de la potenciación, nuestra definición de potencia al ser tan similar a la que se usa en los números enteros, nos permite extender este resultado a nuestro conjunto, simplemente tratando a $a + bx$ como $a + bi$, se tiene asi:

**Teorema 5(μ):**

$$a + bi\ ^n = \sum_{k=0}^{k=n} \binom{n}{k}\ a^k (bi)^{n-k}$$

$$(ka + kbi)^n = k^n (a + bi)^n$$

Si se quiere cambiar a la representación $(a, b)$ de una de las potencias $a, b\ ^n$, bastará con desarrollar esta suma y se cumple que las potencias pares de $b$ aparecerán en la primera componente (incluido $a^k b^0$) y las impares de $b$ en la segunda componente. Por ejemplo para $i^2 = r^2$:

$$(a + bi)^2 = a^2 + 2abi + (bi)^2 = a^2 + 2abi + b^2 r^2$$

Haciendo uso del Teorema 1, podemos cambiar la representación de esta igualdad ubicando las partes enteras en la primera componente y las que contengan $i$ en la segunda:

$$(a,b)^2 = (a^2 + b^2r^2, 2ab)$$

Aplicando para una tercera potencia de $a + bi$:

$(a + bi)^3 = a^3 + 3a^2(bi) + 3a(bi)^2 + (bi)^3$, aplicando el Teorema 5.

$(a + bi)^3 = a^3 + 3a^2(bi) + 3ab^2r^2 + b^3i^3$, aplicando que $i^2 = r^2$, y aplicando $b^n i^n = (bi)^n$

$(a + bi)^3 = a^3 + 3a^2(bi) + 3ab^2r^2 + b^3i^2i$, ya que $i^n = i^{n-1}i$

$(a + bi)^3 = a^3 + 3a^2(bi) + 3ab^2r^2 + b^3r^2i$, ya que $i^2 = r^2$

Notemos que siempre que la potencia de $bi$ sea impar, el factor $i$ se conserva porque:

$$i^0 = 1, i^1 = i, i^2 = r^2, i^3 = r^2i, i^4 = r^4, i^5 = r^4i \ldots \ldots$$

Por lo cual estos términos están en la segunda componente al cambiar de representación:

$(a,b)^3 = (a^3 + 3ab^2r^2, 3a^2b + b^3r^2)$, por T1

Hagamos un ejemplo aplicando directamente el binomio, en $M\ 9$ para $2{,}1\ ^3$:

$$2{,}1\ ^3 = (2+i)^3 = \sum_{k=0}^{k=3} \binom{3}{k} 2^k (1*i)^{3-k}$$

$$(2+i)^3 = \binom{3}{0} 2^0(1*i)^{3-0} + \binom{3}{1} 2(1*i)^{3-1} + \binom{3}{2} 2^2(1*i)^{3-2} + \binom{3}{3} 2^3(1*i)^{3-3}$$

$$(2+i)^3 = 1*1*i^3 + 3*2*\ i\ ^2 + 3*2^2\ i\ ^1 + 1*2^3(i)^0$$

$$(2+i)^3 = i^2i + (6*9) + 12i + 8$$

$$(2+i)^3 = 9i + (6*9) + 12i + 8$$

En la representación de parejas ordenadas sería:

$$(2{,}1)^3 = (54 + 8{,}9 + 12)$$

$$(2,1)^3 = (62,21)$$

En cuanto a los elementos del conjunto, las potencias de los elementos particulares, que multiplicados dan $(0,0)$, tienen una propiedad muy interesante como conjunto con la multiplicación, se muestra en el siguiente teorema:

**Teorema 6:** En $M\ i^2\ , (r,1)^n = \ 2r\ ^{n-1}(r,1)$ con $i^2 = r^2, i \neq \pm r$.

**Demostración**

Por inducción sobre $n$, probemos que el resultado se cumple para el primer elemento 2:

$$r,1\ ^2 = \ r,1\ \ r,1\ \text{, por D6}$$

$$r,1\ \ r,1\ = \ r^2 + r^2, r + r\ \text{, por T1}$$

$$r^2 + r^2, r + r\ = \ 2r^2, 2r\ \text{, ya que es una suma en } \mathbb{Z}$$

$$2r^2, 2r\ = 2r\ r,1\ \text{, por D5}$$

$$r,1\ ^2 = 2r\ r,1\ \text{, por la propiedad transitiva de la igualdad}$$

Supongamos que el teorema es válido hasta $k$

$$(r,1)^k = \ 2r\ ^{k-1}\ r,1\ \text{, es nuestra hipótesis de inducción}$$

$r,1\ ^k(r,1) = \ 2r\ ^{k-1}(\ r,1\ (r,1))$, multiplicando a ambos lados por $(r,1)$ y por la propiedad 5 de T3

$$(r,1)^{k+1} = \ 2r\ ^{k-1}\ r,1\ ^2\text{, por D6}$$

$(r,1)^{k+1} = \ 2r\ ^{k-1}((2r)(r,1))$, se probó en la primer parte de esta demostración que $r,1\ ^2 = 2r\ r,1$

$$(r,1)^{k+1} = (\ 2r\ ^{k-1}\ 2r\ )(r,1)\text{, por la propiedad 1 de T3}$$

$(r,1)^{k+1} = \ 2r\ ^{(k+1)-1}(r,1)$, por la propiedad $aa^k = a^{k+1}$ de la potenciación en $\mathbb{Z}$

Por lo cual se cumple el teorema.

El teorema anterior funciona de igual manera cuando se trabaja con $-r$ en lugar de $r$, este hecho indica hemos demostrado con este es que el conjunto de los elementos que multiplicados son $(0,0)$, con la operación de multiplicación son un conjunto cerrado en cada $M\ i^2$ .

Si tomamos como conjunto $D_0 = \{\ x,y\ \in M\ i^2\ :\ x,y\ = (ar,a) \vee\ x,y\ = (-ar,a)\}$, resultados anteriores nos permiten justificar la cerradura de $(D_0,*)$

$(0,0) \in D_0$ pues $0,0\ = (0r,0)$

Se cumple para la multiplicación de dos elementos similares $ar,a\ *\ br,b\ = 2abr\ \ r,1\ = (\ 2abr\ r,2abr)$. De igual manera para $-ar,a\ \ -br,b\ = (\ 2abr\ r,2abr)$.

Se cumple para la multiplicación de elementos distintos, $a\ r,1\ *b\ -r,1\ =\ ab\ \ 0,0\ =\ 0,0$ .

En conclusión $(D_0,*)$ es un conjunto cerrado, propiedad que exploraremos más adelante, este tipo de conjuntos tienen una identidad especifica que es útil para el estudio en la sección de divisibilidad.

Notemos en la propiedad $a\ r,1\ *b\ -r,1\ =\ 0,0$ , o de manera más reducida $r,1\ \ -r,1\ =\ 0,0$ , aparecen elementos de naturaleza similar (solo varia un signo de uno a otro), para generalizar sobre nuestros conjuntos $M(i^2)$ definamos tal relación:

**Definición 7(μ):** Se define el semi-conjugado de un número en $M(i^2)$como $a,b\ = (-a,b)$

Existe una propiedad en los números complejos-gaussianos similar a esta, la relación entre $a+bi$ y $a-bi$, la cual abordamos en la siguiente sección.

### 3.5 El conjugado de un número

**Definición 8(μ):** Se define el conjugado de un número en $M(i^2)$como $a,b\ = (a,-b)$.

**Teorema 7, las propiedades de los conjugados (μ):** $\forall\ a,b\quad c,d\quad x,y\ \in M\ i^2\ \forall n > 1, n \in \mathbb{N}, i^2 = r^2, r \in \mathbb{Z}, i \neq \pm r.$

1) $a,b\ =\ a,b\ = ((a,b))$
2) a)$(a,b)(c,d) = (a,b) *\ \ c,d\ =\ a,b\ *(c,d)$
   b) $(a,b)(c,d) = (a,b) *\ \ c,d\ =\ a,b\ *(c,d)$

3) a)$a\ \ c,d\ + (x,y) = a\ (c,d) + (x,y)$
   b) $a\ \ c,d\ + (x,y) = a\ (c,d) + (x,y)$

4) a) $a,b\ =\ a,b\ \rightarrow b = 0$
   b) $a,b\ = (a,b) \rightarrow a = 0$
5) $a,b\ ^n =\ a,b\ ^n$
6) a) $a,b\quad a,b\ =\ a^2 - b^2r^2, 0$
   b) $a,b\quad a,b\ =\ b^2r^2 - a^2, 0$

7)a)$(\ a,b\ ) = (\ a,b\ ) = -(a,b)$

b)$-\ a,b\ = (a,b) \wedge -\ a,b\ = (a,b)$

**Demostración**

1) $a,b\ =\ a,b\ = ((a,b))$

$a,b\ =\ a,-b\ $, por D8

$a,-b\ =\ a,-\ -b\ $, por D8

$a,-b\ =\ a,b\ $, porque $b \in \mathbb{Z}$, se tiene $-(-b) = b$

$a,b\ = (a,b)$, por propiedad transitiva de la igualdad

$((a,b)) = (-a,b)$, por D7

$(-a,b) =\ -(-a),b\ $, por D7

$(-a,b), =\ \ a,b\ $, porque $a \in \mathbb{Z}$, se tiene $-(-a) = a$

$((a,b)) = (a,b)$, por propiedad transitiva de la igualdad

2) a)$(a,b)(c,d) = (a,b) * \ c,d \ = \ a,b \ *(c,d)$

$(a,b)(c,d) = (ac + bdr^2, ad + bc)$, por T1

$(ac + bdr^2, ad + bc) = (ac + bdr^2, -ad - bc)$ por D8

$(a,b) * \ c,d \ = \ a,-b \ \ c,-d$ , por D8

$a,-b \ \ c,-d \ = (ac + bdr^2, -ad - bc)$, por T1

$(a,b)(c,d) = (a,b) * \ c,d \ \ $ , por transitividad de la igualdad.

b) $(a,b)(c,d) = (a,b) * \ c,d \ = \ a,b \ *(c,d)$

$(a,b)(c,d) = (ac + bdr^2, ad + bc)$, por T1

$(ac + bdr^2, ad + bc) = (-ac - bdr^2, ad + bc)$ por D7

$-ac - bdr^2, ad + bc \ = (-1)(ac + bdr^2, -ad - bc)$, por D5

$-1 \ \ ac + bdr^2, -ad - bc \ = (-1)(\ a,b \ * \ c,d \ )$, se demostró en la parte a) de esta propiedad.

$-1 \ \ a,b \ * \ c,d \ = \ -1 \ \ a,b \ * \ c,d \ = \ -1 \ \ c,d \ * \ a,b$ , por T2(propiedad conmutativa de la multiplicación) y la propiedad 5 de T3

$-1 \ \ a,b \ * \ c,d \ = \ -1 \ a,-b \ * \ c,d \ = \ -1 \ c,-d \ * \ a,b$ , por D8

$-1 \ \ a,b \ * \ c,d \ = (-a,b) * \ c,d \ = (-c,d) * \ a,b$ , por D5

$-1 \ \ a,b \ * \ c,d \ = (a,b) * \ c,d \ = \ a,b \ *(c,d)$, por D7

$(a,b)(c,d) = (a,b) * \ c,d \ = \ a,b \ *(c,d)$ , por transitividad de la igualdad.

3) a)$a \ \ c,d \ + (x,y) = a \ (c,d) + (x,y)$

$a \ \ c,d \ + (x,y) = \ \ ac, ad \ + (x,y)$, por D5

$ac, ad \ + (x,y) = \ \ ac + x, ad + y \ \ $ , por T1

$ac + x, ad + y \ = \ \ ac + x, -ad - y \ \ $ , por D8

$a \ (c,d) + (x,y) = a \ \ c,-d \ + \ \ x,-y \ \ $ , por D8

$$a\ c,-d\ +\ x,-y\ =\ ac,-ad\ +(x,-y), \text{ por D5}$$

$$ac,-ad\ +\ x,-y\ =(ac+x,-ad-y), \text{ por T1}$$

$$a\ c,d\ +(x,y)=a\ (c,d)+(x,y), \text{ por propiedad transitiva de la igualdad}$$

b) $a\ c,d\ +(x,y)=a\ (c,d)+(x,y)$

$$a\ c,d\ +(x,y)=\ ac,ad\ +(x,y), \text{ por D5}$$

$$ac,ad\ +(x,y)=\ ac+x,ad+y\ , \text{ por T1}$$

$$ac+x,ad+y\ =\ -ac-x,ad+y\ , \text{ por D7}$$

$$a\ (c,d)+(x,y)=a\ -c,d\ +\ -x,y\ , \text{ por D7}$$

$$a\ -c,d\ +\ -x,y\ =\ -ac,ad\ +(-x,y), \text{ por D5}$$

$$-ac,ad\ +\ -x,y\ =(-ac-x,ad+y), \text{ por T1}$$

$$a\ c,d\ +(x,y)=a\ (c,d)+(x,y), \text{ por propiedad transitiva de la igualdad}$$

4)a) $a,b\ =\ a,b\ \rightarrow b=0$

$$a,b\ =\ a,b\ , \text{es nuestra hipótesis}$$

$$a,b\ =\ a,-b\ , \text{por D8}$$

$b=-b$, por la definición de igualdad en parejas ordenadas

$b=0$, ya que $b\in\mathbb{Z}$.

b) $a,b\ =(a,b)\rightarrow a=0$

$$a,b\ =\ a,b\ , \text{es nuestra hipótesis}$$

$$a,b\ =\ -a,b\ , \text{por D7}$$

$a=-a$, por la definición de igualdad en parejas ordenadas

$a=0$, ya que $a\in\mathbb{Z}$.

5) $a,b\ ^{n} = \ a,b\ ^{n}$

Se demostrara por inducción sobre $n$, primero demostremos que se cumple para el caso inicial para $n = 2$ :

$$a,b\ ^{2} = \ a^2 + b^2, 2ab \ \text{ por D6 usando T5}$$

$$a^2 + b^2, 2ab \ = \ a^2 + b^2, -2ab \ \text{ , por D8}$$

$$a,b\ ^{2} = \ a,-b\ ^{2}, \text{ por D8}$$

$$a,-b\ ^{2} = \ a^2 + b^2, -2ab \ \text{ , por D6 usando T5}$$

$$a,b\ ^{2} = \ a,b\ ^{2}, \text{ por propiedad transitiva de la igualdad.}$$

Supongamos que se cumple hasta $n$ que $a,b\ ^{n} = \ a,b\ ^{n}$:

$a,b\ ^{n} * (a,b) = \ a,b\ ^{n} * (a,b)$, multiplicando por $(a,b)$ a ambos lados de la igualdad de nuestra hipótesis de inducción

$$a,b\ ^{n} * (a,b) = \ a,b\ ^{n+1} \text{ , por D6}$$

$a,b\ ^{n} * (a,b) = \ a,b\ ^{n} * (a,b)$, por la propiedad 2 de T7

$$a,b\ ^{n} * (a,b) = \ a,b\ ^{n+1}, \text{ por D6}$$

$$a,b\ ^{n+1} = \ a,b\ ^{n+1}, \text{ por propiedad transitiva de la igualdad.}$$

6)a) $a,b \quad a,b \ = \ a^2 - b^2r^2, 0$

$$a,b \quad a,b \ = (a,b)(a,-b), \text{ por D8}$$

$$a,b \quad a,-b \ = \ a^2 - b^2r^2, 0 \ \text{ , por T1}$$

b) $a,b \quad a,b \ = \ b^2r^2 - a^2, 0$

$$a,b \quad a,b \ = (a,b)(-a,b), \text{ por D7}$$

$$a,b \quad -a,b \ = \ b^2r^2 - a^2, 0 \ \text{ , por T1}$$

7)a)$(\ a,b\ ) = (\ a,b\ ) = -(a,b)$

b)$-\ a,b\ = (a,b) \wedge -\ a,b\ = (a,b)$

c) $a,b\quad a,b\ = (a,b)^2$

Se obtiene directamente de las definiciones D7 y D8.

La propiedad 6 nos da relación entre un número, sus conjugados y lo que a continuación determinaremos como su norma, la norma de un número resultara ser o la multiplicación de el por su conjugado, o la multiplicación de el por su semi-conjugado, es esta relación la que nos dará más adelante una manera de dividir en nuestras estructuras, sin embargo antes de entrar a trabajar esto en profundidad definamos la herramienta que nos falta.

### 3.6 $M(i^2)$ como espacio semi-normado

**Definición 9(μ):** La norma de un número $M(i^2)$ se define como la función:

$\| \|: M(i^2) \to \mathbb{N},\ \ a,b\ \to \|\ \ a,b\ \| = |a^2 - b^2r^2|$, con $i^2 = r^2, r \in \mathbb{Z}$

**Teorema 8, propiedades de la norma:** $\forall\ a,b\quad c,d\quad x,y\ \in M\ i^2\ \forall n > 1, n \in \mathbb{N}$

1) $\|\ \ a,b\ \| \geq 0$
2) $\|\ \ a,b\ \| = \|\ \ a,b\ \|$
3) $\|\ \ a,0\ \| = a^2$
4) $|\ a,b\quad a,b\ | = \|\ \ a,b\ \|^{\ 2}$
5) $\|\ k\ \ a,b\ \| = k^2\ \|\ \ a,b\ \|$
6) $\|\ \ a,b\quad c,d\ \| = \|\ \ a,b\ \| \| \ \ c,d\ \|$
7) $\|\ \ a,b\quad a,b\ \| = \|\ \ a,b\ \|^2$
8) $\|\ \ a,b\ \|^n = \|\ \ a,b\ ^{\ n}\ \|$

**Demostración:**

1) Se tiene por la definición de norma y la propiedad de $a^2 - b^2r^2\ \geq 0$ del valor absoluto.

2) $\| \ a,b \ \| = \| \ a,b \ \|$

$\| \ a,b \ \| = \ a^2 - b^2r^2$ , por D9

$\| \ a,b \ \| = \| \ a,-b \ \| = \ a^2 - (-b)^2r^2$ , por D9 y D8

$a^2 - b^2r^2 \ = \ a^2 - (-b)^2r^2$ , ya que en $\mathbb{Z}$, $(-b)^2 = b^2$

$\| \ a,b \ \| = \| \ a,b \ \|$, por la propiedad transitiva de la igualdad

3) $\| \ a,0 \ \| = \ a^2 - 0^2r^2 \ = \ a^2$ por D9 y ya que $a^2 \ = a^2$ se tiene la propiedad.

4) $| \ a,b \ \ a,b \ | = \| \ a,b \ \|$

$| \ a,b \ \ a,b \ | = \ a^2 - b^2r^2, 0 \ = \ a^2 - b^2r^2$ , por D8 y por T6, y esto último es

$\| \ a,b \ \|$ por D9.

5) $\| \ k \ a,b \ \| = k^2 \| \ a,b \ \|$

$\| \ k \ a,b \ \| = \| \ ka, kb \ \| = \ a^2k^2 - b^2r^2k^2$ , por D5 y D9

$a^2k^2 - b^2r^2k^2 \ = \ k^2 \ a^2 - b^2r^2 \ = |k^2| * | \ a^2 - b^2r^2, 0 \ |$ por la propiedad distributiva de la multiplicación respecto a la suma $\mathbb{Z}$, en y por la propiedad del valor absoluto ( $ab \ = \ a \ \ b$ )

$|k^2| * \ a^2 - b^2r^2, 0 \ = k^2 \| \ a,b \ \|$ por la propiedad $a^2 \ = a^2$ y D9

$\| \ k \ a,b \ \| = k^2 \| \ a,b \ \|$, por propiedad transitiva de la igualdad.

6) $\| \ a,b \ \ c,d \ \| = \| \ a,b \ \| \| \ c,d \ \|$

$\| \ a,b \ \ c,d \ \| = \| \ ac + bdr^2, ad + bc \ \| = \ (ac + bdr^2)^2 - (ad + bc)^2r^2$ , por T1 y D9

$$(ac + bdr^2)^2 - (ad + bc)^2 r^2 \;=\; a^2c^2 - a^2d^2r^2 - b^2c^2r^2 + b^2d^2k^4 \;,$$

desarrollando los cuadrados de los términos

Por otro lado

$\| \;a,b\; \| \| \;c,d\; \| = \; a^2 - b^2r^2 \;*\; c^2 - d^2r^2 \;=\; (a^2 - b^2r^2)(c^2 - d^2r^2)$ por la D9 y la propiedad del valor absoluto ( $ab \;=\; a \;\; b$ )

$(a^2 - b^2r^2)(c^2 - d^2r^2) \;=\; a^2c^2 - a^2d^2r^2 - b^2c^2r^2 + b^2d^2k^4$ , desarrollando el producto

$\| \;a,b\;\; c,d\; \| = \| \;a,b\; \| \| \;c,d\; \|$, por la propiedad transitiva de la igualdad.

7) $\| \;a,b\;\; a,b\; \| = \| \;a,b\; \|^2$

$\| \;a,b\;\; a,b\; \| = \| \;a,b\; \| * \| \;a,b\; \|$, por la propiedad 6 de T8

$\| \;a,b\; \| * \| \;a,b\; \| = \| \;a,b\; \| * \| \;a,b\; \| = \| \;a,b\; \|^2$, por la propiedad 2 de T8 y por la propiedad de la multiplicación en $\mathbb{N}, aa = a^2$

$\| \;a,b\;\; a,b\; \| = \| \;a,b\; \|^2$, por la propiedad transitiva de la igualdad.

8) $\| \;a,b\; \|^n = \| \;a,b\; ^{\,n} \|$

Se probara esta proposición por inducción sobre $n$, probemos que se cumple para el primer caso $n = 2$:

$\| \;a,b\; \|^2 = \| \;a,b\; \| * \| \;a,b\; \|$, por la propiedad de la multiplicación en $\mathbb{N}, aa = a^2$

$\| \;a,b\; \| * \| \;a,b\; \| = \| \;a,b\;\; a,b\; \| = \| \;a,b\; ^{\,2} \|$ por la propiedad 6 de T8 y D5

$\| \;a,b\; \|^2 = \| \;a,b\; ^{\,2} \|$, por la propiedad transitiva de la igualdad.

Supongamos que se cumple hasta $n$ que $\| \;a,b\; \|^n = \| \;a,b\; ^{\,n} \|$:

$\| \ a,b \ \|^n * \| \ a,b \ \| = \| \ a,b \ ^n \| * \| \ a,b \ \|$, multiplicamos a ambos lados de la igualdad por $\| \ a,b \ \|$

$\| \ a,b \ \|^n * \| \ a,b \ \| = \| \ a,b \ \|^{n+1}$, por la propiedad de la multiplicación en $\mathbb{N}, aa = a^2$

$\| \ a,b \ ^n \| * \| \ a,b \ \| = \| \ a,b \ ^n \ a,b \ \| = \| \ a,b \ ^{n+1} \|$, por la propiedad 6 del teorema 8 y D5,

$\| \ a,b \ ^{n+1} \| = \| \ a,b \ \|^{n+1}$, por la propiedad transitiva de la igualdad.

Por inducción sobre $n$ se cumple la propiedad como se quería demostrar.

Algunas propiedades de la norma que usualmente se cumplen pero que aquí no se han podido comprobar son:

- $\| \ a,b \ \| = 0 \leftrightarrow \ a,b \ = (0,0)$, hay más elementos además del $0,0$ cuya norma es 0, por ejemplo en $M \ 16 \ , \| \ 4,1 \ \| = 0$ , en $M \ 25 \ , \| \ 20,4 \ \| = 0$, en $M \ 9 \ , \| \ -15,5 \ \| = 0$, a continuación se menciona que elementos corresponden a la norma cero según sea el valor de $i^2$.
- $\| \ k \ a,b \ \| = \ k \ * \| \ a,b \ \|$, en el teorema anterior se comprobó que se cumple una propiedad similar.
- $\| \ a,b \ + \ c,d \ \| \leq \| \ a,b \ \| + \| \ c,d \ \|$, por ejemplo probemos en $M \ 4$ , a manera de contraejemplo $(5,4)$:

$$\| \ 5,4 \ + \ 5,4 \ \| \leq \| \ 5,4 \ \| + \| \ (5,4) \ \|$$

$$\| \ 2 \ 5,4 \ \| \leq 2 \ \| \ 5,4 \ \|$$

$$2^2 \ \| \ 5,4 \ \| \leq 2 \ \| \ 5,4 \ \|, \text{ por la propiedad 5 de T8}$$

Obtuvimos una desigualdad falsa, por lo cual la propiedad no se cumple.

La norma definida con sus propiedades nos permite caracterizar de forma más completa los números de cualquier conjunto $M \ i^2$ , en particular aquellos números cuya multiplicación

da $(0,0)$, por la propiedad 6 del Teorema 9 se tiene que la norma de al menos uno de aquel par es 0, se puede comprobar fácilmente que esta norma corresponde a $(\pm ar, a)$:

$$\| \ \pm ar, a \ \| = \| \ a \ \pm r, 1 \ \|, \text{ por D5}$$

$$\| \ a \ \pm r, 1 \ \| = a^2 \ \| \ \pm r, 1 \ \|, \text{ por la propiedad 5 de T8}$$

$$a^2 \ \| \ \pm r, 1 \ \| = a^2 \ \ \pm r \ ^2 - r^2 \ = a^2 \ r^2 - r^2 \ = 0, \text{ por D9, ya que } r^2 = (-r)^2$$

Los elementos con esta norma, al poder ser descompuestos de infinitas maneras, como comprobamos en la sección 3.3, son los que dañan la propiedad cancelativa, si los excluimos se cumple que:

**Teorema 9:** $\forall \ a, b \ \ c, d \ \ e, f \ \in M \ i^2 \ , \| \ a, b \ \| \neq 0, \ a, b \ \ c, d \ = \ a, b \ \ e, f \ \rightarrow \ c, d \ = (e, f)$.

**Demostración**

Sean $a, b \ \ c, d \ \ e, f \ \in M \ i^2 \ \ tales \ que \| \ a, b \ \| \neq 0 \ y \ \ a, b \ \ c, d \ = \ a, b \ \ e, f$

$a, b \ \ c, d \ - \ a, b \ \ e, f \ = (0,0)$, sumando el inverso de $(a, b)(e, f)$ a ambos lados de la igualdad

$a, b \ \ c, d \ - \ e, f \ = (0,0)$, por la propiedad 4 de la multiplicación en T2

Dándole el valor a $c, d \ - \ e, f$ de un $(h, k)$ y sustituyendo $a, b \ \ h, k \ = (0,0)$

$$ah + bkr^2, ak + bh \ = (0,0), \text{ por T1}$$

$ah + bkr^2 = 0 \wedge ak + bh = 0$, ahora por la definición de igualdad en parejas ordenadas

$ahk + bk^2r^2 = 0 \wedge ahk + bh^2 = 0$, multiplicando la primera ecuación anterior por $k$ y la segunda por $h$.

$b \ k^2r^2 - h^2 \ = 0$, restando la segunda ecuación de la primera y aplicando propiedad distributiva.

$b = 0 \ \vee k^2r^2 = h^2$, por la propiedad en $\mathbb{Z}, ab = 0 \rightarrow a = 0 \vee b = 0$

*Caso a)* $b = 0$*:*

Siguiendo las dos ecuaciones anteriores se deduce que $ak = 0 \ \wedge ah = 0$ y de ello se deduce que $a = 0 \ \vee (h = 0 \ \wedge k = 0)$

Si $a = 0$ entonces $a, b \ = (0,0)$, llegando a una contradicción pues se supuso que $\| \ a, b \ \| \neq 0$

En el segundo caso se cumple que $h, k \ = \ 0,0 \ = (c - e, d - f)$, por lo cual $c = e \ \wedge d = f$, en conclusión $(c, d) = (e, f)$.

*Caso b)* $k^2r^2 = h^2$*:*

En este caso si $h = \pm kr$, dada la ecuación $a, b \ \ h, k \ = (0,0)$ por T4, $a, b \ = (\mp br, b)$, llegando así a una contradicción pues se supuso que $\| \ a, b \ \| \neq 0$.

En conclusión la propiedad cancelativa se cumple salvo para los elementos divisores de (0,0), es decir, aquellos que tienen norma 0.

Como probamos anteriormente, este conjunto de elementos que notamos como $D_0$ es cerrado para la multiplicación, al realizar multiplicaciones en el siempre el resultado está en el conjunto, sin embargo no abordamos el problema de encontrar el resultado de las multiplicaciones, si por ejemplo queremos encontrar el elemento de $D_0$ correspondiente a $2,1 \ \ 2,1 \ \ 2,1 \ \ 4,2 \ \ 4,2 \ \ 4,2 \ \ 4,2 \ \ 4,2 \ \ 4,2$ , en $M\ 4$ , o de $9,8 + 9,8 + 9,8 + 9,8 + 9,8 + 9,8 + 9,8 + 7,3 + 7,3 + 7,3 + 7,3 + 7,3 + 7,3$ aunque sabemos rápidamente que el primer resultado pertenece a $D_0$, aun no contamos con un proceso que nos permita hallar tal elemento rápidamente, dimos una aproximación de esto al definir las potencias de un número, una herramienta que surgió fue el binomio de Newton extendido a estas estructuras, sin embargo el relacionar más de un numero reiterado en las operaciones es algo que aún no abordamos.

### 3.7 El sentido de iteración en las operaciones

A las operaciones multiplicación y potenciación, como es usual en $\mathbb{Z}$, es deseable dar un significado a estas operaciones de suma iterada y multiplicación iterada respectivamente, de hecho este recurso lo utilizamos en la definición 5 para definir las potencias de un numero en $M(r^2)$, sin embargo para la multiplicación de dos números $a,b$ , $(c,d)$no es posible, no obstante nuestro producto por escalar nos da la posibilidad de tener una base teórica para ver la multiplicación asociada a las sumas iteradas, gracias a ello podemos encontrar nuevas propiedades de las operaciones:

**Definición 10(μ):** Sea $a,b \in M(i^2)$ y $n$ un número natural:

$$n = 0, n\ a,b = 0,0\ ,\ a,b\ ^{n} = (1,0)$$

$$n > 0, n+1\ a,b = n\ a,b + a,b\ ,\ a,b\ ^{n+`1} = a,b\ ^{n}(a,b)$$

**Teorema 10 propiedades de la potenciación (μ):** $\forall\ a,b \quad c,d \in M\ i^2\ \forall n,m \in \mathbb{N}$

V. $((a,b)(c,d))^n = (a,b)^n(c,d)^n$

VI. $(a,b)^{m+n} = (a,b)^m(a,b)^n$

VII. $((a,b)^m)^n = (a,b)^{mn}$

VIII. $(ka,kb)^n = k^n(a,b)^n$

**Demostración:**

1. $((a,b)(c,d))^n = (a,b)^n(c,d)^n$

Por inducción sobre $m$, probemos que se cumple para $m = 0$

$$((a,b)(c,d))^0 = (ac + bdk^2, ad + bc)^0$$

$$(ac + bdk^2, ad + bc)^0 = (1,0)$$

$$1,0 = (1,0)(1,0)$$

$$1,0 \quad 1,0 \quad = (a,b)^0(c,d)^0$$

$$((a,b)(c,d))^0 = (a,b)^0(c,d)^0$$

Supongamos ahora que el teorema se cumple hasta $m$

$$((a,b)(c,d))^m = (a,b)^m(c,d)^m$$

$$a,b \quad c,d \quad ^m( \ a,b \quad c,d \ ) = ( \ a,b \ ^m \ c,d \ ^m) \ a,b \quad c,d$$

$$a,b \quad c,d \quad ^{m+1} = ( \ a,b \ ^m \ c,d \ ^m) \ a,b \quad c,d$$

$$a,b \quad c,d \quad ^{m+1} = \ a,b \ ^m( \ c,d \ ^m) \ a,b \quad c,d$$

$$a,b \quad c,d \quad ^{m+1} = ( \ a,b \ ^m \ a,b \ )( \ c,d \ ^m \ c,d \ )$$

$$a,b \quad c,d \quad ^{m+1} = \ a,b \ ^{m+1} \ c,d \ ^{m+1}$$

Por lo cual el principio se cumple en general

2. $(a,b)^{m+n} = (a,b)^m(a,b)^n$

Como $(a,b)^m = \ a,b \quad a,b \ \ldots\ldots (a,b)$ $m$ veces

y $(a,b)^n = \ a,b \quad a,b \ \ldots\ldots (a,b)$ $n$ veces

$(a,b)^m(a,b)^n = \ a,b \quad a,b \ \ldots\ldots (a,b)$ $m+n$ veces

$$(a,b)^m(a,b)^n = \ a,b \ ^{m+n}$$

3.$((a,b)^m)^n = (a,b)^{mn}$

$$((a,b)^m)^n = (a,b)^m(a,b)^m(a,b)^m \ldots\ldots (a,b)^m \ n \text{ veces}$$

$((a,b)^m)^n = ( \ a,b \quad a,b \ \ldots\ldots \ a,b \ m$ veces) ( $a,b \quad a,b \ \ldots\ldots \ a,b \ m$ veces) $\ldots\ldots ( \ a,b \quad a,b \ \ldots\ldots \ a,b \ m$ veces) $n$ veces

$((a,b)^m)^n = \ a,b \quad a,b \ \ldots\ldots \ a,b \ mn$ veces

$$((a,b)^m)^n = (a,b)^{mn}$$

4. $(ka,kb)^n = k^n(a,b)^n$

$(ka,kb)^n = (k(1,0)(a,b))^n = ((k,0)(a,b))^n$, por la propiedad 3 de la multiplicación de T2, D5 y la propiedad 5 de T3.

$(ka,kb)^n = (k,0)^n(a,b)^n$, por la propiedad 1 de T9.

$ka,kb\ ^n = k^n\ a+bi\ ^n$, por el T1

$(ka,kb)^n = k^n(a,b)^n$, por T1 y por el isomorfismo entre los números enteros y $(a,0)$

Tal isomorfismo que nos permite llegar a la última afirmación es un teorema que es demostrable en este punto del documento, pero por conveniencia en cuanto a temática, hace parte de la sección 4, por ahora aceptaremos que se cumple y más adelante en el documento se confirmará esto.

Ya habiendo definido las operaciones base para trabajar en algebra con nuestros números, procedemos a trabajar sobre el problema de encontrar números que cumplan ciertas condiciones y relaciones, la primera manera de relacionarlos entre ellos es a través de las operaciones, demos inicio así al estudio de ecuaciones:

### 3.8Ecuaciones en los $M\ i^2$

#### Ecuaciones lineales con una incógnita:

Al analizar nuestros conjuntos de números, desde el punto de vista del proceso de descomponer, una primera idea es descomponer utilizando la primera operación del conjunto, el hallar las descomposiciones posibles de un número utilizando nos da paso al estudio de las ecuaciones del tipo $a+x=b$, con $a,b$ conocidos, por las propiedades de las operaciones de nuestros conjuntos se conocen todas las posibles soluciones a estas ecuaciones:

**Teorema 11(μ):** Sean $a,b\ ,\ c,d\ \in M\ i^2$ , existe una única solución a la ecuación $(a,b)+(x,y)=(c,d)$ y está dada por $x,y\ =\ c,d\ -(a,b)$

**Demostración**

$(a,b)+(x,y)=(c,d)$, es la ecuación que queremos solucionar

Por T2 existe el inverso aditivo de $(a,b)$, $-\ a,b\ =(-a,-b)$, el inverso aditivo de $(a,b)$

$-a,-b\ +\ \ a,b\ +\ x,y\ \ =(-a,-b)+(c,d)$, sumando $(-a,-b)$ a ambos lados

$-a,-b\ +\ \ a,b\ \ +(x,y)=\ \ c,d\ \ +(-a,-b)$, por T2, usando las propiedades asociativa y conmutativa de la suma

$-a,-b\ +\ \ a,b\ \ +\ x,y\ \ =\ \ 0{,}0\ \ +\ \ x,y\ \ =(x,y)$, por T2 ya que hay elementos neutro e inversos en la suma

$x.y\ \ =\ \ c-a,d-b\ \ $, por propiedad transitiva de la igualdad

Esta solución es única ya que la propiedad cancelativa si se cumple para la suma.

Es importante notar que en la demostración de las propiedades de la suma no se tiene en cuenta quien sea $i^2$, esto implica que estas se cumplen para todos los conjuntos *A* independiente de tal valor, inclusive este teorema.

Con el teorema anterior, tenemos elementos para empezar a pensar cómo resolver todos los tipos de ecuaciones lineales de una incógnita $ax+b=c$ , ya que tenemos $ax=b-c$, el problema se reduce a encontrar dos números cuyo producto sea un tercer número del conjunto, es decir solucionar ecuaciones de la forma $\ a,b\ \ \ x,y\ \ =(c,d)$, que a diferencia del anterior tipo de ecuaciones, no siempre tienen solución ya que en general, en estos conjuntos no se tienen inversos multiplicativos, por lo cual debemos saber cuándo existe o no solución para las ecuaciones $\ a,b\ \ \ x,y\ \ =(c,d)$, con $\ a,b\ ,(c,d)$ dos números conocidos, dándonos paso al problema de la divisibilidad.

# 4. Divisibilidad en conjuntos $M\ i^2$

## 4.1 Definición y propiedades

**Definición 11(μ):**

$$a,b\ |_{r^2}\ c,d\ \leftrightarrow \exists\ e,f\ \in M\ i^2\ :\ a,b\ \ e,f\ =\ c,d\ ,i^{\,2}=r^2$$

Si se cumple esta condición diremos que $(a,b)$ divide a $(c,d)$ o que $(a,b)$ es un divisor de $(c,d)$.

Teniendo una definición genérica según el conjunto $\boldsymbol{M\ i^2}$ en el que estemos trabajando, intentaremos que las demostraciones que se hagan se cumplan para todo $r^2$ y en el caso contrario se hará mención a los casos excepcionales, por ello sin miedo a confusiones utilizaremos simplemente el símbolo | para hablar de divisibilidad. Algunas propiedades de esta relación son:

**Teorema 12:**$\forall\ a,b\ \ c,d\ \ (e,f)\ \ x_1,x_2\ \ \ y_1,y_2\ \ \in M\ i^2\ ,\forall x,y\in\mathbb{Z}:$

1)$(a,b)\ |(0,0)\wedge\pm(a,b)\ |(a,b)$

2) $((a,b)\ |(c,d)\wedge(c,d)\ |(e,f))\rightarrow(a,b)\ |(e,f)$

3) $((a,b)\ |(c,d)\wedge(a,b)\ |(e,f))\rightarrow$
$(a,b)\ |\ c,d\ \ x_1,x_2\ +\ e,f\ \ y_1,y_2\ \wedge(a,b)\ |x\ c,d\ +y\ e,f$

4) $a,b\ \ c,d\ \rightarrow\|\ a,b\ \|\ \|\ c,d\ \|$

**Demostración:**

1)$(a,b)\ |(0,0)\wedge(a,b)\ |(a,b)$

Como $a,b\ \ 0,0\ =(0,0)$ para cualquier $(a,b)$, se tiene por D11 la primera parte

Como $a,b\ \ 1,0\ =(a,b)$ y $a,b\ (\ -1,0\ (-1,0))=(a,b)$, se tiene por D11 la segunda parte.

2) $((a,b)\,|(c,d) \wedge (c,d)\,|(e,f)) \rightarrow (a,b)\,|(e,f)$

$((a,b)\,|(c,d) \wedge (c,d)\,|(e,f))$, es nuestra hipótesis

$\exists\ a_1,b_1\ \in M\ i^2\ :\ a,b\quad a_1,b_1\ =\ c,d\ \wedge \exists\ c_1,d_1\ \in M\ i^2\ :\ c,d\quad c_1,d_1\ =\ e,f$ , por D11

$a,b\quad a_1,b_1\quad c_1,d_1\ = (e,f)$, reemplazando el valor de $c,d$ , de la primera ecuación a la segunda

$a,b\ (\ a_1,b_1\quad c_1,d_1\ ) = (e,f)$, por la propiedad asociativa de la multiplicación en T2

$(a,b)\,|(e,f)$, por D11 ya que la multiplicación es cerrada en $M\ i^2$

3) $((a,b)\,|(c,d) \wedge (a,b)\,|(e,f)) \rightarrow (a,b)\,|\ c,d\quad x_1,x_2\ +\ e,f\quad y_1,y_2$

$((a,b)\,|(c,d) \wedge (a,b)\,|(e,f))$, es nuestra hipótesis

$\exists\ a_1,b_1\ ,\ a_2,b_2\ \in M\ i^2\ :(a,b)\ a_1,b_1\ = (c,d) \wedge (a,b)\ a_2,b_2\ = (e,f)$, por D11

$(a,b)(\ a_1,b_1\quad x_1,x_2\ ) = (c,d)\ x_1,x_2\ \wedge (a,b)(\ a_2,b_2\quad y_1,y_2\ ) = (e,f)\ y_1,y_2$ , multiplicando la primera ecuación a ambos lados por $x_1,x_2$ y la segunda por $y_1,y_2$ , y por la propiedad asociativa de la multiplicación en T2.

Sumando ambas ecuaciones se tiene que

$a,b\quad a_1,b_1\quad x_1,x_2\quad +\quad a,b\quad a_2,b_2\quad y_1,y_2\quad =\quad c,d\quad x_1,x_2\ + (e,f)\ y_1,y_2$

$a,b\quad a_1,b_1\quad x_1,x_2\ +\ a_2,b_2\quad y_1,y_2\quad =\ c,d\quad x_1,x_2\ + (e,f)\ y_1,y_2$ , por la propiedad distributiva de la multiplicación en T2.

$(a,b)\,|\ c,d\quad x_1,x_2\ +\ e,f\quad y_1,y_2$ , por D11

En particular para $x_2 = 0$ y $y_2 = 0$, $x_1 = x$, $y_1 = y$:

$(a,b) \mid x,0 \quad c,d \; + \; y,0 \quad e,f$ , por la propiedad 2 de T2 y reemplazando los valores de $x_1, x_2, y_1, y_2$

$(a,b) \mid x \quad 1,0 \quad c,d \quad + y \quad 1,0 \quad e,f \quad$ , por D5 y la propiedad 5 de T3

$(a,b) \mid x \; c,d \; + y \; e,f$ , por la propiedad 3 de T2; se cumple la segunda parte como se quería demostrar.

4) $a,b \quad c,d \rightarrow \| \; a,b \; \| \; \| \; c,d \; \|$

$a,b \; \mid (c,d)$, es nuestra hipótesis

$\exists \; x,y \; \in M \; i^2 \; : \; a,b \quad x,y \; = \; c,d$ , por D11

$\| \; c,d \; \| = \| \; a,b \quad x,y \; \|$, reemplazando el valor de $c,d$

$\| \; c,d \; \| = \| \; a,b \; \| \| \; x,y \; \|$, por la propiedad 6 de T8

$\| \; a,b \; \| \mid \| \; c,d \; \|$, por la definición de divisibilidad en $\mathbb{N}$

Notemos que estamos planteando el problema de la existencia de una solución a las ecuaciones de la forma $a,b \quad x,y \; = (c,d)$, tal $(x,y)$ existirá cuando $a,b \mid c,d$ ; también al resolver las ecuaciones de este tipo, a diferencia de las ecuaciones $a,b \; + \; x,y \; = (c,d)$, al realizar la operación $a,b \quad x,y$ el valor de $r^2$ si está involucrado al igualar componente a componente :

$a,b \quad x,y \; = (c,d)$, es nuestra hipótesis

$(ax + byr^2, ay + bx) = (c,d)$, por T1

$c = ax + byr^2 \wedge d = ay + bx$, por D2 y T1

Por lo anterior, los divisores de $(c,d)$ deberían estar siempre condicionados al conjunto en el que trabajemos, se muestra que son dependientes del valor $i^2 = r^2$, no obstante por las propiedades que hemos demostrado hasta este punto, se puede verificar que hay casos excepcionales en donde un numero tendrá divisores sin importar cuál sea el conjunto, o en

otros términos, existen términos que poseen divisores universales que son independientes del valor de $i^2$, por ejemplo:

- $2,0$ es siempre divisor de $4,6$
- (3,0) es siempre divisor de (9,3)
- (-5,0) es siempre divisor de (5,-5)

Mostraremos a continuación el proceso para deducir esto, para el primer caso y luego lo generalizaremos:

$$4,6 = 2(2,3) \text{ por D5}$$

$$2\ 2,3 = 2(\ 1,0\ \ 2,3\ ) \text{ por T2 ya que en } M\ i^2 \text{ siempre hay elementos neutros y la propiedad 5 de T3}$$

$$2\ \ 1,0\ \ 2,3\ \ = (2,0)(2,3) \text{ por la propiedad 5 de T3}$$

$$2,0\ \ 2,3\ = (4,6) \text{ por la propiedad transitiva de la igualdad}$$

$$(2,0) \text{ es divisor de } 4,6 \text{ por D11.}$$

Como se ve en el proceso anterior, el 'truco' para encontrar estos divisores generales es hallar el máximo común divisor entre las componentes y usar las propiedades del producto por escalar para descomponer el número en un producto cuyo número de factores depende del número de divisores tenga el máximo común divisor, se tiene por esto el siguiente resultado:

**Teorema 13:**

El número $(a, b)$ tiene al menos $d(mcd(a, b))$ divisores por cada unidad en $M(i^2)$, siendo $d$ la función que determina el número de divisores de un número entero.

**Demostración**

Sean $(a, b)$ y su máximo común divisor $mcd\ a, b = m$, será nuestra hipótesis

$\frac{a}{m}\ m = a$ con $\frac{a}{m} \in \mathbb{Z}$ y $\frac{b}{m}\ m = b$ con $\frac{b}{m} \in \mathbb{Z}$, por la definición de máximo común divisor y de divisibilidad en $\mathbb{Z}$.

$a, b\ = (m\ \frac{a}{m}\ , m\ \frac{b}{m}\ )$, reemplazando los valores de $a\ y\ b$

$m\ \frac{a}{m}\ , m\ \frac{b}{m}\ = m(\frac{a}{m}, \frac{b}{m})$, por D5

Siendo esta alguna pareja ordenada de nuestra estructura $\frac{a}{m}, \frac{b}{m}\ = (x, y)$

Sea $p_1{}^{t_1} p_2{}^{t_2}$ ... $p_k{}^{t_k}$ la descomposición en factores primos de $m$, por el Teorema Fundamental de la Aritmética en $\mathbb{Z}$

$m\ \frac{a}{m}, \frac{b}{m}\ = p_1{}^{t_1}\ 1{,}0\ p_2{}^{t_2}\ 1{,}0\ \ldots\ p_k{}^{t_k}\ 1{,}0\ (x, y)$, por T2

$p_1{}^{t_1}\ 1{,}0\ p_2{}^{t_2}\ 1{,}0\ \ldots\ p_k{}^{t_k}\ 1{,}0\ \ x, y\ =\ p_1{}^{t_1}, 0\ \ p_2{}^{t_2}, 0\ \ldots.\ p_k{}^{t_k}, 0\ (x, y)$, por D5

$a, b\ =\ p_1{}^{t_1}, 0\ \ p_2{}^{t_2}, 0\ \ldots.(p_k{}^{t_k}, 0)(x, y)$, por la propiedad transitiva de la igualdad

Cada $(p_i{}^{t_i}, 0)$ es divisor de $(a, b)$, $1 \leq i \leq k$, por D11

Ahora ya que $k$ es el número de divisores primos de $m$, es nuestra intención averiguar si los divisores compuestos de $m$ también implican un divisor de $(a, b)$:

Supongamos un divisor $l|m$, por definición de divisibilidad $ls = m, s\ \in \mathbb{N}$, se tiene que $a, b\ = ls(x, y)$ y análogo al razonamiento anterior $a, b\ = (l, 0)(s, 0)(x, y)$, por lo cual $(l, 0)$ es un divisor de $(a, b)$, se concluye que $(a, b)$ tiene al menos un divisor por cada divisor de $m$, en otras palabras $(a, b)$ tiene al menos $d(mcd(a, b))$ divisores.

Queda la pregunta, si este es el mínimo de divisores, ¿hay un máximo?, ¿el número de divisores es contable por alguna función en nuestros conjuntos?, más adelante confirmaremos que si es posible acotar el número de divisores de cualquier $a, b$ , hay un máximo y esto implicara que el número de divisores total sea contable finito, este será

dependiente del número de formas posibles en que se puede escribir ‖ $a, b$ ‖ en términos de sumas de cuadrados.

Por otra parte, un problema aún por resolver es el reciproco a solucionar las ecuaciones $a, b \quad x, y = (c, d)$ es : dado $(c, d)$, encontrar los divisores que tiene; al solucionar esto se puede determinar si $(a, b)$ es uno de ellos, es decir al encontrar los divisores de un número se puede aproximar el proceso de solución a las ecuaciones; es usual al comenzar el estudio de la divisibilidad con definir ciertos conceptos, como el de factor primo o unidad, que dan identidad a elementos de los conjuntos que se comportan de manera especial en el proceso de descomponer.

## 4.2. Unidades y asociados

**Definición 12:**

El número $(a, b)$ es una unidad en $M(i^2)$ si y solamente si para todo $(x, y)$ de $M\ i^2$ , $(a, b) | (x, y)$.

Para estudiar la divisibilidad en una determinada estructura $M(i^2)$ es valioso el identificar las unidades como elementos que dividen a todos los demás, lo que nos facilitará el trabajo de encontrar divisores de un números a través de un concepto que se conoce número asociados; anteriormente hemos dedicado una pequeña sección a los divisores de 0, hagámoslo ahora para los divisores de todos los números:

Si pensamos en encontrar números $(x, y)$ que dividan a todos los demás en $M(i^2)$, tendríamos al alcance una primera solución, $1{,}0 \quad a, b = (a, b)$, por definición el elemento neutro de la multiplicación divide a todo elemento del conjunto, o sea que por definición de unidad $(1{,}0)$ es unidad, esta será nuestra unidad base ya que es funcional en todos los conjuntos sin importar el valor de $i^2$, si pensamos en encontrar más unidades $(x, y)$, como una supuesta unidad tendría que dividir a todos los demás números, en particular tendría que dividir a $(1{,}0)$, $(x, y) | (1{,}0)$ pero como $(1{,}0) | a, b \ , \forall (a, b) \in M(i^2)$, por la propiedad 2 de T11, $(x, y) | a, b \ , \forall (a, b) \in M(i^2)$, por esto el encontrar unidades se reduce a encontrar elementos que sean divisores del elemento neutro de la

multiplicación, siguiendo el método analítico supongamos que tal solución existe y encontraremos las condiciones necesarias y suficientes para que tal solución exista:

$x, y \mid (1,0)$, para algún $(x, y)$ será nuestra hipótesis

$\| x, y \| \mid \| 1,0 \|$, por la propiedad 5 de T12

$\| x, y \| \mid |1^2 - 0^2 r^2|$, por D9

$\| x, y \| \mid 1$, resolviendo el valor absoluto

Como 1 no tiene divisores en $\mathbb{N}$ distintos a sí mismo (o sea es la única unidad), como se debe cumplir $\| x, y \| \mid 1$ no queda otra solución más que $\| x, y \| = 1$.

$x^2 - y^2 r^2 = 1$, por D9

$x^2 - (yr)^2 = 1$, por la propiedad en $\mathbb{Z}$, $a^k b^k = (ab)^k$

Con $x, y, r \epsilon \mathbb{Z}$, buscamos dos números cuadrados $x^2, (yr)^2$ cuya distancia entre ellos sea 1, si hacemos una breve lista de los candidatos 0,1,4,9,16 ..., nos damos cuenta rápidamente que las únicas soluciones posibles son $x^2 = 0, (yr)^2 = 1$ y $x^2 = 1, (yr)^2 = 0$, además no hay más casos ya que la distancia entre dos cuadrados siempre va aumentando en 2, cosa que utilizaremos más adelante, se da que inicialmente la diferencia es 1, luego 3, luego 5, luego 7 y así sucesivamente, como demostraron los pitagóricos (Sorándo, Sin fecha); tomemos y analicemos nuestras dos posibles soluciones:

Caso a) $x^2 = 0, (yr)^2 = 1$:

De la primera ecuación se deduce rápidamente que $x = 0$, y que $yr = \pm 1$.

$yr = \pm 1$ Implica que $r \mid \pm 1$, por la definición de divisibilidad en $\mathbb{Z}$

$r = 1 \vee r = -1$, ya que en $\mathbb{Z}$ estas son las únicas unidades

$r^2 = 1$, elevando al cuadrado a ambos lados de las ecuaciones

Con $r = 1, y = \pm 1$ y de igual manera para $r = -1$, reemplazando en la ecuación $yr = \pm 1$

Por lo cual en $M(1)$, es decir en los números de Minkowski, $1{,}0$ , $-1{,}0$ , $0{,}1$ $y$ $(0,-1)$ son unidades y no se encuentran más unidades de este caso.

Caso b) $x^2 = 1, (yr)^2 = 0$:

De la primera ecuación se deduce que $x = \pm 1$ y de la segunda que $yr = 0$, ya que en $\mathbb{Z}, \pm 1, 0$ son las únicas raíces de 1 y 0 respectivamente.

De $yr = 0$ se deduce que $y = 0 \vee r = 0$, esta es una propiedad de la multiplicación en $\mathbb{Z}$.

Con $x = \pm 1$ y $y = 0$, no importando el valor de $r$, obtenemos que $(1{,}0)(-1{,}0)$ son unidades.

Con $x = \pm 1, r = 0$, es decir en $i^2 = 0$, los números duales, el valor de $y$ es variable, debe cumplirse:

$$\pm 1, y \quad a, b \quad = (1{,}0)$$

Resolvamos $1, y \quad a, b \quad = \quad 1{,}0$ :

$$a, b + ay \quad = (1{,}0), \text{ por T2}$$

$a = 1 \wedge b + ay = 0$, por la definición de igualdad entre parejas ordenadas

$b = -y$, usando que $a = 1$ y sumando $-y$ a ambos lados de la segunda ecuación

Se obtiene que $1, y \quad 1, -y \quad = (1{,}0)$ y de manera análoga $-1, y \quad -1, -y \quad = (1{,}0)$

Por lo cual en los números duales $M(0)$, cualquier número de la forma $(\pm 1, y)$ es una unidad.

Como no hay más casos podemos, hagamos un resumen de los resultados obtenidos:

**Teorema 14:** El conjunto de unidades en $M(i^2)$ es:

1. $U = \quad 1{,}0\ ,\ -1{,}0 \quad \cup \{\ x, y\ \epsilon M\ \ i^2\ : x = \pm 1\}$ en $M(0)$
2. $U = \quad 1{,}0\ ,\ -1{,}0\ ,\ 0{,}1\ , (0, -1)$ en $M\ \ 1$
3. $U = \quad 1{,}0\ ,\ -1{,}0 \quad$ para $M\ \ i^2\ , i^2 > 1.$
4. $\|\ \ x, y\ \ \| = 1 \leftrightarrow$ x, y es unidad.

Como pequeño teorema relacionado con este se tiene que:

La definición que sigue tiene dos formas equivalentes, muy similar a como pasa con las representaciones $a + bi$ y $(a, b)$, ambas son muy valiosas para realizar algunas demostraciones y exploraciones, sin embargo para llegar a la equivalencia entre ellas necesitamos el siguiente teorema:

**Teorema 15:**

Dada $(u, v) \in M\ \ i^2$ con $(u, v)$ unidad, $(u, v)$ tiene inverso multiplicativo en $M\ \ i^2$ y también es una unidad

**Demostración**

1. $(u, v)$ tiene inverso multiplicativo en $M\ \ i^2$ , además este es una unidad.

$(u, v)$ es una unidad, será nuestra hipótesis

$\forall (a, b) \in M\ \ r^2\ ,\ \ (u, v) | (a, b)$, por D12

En particular se cumple para $\ a, b\ \ = (1{,}0)$ que $(u, v) | (1{,}0)$

$\exists\ x, y\ \ \in M\ \ i^2\ :\ \ u, v\ \ \ x, y\ \ =\ \ 1{,}0\ \ ,$ por D11

$(u, v)^{-1} = (x, y)$, por la definición de inverso multiplicativo y por la propiedad 2 de T2.

$(u, v)^{-1} | (1{,}0)$, por D11

$\forall (a, b) \in M\ \ r^2\ \ ,\ \ (u, v)^{-1} | (a, b)$, ya que $\ 1{,}0\ \ $ es unidad, por D12 y la propiedad 2 de T12

$(u, v)^{-1}$ es unidad, por D12

Ahora procedamos a definir el significado de número asociado, hay dos posibles formas habituales, utilizaremos la asociada a las unidades como inicial, ya que hemos explorado recientemente este concepto, y procederemos a presentar la segunda en un teorema:

**Definición 13(μ):**

$\forall\ a,b\ \ c,d\ \ \in M\ i^2\ ,\ a,b \sim c,d\ \leftrightarrow\ a,b\ =\ c,d\ \ u,v\ ,\ u,v$ es una unidad

Si $a,b \sim c,d$ se cumple diremos que $a,b$ está asociado a $c,d$ .

**Teorema 16(μ):**

$$\forall\ a,b\ \ c,d\ \ \in M\ i^2\ ,\ a,b \sim c,d\ \leftrightarrow\ a,b \mid c,d\ \wedge\ c,d \mid a,b$$

**Demostración:**

Para demostrar la equivalencia entre proposiciones, demostremos inicialmente que la primera implica la segunda, es decir $a,b\ =\ c,d\ \ u,v\ ,\ u,v\ \ unidad \rightarrow\ a,b \mid c,d\ \wedge\ c,d \mid a,b$

$a,b\ =\ c,d\ \ u,v\ ,\ u,v\ \ unidad$, es nuestra hipótesis

$(c,d)|(a,b)$ por D12

$a,b\ (u,v)^{-1} =\ c,d\ \ u,v\ \ (u,v)^{-1}$, por T15, multiplicando $(u,v)^{-1}$ a ambos lados de la primera ecuación presentada

$a,b\ (u,v)^{-1} =\ c,d\ (1,0)$, por la definición de inverso multiplicativo

$a,b\ (u,v)^{-1} =\ c,d$ , por la propiedad 3 de la multiplicación en T2

$(a,b)|\ c,d$ , por D11

Ahora demostremos que la segunda parte implica la primera, es decir $a,b \mid c,d\ \wedge\ c,d \mid a,b\ \rightarrow\ a,b\ =\ c,d\ \ u,v\ ,\ u,v\ \ unidad$

$a,b\ \ \ c,d\ \wedge\ c,d\ \ \ a,b$ , es nuestra hipótesis

$\| \ a,b \ \| \ | \ \| \ c,d \ \| \wedge \| \ c,d \ \| \ | \ \| \ a,b \ \|$, por la propiedad 4 de T12

$\| \ a,b \ \| = \| \ c,d \ \|$, ya que en $\mathbb{N}$ la relación $|$ es anti simétrica

Ahora utilizando de nuevo una parte de nuestra hipótesis $a,b \ | (c,d)$:

$$\exists \ x,y \ \in M \ i^2 \ : \ a,b \ \ x,y \ = (c,d)$$

$\| \ a,b \ (x,y) \ \| = \| \ c,d \ \|$, aplicando la norma a ambos lados

$\| \ a,b \ \| * \| \ (x,y) \ \| = \| \ c,d \ \|$, por la propiedad 6 de T8

$\| \ a,b \ \| * \| \ (x,y) \ \| = \| \ a,b \ \|$, usando $\| \ a,b \ \| = \| \ c,d \ \|$ y reemplazando en la ecuación anterior

$\| \ x,y \ \| = 1$, por la propiedad cancelativa de la multiplicación en $\mathbb{N}$

$(x,y)$ es unidad, por la propiedad 4 de T14

$a,b \ \ x,y \ = \ c,d \ , (x,y)$ unidad como se quería demostrar.

Las dos relaciones que definidas $|$ y$\sim$, si bien son muy similares, son de naturaleza diferente, se muestran algunas de sus propiedades en el siguiente teorema:

**Teorema 17(μ):** La relación 'ser divisible' $|$ es una relación de pre-orden y la relación 'ser asociado' $\sim$ es una relación de equivalencia:

**Demostración:**

Demostremos primero que $|$ es una relación de pre-orden:

a) La relación $|$ es reflexiva, $\forall \ a,b \ \in M \ i^2 \ , (a,b) | (a,b)$ se tiene por la propiedad 1 del T12.

b) La relación $|$ no es anti simétrica, por ejemplo $(1,0) | (-1,0) \wedge (-1,0) | (1,0)$ pero $1,0 \ \neq (-1,0)$.

c) La relación $|$ es transitiva, $\forall\ a,b\ ,\ c,d\ ,(e,f)\ \in M\ i^2\ ,((a,b)\ |(c,d) \wedge (c,d)\ |(e,f)) \rightarrow (a,b)\ |(e,f)$se tiene por la propiedad 2 del T12.

Demostremos ahora que $\sim$ es una relación de equivalencia:

a) La relación $\sim$ es reflexiva, $\forall\ a,b\ \ \in M\ i^2\ ,(a,b) \sim (a,b)$:

Ya que $a,b\ \ 1,0\ = (a,b)$, con $(1,0)$ una unidad.

b) La relación $\sim$ es simétrica, $\forall\ a,b\ \ \in M\ i^2\ ,(a,b) \sim (c,d) \rightarrow (c,d) \sim (a,b)$:

$a,b\ \sim\ c,d\ $, es nuestra hipótesis

$a,b\ |\ c,d\ \wedge\ c,d\ |\ a,b\ $, por la T16

$c,d\ \ \ a,b\ \wedge\ a,b\ \ \ c,d\ $, ya que $p \wedge q \leftrightarrow q \wedge p$ es tautología

$c,d\ \sim\ a,b\ $, T16.

c) La relación $\sim$ es transitiva, $\forall\ a,b\ ,\ c,d\ ,(e,f)\ \in M\ i^2\ ,((a,b) \sim (c,d) \wedge (c,d) \sim (e,f)) \rightarrow (a,b) \sim (e,f)$:

$((a,b) \sim (c,d) \wedge (c,d) \sim (e,f))$, es nuestra hipótesis

$a,b\ \ u,v\ = (c,d) \wedge\ c,d\ \ w,z\ = (e,f),\ \ u,v\ ,\ w,z\ $ dos unidades, por D12

$a,b\ \ u,v\ \ \ w,z\ = (e,f)$, reemplazando el valor de $(c,d)$ de la primera ecuación en la segunda

$a,b\ (\ u,v\ \ w,z\ ) = (e,f)$, por la propiedad 1 de la multiplicación de T2

Ahora verifiquemos que $(\ u,v\ \ w,z\ )$ es una unidad:

$\|\ u,v\ \| = 1 \wedge \|\ w,z\ \| = 1$, por la parte 4 de T14 ya que $u,v\ ,\ w,z\ $ son unidades

$\|\ u,v\ \| * \|\ w,z\ \| = 1 = \|\ u,v\ \ w,z\ \|$, por la propiedad 6 de T8

$u, v \quad w, z$ , es unidad por la parte 4 de T14

Retomando $a, b \quad u, v \quad w, z \quad = \quad e, f$ , con $u, v \quad w, z$ unidad, por T16 se concluye que $(a, b) \sim (e, f)$ como se quería demostrar.

Por los puntos anteriormente demostrados se tiene que $|$ es una relación de pre-orden y la relación $\sim$ es una relación de equivalencia.

Una relación interesante entre $|$ y $\sim$, que nos facilitará el trabajo de encontrar divisores de un número es:

**Teorema 18(μ):**

$(a, b) \sim (c, d) \wedge (x, y) \,|\, (a, b) \rightarrow (x, y) \,|\, (c, d)$

**Demostración**

$(a, b) \sim (c, d) \wedge (x, y) \,|\, (a, b)$, es nuestra hipótesis

$(c, d) \sim (a, b)$, ya que la relación $\sim$es simétrica por T17 y $\exists \; e, f \; \in M \; i^2 : \; a, b \; = (x, y)(e, f)$ por D11

$c, d \; = \; u, v \quad a, b \; , \; a, b \; = (x, y)(e, f)$ por D13

$c, d \; = (\; u, v \; (e, f))(x, y)$, reemplazando el valor de $(a, b)$ y por las propiedades 1 y 2 de la multiplicación en T2

$(x, y) \,|\, c, d$ , por D11

En otras palabras este teorema nos indica que los números asociados entre si tienen siempre los mismos divisores, así en $M(1)$ por ejemplo $5{,}6 \; , \; 6{,}5 \; , \; -5, -6 \; , (-6. -5)$ tienen los mismos divisores, por lo cual bastará determinar los divisores de uno de ellos para conocer los de todos.

Ya con las suficientes herramientas para comenzar a explorar la divisibilidad, veamos un ejemplo del teorema 12, y establezcamos algunas descomposiciones iniciales de números en nuestros conjuntos, en cualquier $M(i^2)$ es válido:

$$24{,}12 \ = 12(2{,}1)$$

Los divisores de 12 son 1, -1, 2,-2, 3, -3, 4, -4,6-,-6,12.-12, con cada uno de ellos se puede construir un divisor de $24{,}12$ y por lo tanto una descomposición del número, veamos los positivos:

$$24{,}12 \ = \ 1{,}0 \quad 24{,}12 \ = \ 2{,}0 \quad 12{,}6 \ = \ 3{,}0 \quad 8{,}4 \ = \ 4{,}0 \quad 6{,}3 \ = \ 6{,}0 \quad 4{,}2$$
$$= (12{,}0)(2{,}1)$$

Las descomposiciones asociadas a los números negativos son muy similares a estas, ya que en cualquier $M\ i^2\ , (a, b) \sim (-a, -b)$ , y la descomposición por las unidades la tienen todos los números, por la definición de divisibilidad, por ejemplo:

$$(2{,}0)(12{,}6) = -(-2{,}0)(12{,}6) = (-1{,}0)(-2{,}0)(12{,}6)$$

Por esto solo estudiaremos las descomposiciones salvo unidades y asociados; aplicando de nuevo el teorema a estas descomposiciones, sucesivamente, por ejemplo para $(12{,}0)(2{,}1)$ obtenemos:

$$24{,}12 \ = \ 12{,}0 \quad 2{,}1 \ = \ 3{,}0 \ (2{,}0)(2{,}0)(2{,}1)$$

El problema ahora radica en determinar si estos factores tienen más divisores, si es así hay que preguntarse también si las descomposiciones de estos son únicas o hay más de una y si se pueden seguir descomponiendo los factores que se encuentren; los números en los cuales no se puede usar esta herramienta, es decir los casos problemáticos como $2{,}1$ o $3{,}0$ son números en los cuales:

a) $a, b \ = 1$, las componentes del número son primos relativos

b)$(p, 0)$ el número es de esta forma con $p$ primo.

c) También puede aplicarse la herramienta a por ejemplo $0,9 = (3,0)(0,3)$, pero no sabemos si $(0,3)$ tenga más divisores, por lo cual un tercer tipo de numero problemático son los $(0,p)$ con $p$ primo.

Cambiando de representación los casos b) y c), al intentar resolver este problema estaríamos preguntándonos con $p$ primo en $\mathbb{Z}$, ¿$p$ y $pi$ tienen divisores en $M(i^2)$?, ¿los números primos en $\mathbb{Z}$ seguirán siendo primos en $M(i^2)$?si no, ¿los divisores de los números primos en $\mathbb{Z}$ son primos en $M(i^2)$?

Es claro que el camino para encontrar una solución definitiva al problema de la divisibilidad es encontrar una manera de descomponer un número finitamente, es decir llegar a una descomposición cuyos términos no se puedan seguir descomponiendo, esto es, que sean irreducibles, así la idea de número primo, o factor primo, juega un papel muy importante en nuestro estudio, así nace la necesidad de definir esta idea en $M(i^2)$:

**Definición 14(μ):**

Un número $a,b \in M\ i^2$ , $(a,b) \neq u$ unidad, es primo si y solamente si es divisible únicamente por las unidades del conjunto y sus asociados. Si $a,b$ no es primo entonces diremos que es compuesto.

Ya hemos identificado completamente las unidades de cada conjunto $M\ i^2$ , si queremos determinar si $(a,b)$ es primo, tenemos que conocer quiénes son sus asociados y con ellos determinar su conjunto de divisores; respecto a los números asociados, si recordamos D13, podemos deducir que al multiplicar un número $(a,b)$ por una unidad encontraremos un asociado a este, haciendo $a,b * U$ encontraremos el conjunto de todos los asociados a $a,b$ .

Por ejemplo en $M(1)$, para $5,6$ encontremos el conjunto de asociados:

$$(5,6)_{\sim} = \{\ 5,6 \quad 1,0\ ,\ 5,6 \quad -1,0\ ,\ 5,6 \quad 0,1\ ,\ 5,6\ (0,-1)\}$$

Desarrollando las multiplicaciones se tienen los cuatro asociados a $(5,6)$:

$$(5,6)_{\sim} = \{\ 5,6\ ,\ -5,-6\ , (6,5), (-6,-5)\}$$

Entre este conjunto y el conjunto de unidades, $(5,6)$ tendría al menos 8 divisores, determinar si es primo o no depende de si solo tiene 8 divisores o si tiene más, de hecho si solo trabajáramos con los números de Minkowski, definir un número primo como un número que solo tiene 8 divisores, sería equivalente a la definición que tenemos, sin embargo nuestra definición actual tiene una ventaja sobre definir el concepto de numero primo por el número de divisores que tenga, para ilustrar esta situación encontremos los asociados a $(5,6)$ en $M\ 0$ :

$$5,6\ _{\sim} =\ \ 5,6\ \ *(\ \ 1,0\ ,\ -1,0\ \ \cup\ \ x,y\ \epsilon M\ i^2\ : x = \pm 1\ )$$

$$5,6\ _{\sim} =\ (5,6),\ -5,-6\ \ \cup\ \ 5,6\ \ *\{\ x,y\ \epsilon M\ i^2\ : x = \pm 1\}$$

$$5,6\ _{\sim} =\ \ 5,6\ ,\ -5,-6\ \ \cup\{\ 5x, 5y + 6x\ \epsilon M\ i^2\ : x = \pm 1\}$$

$$5,6\ _{\sim} =\ \ 5,6\ ,\ -5,-6\ \ \cup\{\ \pm 5,5y \pm 6\ \epsilon M\ i^2\ : y \in \mathbb{Z}\}$$

Así en $M(0)$, $5,6$ tendrá un asociado para cada valor posible de $y$, en otras palabras ya que en este conjunto tenemos infinitas unidades, tendremos infinitos asociados de $5,6$ (tantos como números enteros hay), no es viable en este caso definir un numero primo por el número de divisores que tiene ya que, aunque en muchos casos un número primo es el tipo de número que tiene menos divisores, en este caso un número con la menor cantidad de divisores posibles tendría ya infinitos divisores.

Encontremos en $M(36)$, como un último ejemplo, el conjunto de números asociados a $5,6$ :

$$(5,6)_{\sim} = \{\ 5,6\ \ 1,0\ ,\ 5,6\ \ -1,0\ \}$$

$$(5,6)_{\sim} = \{\ 5,6\ ,\ -5,-6\ \}\ \text{por T2}$$

Para cualquier $M\ i^2\ , i^2 > 1$, un numero primo solamente tendría 4 divisores, 2 unidades y dos asociados, notemos que uno de los números asociados siempre es el mismo número, esto se debe a que el elemento neutro es una unidad.

Para continuar nuestro estudio, retomemos los casos problemáticos en la divisibilidad hasta el momento, los números que aún no podemos descomponer son $a,b : mcd\ a,b = 1,\ p,0$ con $p$ primo, es natural que al buscar números primos los primeros que se intuyen como candidatos sean los primos usuales, comencemos por abordar este caso:

### 4.3. Los divisores de $(p,0)$

En esta sección utilizaremos el método analítico para aproximar los divisores de cualquier número $p,0$ , no abordamos $(0,p)$ pues este se puede descomponer como $(0,1)(p,0)$; suponemos inicialmente que tales divisores existen, de hecho podemos garantizar al menos 2 en cualquier $M\ i^2$ , $1,0\ \ p,0 = (p,0)$ procuraremos encontrar soluciones distintas a esta y en general las descomposiciones de $(p,0)$ que involucren unidades y asociados a él, es decir, buscamos divisores que nos permita comprobar si $p,0$ es primo o no:

$a,b\ \ c,d = (p,0)$, será nuestra hipótesis

$ac + bdr^2, ad + bc = p,0$ , por T1

$ac + bdr^2 = p \wedge ad + bc = 0$, por la definición de igualdad entre parejas ordenadas

Aplicaremos el método de Cramer para encontrar las soluciones a este sistema en términos de $c$ y de $d$ :

$$\begin{matrix} a & br^2 \\ b & a \end{matrix} = \begin{matrix} p & br^2 \\ 0 & a \end{matrix}, \begin{matrix} a & p \\ b & 0 \end{matrix}$$

El determinante del sistema es $D = a^2 - b^2r^2$, el de c es $D_c = ap$ y el de d es $D_d = -bp$.

$$c = \frac{D_c}{D} = \frac{ap}{a^2 - b^2r}, \ d = \frac{D_d}{D} = \frac{-bp}{a^2 - b^2r^2}.$$

Probemos el funcionamiento de estas soluciones, para entender el significado de tales ecuaciones y como aplicarlas para encontrar divisores en general, empecemos por los números duales:

### 4.3.1 Números duales, $i^2 = 0, i \neq 0$:

$$c = \frac{ap}{a^2}, d = \frac{-bp}{a^2}, \text{ ya que } r^2 = 0$$

$a^2\ ap\ \wedge a^2\ -bp$, ya que estos números deben ser enteros para que $(c,d) \in M\ i^2$

$$a\ p \wedge a^2\ -bp, \text{ pues en } \mathbb{Z}, (\ xy\ xk) \longrightarrow (y\ k)$$

Como $a$ debe ser un divisor de $p$ con $p$ primo, hay 4 posibilidades, todas ellas satisfacen $a^2\ -bp$:

1. a = 1

$c = \frac{p}{1^2}, d = \frac{-bp}{1^2},$ la descomposición de $(p,0)$ sería:

$$1,b\quad p,-bp\ = (p,0)$$

Aplicando la propiedad 5 de T3 y D5:

$$1,b\quad 1,-b\ (p,0) = (p,0)$$

Como $1,b\ \ y\ (1,-b)$ son unidades para cualquier valor de $b$ no encontramos divisores nuevos.

2.$a = -1$

$c = \frac{-p}{(-1)^2}, d = \frac{-bp}{(-1)^2}, b = b$, nuestra ecuación inicial resulta:

$$-1,b\quad -p,-bp\ = (p,0)$$

Aplicando la propiedad 5 de T3 y D5:

$$-1,b\quad -1,-b\ (p,0) = (p,0)$$

Multiplicando por $-1{,}0\ \ -1{,}0\ =\ 1{,}0$ al primer lado de la ecuación y asociando sus factores:

$$((-1{,}0)\ -1,b\ )(\ -1{,}0\ \ -1,-b\ )(p,0) = (p,0)$$

$$(1,-b)(1,b)(p,0)=(p,0)$$

Comprobando así que se encontró la misma solución del caso anterior.

3.$a=p$

$c=\frac{p^2}{p^2}=1,=\frac{-bp}{p^2}=-\frac{b}{p},-dp=b,$ nuestra, escribimos la solución en términos de d para asegurar que los valores son enteros:

$$p,-dp\quad 1,d\ \ =(p,0)$$

Ya que la multiplicación es conmutativa, esta solución es la misma que encontramos en el caso 1.

4.$a=-p$

$c=\frac{-p^2}{(-p)^2}=-1,\ d=\frac{-bp}{(-p)^2}=-\frac{b}{p},-dp=b,d=d,$ nuestra ecuación inicial resulta:

$$-p,-dp\quad -1,d\ \ =(p,0)$$

Ya que la multiplicación es conmutativa, esta solución es la misma que encontramos en el caso 2.

No habiendo más casos posibles se concluye que $(p,0)$ es un número primo en $M\ \ 0\ \ $ ya que sus únicos divisores son unidades $\ 1,-b\quad 1,b\ $, sí mismo y sus asociados $\ p,-bp\ $.

| Conjunto | $M\ \ 0\ ,i^2=0$ |
|---|---|
| Número | $p,0$ |
| Unidades del conjunto | $1,b\ ,\forall b\in\mathbb{Z}$ |
| Asociados al número | $p,bp\ \ \forall b\in\mathbb{Z},p$ primo |
| $(p,0)\ \ $ es primo | Si |

*Tabla 1. Resumen Ejemplo 1,* $\ p,0\ $ *sus divisores en los números duales*

### 4.3.2 Números de Minkowski, $i^2 = 1, i \neq \pm 1$:

$c = \frac{ap}{a^2-b^2}$, $d = \frac{-bp}{a^2-b^2}$, ya que $r^2 = 1$

Para que $c, d \in \mathbb{Z}$ se debe cumplir que:

$$a^2 - b^2 \ ap \wedge a^2 - b^2 \ -bp$$

Luego se tendrá similar al caso anterior que:

$$a^2 - b^2 | p \ \ a + b \ \ \rightarrow a + b | p$$

Como $a + b$ resulta ser un divisor de $p$, con este un número primo, se presentan de nuevo cuatro casos:

**1.$a + b = 1$**

$a = a, b = 1 - a, c = \frac{ap}{a^2-(1-a)^2}$, $d = \frac{-(1-a)p}{a^2-(1-a)^2}$, hallando y reemplazando el valor de $b$

$c = \frac{ap}{2a-1}$, $d = \frac{ap-p}{2a-1}$, desarrollando los denominadores y el numerador del valor de $d$

$2a - 1 \ ap \wedge 2a - 1 \ ap - p$, ya que $c, d$ deben ser números enteros

$2a - 1 | p$, aplicando que en $\mathbb{Z}$, $a|b \wedge a|c \rightarrow a|b \pm c$

De nuevo, como $2a - 1$ es un divisor de $p$, se tienen 4 casos:

a) $2a - 1 = 1$

$a = 1, b = 0, c = p, d = 0$, hallando el valor de $a$ y reemplazando en las ecuaciones anteriores.

La primera solución que encontramos es:

$$1,0 \quad p,0 \ = (p,0)$$

Siendo la descomposición por elemento neutro, no encontramos divisores nuevos en este primer caso.

b)$2a-1=-1$

$a=0, b=1, c=0, d=p$, hallando el valor de $a$ y reemplazándolo para hallar los demás valores.

Obtenemos que:

$$0,1 \quad 0,p \quad = (p,0)$$

Ya que $(0,1)$ es una unidad en $M(1)$ y $(0,p)$ es un asociado a $(p,0)$, no encontramos divisores nuevos en este caso.

c)$2a-1=p$

$$a=\frac{p+1}{2}, b=\frac{1-p}{2}, c=\frac{p+1}{2}, d=\frac{p-1}{2}$$

Es decir, la solución es:

$$\frac{p+1}{2},\frac{1-p}{2} \quad \frac{p+1}{2},\frac{p-1}{2} \quad = (p,0)$$

Aplicando D8 y T2:

$$\frac{p+1}{2},\frac{p-1}{2} \quad \frac{p+1}{2},\frac{p-1}{2} \quad = \quad p,0$$

Para que estas soluciones existan, todas estas componentes que parecen en un principio racionales, deben ser enteras, sin embargo recordemos que $p$ es primo, con $p \neq 2, p$ es impar de la forma $2k+1$, de esta manera $p+1=2k+2, p-1=2k, 1-p=-2k$, son todos múltiplos de dos, o sea que ya de entrada $\frac{p+1}{2}, \frac{1-p}{2}, \frac{p-1}{2}$ son números enteros, es decir que ningún $(p,0)$ en $M\ 1$ , salvo $(2,0)$, es primo.

Aplicando este esquema por ejemplo para $7,0$ :

$$4,-3 \quad 4,3 \quad = (7,0)$$

Sin embargo en $M\ 1$ , ¿serán estos los únicos divisores adicionales de $(p,0)$?

d) $2a - 1 = -p$

$$a = \frac{1-p}{2}, b = \frac{p+1}{2}, c = \frac{p-1}{2}, d = \frac{p+1}{2}$$

La solución que encontramos aquí es:

$$\frac{1-p}{2}, \frac{p+1}{2} \quad \frac{p-1}{2}, \frac{p+1}{2} = (p, 0)$$

Aplicando D8 y T2:

$$\frac{p-1}{2}, \frac{p+1}{2} * (- \frac{p-1}{2}, \frac{p+1}{2}) = p, 0$$

Es una segunda descomposición nueva de $(p, 0)$.

Aplicando el mismo análisis a los otros 3 casos, de manera más resumida obtenemos:

**2.$a + b = -1$**

$$a = a, b = -1 - a, c = \frac{-ap}{2a+1}, d = \frac{-(1+a)p}{2a+1}$$

$$2a + 1 \; -ap \wedge 2a + 1 \; ap - p$$

$$2a + 1| - p$$

Como $2a + 1$ es un divisor de $p$, hay 4 posibilidades:

a) $2a + 1 = 1$

$$a = 0, b = -1, c = 0, d = -p$$

La solución que encontramos es:

$$0,-1 \quad 0,-p \quad = (p,0)$$

Donde $0,-1$ es una unidad y $(0,-p)$ un asociado a $(p,0)$.

b)$2a+1=-1$

$$a=-1, b=0, c=-p, d=0$$

Obtenemos que:

$$-1,0 \quad -p,0 \quad = (p,0)$$

Donde $-1,0$ es una unidad y $(-p,0)$ un asociado a $(p,0)$.

c)$2a+1=p$

$$a=\frac{p-1}{2}, b=\frac{-(p+1)}{2}, c=\frac{-(p-1)}{2}, d=\frac{-(p+1)}{2}$$

La solución encontrada es:

$$\frac{p-1}{2},\frac{-(p+1)}{2} \quad \frac{-(p-1)}{2},\frac{-(p+1)}{2} \quad = (p,0)$$

Aplicando D8 y T2:

$$- \quad \frac{p-1}{2},\frac{p+1}{2} \quad \frac{p-1}{2},\frac{p+1}{2} \quad = \quad p,0$$

La cual es una nueva descomposición de $(p,0)$.

d) $2a+1=-p$

$$a=\frac{-(p+1)}{2}, b=\frac{p-1}{2}, c=\frac{-(p+1)}{2}, d=\frac{-(p-1)}{2}$$

La solución que encontramos aquí es:

$$\frac{-(p+1)}{2},\frac{p-1}{2}\quad\frac{-(p+1)}{2},\frac{-(p-1)}{2}\quad=(p,0)$$

Aplicando D8 y T2:

$$\frac{-(p+1)}{2},\frac{p-1}{2}\quad\frac{-(p+1)}{2},\frac{p-1}{2}\quad=\quad p,0$$

Es una cuarta nueva descomposición para $(p,0)$

**3.$\boldsymbol{a+b=p}$**

$$a=a,b=p-a,c=\frac{a}{2a-p},d=\frac{a-p}{2a-p}$$

$$2a-p\ a\wedge 2a-p\ a-p$$

$$2a-p|p$$

Como $2a-p$ es un divisor de $p$, hay 4 posibilidades:

a) $2a-p=1$

$$a=\frac{p+1}{2},b=\frac{p-1}{2},c=\frac{p+1}{2},d=-\frac{p-1}{2}$$

La solución que encontramos es:

$$(\frac{p+1}{2},\frac{p-1}{2})(\frac{p+1}{2},-\frac{p-1}{2})=(p,0)$$

Aplicando D8:

$$(\frac{p+1}{2},\frac{p-1}{2})(\frac{p+1}{2},\frac{p-1}{2})=(p,0)$$

Es la misma solución hallada en 1.c.

b)$2a-p=-1$

$$a = \frac{p-1}{2}, b = \frac{p+1}{2}, c = \frac{-(p-1)}{2}, d = \frac{p+1}{2}$$

Obtenemos que:

$$\frac{p-1}{2}, \frac{p+1}{2} \quad \frac{-p-1}{2}, \frac{p+1}{2} = (p, 0)$$

Esta solución es la misma encontrada en 1.d.

c)$2a - p = p$

$$a = p, b = 0, c = 1, d = 0$$

La solución encontrada es:

$$p, 0 \quad 1, 0 = (p, 0)$$

Es una de las descomposiciones usuales de $(p, 0)$.

d) $2a - p = -p$

$$a = 0, b = p, c = 0, d = 1$$

La solución encontrada es:

$$0, p \quad 0, 1 = (p, 0)$$

Es también una de las descomposiciones usuales de $(p, 0)$.

**4.$a + b = -p$**

$$a = a, b = -p - a, c = \frac{-a}{2a+p}, d = \frac{-p-a}{2a+p}$$

$$2a + p\ -a \wedge 2a + p\ \ -p - a$$

$$2a + p | p$$

Como $2a + p$ es un divisor de $p$, hay 4 posibilidades:

a) $2a + p = 1$

$$a = -\frac{p-1}{2}, b = -\frac{p+1}{2}, c = \frac{p-1}{2}, d = -\frac{p+1}{2}$$

La solución que encontramos es:

$$(-\frac{p-1}{2}, -\frac{p+1}{2})(\frac{p-1}{2}, -\frac{p+1}{2}) = (p, 0)$$

Aplicando D8:

$$-(\frac{p-1}{2}, \frac{p+1}{2})(\frac{p-1}{2}, \frac{p+1}{2}) = (p, 0)$$

Es la misma solución hallada en 2.c.

b)$2a + p = -1$

$$a = -\frac{p+1}{2}, b = -\frac{p-1}{2}, c = -\frac{p+1}{2}, d = \frac{p-1}{2}$$

Obtenemos que:

$$-\frac{p+1}{2}, -\frac{p-1}{2} \quad -\frac{p+1}{2}, \frac{p-1}{2} \ = (p, 0)$$

Aplicando D8 y T2:

$$-\ \frac{p+1}{2}, \frac{p-1}{2}\ * (-\ \frac{p+1}{2}, \frac{p-1}{2}\ ) = (p, 0)$$

Esta solución es la misma encontrada en 2.d.

c)$2a + p = p$

$$a = 0, b = -p, c = 0, d = -1$$

La solución encontrada es:

$$0, -p \quad 0, -1 \ = (p, 0)$$

Es una de las descomposiciones usuales de $(p, 0)$.

d) $2a + p = -p$

$$a = -p, b = 0, c = -1, d = 0$$

La solución encontrada es:

$$-p, 0 \quad -1, 0 \ = (p, 0)$$

Es también una de las descomposiciones usuales de $(p, 0)$.

Todas las soluciones nuevas encontradas son muy similares, de hecho, todas pueden ser escritas en términos de una sola, asociados y usando los conjugados, escojamos por ejemplo $S = (\frac{p+1}{2}, \frac{p-1}{2})$, obtenemos la siguiente tabla:

| Descomposición de $(p, 0)$ | Caso en que se encontró |
|---|---|
| $S * S$ | *1c, 3a* |
| $(-S) * (S)$ | *2d, 4b* |
| $(S(0,1)) * (S(0,1))$ | *1d, 3b* |
| $(S(0,-1)) * (S(0,1))$ | *2c,4a* |

*Tabla 2. Posibles descomposiciones de $p, 0$ en los números de Minkowski*

Podemos concluir por ello que hemos encontrado 2 divisores de $(p,0)$,$S,S$ y sus asociados, como en los números de Minkowski hay 4 unidades, $(p,0)$ tiene aquí 8 divisores, excepto por $(2,0)$ que es primo.

¿Serán $S\ y\ S$ soluciones generales

| | |
|---|---|
| Conjunto | $M\ 1\ , i^2 = 1$ |
| Número | $p,0$ |
| Unidades del conjunto | $1,0\ ,\ 0,1\ ,\ -1,0\ ,(0,-1)$ |
| Asociados al número | $p,0\ ,\ -p,0\ ,\ 0,p\ ,\ 0,-p\ ,$ |
| $(p,0)$ es primo | No |
| Divisores adicionales | $\frac{p+1}{2},\frac{p-1}{2}\quad \frac{p+1}{2},\frac{1-p}{2}\ ,\ \frac{-p-1}{2},\frac{1-p}{2}\quad \frac{-p-1}{2},\frac{p-1}{2}\ ,$ $\frac{p-1}{2},\frac{p+1}{2}\ ,\ \frac{1-p}{2},\frac{p+1}{2}\ ,\ \frac{1-p}{2},\frac{-p-1}{2}\quad \frac{p-1}{2},\frac{-p-1}{2}$ |

*Tabla 3.Resumen Ejemplo 2, $p,0$ sus divisores en los números de Minkowski*

### 4.3.3 Conjunto M(4) , $i^2 = 4, i \neq \pm 2$:

Si buscamos los divisores en $M(4)$, siguiendo un proceso muy similar se encuentran:

$$\frac{p+1}{2},\frac{p-1}{4}\quad \frac{p+1}{2},-\frac{p-1}{4}\ = (p,0)$$

$$\frac{p-1}{2},\frac{p+1}{4}\quad -\frac{p-1}{2},\frac{p+1}{4}\ = (p,0)$$

En $M(4)$ $1,0\ ,(-1,0)$ son las únicas unidades, como pasa en cualquier $M\ i^2\ > 1$, distinto al ejemplo anterior no podemos escribir un par de soluciones en términos de las otras 2, analizando las condiciones necesarias y suficientes para que estas soluciones existan obtenemos:

- (2,0) es primo.

- Para que $\frac{p+1}{2}, \frac{p-1}{4}$ $\frac{p+1}{2}, -\frac{p-1}{4}$ sea una descomposición de $(p, 0)$ debe suceder que $2|\frac{p-1}{2}$.
- Para que $\frac{p-1}{2}, \frac{p+1}{4}$ $-\frac{p-1}{2}, \frac{p+1}{4}$ sea una descomposición de $(p, 0)$ debe suceder que $2|\frac{p+1}{2}$.

Es decir, no siempre $(p, 0)$, será numero primo y no siempre tendrá divisores adicionales, esto será dependiente a si se cumplen o no las descomposiciones anteriores.

Recordemos que $\frac{p\pm1}{2}$ es siempre un número entero, nunca sucede que $2|\frac{p-1}{2} \wedge 2|\frac{p+1}{2}$ pues:

$2|\frac{p-1}{2}$ significa que $\exists x \in \mathbb{Z}: 2x = \frac{p-1}{2}$ por la definición de divisibilidad en $\mathbb{Z}$

$2x + 1 = \frac{p-1}{2} + 1 = \frac{p+1}{2}$, implicando así que 2 no es divisor de $\frac{p+1}{2}$.

Recíprocamente se cumple:

$2|\frac{p+1}{2} \rightarrow 2x = \frac{p+1}{2}$, $2x - 1 = \frac{p+1}{2} - 1 = \frac{p-1}{2}$, 2 no es divisor de $\frac{p+1}{2}$, pues este último es un impar.

Siempre se puede descomponer $(p, 0) \neq (2,0)$ con algún par de los divisores anteriores, esto sucede porque siempre se cumplirá $2|\frac{p-1}{2} \vee 2|\frac{p+1}{2}$:

Como $2|p - 1 \rightarrow 2x = p - 1, x$ entero, este tiene tres posibilidades:

$a) x = 2r + 1, r \in \mathbb{Z} \rightarrow 2\ 2r + 1\ = p - 1, 4r + 2 + 2 = p + 1, 4\ r + 1\ = p + 1,$

Ya que $4|p + 1$, se puede encontrar el segundo par de divisores.

$b) x = 2r, r \in \mathbb{Z} \rightarrow 4r = p - 1,$ ya que $4|p - 1$, se puede encontrar el primer par de divisores.

$c)\ x = 0, p = 1$ encontraríamos los divisores de $(1,0)$.

Por las consideraciones anteriores podemos concluir que en $M(4)$, $(p,0)$, salvo por $(2,0)$, no es primo y tiene 6 divisores, $(2,0)$ si lo es y tiene solo 4 divisores.

Visto el camino que seguimos en los tres primeros ejemplos, podemos intentar una generalización, cuando $i^2 > 0$, donde hay finitos divisores, para el proceso de hallar los de $(p,0)$:

### 4.3.4 Divisores de $(p,0)$ para $M\ i^2\ ,\ i^2 > 0,\ i^2 = r^2, i \neq \pm r$

Retomemos que nuestras soluciones generales son de la forma:

$$c = \frac{ap}{a^2 - b^2r^2},\ d = \frac{-bp}{a^2 - b^2r^2}.$$

Intentaremos usar estas condiciones para escribir todo en términos de una sola variable $a$ o $b$, haciendo el análisis, ya que $c, d$ deben ser enteros:

$$a^2 - b^2r^2\ \ ap \wedge a^2 - b^2r^2\ \ - bp$$

Cuando esta condición se da, $a^2 - b^2r^2$ también divide a toda combinación lineal de $ap, -bp$ en particular con $r^2$ conocido:

$$a^2 - b^2r^2\ \ ap - bpk, a^2 - b^2r^2\ \ \ a - bk\ \ p$$

Descomponiendo la diferencia de cuadrados tenemos:

$$(a + br)(a - br)|\ \ a - br\ \ p, (a + br)|p$$

Siendo $(a + br)$ un divisor de $p$ hay cuatro casos posibles:

**1.$a + br = 1$**

Escribiendo todas las variables en términos de $b$ se tiene:

$$a = 1 - br, b = b, c = \frac{p - pbr}{1 - 2br},\ d = \frac{-bp}{1 - 2br},$$

$1 - 2br\ \ p - pbr \wedge 1 - 2br\ \ - bp$, ya que $c, d$ deben ser números enteros

De las dos relaciones se obtiene que:

$$1-2br|p-pbr+pbr, 1-2br|p$$

Como $1-2br$ es un divisor de $p$, se tienen 4 casos:

a) $1-2br\ =1$

$$a=1, b=0, c=p, d=0$$

La solución que encontramos es:

$$1{,}0\quad p, 0\ \ =(p,0)$$

b)$1-2br\ =-1, br\ =1$

Se tienen dos posibles casos:

- $b\ =1\wedge r=1$, de donde se obtiene en los números de Minkowski la descomposición $\ 0{,}1\quad 0, p\ \ =(p,0)$
- $b\ =-1\wedge r=-1$, de donde se obtiene en los números de Minkowski la descomposición $\ 0,-1\quad 0,-p\ \ =(p,0)$

c)$1-2br\ =p$

$$a=\frac{p+1}{2}, b=\frac{1-p}{2r}, c=\frac{p+1}{2}, d=\frac{p-1}{2r}$$

La descomposición que encontramos es:

$$\frac{p+1}{2},\frac{1-p}{2r}\quad \frac{p+1}{2},\frac{p-1}{2r}\ \ =(p,0)$$

Para que esta solución exista, debe darse que $\frac{p-1}{2r}$ sea un entero, o equivalente a ello que $\frac{1-p}{2r}$ lo sea, como vimos antes $\frac{p+1}{2}$ es siempre un entero, o sea que la condición es $2r|p-1$.

d) $1-2br\ =-p$

$$a = \frac{1-p}{2}, b = \frac{p+1}{2r}, c = \frac{p-1}{2}, d = \frac{p+1}{2r}$$

La solución que encontramos es:

$$\frac{1-p}{2}, \frac{p+1}{2r} \quad \frac{p-1}{2}, \frac{p+1}{2r} \quad = (p, 0)$$

Para que esta exista debe cumplirse que $2r|p-1$

**2.$a + br = -1$**

$$a = -1 - br, b = b, c = \frac{-p-pbr}{1+2br}, d = \frac{-bp}{1+2br},$$

$1 + 2br \ -p - pbr \wedge 1 + 2br \ - bp$, ya que $c, d$ deben ser números enteros

De las dos relaciones se obtiene que:

$$1 + 2br \ -p - pbr - \ -pbr \ , 1 + 2br \ - p$$

Esta última condición es equivalente en $\mathbb{Z}$ a $1 + 2br|p$ ya que $p$ y $-p$, usando el hecho de que dos números asociados tienen los mismos divisores.

Como $1 + 2br$ es un divisor de $p$, se tienen 4 casos:

a) $1 + 2br \ = 1, br = 0, b = 0$ ya que $r^2 \neq 0$

$$a = -1, b = 0, c = -p, d = 0$$

La solución que encontramos es:

$$-1,0 \quad -p, 0 \quad = (p, 0)$$

b)$1 + 2br \ = -1, br \ = -1$

Se tienen dos posibles casos:

- $b = 1 \wedge r = -1$, de donde se obtiene en los números de Minkowski la descomposición $0,1 \quad 0,p = (p,0)$
- $b = -1 \wedge r = 1$, de donde se obtiene en los números de Minkowski la descomposición $0,-1 \quad 0,-p = (p,0)$

Soluciones que ya fueron encontradas en 1.b)

c)$1 + 2br = p$

$$a = \frac{-(p+1)}{2}, b = \frac{p-1}{2r}, c = \frac{-(p+1)}{2}, d = \frac{-(p-1)}{2r}$$

La descomposición que encontramos es:

$$\frac{-(p+1)}{2}, \frac{p-1}{2r} \quad \frac{-(p+1)}{2}, \frac{-(p-1)}{2r} = (p,0)$$

Para que esta solución exista, debe darse que $\frac{p-1}{2r}$ sea un entero, o equivalente a ello que $\frac{-(p-1)}{2r}$ lo sea, como vimos antes $\frac{(p+1)}{2}$ es siempre un entero y por lo tanto $\frac{-(p+1)}{2}$ también, o sea que la condición es $2r|p-1$.

d) $1 + 2br = -p$

$$a = \frac{p-1}{2}, b = \frac{-(p+1)}{2r}, c = \frac{-(p-1)}{2}, d = \frac{-(p+1)}{2r}$$

La solución que encontramos es:

$$\frac{p-1}{2}, \frac{-(p+1)}{2r} \quad \frac{-(p-1)}{2}, \frac{-(p+1)}{2r} = (p,0)$$

Para que esta exista debe cumplirse que $2r|-(p+1)$ o que $2r|p+1$

**3.$a + br = p$**

$$a = p - br, b = b, c = \frac{p-br}{p-2br}, d = \frac{-b}{p-2br},$$

$p - 2br \ p - br \wedge p - 2br \ -b$, ya que $c, d$ deben ser números enteros

De las dos relaciones se obtiene que:

$$p - 2br \ p - br - \ -b \ r, p - 2br \ p$$

Como $p - 2br$ es un divisor de $p$, se tienen 4 casos:

a) $p - 2br = 1$:

$c = a, d =$−b ya que el denominador es 1

$a = \frac{p+1}{2}, b = \frac{p-1}{2r}, c = \frac{p+1}{2}, d = \frac{-(p-1)}{2r}$

La solución que encontramos es:

$$\frac{p+1}{2}, \frac{p-1}{2r} \quad \frac{p+1}{2}, \frac{-(p-1)}{2r} = (p, 0)$$

Es la misma solución encontrada en 1.c.

b)$p - 2br = -1$:

$a = \frac{p-1}{2}, b = \frac{p+1}{2r}, c = \frac{-(p-1)}{2}, d = \frac{p+1}{2r}$

La solución que encontramos es:

$$\frac{p-1}{2}, \frac{p+1}{2r} \quad -\frac{p-1}{2}, \frac{p+1}{2r} = (p, 0)$$

Es la misma solución encontrada en 1.d.

c)$p - 2br = p, br = 0, b = 0$ ya que $r^2 > 1, \ r^2 \neq 0$

$$a = p, b = 0, c = 1, d = 0$$

La solución que encontramos es:

$$p,0 \quad 1,0 \quad = (p,0)$$

Es la misma solución encontrada en 1.a.

d) $p - 2br \ = -p, br = p$

Se dan dos casos, $r = \pm 1 \vee r = \pm p$, como nuestra condición inicial es $r^2 > 1$, obviaremos el primero, en este se encontrarían las mismas respuestas que en 1.b, por otro lado cuando $r = \pm p$ se obtiene $b = \pm 1$, $a = 0, c = 0, d = \frac{1}{p}$, no se encuentra una solución coherente.

**4.** $\boldsymbol{a + br = -p}$

$$a = -p - br, b = b, c = \frac{-p-br}{p+2br}, d = \frac{-b}{p+2br},$$

$p + 2br \ -p - br \wedge p + 2br \ -b$, ya que $c, d$ deben ser números enteros

De las dos relaciones se obtiene que:

$$p - 2br \ p + br - br, p + 2br \ p$$

Como $p + 2br$ es un divisor de $p$, se tienen 4 casos:

a) $p + 2br \ = 1$:

$c = a, d = -b$ ya que el denominador es 1

$a = \frac{-p-1}{2}$, $b = \frac{1-p}{2r}$, $c = \frac{-p-1}{2}$, $d = \frac{p-1}{2r}$

La solución que encontramos es:

$$\frac{-p-1}{2}, \frac{1-p}{2r} \quad \frac{-p-1}{2}, \frac{p-1}{2r} \ = (p,0)$$

Es la misma solución encontrada en 2.c.

b)$p + 2br = -1$:

$a = \frac{-(p-1)}{2}$, $b = \frac{-(p+1)}{2r}$, $c = \frac{p-1}{2}$, $d = \frac{-(p+1)}{2r}$

La solución que encontramos es:

$$\frac{-(p-1)}{2}, \frac{-(p+1)}{2r} \quad \frac{p-1}{2}, \frac{-(p+1)}{2r} = (p, 0)$$

Es la misma solución encontrada en 2.d.

c)$p + 2br = p, br = 0, b = 0$ ya que $r^2 > 1,\ r^2 \neq 0$

$$a = -p,\ b = 0,\ c = -1,\ d = 0$$

La solución que encontramos es:

$$-p, 0 \quad -1, 0 = (p, 0)$$

Es la misma solución encontrada en 2.a.

d) $p + 2br = -p, br = -p$

Se dan dos casos, $r = \mp 1 \vee r = \mp p$, de manera similar a 2.b, no se encuentran soluciones coherentes para $i^2 > 1$.

En este caso, las cuatro descomposiciones encontradas pueden ser escritas en términos de dos elementos, sus asociados y sus conjugados, a diferencia del caso anterior (esto ocurre porque en general $0,1$ , $(0, -1)$ no son unidades), tomaremos $S1 = (\frac{p+1}{2}, \frac{p-1}{2r})$ y $S2 = (\frac{p-1}{2}, \frac{p+1}{2r})$ obteniendo:

| Descomposición de $(p,0)$ | Caso en que se encontró |
|---|---|
| $S1 * S1$ | *1c, 3a* |
| $(S2) * (S2)$ | *1d, 3b* |
| $-S1 \ * (S1)$ | *2c, 4a* |
| $-S2 \ * (S2)$ | *2c,4a* |

*Tabla 4. Posibles descomposiciones de* $p,0$ *en los números de M* $i^2$ *con* $i^2 > 0$

Podemos concluir por ello que hemos encontrado 4 divisores de $(p,0), S1, S2, S1, S2$ , en general solo tenemos 2 unidades $1,0$ , $(-1,0)$;por ello $(p,0)$ tiene 8 posibles divisores, de nuevo a excepción de $(2,0)$ el cual es primo siempre, solo tiene 4 divisores; cabe además resaltar que estas soluciones coinciden con las que encontramos en los números de Minkowski cuando $i^2 = 1$.

| Conjunto | $M \ i^2 \ , i^2 > 1$ |
|---|---|
| Número | $p,0$ |
| Unidades del conjunto | $1,0 \ , \ -1,0$ |
| Asociados al número | $p,0 \ , \ -p,0$ |
| $(p,0)$ es primo | En general no:<br>En M(4), $(11,0)$ no es primo pero $(13,0)$ si lo es<br>En M(16), $(7,0)$ es primo pero $(23,0)$ no lo es |
| Divisores adicionales | $\frac{p+1}{2}, \frac{p-1}{2r} \quad \frac{p+1}{2}, \frac{1-p}{2r} \quad \frac{-p-1}{2}, \frac{1-p}{2r} \quad , \quad \frac{-p-1}{2}, \frac{p-1}{2r}$<br>$\frac{p-1}{2}, \frac{p+1}{2r} \quad , \quad \frac{1-p}{2}, \frac{p+1}{2r} \quad , \quad \frac{1-p}{2}, \frac{-p-1}{2r} \quad \frac{p-1}{2}, \frac{-p-1}{2r}$ |

*Tabla 5. Resumen General de los divisores de.* $p,0$ *en conjuntos M* $i^2$ *con* $i^2 > 0$

A diferencia de en los números de Minkowski y similar al ejemplo $M(4)$, no se puede asegurar que estos 8 divisores siempre existen, están condicionados a que las dos soluciones principales $S1, S2$ se pertenezcan al conjunto, para esto:

- Para que $S1$ exista se debe dar que $r|\frac{p-1}{2}$
- Para que $S2$ exista se debe dar que $r|\frac{p+1}{2}$

Cuando nos fijamos en $M\ 1$ , al ser $r = 1$, la raíz positiva de $i^2$, siempre se cumple que $1|\frac{p-1}{2} \wedge 1|\frac{p+1}{2}$, esta es la razón por la cual en los números de Minkowski, todo número $(p, 0)$ tiene 8 divisores. No obstante en general, los dos pares de divisores no parecen pertenecer al conjunto, para visualizar mejor esto se organiza la siguiente tabla, analicemos que números son primos según el conjunto en el que se trabaje:

| $\boldsymbol{p}$ | $\boldsymbol{\frac{p-1}{2}}$ | $\boldsymbol{\frac{p+1}{2}}$ | **S1 existe en (+4 divisores)** $\boldsymbol{r}$ =?: | **S2 existe en (+4 divisores)** $\boldsymbol{r}$ =?**:** | **S1 y S2 existen en (+8 divisores)** $\boldsymbol{r}$ =?**:** | $\boldsymbol{(p, 0)}$ **es primo en** $\boldsymbol{r}$ =?**:** | $\boldsymbol{(p, 0)}$ **no es primo en** $\boldsymbol{r}$ =?**:** |
|---|---|---|---|---|---|---|---|
| 2 | x | x | x | x | x | Siempre | x |
| 3 | 1 | 2 | $r = 1$ | $r = 1,2$ | $r = 1$ | $r > 2$ | $r = 1,2$ |
| 5 | 2 | 3 | $r = 1,2$ | $r = 1,3$ | $r = 1$ | $r > 3$ | $r = 1,2,3$ |
| 7 | 3 | 4 | $r = 1,3$ | $r = 1,2,4$ | $r = 1$ | $r > 4$ | $r = 1,2,3,4$ |
| 11 | 5 | 6 | $r = 1,5$ | $r = 1,2,3,6$ | $r = 1$ | $r = 4,$ $r > 6$ | $r = 1,2,3,5,6$ |
| 13 | 6 | 7 | $r = 1,2,3,6$ | $r = 1,7$ | $r = 1$ | $r = 4,5$ $r > 7$ | $r = 1,2,3,6,7$ |
| 17 | 8 | 9 | $r = 1,2,4,8$ | $r = 1,3,9$ | $r = 1$ | $r = 5,6,7$ $r > 9$ | $r = 1,2,3,4,8,9$ |
| 19 | 9 | 10 | $r = 1,3,9$ | $r = 1,2,5,10$ | $r = 1$ | $r = 4,6,7,8$ $r > 10$ | $r = 1,2,3,5,9,10$ |
| 23 | 11 | 12 | $r = 1,11$ | $r = 1,2,3,4,6,12$ | $r = 1$ | $r = 5,7,8,9,10$ $r > 12$ | $r = 1,2,3,4,6,11$ |
| … | …. | … | … | … | … | … | … |

| $p$ | $\frac{p-1}{2}$ | $\frac{p+1}{2}$ | $r \in D_{\frac{p-1}{2}}$ | $r \in D_{\frac{p+1}{2}}$ | $r = 1$ | $r \in \mathbb{N} - (D_{\frac{p-1}{2}} \cup D_{\frac{p+1}{2}})$ | $r \in (D_{\frac{p-1}{2}} \cup D_{\frac{p+1}{2}})$ |
|---|---|---|---|---|---|---|---|

*Tabla 5. Resumen General de los divisores de.* $p,0$ *en conjuntos* $M\ i^2$ *con* $i^2 > 0$

Las columnas 4 y 5, se llenan gracias a la condición S1 y S2 existen si $r$ es un divisor de $\frac{p-1}{2}$ y $\frac{p+1}{2}$ respectivamente; la columna 6 se llena con los $r$ que son divisores comunes entre $\frac{p-1}{2}$ y $\frac{p+1}{2}$, pero dado el hecho $\frac{p-1}{2} + 1 = \frac{p+1}{2}$ y como $mcd\ a, a+1 = 1$, es decir un número natural y su sucesor son siempre primos relativos, implica que el único conjunto en el que ambas soluciones S1 y S2 existen es $M(1)$; $(p,0)$ será primo si ninguno de los divisores adicionales existen, es decir cuando $r \notin (D_{\frac{p-1}{2}} \cup D_{\frac{p+1}{2}})$, lo cual equivale a $r \in \mathbb{N} - (D_{\frac{p-1}{2}} \cup D_{\frac{p+1}{2}})$ y no es primo en el caso contrario $r \in (D_{\frac{p-1}{2}} \cup D_{\frac{p+1}{2}})$.

Los resultados de esta sección nos permite finalmente determinar cuándo un $(p,0)$ es primo:

**Teorema 19:** En $M\ i^2\ , i^2 = r^2, r\ \in \mathbb{Z}, i \neq \pm r$ el número $(p,0)$:

1. Es primo si $p = 2$
2. Con $r^2 = 0$, es primo.
3. Con $r^2 = 1$, no es primo, tomando $S = (\frac{p+1}{2}, \frac{p-1}{2})$, tiene una descomposición única salvo asociados y unidades, como $S * S$, las descomposiciones en términos de los números asociados a $S$ son $S * S$, $(-S) * (S)$, $(S(0,1)) * (S(0,1))$, $(S(0,-1)) * (S(0,1))$,$(p,0)$ tiene 16 divisores.
4. Con $r^2 > 1$, es primo si $r \nmid \frac{p+1}{2} \wedge\ r \nmid \frac{p-1}{2}$.
5. Con $r^2 > 1$, si $(p,0)$ no es primo ocurre que $r \mid \frac{p-1}{2} \veebar r \mid \frac{p+1}{2}$(se da alguna de las dos condiciones pero no ambas), tomando $S1 = (\frac{p+1}{2}, \frac{p-1}{2r})$ si se da la primera condición o $S2 = (\frac{p-1}{2}, \frac{p+1}{2r})$ si se da la segunda, tiene una descomposición única salvo

unidades y asociados como $S * S \ \underline{\vee}\ (S2) * (S2)$, las descomposiciones asociadas no idénticas son $-S1 * S1 \ \underline{\vee}\ -S2 * (S2)$, $p, 0$ tiene 8 divisores.

Faltaría confirmar solamente en esta sección si estos nuevos divisores pueden ser nuevamente descompuestos en términos de otros números, es decir si existe algún $(x, y)$ tal que $(x, y) | (\frac{p+1}{2}, \frac{p-1}{2r})$, por ejemplo, si esto se diera tendríamos una nueva descomposición de $(p, 0)$, en términos de $(x, y)$, por lo cual tendría aún más divisores que los contados en el teorema 19, con esto el trabajo se extendería, sin embargo ya hemos demostrado anteriormente una propiedad que nos indica que no es posible encontrar un $(x, y)$ que cumpla esas condiciones.

### 4.4 Divisores de un número usando normas

El teorema 13 nos permite descomponer números cuyas componentes no sean primos relativos de la forma $mcd\ x, y = m,\ m, 0\ \ \frac{x}{m}, \frac{y}{m} = (v, w)$, donde $v, w$ son primos relativos, además por el teorema fundamental de la aritmética, $m$ puede ser descompuesto de manera única en términos de factores primos, salvo unidades, el orden y asociados, si suponemos que esta descomposición es $m = p_1 * p_2 * p_3 * p_4 \ldots\ldots * p_n$, se puede descomponer de nuevo $m, 0 = p_1, 0\ \ p_2, 0\ \ \ldots\ p_n, 0$ , con $p_i$ primos, resolvimos en la sección anterior la pregunta ¿ $(p_i, 0)$ puede ser descompuesto?, si el caso es afirmativo, el siguiente paso es preguntarse por estos nuevos divisores, $(\frac{p+1}{2}, \frac{p-1}{2r})$, $(\frac{p-1}{2}, \frac{p+1}{2r})$ y sus asociados, con el proceso que hemos seguido tendríamos una descomposición de cualquier número con forma similar a :

$$\frac{p_1+1}{2}, \frac{p_1-1}{2r}\quad \frac{p_1+1}{2}, \frac{-p_1-1}{2r}\quad \frac{p_2-1}{2}, \frac{p_2+1}{2}\quad \frac{-p_2-1}{2}, \frac{p_2+1}{2}\quad (p_3, 0)\ \ldots$$

$$* \ \frac{p_n+1}{2}, \frac{p_n-1}{2r}\quad \frac{p_n+1}{2}, \frac{-p_n-1}{2r}\quad * \ v, w = (x, y)$$

También falta hallar una forma para descomponer cualquier número $v, w$ , en donde las componentes son primos relativos; para ambos casos sirve la misma herramienta, esta es,

utilizar una propiedad que involucra a la relación de divisibilidad y la norma de un número, como vimos en T12:

$$a,b \quad c,d \rightarrow \| \ a,b \ \| \ \| \ c,d \ \|$$

Quizás en una primera impresión no se vislumbra la utilidad de este teorema para encontrar divisores, pero si se tiene en cuenta que $\| \ a,b \ \| \mid \| \ c,d \ \|$ es una condición necesaria para $a,b \mid (c,d)$, se puede transformar esta proposición en el enunciado:

*Todo divisor* $a,b$ *de* $(c,d)$ *debe tener una norma que sea un divisor de la norma de* $(c,d)$.

Con este enunciado, ya se sabe dónde buscar los divisores de un número dada su norma, si por ejemplo buscamos los divisores de $(4{,}3)$ cuya norma es 7 en los números de Minkowski, bastara con buscar en el conjunto de números que tengan norma que dividan a 7, en este caso son 7 o 1 (ya que la norma siempre es un número positivo por su definición), pero la propiedad 4 del teorema 14 nos indica que los únicos números con norma 1 son las unidades, por lo tanto ese conjunto de divisores ya lo conocemos, falta encontrar entonces los números de norma 7 que sean divisores de $4{,}3$ , como nuestra propiedad es una implicación y no un bi-condicional no podremos asegurar que todos los números de norma 7 sean divisores y aunque sabemos para cualquier divisor $a,b$ , $|a^2 - b^2 r^2|$=7, o sea que $a^2 - b^2 r^2 = \pm 7$, es complicado mediante procesos algebraicos llegar a encontrar todos los números que cumplan esta condición, ahora el problema radica en encontrar todos los números de norma 7.

Con la información que se tiene se pueden plantear nuevas estrategias para encontrar todos los números de una determinada norma, pero para abordarlas necesitaremos el siguiente teorema:

**Teorema 20:** $\forall \ a,b \ , \ c,d \ \in M \ i^2 \ , \| \ a,b \ \| = \| \ c,d \ \| \rightarrow ( \ a,b \ \sim \ c,d \ \veebar \ a,b \nmid c,d \ \wedge \ c,d \nmid a,b)$

**Demostración:**

Solo hay dos opciones en la lógica bivalente que manejamos:

a) $a,b \mid (c,d)$

$a,b \mid (c,d) \wedge \| \ a,b \ \| = \| \ c,d \ \|$, son nuestras hipótesis

$\exists \ x,y \ \in M \ i^2 : \ a,b \ \ x,y \ = (c,d)$, por D11

$\| \ a,b \ \ \mathrm{x,y} \ \| = \| \ c,d \ \|$, aplicando normas a cada lado

$\| \ a,b \ \| * \| \ x,y \ \| = \| \ c,d \ \|$, por la propiedad 6 de T8

$\| \ (c,d) \ \| * \| \ x,y \ \| = \| \ c,d \ \|$, por principio de sustitución usando nuestra hipótesis

$\| \ x,y \ \| = 1$, por la propiedad cancelativa en $\mathbb{Z}$

$x,y$ es una unidad, por la propiedad 4 de T14

$a,b \sim c,d$ , por D13

$a,b \mid (c,d) \wedge \ c,d \mid (a,b)$, por T16

b) $a,b \nmid c,d$

Si suponemos que se cumple que $c,d \mid (a,b)$, se deduce siguiendo el proceso del caso anterior, $a,b \mid (c,d)$ y se llegaría a una contradicción por lo cual solo puede suceder $c,d \nmid a,b$ .

El teorema anterior nos indica que al tener dos números de la misma norma, sucede solo uno de los dos casos, o los dos se dividen entre sí o ninguno divide al otro, si sucede el primer caso ambos serán asociados y tendrán los mismos divisores por T18. Teniendo esta información en cuenta y retomando nuestro ejemplo anterior, $4,3$ con norma 7 en los números de Minkowski, sus divisores deben tener norma 1 o 7, de los cuales los que tienen norma 1 son las unidades y por el teorema 20, los que tienen norma 7 son sus asociados, se concluye por D14 que $4,3$ es un numero primo en $M(1)$; en general:

**Teorema 21(μ):** $\forall\ a,b\ \in M\ i^2\ ,\|\ \ a,b\ \ \|= p, p \in \mathbb{N}$ , $p$ primo $\rightarrow\ a,b\ \ $ es primo en $M\ i^2\ .$

**Demostración:**

$\|\ \ a,b\ \ \|= p, p \in \mathbb{N}$ , $p$ primo, es nuestra hipótesis

Supongamos $(c,d) \in M\ i^2\ $ divisor de $(a,b)$

$\|\ \ c,d\ \ \| \mid \|\ \ a,b\ \ \|$, por la propiedad 4 de T12

$\|\ \ c,d\ \ \| \mid p$, por principio de sustitución

$(\|\ \ c,d\ \ \|= 1)$ o $(\|\ \ c,d\ \ \|= p)$, por la caracterización de los números primos en $\mathbb{N}$

$c,d\ $ es una unidad o $\|\ \ c,d\ \ \|=\|\ \ a,b\ \ \|$, por la propiedad 4 de T14 y nuestra hipótesis

$c,d\ $ es una unidad o $\ a,b\ \sim\ c,d\ $ , por T20

$(a,b)$, es primo por D14, ya que tomamos un $\ c,d\ $ fijo pero arbitrario

En el transcurso de este trabajo, hemos identificado y clasificado varios tipos de números de acuerdo a su norma:

- El conjunto que llamamos $D_0$ se caracteriza por contener los elementos que dañan la propiedad cancelativa, son los divisores de $(0,0)$ y su norma es 0.
- El conjunto de $U$ de unidades, se caracteriza por tener los divisores de todos los números, sus elementos tienen norma 1.
- Podemos llamar $P = \{\ x,y\ \in M\ i^2\ :\|\ \ x,y\ \ \|= p\}$, los elementos de este conjunto son todos números primos, ya conocemos estos elementos.

Los teoremas 12 y 20, nos son muy útiles para poder determinar si un número es primo o no de acuerdo a su norma si los aplicamos por ejemplo a $(p,0)$:

$\|\ \ p,0\ \ \|= p^2$, por D9

Un divisor $(x, y)$ de $p, 0$ debe tener norma $1, p \; o \; p^2$, por T12 pues estos son todos los posibles valores en las descomposiciones de esta norma.

Los divisores de norma 1 son las unidades, por la propiedad 4 de T14 y los de norma $p^2$ son asociados a $p, 0$ , por lo cual es interés hallar solo los números de norma $p$ para determinar si es primo o compuesto, pero T19 nos indica los únicos divisores además de las unidades y asociados de $p, 0$ , es fácilmente comprobable aplicando la definición de norma y haciendo los cálculos que todos estos, cuando existen, tienen norma $p$, es decir son estos elementos del conjunto al cual llamamos *P*, por lo tanto son primos (por ello no se puede seguir descomponiendo $(p, 0)$).

Por un lado se tiene que los divisores de $(p, 0)$ son elementos del conjunto *P* pero ¿serán estos todos los elementos del conjunto?, el siguiente procedimiento devela que efectivamente todos los números de norma $p$ tienen la forma encontrada en el teorema 19:

$$\| \;\; a, b \;\; \| = p, \text{ es nuestra hipótesis}$$

$$a^2 - b^2 r^2 = p \vee b^2 r^2 - a^2 = p, \text{ por D9 y definición de valor absoluto}$$

$$a, b \;\; a, b \;\; = p(1,0) \vee \;\; a, b \;\; a, b \;\; = p(1,0), \text{ por D5 y la propiedad 6 de T7}$$

$$a, b \;\; a, b \;\; = (p, 0) \vee \;\; a, b \;\; a, b \;\; = (p, 0), \text{ por D5}$$

$$a, b \;\; \text{es divisor de } (p, 0).$$

Este hecho es importante en cuanto a que los elementos del conjunto *P*, es decir los que tienen norma prima, son dependientes de si existen divisores de $(p, 0)$, para conjuntos con determinados valores de $r^2$, no existirán números de norma 3,5,7,11….., lo cual hace que números cuyas normas sean sus múltiplos sean posiblemente primos, por ejemplo si no existen números de norma 3 en el conjunto los números de norma 6 serán primos, pues las únicas descomposiciones en los números naturales de esta son 6*1 que nos lleva a encontrar divisores que son unidades y asociados, y 2*3, no existiendo números de norma 3 no se pueden encontrar descomposiciones que correspondan a estas normas; teniendo en

cuenta esto y que ya hemos clasificado los números de norma 0, 1, $p$ primo, el siguiente paso en este estudio es intentar clasificar los números de norma compuesta, o encontrar una forma para determinar divisores de estos, claro está recordando que el problema está en el marco de los números cuyas componentes son primos relativos(aquellos que aún no sabemos al 100% como descomponer).

### 4.4.1 Las normas compuestas y diferencias de cuadrados

En esta sección abordaremos el problema de hallar divisores para los números que tienen normas que corresponden a números compuestos, el problema se reduce como notamos en la sección anterior, en encontrar los números que tengan cualquier norma, a partir de estos, determinar si son divisores o no, es decir debemos encontrar números $(a, b)$ que cumplan:

$$a^2 - b^2 r^2 = p_1 p_2 p_3 p_4 \dots . p_n$$

$$b^2 r^2 - a^2 = p_1 p_2 p_3 p_4 \dots . p_n$$

En ambos casos, el calcular la norma consiste en del cuadrado mayor quitar el menor, aunque quizá en esta representación no se visibilicen propiedades que contribuyan a determinar números que cumplan esas condiciones, sin pasar por un largo proceso de análisis como hicimos para encontrar aquellos que tenían norma 1; esto nos fuerza a encontrar otras estrategias para encontrar números, la que usaremos aquí será cambiar la representación de las condiciones, teniendo en cuenta que los números cuadrados no se limitan a su representación numérica, citamos a continuación un fragmento de un artículo que introduce al lector a otra representación de los cuadrados de un número:

*"Al pensar que todo podía explicarse con los números, los Pitagóricos establecieron gran cantidad de clasificaciones entre los éstos y se dedicaron a descubrir sus propiedades. Así iniciaron una rama de las Matemáticas que hoy se conoce como la Teoría de Números, que en el siglo XVII tendría un nuevo impulso con Fermat y ya en el siglo XX ha encontrado aplicaciones insospechadas."*, (Sorándo,s.f)

**Sumas de impares y de pares.**

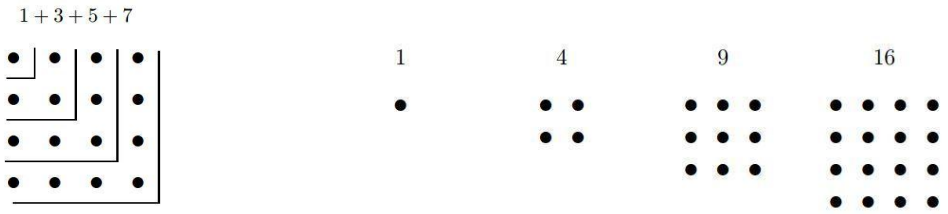
Los Pitagóricos construían sus teoremas juntando piedrecillas para cada número. Así observaron, por ejemplo, que al sumar términos de la sucesión de los números impares:

$1 + 3 = 2^2$, $1 + 3 + 5 = 3^2$ , $1 + 3 + 5 + 7 = 4^2$ y, en general, que: 1 + 3 + 5 + ... + (2n + 1) es un cuadrado perfecto

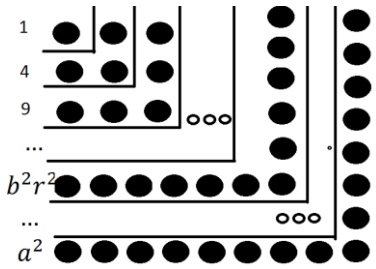
**Números poligonales:**

Para construir con piedras triángulos equiláteros cada vez mayores, se necesitan: 1 , 3 , 6 , 10 , 15 ... etc. Por ello, los Pitagóricos llamaron a éstos los números triangulares. De forma análoga, definieron los números cuadrados, números pentágonos, números hexágonos, etc.

***Tomado de:*** *http://catedu.es/matematicas_mundo/HISTORIA/2_Teoria_Numeros.pdf*




Utilicemos estos hechos en nuestro contexto, si se tiene la norma de un número que sea de la forma $a^2 - b^2r^2$ por ejemplo, donde $a^2 \geq b^2r^2$, en esta representación se vería:




(Sorándo,s.f)

*Recuperado de:* http://catedu.es/matematicas_mundo/HISTORIA/2_Teoria_Numeros.pdf.

La suma $n^2 = 1 + 3 + 5 \ldots + (2n - 1)$, en nuestro caso $b^2r^2$ se representa como la menor suma de impares consecutivos, corresponde a $(br)^2 = 1 + 3 + 5 \ldots + (2|br| - 1)$ y $a^2$

representa la mayor corresponde a $a^2 = 1 + 3 + 5 \ldots + (2|a| - 1)$, la diferencia $a^2 - b^2r^2$ será la suma de impares consecutivos a partir de $2|br| - 1 \ + 2 = 2|br| + 1$ hasta $2|a| - 1$; de manera análoga si $a^2 \leq b^2r^2$, la diferencia $b^2r^2 - a^2$ corresponde a la suma de impares consecutivos desde $2|a| + 1$ hasta $2|br| - 1$:

$$a^2 - b^2r^2 = \sum_{k=|b|+1}^{k=|a|} 2k - 1$$

$$b^2r^2 - a^2 = \sum_{k=|a|+1}^{k=|b|} 2k - 1$$

Obtenemos así, una manera de descomponer la norma de un numero en términos de la suma de impares consecutivos.

Por ejemplo en $M(1)$, para $\| \ \ 3, -5 \ \ \|$, usamos la segunda forma pues $(-5)^2 * 1^2 \geq 3^2$: :

$$(-5)^2 = \sum_{k=1}^{k=5} 2k - 1 = 1 + 3 + 5 + 7 + 9$$

$$3^2 = \sum_{k=1}^{k=3} 2k - 1 = 1 + 3 + 5$$

$$5^2 - 4^2 * 1^2 = \sum_{k=3+1}^{k=5} 2k - 1 = 2\ 4\ \ - 1 + 2\ 5\ \ - 1 = 7 + 9 = 16$$

Los términos que están en la norma como suma de impares consecutivos serán la diferencia simétrica entre los conjuntos de números de la suma de impares que corresponde a $a^2$ y $(br)^2$, esto significa quitar los sumandos impares que tienen en común:

| $a^2$ | 1 | 3 | 5 | 7 | 9 |
|---|---|---|---|---|---|
| $(br)^2$ | 1 | 3 | 5 | | |
| $\lvert a^2 - (br)^2 \rvert$ | X | X | X | 7 | 9 |

Por otra parte, contando con poder representar la norma de esta manera, pensando de manera inversa si en $M(r^2)$, sabemos que $\| \ a,b \ \| = 16$, podemos encontrar todos los posibles valores de $a$, $b$ y $r^2$ para los cuales se cumple esta condición o en otras palabras podemos dada la norma 16 conocer todas las posibilidades de números $a,b$ en todo conjunto $M(r^2)$ que tienen norma 16 usando la descomposición por sumas de impares consecutivos.

Para empezar debemos pensar que el 16 siendo la diferencia de dos cuadrados, es la diferencia entre dos listas de sumas de impares consecutivos y por ello, a su vez es suma de impares consecutivos, cuando lo queremos expresar como norma esto necesariamente se cumple, el método radica en encontrar sumas de impares consecutivos que den como resultado 16, estas serían:

$$1 + 3 + 5 + 7 = 16, 7 + 9 = 16$$

Con esto, se pueden encontrar los cuadrados correspondientes a $a^2, b^2r^2$, consideremos por ejemplo $a^2 \leq b^2r^2$, se tendrá que $16 = b^2r^2 - a^2$,como el numero 16 es una norma, existen dos cuadrados tales que el mayor se resta del menor para obtenerla, si representamos estos cuadrados como suma de impares:

$$(br)^2 = 1 + 3 + 5 \ldots + (2|br| - 1)$$

$$a^2 = 1 + 3 + 5 \ldots + (2|a| - 1)$$

Tomemos una de las cadenas encontradas, por ejemplo para $7 + 9$ , los impares anteriores a 7 deben corresponder a términos de la cadena que configuran al cuadrado menor, en este caso:

$$a^2 = 1 + 3 + 5$$

Y la cadena completa corresponde al cuadrado mayor, esto es la hallada en el menor unida a la norma, en lenguaje algebraico $16 + a^2 = b^2r^2$:

$$(br)^2 = 1 + 3 + 5 + 7 + 9$$

Y encontramos el par, $a^2 = 9, (br)^2 = 25$, considerando $a^2 \geq b^2 r^2$ análogamente se encuentra $a^2 = 25, (br)^2 = 9$, siguiendo el mismo análisis para $1 + 3 + 5 + 7$, teniendo en cuenta que como la sucesión de impares consecutivos está completa , significa que no se quitó alguna suma de impares, es decir el cuadrado menor es nulo, se encuentran los pares de soluciones $a^2 = 0, (br)^2 = 16$ y $a^2 = 16, (br)^2 = 0$, con estos pares podemos dar todos los posibles números:

| Par encontrado | $a$ | $b$ | Conjunto $r^2$ | $(a, b)$ posibles con norma 16 |
|---|---|---|---|---|
| $a^2 = 9$<br>$(br)^2 = 25$ | $\pm 3$ | $\pm 5$<br>$\pm 1$ | 1<br>5 | $3,5\ ,\ -3,5\ ,\ 3,-5\ ,\ -3,-5$<br>$3,1\ ,\ -3,1\ ,\ 3,-1\ ,(-3,-1)$ |
| $a^2 = 25$<br>$(br)^2 = 9$ | $\pm 5$ | $\pm 3$<br>$\pm 1$ | 1<br>3 | $5,3\ ,\ -5,3\ ,\ 5,-3\ ,\ -5,-3$<br>$5,1\ ,\ -5,1\ ,\ 5,-1\ ,\ -5,-1$ |
| $a^2 = 0$<br>$(br)^2 = 16$ | 0 | $\pm 1$<br>$\pm 2$<br>$\pm 4$ | 16<br>4<br>1 | $0,1\ ,\ 0,-1$<br>$0,2\ ,\ 0,-2$<br>$0,4\ ,\ 0,-4$ |
| $a^2 = 16$<br>$(br)^2 = 0$ | $\pm 4$ | Cualquier valor<br>0 | 0<br>Todo conjunto | $4, n\ , \forall n \in \mathbb{Z}$<br>$4,0$ en todo $M(r^2)$ |

No tiene sentido buscar diferencias de cuadrados mayores a 25 que den 9, más adelante se explicita porque, así los números encontrados son todos los de norma 16 posibles en $M(r^2)$.

En general, si la norma de un número es $n$, podemos encontrar los posibles valores de $a$ y $b$ para los cuales se dan las dos diferencias, con una tabla como la siguiente, para los primeros 30 números cuadrados, se facilita el trabajo:

| D | 1 | 3 | | 5 | | 7 | | 9 | | 11 | | 13 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|

| | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| C | 1 | | 4 | | 9 | | 16 | | 25 | | 36 | |
| D | | 15 | | 17 | | 19 | | 21 | | 23 | | 25 |
| C | 49 | | 64 | | 81 | | 100 | | 121 | | 144 | |
| D | | 27 | | 29 | | 31 | | 33 | | 35 | | 37 |
| C | 169 | | 196 | | 225 | | 256 | | 289 | | 324 | |
| D | | 39 | | 41 | | 43 | | 45 | | 47 | | 49 |
| C | 361 | | 400 | | 441 | | 484 | | 529 | | 576 | |
| D | | 51 | | 53 | | 55 | | 59 | | 60 | | 61… |
| C | 625 | | 676 | | 729 | | 784 | | 841 | | 900 | |

Las filas con nombre D, contienen las distancias entre cada para de números cuadrados y las filas con nombre C, los números cuadrados.

Podemos a partir de esta tabla, concretar las estrategias para hallar pares de números cuadrados que puedan ser escritos como normas $b^2r^2 - a^2,\ a^2 - b^2r^2$, por ejemplo nótese que la diferencia entre dos cuadrados es cada vez mayor, por lo cual si se quiere expresar el número 9 por ejemplo, como diferencia de cuadrados, solo tiene sentido buscar distancias entre cuadrados que no excedan al cuadrado que es su término siguiente como diferencia, que es 25.

La estrategia consiste en buscar posibles descomposiciones de $n$ como suma de impares consecutivos y a partir de ellas buscar los cuadrados que correspondan, el primero anterior al primer impar y el segundo siguiente al último impar. Probemos un segundo ejemplo ahora para 9:

$9 = 9$, teniendo en cuenta que la descomposición como "suma de sí mismo" sirve en este caso, obteniendo el par 16, 25.

$9 = 1 + 3 + 5$, obteniendo el par 0, 9.

No habiendo más casos los posibles números con norma 9 deben poder construirse a partir de estos dos pares, para todos los conjuntos de $M\ i^2$ .La elección de los valores de

$a^2, b^2r^2$, los posibles valores de $(a, b)$ con norma 9, salvo asociados, y los valores de $M\ i^2$ serán:

| $a^2$ | $b^2r^2$ | $(a, b)$ en $M\ i^2$ |
|---|---|---|
| 0 | 9 | $0{,}3\ , M\ 1$<br>$0{,}1\ , M\ 9$ |
| 9 | 0 | $3{,}0\ , M\ i^2\ , \forall r^2 = i^2$ |
| 16 | 25 | $4{,}5\ , M\ 1$<br>$4{,}1\ , M\ 25$ |
| 25 | 16 | $5{,}4\ , M\ 1$<br>$5{,}1\ , M\ 16$ |

Algunas observaciones importantes son que:

En $M\ 1$ , obtuvimos dos pares de números no asociados $3{,}0\ ,\ 0{,}3\ ,\ 5{,}4\ , (4{,}5)$ que tienen la misma norma, 9.

Encontramos un solo número que tiene norma 9 globalmente $(3{,}0)$, este será el único número con norma 9 en $M(4)$ y para $i^2 > 25$, los cuales son muchos conjuntos.

Con este proceso, y con la ayuda de la tecnología para ahorrar el uso de las tablas, podemos determinar todos los posibles números de una norma $n$ y sabríamos si para una norma determinada no existen números $(a, b)$ con esa norma y en que conjuntos no existen ¿puede eso llegar a ocurrir?.

En el ejemplo anterior obtuvimos un número con norma 9 para todo conjunto, pero aun cabe la duda ¿hay números para todas las normas?, notemos por ejemplo que en la tabla, no hay distancias entre dos cuadrados equivalentes a 2 o a 6,10, 26 y no se pueden sumar impares consecutivos que den estos números, ¿Cuál es la razón de esto?.

Un número $n$ impar siempre puede ser escrito como suma de 1 impar consecutivo, el mismo, por esto siempre existirá al menos un número con norma $n$ en general, aunque este no pertenezca a todos los conjuntos.

Un número $n$ par, no puede ser escrito como suma de 1 impar consecutivo, se necesitan al menos 2, de hecho toda suma de $2k$ impares es par y análogamente toda suma de $2k+1$ impares es impar, por esto para escribir un numero par en términos de suma de impares consecutivos se necesitaran 2, 4 , 6 , 8…. impares.

Si suponemos una norma $n$ par que puede ser escrita en términos de la suma del mínimo de impares consecutivos, 2, significaría $n = \ 2l+1 \ + \ 2l+3 \ = 4l+4 = 4(l+1)$, seria un múltiplo de 4; si pudiese ser escrito en términos de 4 impares sumariamos dos múltiplos de 4, seguiría siendo $n$ un múltiplo de 4; lo anterior quiere decir que *todo n par que puede ser escrito en términos de impares consecutivos es múltiplo de 4,* lo cual implica que no hay ningún $n$ par con esta condición que solo sea múltiplo de 2, puesto que tiene que serlo también de 4, es decir que no habrá diferencias de cuadrados que correspondan a múltiplos de 2 por un impar, en nuestro contexto significa que no se pueden encontrar, no existen, números con norma 2, 6, 10, 14… $2l$ con $l$ impar, esto se resume en el teorema:

**Teorema 22:**

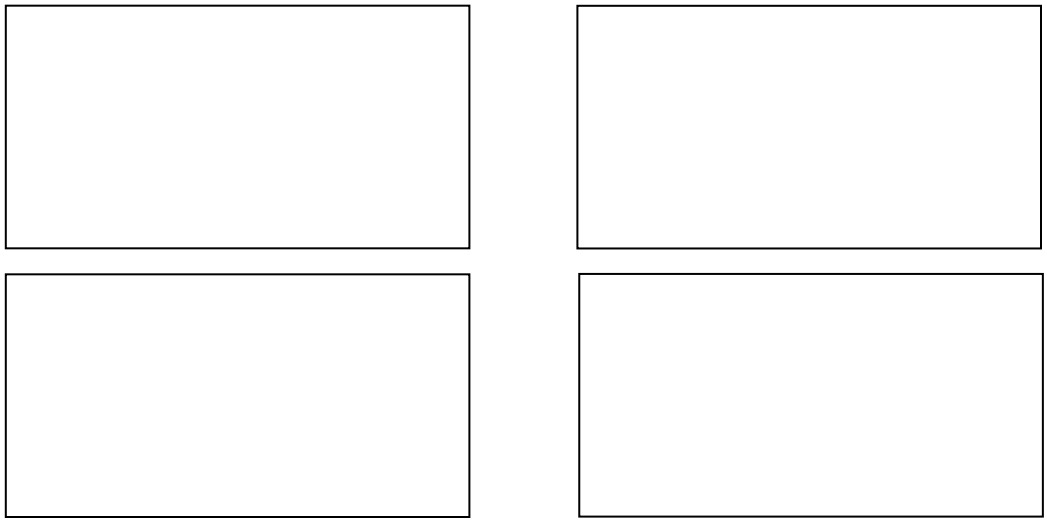
$\forall \ a,b \ \in M \ i^2 : \| \ a,b \ \| \neq 2l, l$ impar.

Del anterior teorema se puede usar para comenzar a descartar posibles descomposiciones, retomando la propiedad 4 del teorema 12, antes sabíamos por ejemplo que para encontrar divisores de un número con norma 20 las opciones eran buscar números que tuviesen normas 1 y 20, 2 y 10 o 4 y 5, como sabemos que el primer par corresponde a las unidades y asociados del número, se descarta estos ya son conocidos, el segundo caso como no hay números con norma 10 también se descarta, los nuevos divisores por encontrar son de norma 4 y 5, hemos logrado disminuir bastante el trabajo de buscar divisores.

Del anterior teorema es casi inmediato afirmar que los números de norma 4 son primos, pues no existen números de norma 2, y si buscamos en la tabla de cuadrados, las únicas opciones son 4 y 0, para un número de norma 4, es decir solo existe uno salvo asociados y además existe en todos los conjuntos, es $(2,0)$, tambien existe $(0,2)$ pero es válido solo para los números de Minkowski e incluso allí es asociado a $(2,0)$; siendo $2,0$ el único

número de norma 4 salvo sus asociados, el único $(p, 0)$ primo en todo conjunto y además permite escribir la descomposición de sus múltiplos fácilmente usando el producto por escalar, este número es quizás el más ideal que vamos a encontrar.

Para llegar al teorema 22 utilizamos que $2l + 1 + 2l + 3 = 4(l + 1)$, este hecho es útil, no hemos profundizado en que no solo esta igualdad comprueba que todo número que es suma de dos impares es múltiplo de 4, otra forma de verla es pensar en que esta es una descomposición de todo múltiplo de 4 como suma de impares consecutivos, se puede usar esto para hallar tales impares dando el múltiplo de 4 que corresponde a la norma, además que esta descomposición resulta ser una sola:



Intentemos extender el proceso para tener una herramienta más para encontrar las diferencias entre los cuadrados que correspondan a la norma que necesitemos, ya conocemos los números que pueden ser escritos como suma de 1 impar y de 2 impares, pero ¿Qué números se podrán escribir como suma de $k$ impares?, ya hemos analizado anteriormente que al sumar un número par de impares da como resultado un par y al sumar un numero impar de impares obtenemos un impar, tomando los dos casos se pueden generar las listas:

*Números pares que pueden ser escritos como suma de impares consecutivos:*

$2a+1 \ + \ 2a+3 \ = 4(a+1)$, múltiplos de 4 como suma de 2 impares

$2a+1 \ + \ 2a+3 \ + \ 2a+5 \ + \ 2a+7 \ = 8 \ a+2$ , múltiplos de 8 como suma de 4 impares

$2a+1 \ + \cdots + (2a+11) = 12(a+3)$, múltiplos de 12 como suma de 6 impares

$2a+1 \ + \cdots + (2a+15) = 16(a+4)$, múltiplos de 16 como suma de 8 impares

Y en general

$2a+1 \ + \cdots + (2a+(4k-1)) = 4k(a+k)$, múltiplos de $4k$ como suma de $2k$ impares.

*Números impares que pueden ser escritos como suma de impares consecutivos:*

$2a+1 \ = 2(a+1)$, todos los impares como suma de 1 impar

$2a+1 \ + \ 2a+3 \ + \ 2a+5 \ = 3 \ 2a+3$ , múltiplos de 3 como suma de 3 impares

$2a+1 \ + \cdots + (2a+9) = 5(2a+5)$, múltiplos de 5 como suma de 5 impares

$2a+1 \ + \cdots + (2a+13) = 7(2a+7)$, múltiplos de 7 como suma de 7 impares

Y en general

$2a+1 \ + \cdots + (2a+(4k+1)) = (2k+1)(2a+(2k+1))$, múltiplos de $2k+1$ como suma de $2k+1$ impares.

Por supuesto hay normas que pueden ser escritas de más de una manera, la descomposición en términos de suma de impares consecutivos no es única. Hay que tener en cuenta que las normas son números enteros positivos, $0 < a$, por esto por ejemplo los números 12 y 24 no tienen representación como suma de 6 impares ya que la igualdad $2a+1 \ + \cdots + (2a+11) = 12(a+3)$, cobra sentido a partir del número 36, y esta además es su única representación, en general el primero grupo de proposiciones solo cobra sentido a partir del

primer valor $a = 0$, es decir desde $4k^2$; otros números como 32, tienen representación como suma de 8,4 números impares como se muestra a continuación:

| Representación en suma de $2k$ impares, múltiplos de $a$ cobran sentido a partir de $b = 4k^2$ | | | | | | | |
|---|---|---|---|---|---|---|---|
| $a$ | 4 | 8 | 12 | 16 | 20 | 24 | 28 |
| $b$ | 4 | 16 | 36 | 64 | 100 | 144 | 196 |
| $k^2$ | 1 | 4 | 9 | 16 | 25 | 36 | 49 |
| $k$ | 2 | 4 | 6 | 8 | 10 | 12 | 14 |

| Numero par/número de descomposiciones como suma de impares que tiene | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| 2/0 | 4/1 | 6/0 | 8/1 | 10/0 | 12/1 | 14/0 | 16/2 | 18/0 | 20/1 |
| 22/0 | 24/2 | 26/0 | 28/1 | 30/0 | 32/2 | 34/0 | 36/2 | 38/0 | 40/2 |
| 42/0 | 44/1 | 46/0 | 48/3 | 50/0 | 52/1 | 54/0 | 56/2 | 58/0 | 60/2 |
| 62/0 | 64/3 | 66/0 | 68/1 | 70/0 | 72/3 | 74/0 | 76/1 | 78/0 | 80/3 |
| 82/0 | 84/2 | 86/0 | 88/2 | 90/0 | 92/1 | 94/0 | 96/4 | 98/0 | 100/2 |

De manera similar, hay números impares que tienen más de una representación como suma de impares consecutivos:

| Representación en suma de $2k + 1$ impares, múltiplos de $a = 2k + 1$ cobran sentido a partir de $b = (2k + 1)^2$ | | | | | | | |
|---|---|---|---|---|---|---|---|
| $a$ | 1 | 3 | 5 | 7 | 9 | 11 | 13 |
| $b$ | 1 | 9 | 25 | 49 | 81 | 121 | 139 |

| Número impar/número de descomposiciones como suma de impares que tiene | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| 1/1 | 3/1 | 5/1 | 7/1 | 9/2 | 11/1 | 13/1 | 15/2 | 17/1 | 21/2 |

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| 23/1 | 25/2 | 27/2 | 29/1 | 31/1 | 33/2 | 35/2 | 37/1 | 39/2 | 41/1 |
| 43/1 | 45/3 | 47/1 | 49/2 | 51/2 | 53/1 | 55/2 | 57/2 | 59/1 | 61/1 |
| 63/3 | 65/2 | 67/1 | 69/2 | 71/1 | 73/1 | 75/3 | 77/2 | 79/1 | 81/2 |
| 83/1 | 85/2 | 87/2 | 89/1 | 91/2 | 93/2 | 95/2 | 97/1 | 99/3 | 101/1 |

Un hecho curioso que surge de las listas anteriores es que si estudiáramos la descomposición por suma de consecutivos impares, los números que solo tienen una descomposición podrían ser definidos como primos y los números primos en los enteros también tienen solo una descomposición como suma de 1 impar, los números que son pares y solo tienen una descomposición son los de la forma $4l, l$ impar, sin embargo surgirían aquí números que no pueden ser descompuestos, lo que haría surgir la necesidad de una definición de divisibilidad, unidades, asociados diferente que abarque estos casos.

Otro hecho que se quiere resaltar de las listas es que hay números como 8, que solo tienen una representación posible, $8 = 3 + 5$, cuyos cuadrados correspondientes 1,9 se asocian a $1{,}1 \ \ en\, M\ \ 9\ ,\ \ 9{,}1\ ,(1{,}9)\ en\, M(1)$, y y aunque tienen norma 8, ninguno de ellos es divisible por $(2{,}0)$, esto es un contraejemplo a un reciproco para la propiedad 4 de T12, es decir que $\| \ \ a, b \ \ \| \mid \| \ \ c, d \ \ \|$ no implica que $a, b \mid c, d$ , entonces, lo que nos abre camino a la siguiente pregunta que debemos responder, en esta sección hemos desglosado un método para hallar números $(x, y)$ de una determinada norma $d$, ya que buscábamos divisores de un $(a, b)$ cuya norma corresponde a $dm$, pero al encontrar tales números siguiendo las diferencias de cuadrados ¿Cómo podemos saber si $(x, y)$ es o no divisor de $(a, b)$?.

### 4.4.2 El algoritmo de la división

Cuando aprendemos a relacionar los números con el proceso de repartir es inevitable pasar por el algoritmo de la división, el cual está respaldado por varias propiedades importantes de los números racionales, si quisiéramos saber si $n$ puede ser repartido en $k$ partes iguales en $\mathbb{N}$ este sería el primer lugar al que acudiríamos, este problema más adelante se generaliza perdiendo el contexto real y ganando validez en las matemáticas formales, el método se

transforma en la herramienta básica para saber si $k$ divide a $n$, un punto en común con la pregunta que tenemos.

El algoritmo de la división euclidea en los números naturales nos permite afirmar que todo número $n$, a partir de uno menor que el $k \neq 0$, puede ser escrito como $n = kd + r$, donde $d$ es el máximo número natural que cumple $kd \leq n, r < k$, cuando $r = 0$, tenemos que $k|n$, además la pareja $(d, r)$ es única; la versión en los números enteros es muy similar, afirma que dados un par de números enteros $n, k, k \neq 0$ siempre se puede expresar el primero como $n = kd + r$, con $0 \leq r < k$ . Las dos definiciones son muy similares, notemos que ambas necesitan de que varios elementos específicos estén bien definidos para funcionar como una norma, una relación de orden total entre los elementos del conjunto y una relación de orden para la norma con los elementos del conjunto, y un elemento que permita afirmar que $(d, r)$ es única, en este caso, que la propiedad cancelativa se cumpla.

Otro camino para definir un algoritmo de la división es usando la propiedad del inverso multiplicativo en los campos, tomando $r$ siempre como 0 y $d = n * k^{-1}$, se tendrá $n = k * n * k^{-1} + 0$, donde la pareja $(n * k^{-1}, 0)$ es siempre única, esto necesita que en el conjunto se tengan inversos multiplicativos.

Nuestros conjuntos $M(i^2)$ carecen de varios de los elementos necesarios para definir un algoritmo de la división que se comporte de la misma manera que las anteriores, sin embargo varios de los elementos de los que disponemos tienen propiedades que pueden suplir las que faltan, como se hace en los enteros gaussianos, haremos un algoritmo de la división que toma algo similar a cada definición dada, para ello necesitaremos:

**Definición 15:**

$\forall\ a, b\ \in\ M\ i^2\ \forall x \in\ \mathbb{Z}$, Se define la división por escalar $/ : \mathbb{Z} * M(i^2) \rightarrow M(i^2)$ como

$\frac{(a,b)}{x(1,0)} = \frac{(a,b)}{x}$, $\frac{a,b}{x} = \frac{a}{x}, \frac{b}{x}\ si\ x\ a \wedge x\ b, \frac{a,b}{x} = (\frac{a-r_1}{x}, \frac{b-r_2}{x})$ si $x \nmid a \vee x \nmid b$, siendo $r_1, r_2$, los residuos de aplicar el algoritmo de la división en $\mathbb{Z}$ a $a, b$ dividendos respectivamente con $x$ como divisor.

Con esta nueva definición, las propiedades de los conjugados, las propiedades de la norma y de la divisibilidad ya podemos proceder a plantear un método para dividir análogo al de los ejemplos, sin embargo el siguiente teorema nos da un poco más de autoridad para relacionar el producto por escalar usado en $\mathbb{Z}$ junto a $M(i^2)$, teniendo en cuenta que estamos usando el hecho de que $a^2 - b^2 i^2 = (a + bi)(a - bi)$ y que este número puede ser tratado tanto como entero como número en $M(i^2)$ y esta es una clave para el algoritmo, así se plantea:

**Teorema 23(μ):** Toda estructura $M(i^2)$ tiene un subconjunto isomorfo a $\mathbb{Z}$.

Tal conjunto es $A = \{ x, y \in M\ i^2 : y = 0\}$ con las operaciones dadas por $M\ i^2$ .

**Demostración**

Tomando la representación $a + 0i$, resulta evidente que la función $f: A \to \mathbb{Z}, f\ a + 0i = a$, es biyectiva, siendo el núcleo de esta el neutro de $A$, falta demostrar que las operaciones se conservan:

a) Isomorfismo de sumas: $f\ \ a + 0i + b + 0i\ \ = f\ \ a + b + 0i\ \ = a + b$, por la definición de + y de la función, y de nuevo por la definición de la función $a + b = f\ a + 0i + f(b + 0i)$, por ultimo por propiedad transitiva de la igualdad $f\ \ a + 0i + b + 0i\ \ = f\ a + 0i + f(b + 0i)$.
b) Isomorfismo de multiplicaciones: $f\ \ a + 0i\ \ b + 0i\ \ = f\ ab + 0i$ por la definición de multiplicación y por la definición de la función $f\ ab + 0i = ab$, de nuevo por la definición de la función $ab = f\ a + 0i\ f\ b + 0i$ y por propiedad transitiva de la igualdad $f\ a + 0i\ f\ b + 0i\ = f\ \ a + 0i\ \ b + 0i$

Como observación, se podría pensar que existe un segundo subconjunto de $M(r^2)$ isomorfo a $\mathbb{Z}$ análogo al presentado, $B = \{ x, y \in M\ r^2 : x = 0\}$, sin embargo en este conjunto la operación * no está bien definida ya que el producto de dos de sus elementos no siempre es elemento del conjunto, por ejemplo $0, a\ \ 0, a\ = (a^2 r^2, 0)$, con $a \neq 0, r^2 \neq 0$.

**Definición 16:**

$\forall\ a,b\quad c,d\ \in\ M\ i^2\ ,\|\quad c,d\quad \|\neq 0$, Se define la división $/: M(i^2) * M(i^2) \to M(i^2)$ como

$$\frac{(a,b)}{(c,d)} = \frac{(a,b)(c,d)}{(c,d)(c,d)}$$

Si $(a,b)\ |(c,d)$ diremos que la división es exacta.

Pensemos en los números de Minkowski $3{,}4\quad 2,-1\ = (2{,}5)$ con normas 7,3 y 21 respectivamente, para comprobar el funcionamiento del método para dividir articulando las dos últimas definiciones, demostremos que $3{,}4$ es divisor de $(2{,}5)$ a través de $2,-1$ :

$\frac{(2,5)}{(3,4)} = \frac{(2,5)(3,4)}{(3,4)(3,4)}$, por D16

$\frac{(2,5)}{(3,4)} = \frac{(2,5)(3,4)}{(-7,0)} = \frac{(2,5)(3,4)}{-7(1,0)} = \frac{(2,5)(3,4)}{-7}$, por la propiedad 6 de T7, D5 y D15

$\frac{(2,5)}{(3,4)} = \ -\frac{14}{-7}, \frac{7}{-7}\ = (2,-1)$, por D15

Ahora intentemos seguir el proceso para una división no exacta, también en los números de Minkowski $(2{,}0)$ de norma 4 no es un divisor de $(3{,}1)$ de norma 8 pues no existe ningún número de norma 2, aun así, si aplicamos el algoritmo de la división:

$$\frac{(3,1)}{(2,0)} = \frac{(3,1)(2,0)}{(2,0)(2,0)}$$

$$\frac{(3,1)}{(2,0)} = \frac{(6,2)}{4}$$

$\frac{(3,1)}{(2,0)} = \ \frac{6-2}{4}, \frac{2-2}{4}\ = (1{,}0)$, pues $6 = 4\ 1\ + 2, 2 = 4\ 0\ + 2$

$1{,}0\quad 2{,}0\ = (2{,}0)$ el residuo es $(1{,}1)$ de norma 0

Esta división aunque es inexacta nos permite encontrar un par de números que permiten escribir a $3{,}1 = 2{,}0\ 1{,}0 + (1{,}1)$, con la condición $\| 1{,}1 \| < \| 2{,}0 \|$, además este par es único pues al aplicar el algoritmo de la división en $\mathbb{Z}$ los resultados $6 = 4\ 1 + 2, 2 = 4\ 0 + 2$, también lo son.

El algoritmo de la división nos permite saber si la ecuación $a, b\ x, y = (c, d)$ tiene solución con $a, b$ , $(c, d)$ conocidos, haciendo el proceso de dividir, sin embargo como se vio en el ejemplo anterior, no es suficiente hallar una descomposición $a, b\ x, y + (r, r_1) = (c, d)$, tal que $(r, r_1) = 0$ para poder concluir que $a, b\ x, y = (c, d)$ , a diferencia de en los números enteros y naturales en donde si $bq + r = a$, con $r = 0$, se puede concluir que $bq = a$, ya que esta propiedad se pierde en nuestros conjuntos, puesto que tenemos divisores de 0, surgen problemas para demostrar varias otras que dependían de este resultado, como un primer ejemplo, la unicidad de la descomposición dada por el algoritmo de la división.

Tal como está definido el algoritmo de la división nos permite encontrar un par de números que cumplen $a, b\ p, q + (r, r_1) = (c, d)$, sin embargo no podemos asegurar que este par sea único. Es claro que al aplicar la división $\frac{c,d}{(a,b)}$ se obtiene solo un par, pero no hacen falta condiciones para declarar el par obtenido por el algoritmo de la división como la única división.

Por ejemplo en $\mathbb{Z}$, al hacer la división $\frac{7}{3}$ se obtiene $7 = 3 * 2 + 1$ tal que $1 < 3$, pero también existe $7 = 3 * 3 - 2$ tal que $-2 < 3$, para solventar esto, se pone condición que $r$ sea entero positivo por lo cual nace la necesidad también aquí de definir ¿Qué es un entero positivo en $M(i^2)$? , para esto nos hace falta una relación de orden que haga distinción entre los números positivos y los demás del conjunto.

### 4.5 Relaciones de orden en $M(i^2)$

Como referentes de relaciones de orden tenemos $<$ tanto en los números naturales como en los números enteros, sin embargo se podría decir que la de los números enteros es más completa puesto que subconjunto $\mathbb{Z}^+$ con $\leq$ es otra representación del orden en los

números naturales, si pensamos en la definición conjuntista de relación de orden, la de los números naturales es un subconjunto de la de los números enteros.

Recordemos que en los números naturales no existen inversos aditivos es decir $a \neq 0, \nexists n \in \mathbb{N}: a + n = 0$, esto implica que no todas las ecuaciones $a + x = b$ para $a, b$ conocidos tengan solución, este hecho es la herramienta que se usa para definir la relación $\leq$ en $\mathbb{N}$ como sigue:

$$a \leq b \leftrightarrow \exists n \in \mathbb{N}: a + n = b, a < b \text{ si } a \leq b \wedge b \neq 0$$

Esta forma de definir es muy similar a la que utilizamos con $|$, no obstante en los conjuntos $M(i^2)$ si existen inversos aditivos lo que implica que todas las ecuaciones de la forma $(a, b) + (x, y) = (c, b)$, con $a, b\ , (c, b)$ conocidos tienen solución única $x, y = c, b\ - (a, b)$, por esto si definimos la relación de orden como:

$$(a, b) \preccurlyeq (c, d) \leftrightarrow \exists (n, m) \in \mathbb{N}: (a, b) + (n, m) = (c, d), (a, b) \prec (c, d) \text{ si } (a, b) \preccurlyeq (c, d) \wedge (c, d) \neq 0$$

Resulta que $\forall\ a, b\ , (c, d) \in M(i^2)$, $(a, b) \preccurlyeq (c, d) \wedge (c, d) \preccurlyeq (a, b)$, lo cual hace que la relación fuese además de reflexiva y transitiva, simétrica por lo cual $\preccurlyeq$ es de equivalencia y además todos los números $M(i^2)$ resultarían equivalentes entre sí.

La segunda opción es intentar hacer una relación análoga a la de los números enteros y en los gaussianos duales (Brausín & Pérez, 2012):

$$\forall \in \mathbb{Z}: a \leq b \leftrightarrow b - a \in P, P \text{ el conjunto de enteros positivos}$$

Esta definición necesita de que definamos un conjunto de números $M(i^2)$ positivos, tal conjunto $P$ en los enteros cumple las siguientes condiciones para obtener una relación de orden total:

i. $a \in P \rightarrow -a \notin P\ \underline{V}\ a = 0$
ii. $a, b \in P \rightarrow a + b \in P$
iii. $a, b \in P \rightarrow a * b \in P$

**Definición 17(μ):**

Un conjunto de números $M\ i^2\ -$positivos denotados por $M\ i^2\ -P$ debe cumplir:

i. $(a,b) \in P \rightarrow (-a,-b) \notin P$

ii. $a,b\ ,\ c,d\ \in P \rightarrow\ a,b\ +(c,d) \in P$

iii. $a,b\ ,\ c,d\ \in P \rightarrow\ a,b\ *\ c,d\ \in P$

Para comprender mejor y declarar las condiciones para que la relación de orden sea total conviene resaltar la algunas propiedades de $(M\ i^2\ ,+)$ que aún no habíamos enunciado:

**Teorema 24(μ):** $\forall\ a,b\ \in M\ i^2\ :(a,b) \neq (0,0) \rightarrow (a,b) \neq (-a,-b)$

**Demostración:**

Suponiendo lo contario $a,b\ \neq\ 0,0\ \rightarrow\ a,b\ =\ -a,-b$ ,por lo que por D2, $a = -a \wedge b = -b$, pero ya que $a,b\ \in\ \mathbb{Z}$, se concluye que $a = 0 \wedge b = 0$.

**Teorema 25:** $\forall\ a,b\ \in D_0, \forall\ c,d\ \in M\ i^2\ :\ a,b\ *(c,d) \in D_0$

Demostración:

En el T4 caracterizamos el conjunto $D_0$:

$$D_0 = \{\ a,b\ \in M\ i^2\ :\ \text{a,b}\ =\ \pm xr,x\ ,\forall\ x \in\ \mathbb{Z}\}$$

Para algunos $xr,x\ ,(a,b)$ fijos pero arbitrarios, la demostración para $-xr,x$ resulta análoga:

$$xr,x\ *\ a,b\ = x(\ r,1\ \ a,b\ ),\text{ por D5 y T2}$$

$$x\ \ r,1\ \ a,b\ \ = x((ra+br^2,br+a)),\text{por D4}$$

$$x\ \ ra+br^2,br+a\ \ = x((r(a+br),br+a)),\text{ por la propiedad distributiva de la multiplicación respecto a la suma en } \mathbb{Z}$$

$$x\ \ r\ a+br\ ,br+a\ \ = x\ a+br\ *(r,1)),\text{ por D5}$$

Como $x,\ a+br$ son enteros, $x\ a+br = y, y \in \mathbb{Z}$, luego sustituyendo en la ecuación anterior:

$$x\ a+br\ *(r,1)) = y(r,1) = (yr,y), \text{ por D5}$$

$$(yr,y) \in D_0, \text{ por T4}$$

Para definir una relación $\preccurlyeq$ de orden total, es claro que $(0,0)$ no sea positivo es una propiedad que buscamos que se cumpla la tricotomía, en particular se quiere que $(a,b) \in P \rightarrow (-a,-b) \notin P$, pero $0,0 = -(0,0)$ ya que es elemento neutro, por lo cual se deduciría que $(0,0) \in P \wedge (-0,-0) \notin P$, por lo cual la relación no sería de orden total.

Si un par de divisores de $0,0$ , $ar,a$ , $(-br,b)$ son positivos, como buscamos que se cumpla $ar,a\ (-br,b) \in P$ eso significaría $(0,0) \in P$, y volveríamos al caso anterior, por lo cual este caso también lo debemos evitar, para ello decidiremos que los números positivos tendrán primera componente positiva y con esto también aseguramos la primera propiedad, suma de positivos es positiva.

Si analizamos las posibilidades de las segundas componentes, para $a,b$ , $c,-d \in P \rightarrow a,b * c,-d = (ac-bdr^2, bc-ad)$, como buscamos que $ac-bdr^2 > 0$, la solución que se tiene es definir que en los positivos también se cumple $a > bk$ , lo que equivale a establecer $a^2 > b^2r^2$ o $a^2 - b^2r^2 > 0$, el lector ya habrá advertido que esta cantidad es el valor de la norma de $a,b$ , por esto tenemos que descartar que todo divisor de 0 sea positivo.

Si $a,b \neq 0,0$ , $a,b \in D_0$ no puede ser positivo, entonces como queremos que se cumpla la propiedad de tricotomía $-a,-b = (-1,0)(a,b)$ debe ser positivo, pero por T25 sabemos que $(-1,0)(a,b) \in D_0$ por lo cual no sería posible definir una relación de orden que cumpla la tricotomía usual, es decir que sea de orden total, pues no sería posible decidir si los divisores de 0 son positivos o no.

No obstante podemos ajustar la propiedad de tricotomía para que se pudiesen definir números positivos en los conjuntos $M\ i^2$ de la siguiente forma:

**Definición 18:**

Si $\forall\ a,b\ \in M\ i^2$ , con un conjunto de los números $M\ i^2\ - P$ se cumple una y solo una de las siguientes condiciones:

i. $(a,b) \in P$
ii. $(-a,-b) \in P$
iii. $(a,b) \in D_0$
iv. $P$ es un conjunto cerrado para + y *

Entonces diremos que el conjunto $M\ i^2$ está totalmente $i^2$ −ordenado.

Consideremos que si definimos un conjunto de enteros positivos siguiendo el análisis anterior:

$$P = \{(a,b) \in M\ i^2\ : (a > 0 \wedge a^2 - b^2r^2 > 0)\}$$

Dicho conjunto no puede cumplir las condiciones de D17 todas simultáneamente, pues $a > 0$, garantiza que se cumplan las condiciones 1,2 pero no concluye respecto a la 3, la condición $a^2 - b^2r^2 \wedge a > 0$ garantiza las condiciones 1,3 pero hace que no se pueda concluir respecto a la 2, pues $a^2 - b^2r^2 > 0, c^2 - d^2r^2 > 0$ no garantiza que $a,b\ + c,d\ = (a+c, b+d)$ cumpla la condición 3, $(a+c)^2 - \ b+d\ ^2r^2 > 0$, esto se debe al comportamiento que tiene la norma de un numero respecto a la suma:

**Teorema 26(μ):** $\forall\ a,b\ ,\ c,d\ \in M\ i^2$ :

$$a,b\ +\ c,d\ \ =\ \ a^2 -\ br^{\ 2}\ +\ c^2 -\ dr^{\ 2}\ + 2(ac - bdr^2)$$

Este teorema se obtiene directamente del desarrollo de $a,b\ +\ c,d$ , este comportamiento, es decir la existencia de ese factor adicional $2(ac - bdr^2)$ implica que la norma de una suma no es la suma de las normas de los resultados.

Este hecho no solo implica que no se pueda definir un conjunto de números positivos que se comporte bien con ambas operaciones, esto es que cumpla los dos últimos requisitos de D17 simultáneamente y además determine una relación de orden total, sino que afecta a

otros resultados como que no se cumpla la desigualdad triangular en $M\ i^2$ o que los cocientes y residuos obtenidos al aplicar el algoritmo de la división no sean únicos.

Con una relación orden definida a partir de los números positivos, si aceptamos la condición $a > 0$, se podrán demostrar resultados de $\geqslant$ que sean relativos a la suma, y no para el producto, en contraparte la condición $a^2 - b^2r^2 > 0$, contribuye a la demostración de propiedades de $\geqslant$ relativos al producto, pero no permite que la suma de dos positivos sea positiva, al estar este documento enfocado al estudio de la teoría de números principalmente con la multiplicación, se tomará la segunda opción. Sin embargo, Aceptando $a^2 - b^2r^2 > 0$ si no tenemos $a > 0$, no se puede asegurar que el conjunto de los números positivos cumpla la propiedad de tricotomía, pues:

$$P\ i^2\ = \{(a,b) \in M\ i^2\ : a^2 - b^2r^2 > 0\}$$

Sea $a,b\ \in M\ i^2$ :

$$(a,b)\ = 0 \rightarrow (a,b) \in D_{\mathbf{0}} \text{ por el corolario de T14}$$

$$a^2 - b^2r^2 > 0 \vee a^2 - b^2r^2 < 0, \text{ por la propiedad de tricotomía en } \mathbb{Z}$$

$$a^2 - b^2r^2 > 0 \rightarrow (a,b) \in\ P\ i^2 \text{ por la definición de } P\ i^2$$

$$a^2 - b^2r^2 < 0 \rightarrow (a,b) \notin\ P\ i^2 \text{ por la definición de } P\ i^2$$

$$a^2 - b^2r^2 < 0 \rightarrow\ -a\ ^2 -\ -b\ ^2r^2 < 0, \text{ ya que en } \mathbb{Z}, a^2 = -a^2$$

$$(-a,-b) \notin\ P\ i^2$$

Sin embargo, si intentamos podemos arreglar el fallo en esta condición tomando $a^2 - b^2r^2\ > 0$, pero como esto siempre se cumple, no tendría sentido definir un conjunto de números positivos. No obstante al tomar la norma $a^2 - b^2r^2$ para definir una relación de orden, como solo se tienen dos casos $a^2 - b^2r^2\ > 0 \vee\ a^2 - b^2r^2\ = 0$, se tendría una relación de orden más similar (de hecho heredada directamente y por tanto isomorfa en el conjunto cociente) a la que se tiene en $\mathbb{N}$, la definiremos como sigue:

**Definición 19(μ):**

$$\forall\ a,b\ ,\ c,d\ \in M\ i^2\ :\ a,b\ \leq\ c,d\ \leftrightarrow\quad a,b\quad \leq\quad c,d\quad ,$$

$$a,b\ <\ c,d\ \text{ significa }\quad a,b\quad <\quad c,d$$

A $a,b\ \geq\ c,d$ le daremos el significado $c,d\ \leq\ a,b$ .

**Teorema 27:**$\leq$ es una relación de pre orden en $M\ i^2$

Demostración:

i. $\leq$ es reflexiva:

$$a,b\quad \leq\ (c,d)\ \text{ , por la propiedad reflexiva de } \leq \text{ en } \mathbb{N}$$

$$a,b\ \leq\ a,b\ \text{ por D19}$$

ii. $\leq$ es transitiva:

$a,b\ \leq\ c,d\ \wedge\ c,d\ \leq (e,f) \rightarrow\quad a,b\quad \leq\quad c,d\quad \wedge\quad c,d\quad \leq\quad e,f\quad ,$ por la D19

$(\ a,b\quad \leq\quad c,d\quad \wedge\quad c,d\quad \leq\quad e,f\quad ) \rightarrow\quad a,b\quad \leq\quad e,f\quad$ por la propiedad transitiva de $\leq$ en $\mathbb{N}$

$$a,b\ \leq (e,f), \text{ por la D19}$$

La relación que definimos no es simétrica ya que existen números con la misma norma que no son iguales, como hemos visto anteriormente por ejemplo $(a,b)$ y $(-a,-b)$ o $(a,b)$ y $(a,b)$ o $(a,b)$ y $(a,b)$.

Que no se tenga la propiedad anti simétrica en la relación de orden que definiremos en $M\ i^2$ , implica varios hechos, el primero de ellos es que esta relación induce una relación de equivalencia sobre el conjunto dada por $a,b\ \leq\ c,d\ \wedge\ c,d\ \leq\ a,b$ , muy similar a la inducida por $(a,b)\ |(c,d) \wedge (c,d)\ |(a,b)$, ahora tenemos una segunda manera de asociar los números:

**Definición 20(μ):**

$$\forall\ a,b\ ,\ c,d\ \in M\ i^2\ :\ a,b\ \approx\ c,d\ \leftrightarrow (\ a,b\ \leq\ c,d\ \wedge\ c,d\ \leq\ a,b\ )$$

**Teorema 28:** $a,b\ \approx\ c,d\ \leftrightarrow\ (a,b)\ =\ (c,d)$

Demostración:

i. $a,b\ \approx\ c,d\ \rightarrow\ (a,b)\ =\ (c,d)$

$a,b\ \approx\ c,d$ , es nuestra hipótesis

$a,b\ \leq\ c,d\ \wedge\ c,d\ \leq\ a,b$ , por D20

$a,b\ \leq\ (c,d)\ \wedge\ c,d\ \leq\ (a,b)$ , por D19

$(a,b)\ =\ (c,d)$ , por la propiedad anti- simétrica de $\leq$ en $\mathbb{N}$

ii. $(a,b)\ =\ (c,d)\ \rightarrow\ a,b\ \approx\ c,d$

$(a,b)\ =\ (c,d)$ , es nuestra hipótesis

$(a,b)\ \leq\ c,d\ \wedge\ c,d\ \leq\ a,b$ , por definición de $\leq$ y la tautología

$p \rightarrow p \vee p$

$a,b\ \approx\ c,d$ , por D20

Los números asociados por $\approx$ tienen todos la misma norma, ya hemos caracterizado algunos conjuntos de números asociados por esta relación de equivalencia como en el caso de $U, D_0$, respecto a la idea de orden que seguimos ninguna unidad es mayor que otra y ningún divisor de 0 es mayor que otro.

**Teorema 29(μ):** $\approx$ es una relación de equivalencia

Demostración:

i. La relación $\approx$ es reflexiva, puesto que $(a,b)\ =\ (a,b)$ y por T28 se tiene la propiedad.

ii. La relación $\approx$ es simétrica, $\forall\ a,b\ \in M\ i^2$ :

$$a,b\ \approx\ c,d\ \text{ es nuestra hipótesis}$$

$$(a,b)\ =\ (c,d)\ \text{ por T20}$$

$$(c,d)\ =\ (a,b)\ \text{ , ya que la igualdad es simétrica}$$

$$c,d\ \approx\ a,b\ \text{ , por T20}$$

iii. La relación $\approx$ es transitiva, $\forall\ a,b\ ,\ c,d\ ,\ e,f\ \in M\ i^2$ :

$$((a,b)\approx\ (c,d)\wedge(c,d)\ \approx\ (e,f)),\ \text{es nuestra hipótesis}$$

$$(a,b)\ =\ (c,d)\ \wedge\ (c,d)\ =\ (e,f)\ \text{ , por T20}$$

$$(a,b)\ =\ (e,f)\ \text{ , la igualdad es transitiva}$$

$$a,b\ \approx\ e,f\ \text{ , por T20}$$

Por tanto $\approx$ es de equivalencia.

Siendo esta relación de orden favorable en cuanto a propiedades que tienen que ver con el producto, algunas de las más notorias son:

**Teorema 30:** $\forall\ a,b\ ,\ c,d\ ,\ e,f\ \in M\ i^2\ ,\ e,f\ \notin D_0$:

1. $a,b\ <(c,d)\leftrightarrow\ a,b\ (e,f)<(c,d)(e,f)$

Demostración:

Inicialmente demostremos que $a,b\ <(c,d)\rightarrow\ a,b\ (e,f)<(c,d)(e,f)$

$$a,b\ <\ c,d\ \wedge\ e,f\ \notin D_0\ \text{es nuestra hipótesis}$$

$$(e,f)\ \neq 0,\ \text{por el corolario de T4}$$

$$(e,f)\ >0,\ \text{por la propiedad 1 de T8}$$

$$(a,b)\ <\ (c,d)\ \text{ , por D19}$$

$$(a,b)\ *\ e,f\ <\ c,d\ *\ (e,f)\ \text{ , por la monotonía de la multiplicación respecto a}\ <\ \text{en}\ \mathbb{N}$$

$$a,b\ *(e,f)\ <\ c,d\ *(e,f)\ \text{ , por la propiedad 6 de T8}$$

$$a,b\ (e,f) < (c,d)(e,f)$$, por D20

Ahora demostremos que $a,b\ (e,f) < (c,d)(e,f) \rightarrow\ a,b\ < (c,d)$

$$a,b\ (e,f) < (c,d)(e,f)$$, es nuestra hipótesis

$$a,b\ *(e,f)\ <\ c,d\ *(e,f)$$ , por D20

$$(a,b)\ *\ e,f\ <\ c,d\ *\ (e,f)$$ , por 6 de T8

$$(a,b)\ <\ (c,d)$$ , por la propiedad cancelativa de * respecto a $<$ en $\mathbb{N}$

$$a,b\ < (c,d)$$, por D20

**Corolario:** $\forall x,y \in \mathbb{Z}: x \leq y \rightarrow\ x,0\ \leq (y,0)$

2. $\exists\ x,y\ \in M\ i^2\ ,\forall\ a,b\ \in M\ i^2\ :\ x,y\ \leq\ a,b\ \rightarrow\ x,y\ \in D_0$

Sea $N =\ n \in \mathbb{N}: n =\ a,b\ ,\forall\ a,b\ \in M\ i^2$ , $N$ tiene mínimo por el principio de buen orden en $\mathbb{N}$, y además como $0,0\ = 0,0 \in N$, por tanto $\min N = 0$, por la definición de $N, \exists\ a,b\ \in M\ i^2\ :\ a,b\ = 0$, ahora como $x,y\ \leq\ a,b$ por D20 se tiene que $x,y\ \leq\ (a,b)$ , $(x,y)\ \leq 0$, se concluye que por la propiedad 1 de T8 $(x,y)\ = 0$ y por el corolario de T4 $x,y\ \in D_0$.

**3.** $a,b\ \leq\ a,b\ ^2$

Se tienen dos casos $(a,b)\ = 0 \vee\ a,b\ > 0$, si se tiene el primero entonces, $a,b\ ^2\ =\ a,b\ ^2 = 0^2 = 0$ por la propiedad 8 de T8, y se cumple que $0 \leq 0$, osea que $(a,b)\ \leq\ a,b\ ^2$ .

Para el segundo caso $a,b\ > 0$, $a,b\ <\ a,b\ ^2$, pues en los naturales se cumple el teorema, $a,b\ ^2 =\ a,b\ ^2$ por la propiedad 8 de T8, reemplazando en $a,b\ <\ a,b\ ^2$ y por D20 se tiene $a,b\ \leq\ a,b\ ^2$

**4.** $a,b \mid c,d\ \rightarrow\ a,b\ \leq (c,d)$

$$a,b \mid c,d\ \rightarrow\ (a,b) \mid (c,d)$$ , por la propiedad 4 de T21

$(a,b) \leq (c,d)$ , ya que se tiene el teorema para $(a,b)$ , $(c,d) \in \mathbb{Z}$

$a,b \leq (c,d)$, por D20

**Corolario:** $a,b \sim c,d \rightarrow a,b \approx c,d$

Esta relación de pre- orden es compatible con varios de los elementos que tenemos para trabajar con divisibilidad, por ejemplo para el algoritmo de la división.

Por el propio proceso de división escalar y la elección del escalar para dividir en el algoritmo de la división se puede asegurar la reformulación de este:

$\forall\ a,b \quad c,d \in M\ i^2$ , $c,d \neq 0, \exists\ p,q$ , $r,s \in M\ i^2 : a,b = p,q + (r,s)$ con $r,s < (c,d)$, sin embargo no podemos asegurar que sean únicos, de hecho la elección del residuo no lo es, dos residuos $r,s$ y $r,-s$ o cualquiera de los asociados a estos son admitidos por la relación de orden y este es un primer problema de cara a intentar demostrar el TFA.

### 4.6 Máximo común divisor

Con las herramientas que hemos obtenido en las secciones y capítulos anteriores, ya podemos escribir cualquier número en términos de una multiplicación, no solo eso, ya podemos determinar si un número es o no primo, claro está que el método de determinar todos los números de una determinada norma y para cada uno aplicar el algoritmo de la división quizás no sea el más práctico, por lo cual nace la necesidad de encontrar herramientas que permitan minimizar el trabajo de descomponer un número. Tampoco hemos respondido a la pregunta, ¿las descomposiciones en factores primos de un número compuesto son únicas? en $M(i^2)$,

La relación $\leq$ nos da un camino para comenzar a simplificar el trabajo y da un punto común para las posibles descomposiciones de un número compuesto. Comencemos por definir los elementos que nos permiten hablar de un máximo común divisor. Tanto en $\mathbb{N}$ como en $\mathbb{Z}$ el máximo común divisor es máximo desde el punto de vista de las dos relaciones $\leq, |$, y además también es único, se puede usar cualquiera de las dos relaciones

para definir el máximo común divisor, los elementos básicos son compatibles de la misma forma con ambos pre ordenes, sin embargo, con la relación | no es posible comparar todos los elementos, por ejemplo $(a,b)$ y $(a,-b)$ en general ninguno divide al otro y no son asociados, en este sentido $\leq$ tiene una ventaja y es por ello que la utilizaremos para definir el máximo común divisor :

**Definición 21(μ):** Sea $S \subseteq M\ i^2\ , S \neq \emptyset, \leq$ una relación de pre orden en $M\ i^2$ :

$(x,y) \in M(i^2)$ es una cota superior de $S$ si y solamente si $\forall\ u,v\ \in S,\ u,v\ \leq (x,y)$.

$(x,y) \in M(i^2)$ es una cota inferior de $S$ si y solamente si $\forall\ u,v\ \in S,\ x,y\ \leq (u,v)$.

Si $(x,y)$ es una cota superior de $S$ y $(x,y) \in S$, se dice que $(x,y)$ es máximo de $S$, esto se nota $(x,y) = \max S$; análogamente si $(x,y)$ es una cota inferior de $S$ y $(x,y) \in S$, se dice que $(x,y)$ es un mínimo de $S$ y se nota $(x,y) = \min S$.

El mínimo cumple una propiedad muy importante respecto a $\mathbb{N}$ y $\mathbb{Z}$, un conjunto que está acotado inferiormente y además no sea vacío siempre tiene un mínimo, en $\mathbb{N}$ como 0 es cota inferior del conjunto se tendrá que todo $A \subseteq \mathbb{N}$ tiene un mínimo, en $\mathbb{Z}$ por otro lado es necesario agregar la condición ¨todo conjunto acotado inferiormente¨, para nuestros conjuntos en base a la relación de orden $\leq$, como consecuencia de que toda norma sea un número natural, se tiene un resultado similar al de $\mathbb{N}$:

**Teorema 31(μ):** Todo conjunto no vacío de $M\ i^2$ tiene mínimo.(Principio del buen orden)

Demostración:

Sea $A \subseteq M\ i^2$ , y sea $N = \{n \in \mathbb{N}: \exists\ x,y\ \in A, n =\ (x,y)\ \}$, como $N \subseteq \mathbb{N}$ siendo el conjunto de todas las normas de los elementos de $A$, se tiene que $N$ tiene mínimo, llamemos a este $m$, por definición de mínimo $\mathbb{N}$, $\forall l \in N, m \leq l$, lo por la definición de $N$, $\exists\ x,y\ ,\ a,b\ \in A: m =\ \ x,y\ \ , l =\ \ a,b\ \ $, sustituyendo en la desigualdad se tiene que $x,y\ \leq\ a,b\ $ por lo cual por D19 $x,y\ \leq (a,b)$, ya que tomamos a $l$ cualquier norma de $A$ se tiene que se cumple $x,y\ \leq (a,b)$ para cualquier $a,b\ \in A$, por D21 se concluye que $x,y\ = \min A$.

Usualmente se demuestra que existe un único mínimo en el conjunto suponiendo que existen dos, $\exists\ a,b\ ,\ a',b'\ \in A: \forall\ x,y\ \in A,\ a,b\ \leq\ x,y\ \wedge (a',b') \leq (x,y)$, y de esto ya que $a,b\ ,\ a',b'\ \in A$ y ambos son mínimos se obtiene que $a,b\ \leq\ a',b'\ \wedge\ a,b\ \leq\ a',b'$ , este punto es importante, con esta información si nuestra relación $\leq$ de $M\ i^2$ fuese anti simétrica se concluiría $a,b\ =\ a',b'$ , sin embargo esto no sucede, como se pierde la propiedad de anti simetría solo podemos afirmar por D20 $a,b\ \approx\ a',b'$ y por T28 $(a,b)\ =\ (a',b')$ .

Del análisis anterior, podemos rescatar este resultado:

**Teorema 32(μ):** $\forall A \subseteq M\ i^2\ , A \neq \emptyset: (\ a,b\ = \min A \wedge\ c,d\ = \min A) \rightarrow\ a,b\ \approx\ c,d$

Los dos resultados anteriores pueden resumirse en hay elementos en todo subconjunto no vacío de $M\ i^2$ cuya norma es mínima, en general no hay uno solo .

¿Significa entonces que deberíamos elegir la relación de divisibilidad para definir mínimos?, si lo hubiésemos hecho usando la relación $|$ , hay conjuntos en los cuales el mínimo ni siquiera existiría, pues tal mínimo tendría que ser un divisor de todos los del conjunto, basta con elegir algunos números que no son comparables para ello o conjuntos cuyos elementos no tengan todos divisores en comunes , por ejemplo en $M\ 1\ , A = \{\ 2,0\ ,\ 3,1\ , (3,-1)\}$ o $A = \{\ 4,2\ ,\ -4,-2\ ,\ 4,3\ \}$, por tanto tenemos otra ventaja al elegir definir máximo y mínimo con $\leq$, se tiene un principio de buen orden para todo conjunto no vacío.

De manera similar a como pasa con los mínimos, los conjuntos no vacíos y acotados superiormente tanto en $\mathbb{N}$ como en $\mathbb{Z}$ tiene un máximo, en los números naturales donde el orden es el más similar esto es equivalente a establecer que $A$ es finito y de la misma manera se cumple:

Se tiene por las propiedades de los conjuntos acotados en $\mathbb{N}$:

**Teorema 33(μ):** Todo conjunto no vacío de $M\ i^2$ finito tiene máximo.

Lema: $: M\ i^2\ \rightarrow \mathbb{N}$ es función

Demostración:

Inicialmente demostremos que $\forall A \subseteq M\ i^2\ A \neq \emptyset, A$ es finito$\rightarrow A$ tiene máximo.

Sea $N = \{n \in \mathbb{N}: \exists\ x, y\ \in A, n = \ (x, y)\ \}$, como $N \subseteq \mathbb{N}$ siendo el conjunto de todas las normas de los elementos de $A$, como es función y como $A$ es finito, se tiene que la imagen directa $A$ es finita[5], con $N = \ A$ se tiene que $N$ es finito y por tanto tiene máximo, llamemos a este $m$, por definición de máximo en $\mathbb{N}$, $\forall z \in N, z \leq, m$ lo por la definición de $N$, $\exists\ x, y\ ,\ a, b\ \in A: m = \ x, y\ , z = \ a, b\ $, sustituyendo en la desigualdad se tiene que $a, b\ \leq\ x, y$ por lo cual por D19 $(a, b) \leq\ x, y$ , ya que tomamos a $z$ cualquier norma de $A$ se tiene que se cumple $x, y\ \leq (a, b)$ para cualquier $a, b\ \in A$, por D21 se concluye que $x, y\ = \max A$.

También se puede confirmar aquí que si el conjunto no vacío tiene máximo, entonces es finito, sin embargo este resultado pero para demostrarlo necesitaríamos admitir como ciertos algunos otros teoremas de la teoría de conjuntos, ya que ese resultado no se utiliza para alguna de las demostraciones consecuentes, no se demostrará, sin embargo, el lector puede practicar probando que efectivamente se cumple que un subconjunto de $M\ i^2$ tiene máximo es equivalente a que es finito.

De la misma forma a como pasa con el mínimo, el máximo de un conjunto tampoco es único, cualquier conjunto que tenga varios números con la misma norma y que esta sea máxima, no tiene un único máximo, por ejemplo $A = \{(-2n, 0) \ldots (0,0),\ 2,0\ ,\ 4,0\ ,\ 6,0\ \ldots (2n, 0)\}$ para un $n$ conocido. Se puede comprobar de forma muy similar a como se hace para el mínimo el siguiente resultado:

**Teorema 34(μ):**

$$\forall A \subseteq M\ i^2\ , A \neq \emptyset: (\ a, b\ = \max A \wedge\ c, d\ = \max A) \rightarrow\ a, b\ \approx\ c, d$$

Podemos solventar la situación de que no haya un máximo o un mínimo único, pues se necesita que asi sea para hablar de sus propiedades, ya que cuando hay más de un máximo

[5] (Busqué, Saorín, & Simón, 2011-2012), Teoría de conjuntos y números.

y más de un mínimo todos tienen la misma norma, se puede definir un conjunto análogamente a como se hizo para $U$ y $D_0$ , esto es, podemos definir el conjunto de todos los mínimos y el conjunto de todos los máximos como sigue:

**Definición 22(μ):**

$$MIN\ A = \{(x, y) \in A : (x, y = \min A)\}$$

$$MAX\ A = \{(x, y) \in A : (x, y = \max A)\}$$

Estos conjuntos cumplen propiedades que se derivan directamente de las demostradas para $max$ y $min$:

**Teorema 35(μ):**

1. Todo subconjunto $A$ no vacío de $M\ \ i^2$ tiene un subconjunto $MIN\ A$ no vacío.
2. Todo conjunto $A$ finito no vacío de $M\ \ i^2$ tiene un subconjunto $MAX\ A$ no vacío.
3. $MAX\ A \subseteq A \wedge MIN\ A \subseteq A$

Demostración:

1. Ya que para $A \neq \emptyset, A \subseteq M\ \ i^2$ , se tiene que $\exists\ m, n\ \in A : (m, n)$ es mínimo, por D22 $m, n\ \in MIN\ A$ y se tiene el teorema.

2. Ya que para $A \neq \emptyset, A \subseteq M\ \ i^2$ , $A$ finito se tiene que $\exists\ m, n\ \in A : (m, n)$ es máximo, por D22 $m, n\ \in MAX\ A$ y se tiene el teorema.

3. Esta propiedad se obtiene de forma inmediata por la definición de $MAX\ A$ y $MIN\ A$.

Sin embargo con la nueva definición de máximo y mínimo, que por acuerdo es la que usaremos de ahora en adelante, ya podremos comprobar la unicidad del conjunto máximo y el conjunto mínimo de un conjunto:

**Teorema 36(μ):**

$\forall A \subseteq M\ i^2\ , A \neq \emptyset : MIN\ A$ es único y $MAX\ A$ es único.

Demostración:

Con $A \neq \emptyset$, por T35 sabemos que $A$ tiene un conjunto mínimo y conjunto máximo no vacíos. Supongamos que no se cumple el teorema, por lo cual supondremos para la primera parte que existen $X, Y$ tales que $X = MIN\ A \wedge Y = MIN\ A$. Para un $a, b\ \in X,\ a, b\ = \max A$ por la definición de $X$ y D22, también por la definición de $Y$ y D22 se tiene que $a, b\ \in Y$, por tanto $X \subseteq Y$, de manera recíproca se llega a que $Y \subseteq X$ y por definición de igualdad entre conjuntos $X = Y$.

De manera análoga se demuestra que dos conjuntos máximos de $A$ deben ser iguales.

Con los máximos de un conjunto completamente definidos, como el conjunto de números con norma máxima dentro del referente, podemos proceder con el siguiente paso, definir los divisores comunes:

**Definición 23(μ):** $\forall\ a, b\ (c, d)\ x, y\ \in M\ i^2\ : (x, y)$ es divisor común de $a, b\ (c, d) \leftrightarrow x, y\ |(a, b) \wedge\ x, y\ |(c, d)$

Esta definición no aporta algún elemento que no conociésemos en nuestro estudio hasta el momento, de hecho en T12 ya estudiamos algunas propiedades de los divisores comunes, por lo cual contamos con herramientas para hacer uso de esta definición, ahora el siguiente paso es definir el máximo común divisor de dos números en $M\ i^2$ :

**Definición 24(μ):** Sea $D = \ x, y\ \in M\ i^2\ :\ x, y\ \ a, b\ \wedge\ x, y\ \ c, d\ \ , M = MCD\ \ a, b\ ,\ c, d\ \ \leftrightarrow M = MAX\ D$

Un primer resultado que hereda esta definición de las propiedades del conjunto máximo es:

**Teorema 37(μ):** $MCD(\ a, b\ , (c, d))$ es único.

Notemos que el máximo común divisor en $M(i^2)$ es un conjunto no un número, sin embargo todos sus elementos tienen la misma norma, es de esperarse que el máximo común divisor, si fuese definido como elemento, no sería único, ya que es el máximo de un conjunto de divisores, y como $a, b$ , $(-a, -b)$ son dos números que siempre son divisores de los mismos números, es decir, si uno divide a un número el otro también lo hace, y además tienen normas iguales, estos dos serian máximos comunes divisores, notemos también que este ejemplo de un par de números que están en el máximo común divisor, determina dos números asociados.

En $\mathbb{Z}$ por ejemplo se da un caso similar, 2 y -2 son divisores comunes de todo número par, sin embargo $mcd\ 14{,}10\ = 2$, entonces ¿Cómo se elige este número y se descarta al otro?, en $\mathbb{Z}$ hay solución a esto puesto que $mcd(a, b)$ se define como un entero positivo, tomando así el conjunto de los enteros positivos como herramienta pero como vimos en la sección 4.5 esto es algo que en $M(i^2)$ no tenemos.

Por otro lado, en los números enteros la forma para relacionar a los enteros positivos y los negativos cumple propiedades muy especiales, (1) todo número de norma 2 divide a todo número de norma 4 por ejemplo, teniendo en cuenta que en $\mathbb{Z}$ la norma es , de esto (2)todos los números de la misma norma están asociados por la relación de equivalencia que determina la divisibilidad, por ello $a\ = x \leftrightarrow a = \pm x$.

La segunda propiedad no se cumple pues en general conocemos $(a, b)$ y $(a, b)$ tales que no son asociados por la relación $\sim$ y que tienen la misma norma, además si encontramos en el mismo conjunto (como vimos en la sección 4.4) dos sumas de cuadrados consecutivos para la misma norma que determinen números en el mismo conjunto, se habrán hallado dos números con la misma norma que no están relacionados ni con la relación de conjugado, por ejemplo $(3{,}0)$ y $(5{,}4)$ en $M(1)$ y sabemos que no pueden estar asociados por T20 (Es importante para demostrar o refutar el TFA mas adelante ).

Respecto a la primera propiedad, admitir que se cumple sería equivalente a decir que siempre que se aplique el algoritmo de la división a un número de norma $nk$ por uno de norma $k$, el residuo será (0,0) y en específico para nuestros números $(a, 0)$ significaría que

todo número de norma $nk$, tiene componentes que son múltiplos de $(a,0)$ lo cual no es cierto, por ejemplo para $(9,1)$ con norma 80, en $M(1)$, $(2,0)$ con norma 4 no puede dividirlo pues no divide al máximo común divisor de sus componentes.

No obstante, en algunos casos se puede tener que haya números de la misma norma no asociados con divisores equivalentes, no podemos determinar con un algoritmo simple todos los números de norma $n$, sin embargo, podemos decidir sobre los que conocemos:

**Teorema 38(μ):** $\forall\ a,b\ \in M\ i^2\ ,\ a,b\ \approx\ a,b\ \approx\ a,b\ \approx -(a,b)$

Es inmediato teniendo en cuenta que $x^2 = (-x)^2$ en $\mathbb{Z}$.

Para el conjunto de números asociados por ≈, ya sabemos que si uno pertenece entonces al menos hay cuatro, de manera similar si tenemos el conjunto de divisores de $(x,y)$, $D_{(x,y)}$, $a,b\ \in D_{(x,y)}$ al menos dos números asociados de la misma norma pertenecen, $a,b\ , -(a,b)$ y los otros dos conocidos $a,b\ ,\ a,b$ estarán en el conjunto $D_{(x,y)}$.

Por este hecho se tiene el resultado:

**Teorema 39(μ):**

$$\forall\ a,b\quad c,d\ \in M\ i^2\ ,(x,y)\in\ MCD\quad a,b\quad c,d\quad \rightarrow (x,y)\in\ MCD\quad a,b\ ,\ c,d$$

Y en general para todo divisor:

**Teorema 40(μ):** $\forall\ a,b\ (x,y)\in M\ i^2\ ,(x,y)|\ a,b\ \rightarrow (x,y)|\ a,b$

Demostración:

$(x,y)|\ a,b$ es nuestra hipótesis

$x,y\quad m,n\ =\ a,b$ , para algún $m,n$ por D11

$xm+ynr^2, xn+ym\ = (a,b)$ por D4

$xm+ynr^2 = a \wedge\ xn+ym = b$ por D2

$-xn - ym = -b$, multiplicando por -1 a ambos lados de la igualdad

$(xm + (-y)(-n)r^2, -xn - ym \ = (a, b)$, por D2 y ya que $ny = (-n)(-y)$ en $\mathbb{Z}$

$x, -y \quad m, -n \ = \ a, -b$ , por D4

$(x, y) \mid \ a, b$ por D11 y D8

Este teorema nos indica que un número y su conjugado aunque no estén asociados, tienen cierta identidad el uno con el otro, en este caso toda descomposición de un número determina una descomposición de su conjugado en la cual los factores de una son los conjugados de la segunda descomposición, o a cada elemento que divide a $a, b$ le corresponde un divisor del conjugado $a, b$ , $a, b$ y $a, b$ , tienen la misma cantidad de divisores con las mismas normas tales que siempre un divisor es conjugado del otro, eso es algo muy valioso si buscamos que las descomposiciones de un número sean únicas. Por otro lado, $a, b$ y $a, b$ no están asociados por $\sim$ usualmente, pero si alguno es divisor del otro deben ser asociados gracias a T20, los casos en los que se cumple esto son:

**Teorema 41:** $\forall \ a, b \ \in M \ i^2 : (a, b) \mid \ a, b$ implica que:

1. $i^2 = 0$ entonces $a, b \ = (2b, -b) \vee \ a, b \ = (a, 0)$
2. $i^2 > 0$ entonces $a, b \ = (a, 0)$

Aunque con los teoremas anteriores, para un número y su conjugado respondimos a la pregunta, ¿Qué características tienen los números de la misma norma que tienen divisores comunes?, se pueden dar varios casos, que tengan todos los divisores comunes, como sucede cuando $(a, b) \sim (c, d)$, que $MCD \quad a, b \ , \ c, d \quad = \{ \ a, b \ , (-a, -b)\}$, que tengan algunos divisores comunes, o que no tengan ningún divisor en común, surge en este último caso, la definición que sigue:

**Definición 25(μ):** $a, b \ , (c, d)$ son primos relativos$\leftrightarrow MCD \quad a, b \ , \ c, d \quad = U$

Esta definición es de vital importancia en la búsqueda de las descomposiciones únicas de un número, pues es un punto en común entre los divisores que tiene un número y por tanto, de sus descomposiciones en factores primos, con esta ya no es posible dar respuesta a la cuestión ¿La descomposición en factores primos de un número en $M(i^2)$ es única?.

### 4.7 El Teorema Fundamental de la Aritmética

A lo largo de este documento, se han ido definiendo herramientas para el estudio de las descomposiciones de los elementos de $M(i^2)$ en otros que los configuran, ya sea con la suma o con el producto, y recíprocamente para poder estudiar las partes que componen un número o un conjunto, respecto a él.

El estudiar las propiedades algebraicas de un número, nos familiarizamos con las propiedades de los elementos de cada conjunto $M(i^2)$, se encontraron elementos con propiedades inusuales, como son los divisores del neutro de la suma $(0,0)$ y números que cumplían la función de neutro dependiendo de con quien se les multiplicara, la existencia del primer tipo de números en estos conjuntos afecto a varias propiedades algebraicas, como la propiedad cancelativa de la multiplicación, y mientras más fuimos avanzando en el estudio surgieron nuevas propiedades de estos números que de cierta manera eran un obstáculo para demostrar varios resultados que se tienen en $\mathbb{Z}$ y $\mathbb{N}$, como al definir números positivos y al encontrar residuos por el algoritmo de la división con norma 0 sin ser estos 0.

Se tomaron una segunda representación de $M(i^2)$ y un producto por escalar con el fin de simplificar el trabajo de multiplicar dos números, no obstante el producto por escalar sirvió como herramienta para determinar divisores de $(a,b)$ en cualquier conjunto sin depender de $i^2$, siempre y cuando $mcd\ a,b \neq 1$, y asociado a este la descomposición de un número de la forma $(ak^2,b)$ como $ak^2,b = (b,a)(0,1)$ estas fueron las dos primeras descomposiciones de un número que se encontraron.

Con el producto por escalar se solucionó el problema de descomponer números cuyas componentes no fueran primos relativos, sin embargo este por sí solo no fue suficiente para descomponer todo número ya que no aporta nueva información sobre $a,b$ , $mcd\ a,b =$

1, por lo cual se definieron nuevas herramientas como las potencias, los conjugados, la norma y las propiedades de recurrencia de + y * que más adelante junto a una relación de divisibilidad aportarían nuevos elementos para descomponer los casos problemáticos, $a, b$ .

El problema se atacó indirectamente definiendo las unidades y asociados para así intentar caracterizar el conjunto de divisores de un número y se definieron números primos pensando en encontrar las descomposiciones definitivas de un $(a, b)$, o en otras palabras buscando escribirlo en términos de elementos irreducibles, con esta idea en mente, se retomó el caso de los números $(p, 0)$ que permiten realizar el producto por escalar y se hallaron las condiciones necesarias y suficientes para que $(p, 0)$ fuese primo, $r \nmid \frac{p+1}{2} \wedge r \nmid \frac{p-1}{2}$.

Además de hallar la forma de números primos en este estudio, al realizar la exploración se encontró que un número $(a, b)$ que tiene norma prima $(a, b) = p$, es primo, surgió de aquí la idea de utilizar la norma para determinar si un número es primo o es compuesto además la exploración se basó en la premisa: si un numero $(a, b)$es divisor de otro $c, d$ entonces $(a, b)$ es divisor de $(c, d)$ , utilizando este hecho se trató de descomponer la norma $(c, d)$ para hallar los posibles números $(x, y)$ que cumplieran, $(x, y) \mid (a, b)$ , hacerlo con ecuaciones Diofanticas resultaría en un proceso muy dispendioso como paso en la sección 4.3, afortunadamente se encontró una nueva representación para la norma de un número que nos dio un nuevo camino para encontrar los divisores de un número, esto es, la descomposición de la norma en sumas consecutivas de números impares.

Con esta nueva representación se halló un método que permite encontrar todos los elementos de $M(i^2)$ de una determinada norma en todo conjunto, resolviendo así el problema de hallar números que cumplan $(x, y) \mid (a, b)$ y con el hallamos las condiciones necesarias y suficientes para que un número fuera primo en $M\ i^2$ , sin embargo aún faltaba el determinar si $x, y$ encontrados satisfacían $(x, y) \mid (a, b)$, esto nos llevó a definir un método para determinar para dividir, el algoritmo de la división.

Con las dos últimas herramientas resolvimos la cuestión, ¿cómo descomponer un número?, aunque en los conjuntos $M(i^2)$ los algoritmos para ello resultan más densos que en otros conjuntos; procedimos así a abordar el problema ¿la descomposición de un numero compuesto en factores primos es única? y el definir herramientas para atacar este problema, como la relación de orden y el máximo común divisor, nos llevó a esta sección y a los últimos 3 teoremas de este documento.

Si queremos descomponer $a,b \in M\ i^2$ , $a,b \notin D_0$,en términos de factores primos:

Verificamos $m = mcd\ a,b$ ,

Si $m = 1$ procedemos a determinar $n = (a,b)$ , determinamos los $x,y \in M\ i^2 : (x,y) \mid (a,b)$ por sumas de impares consecutivos, luego se aplica el algoritmo de la división y se eligen las descomposiciones en las cuales el residuo sea $(0,0)$, luego de esto, se repite el proceso, si en algún momento no existe ningún número $(x,y)$ que sea divisor de $(a,b)$ se tendrá que este último es primo.

Si $m > 1$, descomponermos por producto por escalar $a,b = (m,0)(\frac{a}{m},\frac{b}{m})$, luego descomponemos $(m,0)$ en los factores $(p_1,0)(p_2,0) \dots (p_n,0)$ tales que $m = p_2 p_2 \dots p_n$ por el TFA en $\mathbb{Z}$, luego de esto verificamos si para algún $p_k$ $1 \leq k \leq n$ cumple que $r|p_k$, y de ser así descomponemos tales $(p_k,0)$ como $\frac{p_k+1}{2},\frac{p_k-1}{2r}$ $\frac{p_k+1}{2},\frac{1-p_k}{2r}$ , o cualquiera de las descomposiciones asociadas que surgen. Así se tendrá una descomposición de $a,b$ similar a: $a,b = (p_1,0)$ $\frac{p_2+1}{2},\frac{p_k-1}{2r}$ $\frac{p_2+1}{2},\frac{1-p_k}{2r}$ $\dots (p_n,0)(\frac{a}{m},\frac{b}{m})$, con todos los factores salvo $(\frac{a}{m},\frac{b}{m})$ primos, como $mcd\ \frac{a}{m},\frac{b}{m} = 1$ se reduce al caso anterior el resto de la descomposición.

Este proceso asegura que:

**Teorema:** Todo número compuesto puede ser escrito como producto de factores primos.

**Corolario:** Todo número compuesto tiene al menos un divisor primo.

Se resalta de este proceso que cuando $mcd\ a,b\ = 1$, ya no pueden aparecer más factores $(p_k, 0)$ en la descomposición del número, porque si así fuese por ejemplo si el proceso termina con dos factores, $(p_k, 0)\ x, y\ = (a, b)$ tales que $(p_k, 0)$, $x, y$ son primos, entonces $p_k x, p_k y\ = (a, b)$ y en conclusión $mcd\ a,b\ = p_k$ lo cual sería una contradicción. De esto se tiene que $(p_k, 0) \nmid\ a,b\ \leftrightarrow mcd\ a,b\ = 1$ (1).

También nótese que al contrario, si pueden aparecer términos $(r, s)$ tales que $mcd\ r,s\ = 1$ y $r,s\ *\ r,-s\ = (p_k, 0)$, pero esto solo sucede una vez puesto que $(p_k, 0)\ = {p_k}^2$ y $(r, s)\ = p$, por lo tanto $r,s\ ,\ r,-s$ son primos y no se les puede seguir dividiendo (2).

Otro hecho es que una de las propiedades de los conjugados es que $a,b\ \ a,b\ = a^2 - b^2 r^2, 0\ \vee\ a,b\ \ a,b\ =\ b^2 r^2 - a^2, 0$ , P-6 de T7 (3)

Si consideramos que existe $(a, b)$ en $M\ i^2$ tal que, $(a, b)\ = n$, entonces

$a,b\ \ a,b\ =\ n,0\ \vee\ a,b\ \ a,b\ =\ n,0$

Y además podemos descomponer a $n,0$ tal que:

$$n,0\ = (p_1, 0)(p_2, 0) \dots (p_n, 0)$$

Estas dos descomposiciones de $n,0$ son distintas, sin embargo:

$$a,b\ \ a,b\ = (p_1, 0)(p_2, 0) \dots (p_n, 0)$$

$$\vee\ a,b\ \ a,b\ = (p_1, 0)(p_2, 0) \dots (p_n, 0)$$

Sin pérdida de generalidad tomemos el primer caso:

$$a,b\ \ (a,-b) = (p_1, 0)(p_2, 0) \dots (p_n, 0)$$

Aplicamos el proceso de descomponer $a,b$ si $mcd\ a,b\ > 1$, factorizamos el mcd por producto por escalar:

$$m,0\ \ m,0\ \ \frac{a}{m},\frac{b}{m}\ \ \frac{a}{m},-\frac{b}{m}\ = (p_1, 0)(p_2, 0) \dots (p_n, 0)$$

Ahora como ningún $p_k$ es divisor de $\frac{a}{m},\frac{b}{m}$ ni de $(\frac{a}{m},-\frac{b}{m})$, dependerá de si algún producto $(p_k,0)\ p_r,0\ \ldots\ p_s,0\ =(m,0)(m,0)$ el si estas dos descomposiciones son distintas o no, si no es el caso, se tiene que las dos descomposiciones son diferentes, en caso contrario sabemos que no se puede dar que se cancelen todos los términos pues ningún $x,0\ ,x>1$ es divisor de $\frac{a}{m},\frac{b}{m}$ , por lo cual si fueran dos descomposiciones asociadas, por lo cual cancelamos $(p_k,0)\ p_r,0\ \ldots\ p_s,0$ y $(m,0)(m,0)$:

$$\frac{a}{m},\frac{b}{m}\quad\frac{a}{m},-\frac{b}{m}\ =(p_1,0)\ldots(p_{k-1},0)(p_{k+1},0)\ldots(p_n,0)$$

Ahora como $x,0\ ,x>1$ no es divisor de $\frac{a}{m},\frac{b}{m}$ , la descomposición será única solamente si $\frac{a}{m},\frac{b}{m}\quad\frac{a}{m},-\frac{b}{m}$ una descomposición de $\frac{a}{m},\frac{b}{m}\quad\frac{a}{m},-\frac{b}{m}$ tiene divisores de $(p_k,0)$ $\forall p_k$, en caso contrario las dos descomposiciones iniciales son distintas y no asociadas.

La recopilación de este proceso da como resultado:

**Teorema 44:** Sea $a,b\ ,\ (a,b)\ =n,n=p_2p_2\ldots p_n$ su descomposición en factores primos, las dos descomposiciones de $(n,0)$:

$$n,0\ =(p_1,0)(p_2,0)\ldots(p_n,0)$$

$$n,0\ =(a,b)(a,-b)$$

Son dos descomposiciones distintas no asociadas de $(n,0)$ si y solamente si $MCD\quad a,b\ ,\ p_k,0\quad=U$ para algún $1\leq k\leq n$

**Corolario:** Si $(n,0)$ no tiene descomposición única en $M(i^2)$ entonces $(na,nb)$ no tiene descomposición única en $M(i^2)$.

En general en $M(i^2)$ no se puede asegurar que sean distintas o que sean iguales, esto es dependiente de si los elementos de la descomposición son o no primos relativos, es decir, no comparables con la relación de divisibilidad, por ejemplo en $M(1)$:

$8,0 = 3,1 \ \ 3,-1 = (2,0)(2,0)(2,0)$ Estas son dos descomposiciones distintas no asociadas.

## 5. Programas para encontrar los divisores de un numero en $M(i^2)$

Para el desarrollo de este trabajo fue necesario el uso de un software que permitiese comprobar varios de los resultados respecto a la divisibilidad que se demostraron, como la manera de descomponer números con el producto por escalar, la existencia de números que dividen a $(p, 0)$ y la descomposiciones de normas por sumas de impares consecutivos. En una primera fase exploratoria, se analizaron listas de números para determinar qué propiedades cumplían y que tenían en común números de ciertas propiedades.

Un software desarrollado en Matlab permitió encontrar 2 estilos de descomposiciones distintas que más adelante en una fase de análisis de las proposiciones demostradas y las necesarias para demostrar el TFA en las estructuras $(M\ i^2\ ,+,*)$ se llegó a que en muchos casos, dos de estas formas de descomponer dan como resultado dos composiciones distintas del mismo número.

A continuación se incluye el código fuente de los programas necesarios para encontrar la descomposición por producto por escalar y por cambio de componente.

### 5.1. Programa para encontrar los divisores positivos de un número entero

El usuario debe ingresar un número y este programa guarda en una matriz todos los divisores positivos de este usando el residuo que se da a partir del algoritmo de la división.

```
clc,clear
display('Este programa muestra los divisores positivos de un numero a ');
a=input('Introduzca a ');
c1=0;
```

```
if a<0
    a=abs(a);
end

for i=1:1:a
  d=a/i-floor(a/i);
if d==0
     c1=c1+1;
    k(c1)=i;%almacena los divisores de a
end
end
display(k);
```

La siguiente es un equivalente a este programa como función, en lugar de mostrar al usuario los divisores del número, los almacena en una matriz:

```
function [x]=divk(a)
c1=0;
if a<0
    a=abs(a);
end
for i=1:1:a
  d=a/i-floor(a/i);
if d==0
     c1=c1+1;
    x(c1)=i;%almacena los divisores de a
end
end
end
%cuando el numero es primo el programa solo devuelve una matriz 1,2
```

Se incluye el código fuente de este programa en versión función y ejecutable para que el lector tenga una referencia de cómo convertir los programas de librerías a ejecutables y

viceversa, ya que las librerías-funciones no se pueden ejecutar por si solas, deben ser llamadas desde otro programa.

### 5.2. Programa para encontrar el máximo común divisor de dos números enteros

Este programa depende de que el programa 1 sea definido como función y este en la librería, aquí se le llama divk a la función que permite encontrar la lista de divisores de dos números, con las listas de ambos números a los cuales se les hallara el máximo común divisor, el programa selecciona los números en la lista que son iguales y los guarda en una matriz, luego de ello elije el máximo.

```
function [mx]=mcd(a,b)
if a<0
    a=abs(a);
end
if b<0
    b=abs(b);
end
c1=0;

k1=divk(a);%encontramos la lista de divisores de a y de b
k2=divk(b);

s1=size (k1);%numero de divisores de a
s2=size(k2);%numero de divisores de b
c1=0;
for i=1:1:s1(2)
 for j=1:1:s2(2)
   if k1(i)==k2(j) %identifica los divisores comunes y los almacena
    c1=c1+1;
    k3(c1)=k1(i);
   end
 end
end
```

```
s3=size(k3);
mx=k3(s3(2));
end
```

### 5.3. Programa para determinar si un número es o no divisible por cambio de componente

Este programa está hecho para trabajar con números de $M(i^2)$, ingresando el número y el valor de $i^2$determina si $(0,1)$ es divisor de $a,b$ , en tal caso el otro divisor es $(\frac{a}{r^2},b)$, esta declarado como una función y debe ser incluido en la librería.

```
function[f1]=dosprimo(a,b)
r=input('Inserte el valor de i^2 ');
d=(a/r)-floor(a/r);
if d==0

    f1(1,1)=0;
    f1(1,2)=1;
    f1(2,1)=b;
    f1(2,2)=a/r;
else

 f1=[a b];
end
end
```

### 5.4. Programa para hallar la factorización por producto por escalar

Este programa está hecho para trabajar con números de $M(i^2)$, depende del programa 2 , ingresando el número determina la descomposición de $a,b$ y la almacena en una matriz, para el caso en que $mcd\ a,b = 1$, el programa almacena el mismo número en la matriz, está declarado como y debe ser incluido en la librería.

```
function unoprimo
a=input('a')
b=input('b')
```

```
if or(a==0,b==0)==1  %comprobamos que ninguno de los dos es 0 y si es asi
el maximo es la suma
 display('algun elemento es 0')
    mx=a+b;
 dc=[a b];
else
mx=mcd(a,b);    %usamos la funcion para calcular el maximo comun divisor

if mx==1
    display('(a,b) es 1-primo');
    dc=[a b];
else
   display('(a,b) es factorizable por producto por escalar,es 1-
compuesto')
Fact=tfaritm(mx);
s4=size(Fact);%determina el numero de divisores de mcd(a,b)
s=s4(2);
for i=1:1:s
dc(i,1)=Fact(i);
dc(i,2)=0;% se almacena la factorizacion
end
dc(s+1,1)=a/mx;
dc(s+1,2)=b/mx;
end
end
end
```

### 5.5. Programa para aplicar el TFA a un número entero

Este programa dado un número entero lo descompone en sus factores primos únicos y guarda el resultado, está pensado para encontrar la descomposición por producto por escalar de un numero en escalares primos, $ka, kb = a, b \ p_1, 0 \ p_2, 0 \ \dots (p_n, 0)$, con $a, b = 1$, el programa calcula la factorización única del entero ingresado y lo guarda en una matriz, está declarado como una función y debe incluirse en las librerías.

```
function [fact]=tfaritm(a1)

if a1==0   %confirma si el dato es 0
  fact=a1;
  p=0;
else
p=1;
c1=0;
c2=0;
while p==1 %si el numero no es 0 aplica el tfa
   c2=c2+1;
    for i=1:1:a1
       d=a1/i-floor(a1/i);%condicion para determinar si un numero entero
divide o no a otro
       if d==0
         c1=c1+1;
         dv(c2,c1)=i;%almacena los divisores de a
       end
    end
    display(dv);
    s1=size(dv);
    s=s1(2);
    if s>2;
      if dv(c2,3)==0
        p=0;
      else
        p=1;
        a1=a1/dv(c2,2);
        c1=0;
      end

    fact(c2)=0;
for i=1:1:c2
    fact(i)=dv(i,2);
end
else if s==2
```

```
        fact=dv;
        p=0;
end
end
end
end
end
```

Todas estas funciones se pueden utilizar en cualquier programa que el usuario desee simplemente incluyéndolas en la misma carpeta donde creara el programa nuevo.

## 6. Conclusiones

En los conjuntos $M(i^2)$ se tienen divisores de (0,0), el neutro de la suma, lo cual provoca que varios teoremas que se tienen en los dominios de integridad no se cumplan en estos conjuntos, como el Teorema de Bézout y el Lema de Euclides necesarios para demostrar el TFA-unicidad.

En $M(i^2)$ se puede descomponer todo numero en términos de factores primos, sin embargo en general las descomposiciones halladas no serán únicas, en otras palabras se cumple una versión del TFA(existencia) pero no del TFA(unicidad).

No se pueden definir relaciones de orden total definiendo números $M\ i^2$ −positivos, y no es posible definir una relación de orden que cumpla la tricotomía usar y sea total.

Las relaciones ‘menor que’ y de divisibilidad son preordenes y determinan en el conjunto relaciones de equivalencia que cuando se hace el paso al conjunto cociente determinan dos conjuntos isomorfos a números naturales y enteros respectivamente.

La existencia en los conjuntos $M(i^2)$ de números cuya norma es la misma y no están asociados, tiene como implicación que la mayoría de las propiedades relativas a la unicidad de los elementos no se cumplan, los casos más notables se dan al estudiar el máximo común divisor y el TFA.

Aunque se cumplen la mayoría de los teoremas necesarios para construir el TFA en $M(i^2)$, análogos a los presentados en el marco de referencia de construcción de una versión del TFA en los números naturales, la existencia de divisores de (0,0) no permite concluir el resto de ellos, uno de los mayores problemas de esto fueron aquellos que dependen del residuo del algoritmo de la división de $M(i^2)$.

Se lograron varios métodos de descomposición de números, uno que determina descomposiciones válidas para cualquier conjunto sin depender del valor de $i^2$ y otras que requieren un análisis de la norma del número.

Como definimos los conjuntos $M(i^2)$, con $i^2 = r^2, r \in \mathbb{Z}, i \neq \pm r$ al aplicar la raíz cuadrada a ambos lados $\overline{i^2} = \overline{r^2} = \overline{r^2 * 1} = \overline{r^2} * \overline{1} = \pm r * \overline{1}$, lo cual nos lleva a implícitamente aceptar para que se cumpla $i \neq \pm r$ que existe un nuevo elemento $x$ tal que $x^2 = 1, x \neq \pm 1$, siguiendo esta idea, esto fue una anotación de uno de los lectores que revisaron este trabajo por lo cual en la fase final de revisión de este, confirmamos que se desarrolló teoría de números en conjuntos isomorfos a los números de Minkowski, es decir todo conjunto $M\ i^2\ , i^2 \neq 0$, es en realidad una representación u otra cara de $M(1)$.

## 7. Anexos

*Tabla de resúmenes de Teoremas y definiciones de* $M(i^2)$

| Orden cronológico | Resumen | Enunciado |
|---|---|---|
| Propiedades algebraicas | | |
| D1(3.1) | Conjuntos $A$ | $A = \{a + bi: a, b \in \mathbb{Z} \wedge i^2 = r, r \in \mathbb{Z}\}$ |
| D2(3.1) | Igualdad $a + bi$ | $\forall a + bi, c + di \in M\ i^2\ , a + bi = c + di \leftrightarrow a = c \wedge b = d$ |
| D3(3.1) | Conjuntos $M(i^2)$ | $M(i^2) = \{a + bi: a, b \in \mathbb{Z} \wedge i^2 = r^2, r \in \mathbb{Z}\}$ |
| D4(3.1) | Operaciones, suma y multiplicación | $+: \forall a + bi \in M(i^2), (a + bi) + (c + di) = (a + c) + (b + d)i$ <br> $*: \forall a + bi \in M(i^2),\ a + bi * (c + di) = (ac + bdr^2) + (bc + ad)i$ |
| Otra representación para los números $M(i^2)$ | | |
| T1(3.2) | El isomorfismo con $(a, b)$ | $(M(r^2), +, *) \approx (A_{r^2}, +', *')$ <br> $A_{r^2} = \ a, b : a, b \in \mathbb{Z}$ <br> $+': \forall a, b \in A_{r^2}, (a, b) + (c, d) = (a + c, b + d)$ <br> $*': \forall a, b \in A_{r^2},\ a, b\ *' (c, d) = (ac + bdr^2, ad + bc)$ |
| T2(3,2) | Estructura de dos operaciones | $(M(i^2), +, *)$, es un anillo conmutativo con unidad. |
| El producto por escalar | | |
| D5(3.3) | Producto por escalar | $\forall\ a, b \in M\ i^2\ \forall x \in \mathbb{Z},\ .: \mathbb{Z} * M(i^2) \rightarrow M(i^2)$ Se define como $x\ a, b = (xa, xb)$. |

| | | |
|---|---|---|
| T3(3.3) | Propiedades del producto por escalar | $\forall\ a,b\ ,(c,d) \in M(i^2)\ \forall x,y \in \mathbb{Z}$:<br>1. $x\ \ y\ \ a,b\ \ = (xy)(a,b)$<br>2. $1\ \ a,b\ \ = (a,b)$<br>3. $x\ \ \ a,b\ \ +\ \ c,d\ \ \ = x\ \ a,b\ \ + x(c,d)$<br>4. $\ x+y\ \ \ a,b\ \ = x\ \ a,b\ \ + y(a,b)$<br>5. $\ x\ \ a,b\ \ \ \ c,d\ \ = x\ \ \ a,b\ \ \ c,d\ \ \ = (a,b)(x(c,d))$<br>6. $x \neq 0\ \wedge x\ \ a,b\ \ = x(c,d) \rightarrow (a,b) = (c,d)$ |
| T4(3.3) | Elementos semi-neutros(absorbentes) y divisores la norma de un número es 0 si equivale a que el número es divisor de (0,0) | En $M(i^2)$, con $i^2 = r^2$<br>$\forall a,y,b \in \mathbb{Z},\ \pm ar,a\ \ 1 \mp ry,y\ =\ \pm ar,a\ \ y\ \ \ br,b\ \ -ar,a\ =$ $(0,0)$.<br><br>**Corolario:** $a^2 - b^2r^2\ = 0 \leftrightarrow\ \ a,b\ \ \text{es un divisor de } (0,0).$ |
| Potencias de números M$(i^2)$ | | |
| D6(3.4) | Definición de potencias | $\forall n \in \mathbb{Z}, \forall\ a,b\ \in M\ i^2$<br>$a,b\ ^0 = (1,0) \wedge\ \ a,b\ ^n = (a,b)\ \ a,b\ ^{n-1}$ |
| T5(3.4) | Binomio de Newton extendido a M$(i^2)$ | $a+bi\ ^n = \sum_{k=0}^{k=n} \binom{n}{k}\ a^k(bi)^{n-k}$<br>$(ka+kbi)^n = k^n(a+bi)^n$ |
| T6(3.4) | Potencias de $D_0$ | En $\ M\ i^2\ ,(r,1)^n =\ \ 2r\ ^{n-1}(r,1)$ con $i^2 = r^2$ |
| D7(3.4) | Semi- conjugado | $a,b\ \ = (-a,b)$ |
| El conjugado de un número | | |
| D8(3.5) | Conjugado | $a,b\ \ = (a,-b).$ |
| | | $\forall\ a,b\ \ \ c,d\ \ \ x,y\ \ \in M\ i^2\ \ \forall n > 1, n \in \mathbb{N}, i^2 = r^2, r \in \mathbb{Z}.$<br>1. $\ \ a,b\ \ =\ \ a,b\ \ = ((a,b))$<br>2. a)$(a,b)(c,d) = (a,b) *\ \ c,d\ \ =\ \ a,b\ \ *(c,d)$ |

| | | |
|---|---|---|
| T7(3.5) | Propiedades de los conjugados | b) $(a,b)(c,d) = (a,b) * \ c,d \ = \ a,b \ *(c,d)$<br>3. a)$a \ c,d \ +(x,y) = a\,(c,d) + (x,y)$<br>b) $a \ c,d \ +(x,y) = a\,(c,d) + (x,y)$<br>4. a) $a,b \ = \ a,b \ \rightarrow b = 0$<br>b) $a,b \ = (a,b) \rightarrow a = 0$<br>5. $a,b \ ^{n} = \ a,b \ ^{n}$<br>6. a) $a,b \ \ a,b \ = \ a^2 - b^2r^2, 0$<br>b) $a,b \ \ a,b \ = \ b^2r^2 - a^2, 0$<br>7. a)$(\ a,b \ ) = (\ a,b \ ) = -(a,b)$<br>b)$- \ a,b \ = (a,b) \wedge - \ a,b \ = (a,b)$ |
| $M(i^2)$ como espacio semi-normado | | |
| D9(3.6) | Norma | $\| \ \|: M(i^2) \rightarrow \mathbb{N}, \quad a,b \ \rightarrow \| \ a,b \ \| = \lvert a^2 - b^2r^2 \rvert$, con $i^2 = r^2, r \in \mathbb{Z}$ |
| T8(3.6) | Propiedades de la norma | $\forall \ a,b \ \ c,d \ \ x,y \ \in M \ i^2 \ \forall n > 1, n \in \mathbb{N}$<br>1. $\| \ a,b \ \| \geq 0$<br>2. $\| \ a,b \ \| = \| \ a,b \ \|$<br>3. $\| \ a,0 \ \| = a^2$<br>4. $\lvert \ a,b \ \ a,b \ \rvert = \| \ a,b \ \|$<br>5. $\| \ k \ a,b \ \| = k^2 \| \ a,b \ \|$<br>6. $\| \ a,b \ \ c,d \ \| = \| \ a,b \ \| \| \ c,d \ \|$<br>7. $\| \ a,b \ \ a,b \ \| = \| \ a,b \ \|^2$<br>8. $\| \ a,b \ \|^n = \| \ a,b \ ^{n} \|$ |
| T9(3.6) | Propiedad cancelativa | $\forall \ a,b \ \ c,d \ \ e,f \ \in M \ i^2 \ , \| \ a,b \ \| \neq 0,$ |

| | | |
|---|---|---|
| | | $a,b\ \ c,d\ =\ a,b\ \ e,f\ \rightarrow\ c,d\ =(e,f).$ |
| El sentido de iteración en las operaciones | | |
| D10(3.7) | Multiplicación y potencia como iteraciones | Sea $a,b\ \in M(r^2)$ y $n$ un número natural:<br>$n=0,n\ a,b\ =\ 0{,}0\ ,\ a,b\ ^{n}=(1,0)$<br>$n>0,n+1\ a,b\ =n\ a,b\ +\ a,b\ ,\ a,b\ ^{n+`1}=\ a,b\ ^{n}(a,b)$ |
| T10(3.7) | Propiedades de la potenciación | $\forall\ a,b\ \ c,d\ \in M\ r^2\ \forall n,m\in\mathbb{N}$<br>1. $((a,b)(c,d))^n=(a,b)^n(c,d)^n$<br>2. $(a,b)^{m+n}=(a,b)^m(a,b)^n$<br>3. $((a,b)^m)^n=(a,b)^{mn}$<br>4. $(ka,kb)^n=k^n(a,b)^n$ |
| Ecuaciones en los $M\ i^2$ | | |
| T11(3.8) | Solución a ecuaciones lineales con la operación suma | $a,b\ ,\ c,d\ \in\ M\ i^2\ ,\exists!\ (x,y)\in\ M\ i^2\ :\ (a,b)+(x,y)=$<br>$(c,d)\ \ x,y\ =\ c,d\ -(a,b)$ |
| Divisibilidad en $M(i^2)$:Definicion y propiedades | | |
| D11(4.1) | Divisibilidad | $a,b\ \vert_{r^2}\ c,d\ \leftrightarrow\exists\ e,f\ \in M\ i^2\ :\ a,b\ \ e,f\ =\ c,d\ ,i^{\ 2}=r^2$ |
| T12(4.1) | Propiedades de la divisibilidad | $\forall\ a,b\ \ c,d\ \ (e,f)\ \ x_1,x_2\ \ y_1,y_2\ \in M\ i^2\ ,\forall x,y\in\mathbb{Z}:$<br>1. $(a,b)\ \vert(0,0)\wedge\pm(a,b)\ \vert(a,b)$<br>2. $((a,b)\ \vert(c,d)\wedge(c,d)\ \vert(e,f))\rightarrow(a,b)\ \vert(e,f)$<br>3. $a,b\ \ c,d\ \wedge\ a,b\ \ e,f\ \rightarrow\ a,b\ \ c,d\ \ x_1,x_2\ +$<br>$e,f\ \ y_1,y_2\ \wedge\ a,b\ \ x\ c,d\ +y\ e,f$<br>4. $a,b\ \ c,d\ \rightarrow\Vert\ \ a,b\ \ \Vert\ \ \Vert\ \ c,d\ \ \Vert$ |
| T13(4.1) | Divisores por producto por escalar | $(a,b)$ tiene al menos $d(mcd(a,b))$ divisores por cada unidad en $M(i^2)$ |
| Unidades y asociados | | |
| D12(4.2) | Unidad | $(a,b)$ es una unidad en $M\ i^2\ \ \leftrightarrow\forall\ (x,y)\in M\ i^2\ ,\ (a,b)\vert(x,y)$ |
| T14(4.2) | Conjunto de unidades | El conjunto de unidades en $M(i^2)$ es:<br>1. $U=\ \ 1{,}0\ ,\ -1{,}0\ \ \cup\{\ x,y\ \epsilon M\ i^2\ :x=\pm1\}$ en $M(0)$ |

| | | |
|---|---|---|
| | | 2. $U = \ 1,0\ ,\ -1,0\ ,\ 0,1\ ,(0,-1)$ en $M\ 1$<br>3. $U = \ 1,0\ ,\ -1,0$ para $M\ i^2\ , i^2 > 1.$<br>4. $\| \ x,y\ \| = 1 \leftrightarrow$ x, y es unidad. |
| T15(4.2) | Propiedades de las unidades | $\forall (u,v) \in M\ i^2\ ,\ (u,v)$ unidad, $\exists!\ u,v\ ^{-1} \in M\ i^2\ ,\ u,v\ ^{-1}$ unidad. |
| D13(4.2) | Primera forma de Asociados | $\forall\ a,b\ \ c,d\ \in M\ i^2\ ,\ a,b \sim c,d \leftrightarrow$<br>$a,b\ = \ c,d\ \ u,v\ ,\ u,v$ es una unidad |
| T16(4.2) | Segunda forma de asociados | $\forall\ a,b\ \ c,d\ \in M\ i^2\ ,\ a,b \sim c,d$<br>$\leftrightarrow\ a,b \mid c,d\ \wedge\ c,d \mid a,b$ |
| T17(4.2) | Propiedades de las relaciones $\mid, \sim$ | La relación 'ser divisible' $\mid$ es una relación de pre-orden y la relación 'ser asociado' $\sim$ es una relación de equivalencia: |
| T18(4.2) | Dos números asociados tienen los mismos divisores | $(a,b) \sim (c,d) \wedge (x,y) \mid (a,b) \rightarrow (x,y) \mid (c,d)$ |
| D14(4.2) | Número primo y número compuesto. | Un número $a,b\ \in M\ i^2\ , (a,b) \neq u$ unidad, es primo si y solamente si es divisible únicamente por las unidades del conjunto y sus asociados. Si $a,b$ no es primo diremos que es compuesto. |
| Los divisores de $(p,0)$ | | |
| T19(4.3) | $(p,0)$ ¿primo o | En $M\ i^2\ , i^2 = r^2, r\ \in \mathbb{Z}$, el número $(p,0)$:<br>1. Es primo si $p = 2$<br>2. Con $r^2 = 0$, es primo.<br>3. Con $r^2 = 1$, no es primo, tomando $S = (\frac{p+1}{2}, \frac{p-1}{2})$, tiene una descomposición única salvo asociados y unidades, como $S * S$, las descomposiciones en términos de los números asociados a $S$ son $S * S$, $(-S) * (S)$, $(S(0,1)) * (S(0,1))$, $(S(0,-1)) * (S(0,1))$,$(p,0)$ tiene 16 divisores.<br>4. Con $r^2 > 1$, es primo si $r \nmid \frac{p+1}{2} \wedge\ r \nmid \frac{p-1}{2}$. |

| | | |
|---|---|---|
| | compuesto? | 5. Con $r^2 > 1$, si $(p, 0)$ no es primo ocurre que $r \mid \frac{p-1}{2} \veebar r \mid \frac{p+1}{2}$(se da alguna de las dos condiciones pero no ambas), tomando $S1 = (\frac{p+1}{2}, \frac{p-1}{2r})$ si se da la primera condición o $S2 = (\frac{p-1}{2}, \frac{p+1}{2r})$ si se da la segunda, tiene una descomposición única salvo unidades y asociados como $S * S \veebar (S2) * (S2)$, las descomposiciones asociadas no idénticas son $-S1 * S1 \veebar -S2 * (S2)$, $p, 0$ tiene 8 divisores. |
| Divisores de un número usando normas | | |
| T20(4.4) | Dos números con la misma norma o son asociados o ninguno divide al otro | $\forall\ a,b\ ,\ c,d\ \in M\ i^2\ , \|\ a,b\ \| = \|\ c,d\ \| \rightarrow (\ a,b \sim c,d \veebar a,b \nmid c,d \wedge c,d \nmid a,b)$ |
| T21(4.4) | Los números de norma prima son primos | $\forall\ a,b\ \in M\ i^2\ , \|\ a,b\ \| = p, p \in \mathbb{N}$ , $p$ primo $\rightarrow\ a,b\ $ es primo. |
| T22(4.4) | No hay números de norma 2i | $\nexists\ a,b\ \in M\ i^2 : \|\ a,b\ \| = 2l, l$ impar. |
| D15(4.4) | División escalar | $\forall\ a,b\ \in\ M\ i^2\ \forall x \in\ \mathbb{Z}$, Se define la división escalar $/ : \mathbb{Z} * M(i^2) \rightarrow M(i^2)$ como $\frac{(a,b)}{x(1,0)} = \frac{(a,b)}{x}$, $\frac{a,b}{x} = \frac{a}{x}, \frac{b}{x}\ si\ x\ a \wedge x\ b, \frac{a,b}{x} = (\frac{a-r_1}{x}, \frac{b-r_2}{x})$ si $x \nmid a \vee x \nmid b$, siendo $r_1, r_2$, los residuos de aplicar el algoritmo de la división en $\mathbb{Z}$ a $a,b$ dividendos respectivamente con $x$ como divisor. |
| T23(4.4) | Isomorfismo entre $\mathbb{Z}$ y un subconjunto de | Toda estructura $M(i^2)$ tiene un subconjunto isomorfo a $\mathbb{Z}$. Tal conjunto es $A = \{\ x,y\ \in M\ i^2\ : y = 0\}$ con las operaciones |

| | | |
|---|---|---|
| | $M(i^2)$ | dadas por $M\ i^2$ . |
| D16(4.4) | División | $\forall\ a,b\ \ c,d\ \in M\ i^2\ ,\|\ \ c,d\ \|\neq 0$, Se define la división $/: M(i^2) * M(i^2) \to M(i^2)$ como $\frac{(a,b)}{(c,d)} = \frac{(a,b)(c,d)}{(c,d)(c,d)}$ Si $(a,b)\ \|(c,d)$ diremos que la división es exacta. |
| Relaciones de orden en $M(i^2)$ | | |
| D17(4.5) | Condiciones de los números positivos | Un conjunto de números positivos $P$ para $M(i^2)$ debe cumplir: i. $(a,b) \in P \to (-a,-b) \notin P$ ii. $a,b\ ,\ c,d\ \in P \to\ a,b\ +(c,d) \in P$ iii. $a,b\ ,\ c,d\ \in P \to\ a,b\ *\ c,d\ \in P$ |
| T24(4.5) | Todo número no nulo es distinto a su inverso | $\forall\ a,b\ \in M\ i^2 : (a,b) \neq (0,0) \to (a,b) \neq (-a,-b)$ |
| T25(4.5) | El conjunto de divisores de 0 es cerrado respecto a * | $\forall\ a,b\ \in D_0, \forall\ c,d\ \in M\ i^2\ :\ a,b\ *(c,d) \in D_0$ |
| D18(4.5) | Propiedad de tricotomía en $M\ i^2$ | Si $\forall\ a,b\ \in M\ i^2$ , con un conjunto de los números positivos $P$,se cumple una y solo una de las siguientes condiciones: i. $(a,b) \in P$ ii. $(-a,-b) \in P$ iii. $(a,b) \in D_0$ Entonces diremos que el conjunto $M\ i^2$ está totalmente ordenado. |
| T26(4.5) | La norma de una suma | $\forall\ a,b\ ,\ c,d\ \in M\ i^2$ : $a,b\ +\ c,d\ = a^2 - br^2 + c^2 - dr^2 + 2(ac - bdr^2)$ |
| D19(4.5) | Definición de $\leq$ | $\forall\ a,b\ ,\ c,d\ \in M\ i^2 : a,b \leq c,d \leftrightarrow a,b \leq c,d$ , $a,b < c,d$ significa $a,b < c,d$ |

| | | |
|---|---|---|
| | | A $a,b \geq c,d$ le daremos el significado $c,d \leq a,b$ . |
| T27(4.5) | $\leq$ es pre orden | $\leq$ es una relación de pre orden en $M\ i^2$ |
| D20(4.5) | Definición de $\approx$ | $\forall\ a,b\ ,\ c,d\ \in M\ i^2 : a,b \approx c,d \leftrightarrow (\ a,b \leq c,d \wedge c,d \leq a,b\ )$ |
| T28(4.5) | Segunda forma de la definición de $\approx$ | $a,b \approx c,d \leftrightarrow (a,b) = (c,d)$ |
| T29(4.5) | $\approx$ es de equivalencia | $\approx$ es una relación de equivalencia |
| T30(4.5) | Propiedades de $\leq$ y $\approx$ | $\forall\ a,b\ ,\ c,d\ ,\ e,f\ \in M\ i^2\ ,\ e,f\ \notin D_0$:<br>1. $a,b < (c,d) \leftrightarrow a,b\ (e,f) < (c,d)(e,f)$<br>Corolario: $\forall x,y \in \mathbb{Z}: x \leq y \rightarrow x,0 \leq (y,0)$<br>2. $\exists\ x,y\ \in M\ i^2\ ,\forall\ a,b\ \in M\ i^2 : x,y \leq a,b \rightarrow x,y \in D_0$<br>3. $a,b \leq a,b^{\ 2}$<br>4. $a,b \mid c,d \rightarrow a,b \leq (c,d)$<br>Corolario: $a,b \sim c,d \rightarrow a,b \approx c,d$ |
| D21(4.6) | Definición de cotas, mínimo y máximo de un conjunto | Sea $S \subseteq M\ i^2\ , S \neq \emptyset, \leq$ una relación de pre orden en $M\ i^2$ :<br>$(x,y) \in M(i^2)$ es una cota superior de $S$ si y solamente si $\forall\ u,v\ \in S,\ u,v\ \leq (x,y).$<br>$(x,y) \in M(i^2)$ es una cota inferior de $S$ si y solamente si $\forall y \in S,\ x,y\ \leq (u,v).$<br>Si $(x,y)$ es una cota superior de $S$ y $(x,y) \in S$, se dice que $(x,y)$ es máximo de $S$, esto se nota $(x,y) = \max S$; análogamente si $(x,y)$ es una cota inferior de $S$ y $(x,y) \in S$, se dice que $(x,y)$ es un mínimo de $S$ y se nota $(x,y) = \min S$. |
| T31(4.6) | Principio del buen orden | Todo conjunto no vacío de $M\ i^2$ tiene mínimo |
| T32(4.6) | Los números que son mínimos tienen la misma norma | $\forall A \subseteq M\ i^2\ , A \neq \emptyset$: $a,b = \min A \wedge c,d = \min A \rightarrow a,b \approx c,d$ |

| | | |
|---|---|---|
| T33(4.6) | Equivalente para máximos del PBO | Todo conjunto no vacío de $M\ i^2$ es finito tiene máximo. |
| T34(4.6) | Todos los números que son máximos tienen la misma norma | $\forall A \subseteq M\ i^2\ , A \neq \emptyset$: $a,b\ = \max A \wedge\ c,d\ = \max A\ \rightarrow$ $a,b\ \approx\ c,d$ |
| D22(4.6) | El conjunto máximo y el conjunto mínimo de un conjunto | $MIN\ A = \{(x,y) \in A: (x,y = \min A)\}$ $MAX\ A = \{(x,y) \in A: (x,y = \max A)\}$ |
| T35(4.6) | PBO para los conjuntos máximo y mínimo | 1. Todo subconjunto $A$ no vacío de $M\ i^2$ tiene un subconjunto $MIN\ A$ no vacío.<br>2. Todo conjunto $A$ finito no vacío de $M\ i^2$ tiene un subconjunto $MAX\ A$ no vacío<br>3. $MAX\ A \subseteq A \wedge MIN\ A \subseteq A$ |
| T36(4.6) | Los conjuntos máximo y mínimo son únicos. | $\forall A \subseteq M\ i^2\ , A \neq \emptyset: MIN\ A$ es único y $MAX\ A$ es único. |
| D23(4.6) | Divisores comunes | $\forall\ a,b\ (c,d)\ x,y\ \in M\ i^2 : (x,y)$ es divisor común de $a,b\ (c,d) \leftrightarrow\ x,y\ \vert(a,b) \wedge\ x,y\ \vert(c,d)$ |
| D24(4.6) | Conjunto máximo común divisor de dos números | $D =\ \ x,y\ \in M\ i^2\ :\ x,y\ \ a,b\ \wedge\ x,y\ \ c,d\ \ ,$ $M = MCD\ \ a,b\ \ c,d\ \ \leftrightarrow M = MAX\ D$ |
| T37(4.6) | Unicidad de MCD | $MCD(\ a,b\ ,(c,d))$ es único. |
| T38(4.6) | Se conocen 4 números de la misma norma no asociados 3 a 3 por ~ pero si por ≈ | $\forall\ a,b\ \in M\ i^2\ ,\ a,b\ \approx\ a,b\ \approx\ a,b\ \approx -(a,b)$ |

| | | |
|---|---|---|
| T39(4.6) | Máximo común divisor y conjugados | $\forall\ a,b\ \ c,d\ \in M\ i^2\ ,(x,y) \in\ MCD\ \ a,b\ \ c,d\ \ \rightarrow (x,y)\ \in\ MCD\ \ a,b\ ,\ c,d$ |
| T40(4.6) | Un número y su conjugado tienen divisores tales que cada uno es el conjugado del otro | $\forall\ a,b\ (x,y) \in M\ i^2\ ,(x,y)\|\ a,b\ \rightarrow (x,y)\|\ a,b$ |
| T41(4.6) | Números que pueden ser divisores (y asociados) de sus conjugados | $\forall\ a,b\ \in M\ i^2\ :(a,b)\|\ a,b$ implica que:<br>3. $i^2 = 0$ entonces $a,b\ = (2b,-b) \vee\ a,b\ = (a,0)$<br>4. $i^2 > 0$ entonces $a,b\ = (a,0)$ |
| D25(4.6) | Primos relativos | $a,b\ ,(c,d)$ son primos relativos$\leftrightarrow MCD\ \ a,b\ ,\ c,d\ \ = U$ |
| T42(4.7) | Descomposiciones distintas de un número | Sea $a,b\ ,\ (a,b)\ = n, n = p_2 p_2 \dots p_n$ su descomposición en factores primos, las dos descomposiciones de $(n,0)$:<br>$n,0\ = (p_2,0)(p_2,0) \dots (p_n,0)$<br>$n,0\ = (a,b)(a,-b)$<br>Son dos descomposiciones distintas no asociadas de $(n,0)$ si y solamente si $MCD\ \ a,b\ ,\ p_k,0\ \ = U$ para algún $1 \leq k \leq n$<br>**Corolario:** Si $(n,0)$ no tiene descomposición única en $M(i^2)$ entonces $(na,nb)$ no tiene descomposición única en $M(i^2)$. |
| T43(4.7) | Los números compuestos son divisibles por un primo | Todo número en $M\ i^2$ compuesto tiene al menos un divisor primo |
| | Teorema | Todo número compuesto en $M\ i^2$ puede descomponerse como |

| | | |
|---|---|---|
| TFA(4.7) | fundamental-existencia | producto de factores primos. |

# 8.Bibliografía


Arrondo, E. (2009). *Apuntes de Teoría de Números.* Universidad Complutense de Madrid, Madrid. Recuperado el Mayo de 2016, de http://www.mat.ucm.es/~arrondo/ten.pdf

Brausín, M., & Pérez, A. (2012). *Estudio de Congruencias en Números Gussianos Duales.* Trabajo de grado, Universidad Pedagógica Nacional.

Busqué, C., Saorín, M., & Simón, J. (2011-2012). *Curso de Conjuntos y números.Guiones de clase.* Recuperado el 4 de Junio de 2016, de http://www.um.es/docencia/jsimon/depmat/2011-2012/CyN/GuionesdeClase.pdf

*CALCULUS, One Variable- Calculus, with an introduction to Linear Algebra* (Vol. 1). (1984). Barcelona-España: REVERTÉ, S.A.

*Disfruta Las Matemáticas.com*. (2011). Recuperado el Diciembre de 2015, de http://www.disfrutalasmatematicas.com/numeros/pitagoricas-ternas.html

Gonzáles, F. (2004). *Apuntes de Matemática Discreta-10. Divisibilidad.Algoritmo de la División.* Universidad de Cádiz, Andalucía. Recuperado el Octubre de 2015, de http://www2.uca.es/matematicas/Docencia/ESI/1710003/Apuntes/Leccion1.pdf

Gonzáles, F. (2004). *Apuntes de Matemática Discreta-11.Teorema Fundamental de la Aritmética.* Andalucía. Recuperado el Noviembre de 2015, de http://www2.uca.es/matematicas/Docencia/ESI/1710003/Apuntes/Leccion11.pdf

Ivorra, C. (2011). *Teoría de Números.* Valencia, España. Recuperado el Septiembre de 2015, de https://www.uv.es/ivorra/Libros/Numeros.pdf

LeVeque, W. (1968). *Teoría Elemental de los Números.* Universidad de Michigan . México: Herrero Hermanos, Sucs, S.A.

Rafael, F., & Isaacs, G. (2005). *Divisibilidad.* Universidad Industrial de Santander , Bogotá D.C. Recuperado el 20 de Marzo de 2016, de http://matematicas.uis.edu.co/~risaacs/AMA/doc/lindifaanti.pdf

Rubiano, G., Jiménez, L., & Rubiano, G. (2004). *Teoría de Números para principìantes* (2 ed.). (B. Jiménez, & J. Gordillo, Edits.) Bogotá D.C, Colombia : Universidad Nacional de Colombia.

Recuperado el Diciembre de 2015, de http://ciencias.uis.edu.co/conjuntos/doc/Tmerospaprinci.pdf

Sanchez, Y., Angel, L., & Luque, C. (2013). *¿Son necesarios los enteros para demostrar el Teorema Fundamental de la Aritmetica?* Bogotá D.C.

Sorándo, J. (Sin fecha). *Matemáticas en tu mundo.* Recuperado el Marzo de 2016, de La Teoría de Números: http://catedu.es/matematicas_mundo/HISTORIA/2_Teoria_Numeros.pdf

Urbina, L. (2006). *Notas en Desigualdades.* Asociación Venezolana de Competencias en Matemáticas(ACM), Venezuela. Recuperado el 16 de Abril de 2016, de http://www.acm.ciens.ucv.ve/main/entrenamiento/material/desigualdades_urbina.pdf