Facultad de Ciencia y Tecnología
Departamento de Matemáticas

UNA CARACTERIZACIÓN DE NÚMEROS PRIMOS EN $\mathbb{Z}(\sqrt{2})$ DESDE EL PROCESO DE ANALIZAR

Para optar por el título de:
Licenciado en Matemáticas

Presentado por:
Rubén Darío Torres García
Harry Cristhian Torres Moreno

Asesor: Juan Carlos Ávila Mahecha

Bogotá, Enero de 2016

Dedicado a mi madre Martha Moreno (QEPD) y a mi padre Adonaí Torres
Harry C. Torres

Dedicado a mi madre Teresa García y a Camila Mondragón
Rubén D. Torres

Agradecimientos

Agradecemos a los profesores del seminario de álgebra de la Universidad Pedagógica Nacional y en especial al profesor Juan Carlos Ávila Mahecha por sus inmensos aportes en este trabajo.

RESUMEN ANALÍTICO EN EDUCACIÓN - RAE

1. Información General	
Tipo de documento	Trabajo de Grado
Acceso al documento	Universidad Pedagógica Nacional. Biblioteca Central
Título del documento	Una caracterización de números primos en el conjunto $\mathbb{Z}(\sqrt{2})$ Desde el proceso de analizar
Autor(es)	Torres García, Rubén Darío; Torres Moreno, Harry Cristhian
Director	Ávila Mahecha, Juan Carlos
Publicación	Bogotá. Universidad Pedagógica Nacional, 2015. 77 p.
Unidad Patrocinante	Universidad Pedagógica Nacional.
Palabras Claves	DIVISIBILIDAD, UNIDAD, NÚMERO PRIMO, TEOREMA FUNDAMENTAL DE LA ARITMÉTICA

2. Descripción

Este trabajo busca caracterizar y definir algunos elementos diferenciados en el conjunto $\mathbb{Z}(\sqrt{2})$, desde el proceso de analizar, cuya característica principal radica en que todos sus elementos poseen infinitos divisores. Los elementos diferenciados estudiados en este trabajo son: Unidades, números primos y números compuestos. Además, se expone un acercamiento al teorema homólogo al teorema fundamental de la aritmética en $\mathbb{Z}(\sqrt{2})$.

3. Fuentes

1. Entero Gaussiano. Disponible en: es.wikipedia.org, Directorio: wiki, File: Entero_gaussiano.

2. Jiménez L., Gordillo J. & Rubiano G. (2004). Teoría de números (para principiantes). Bogotá: Universidad Nacional de Colombia, Sede Bogotá. Facultad de Ciencias.

3. Lefèvre V. (1993). Entiers de Gauss. Disponible en: www.vinc17.org, Directorio: math, File: entgauss.pdf.

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

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

6. Parra R. ECUACION PELL. Disponible en: hojamat.es, Directorio: parra, File: pell.pdf

7. Pettofrezzo A. & Byrkit D. (1972). INTRODUCCION A LA TEORIA DE LOS NUMEROS. España: Ediciones del Castillo, S. A.

4. Contenidos

En el capítulo 1 se presenta una breve introducción que expone un poco sobre el trabajo que ha venido desarrollando el seminario de álgebra de la Universidad Pedagógica Nacional en los últimos semestres. El capítulo 2 alude a los conceptos preliminares donde se define el conjunto $\mathbb{Z}(\sqrt{2})$, además se define la suma, la multiplicación y la relación de divisibilidad en éste conjunto. En el capítulo 3 se hace un estudio detallado sobre las Unidades en $\mathbb{Z}(\sqrt{2})$, en este capítulo se caracterizan las unidades y se establece un algoritmo mediante la función N para identificar cuando un elemento en $\mathbb{Z}(\sqrt{2})$ es una unidad o no. En el capítulo 4 se definen y se caracterizan algunos números primos en $\mathbb{Z}(\sqrt{2})$, además, se establecen algoritmos mediante la función N para identificar números primos en este conjunto. En el capítulo 5 se presentan algunos criterios de divisibilidad. En el capítulo 6 se realiza una propuesta que genera un acercamiento al teorema homólogo al teorema fundamental de la aritmética en $\mathbb{Z}(\sqrt{2})$. En el capítulo 7 se proponen algunos temas de estudios para trabajos posteriores. Por último en el capítulo 8 y 9 se presentan las conclusiones obtenidas en el desarrollo de este trabajo y las referencias bibliográficas que se usaron.

5. Metodología

Las ideas fundamentales de este trabajo surgen de las distintas sesiones que se desarrollaron en el seminario de álgebra del departamento de matemáticas de la Universidad Pedagógica Nacional en los últimos semestres. Inicialmente se realizó una exploración mediante el uso de dos software, el primero elaborado por el estudiante de la licenciatura en matemáticas, Nicolás Mahecha y el segundo elaborado por el profesor Yeison Sánchez del departamento de matemáticas de la Universidad Pedagógica Nacional, seguidamente, con base a los resultados obtenidos mediante la exploración de los dos software, se realizaron algunas conjeturas y posteriormente se procedió a demostrarlas en su mayoría. Por otra parte, algunas definiciones fundamentales se tomaron en base a un consenso que se realizó en el seminario de álgebra, dado que el objetivo de éste es establecer algunas definiciones sobre algunos elementos de la teoría de números en estructuras algebraicas no usuales.

6. Conclusiones

1. La principal característica del conjunto $\mathbb{Z}(\sqrt{2})$ radica en que todos sus elementos tienen infinitos divisores, diferente a lo que sucede en el conjunto de los números naturales y enteros. Lo cual representa un cambio en torno a la noción que se tenía respecto a las unidades, números primos y números compuestos.

2. Una forma que permite encontrar unidades en $\mathbb{Z}(\sqrt{2})$ es mediante el uso de la ecuación de Pell-Fermat $a^2 - 2b^2 = \pm 1$, donde hay infinitas soluciones, así, se tiene que en $\mathbb{Z}(\sqrt{2})$ hay infinitas unidades, muy distinto a lo que se sucede en el conjunto de los números naturales y enteros.

3. Un algoritmo que permite identificar si una pareja de la forma $(2n, m)$ es primo o no es

verificar que $(2\mathrm{n},\mathrm{m})|(0,1)$, si $(2\mathrm{n},\mathrm{m})|(0,1)$ entonces $(2\mathrm{n},\mathrm{m})$ es primo.

4. Un algoritmo para identificar si $(a,b) \in \mathbb{Z}(\sqrt{2})$ es primo o no, sin necesidad de elaborar una lista de sus divisores, es aplicando la función N, así, si $\mathrm{N}(\mathrm{a},\mathrm{b}) = \mathrm{x}$ donde $\mathrm{x} = |\mathrm{p}|$ siendo p un número primo ó $\mathrm{x} = \mathrm{p}^2$ donde p es un número primo de la forma $4n+1$ con n impar ó $\mathrm{x} = \mathrm{p}^2$ donde p es un número primo de la forma $4n+3$ con n par, entonces (a,b) es primo.

5. En N_2, bajo la definición usual de unidad, se tiene que análogamente al conjunto de los números naturales, 1 es la unidad.

6. En N_2, a pesar de ser un subconjunto de los números naturales, existen elementos que son primos en este conjunto y que a su vez no son números primos en los naturales.

7. En $\mathbb{Z}(\sqrt{2})$ se pueden establecer criterios de divisibilidad.

8. Es posible realizar un acercamiento al teorema homólogo al teorema fundamental de la aritmética en $\mathbb{Z}(\sqrt{2})$

9. Como futuros profesores de matemáticas, es importante reflexionar en torno a la noción que se tiene de unidad, número primo y número compuesto, por lo tanto, las definiciones usuales que se presentan sobre estos elementos diferenciados no siempre funcionan.

Elaborado por:	Torres García, Rubén Darío; Torres Moreno, Harry Cristhian
Revisado por:	Ávila Mahecha, Juan Carlos

Fecha de elaboración del Resumen:	20	01	2016

Índice general

Objetivos

Objetivo General

Definir y caracterizar algunos números primos en $\mathbb{Z}(\sqrt{2})$.

Objetivos Específicos

- Indagar y concertar definiciones de unidades y números primos en conjuntos numéricos conocidos observando si estos funcionan para el conjunto $\mathbb{Z}(\sqrt{2})$
- Definir y caracterizar las unidades en $\mathbb{Z}(\sqrt{2})$
- Establecer algoritmos que permitan identificar unidades en $\mathbb{Z}(\sqrt{2})$
- Establecer algoritmos que permitan identificar números primos en $\mathbb{Z}(\sqrt{2})$.
- Establecer criterios de divisibilidad en $\mathbb{Z}(\sqrt{2})$.
- Definir y caracteriza algunos números compuestos en $\mathbb{Z}(\sqrt{2})$
- Establecer un acercamiento al teorema homólogo al teorema fundamental de la aritmética en $\mathbb{Z}(\sqrt{2})$

Capítulo 1

Introducción

El Grupo de Álgebra de la Universidad Pedagógica Nacional estudia actualmente el proceso matemático de analizar, una estrategia utilizada para desarrollar su investigación, y a su vez la motivación por parte de los estudiantes, es a través del seminario de álgebra, espacio de libre asistencia en el cual sus participantes (estudiantes de la licenciatura) han adoptado problemas que tienen que ver con la divisibilidad en diversos conjuntos no usuales y con ello intentar responder a las preguntas: ¿qué es un número primo? ¿qué es un número compuesto? ¿existen teoremas homólogos al teorema fundamental de la aritmética? etc.

En terminos generales, el proceso de analizar es aquel que busca describir los objetos de una estructura matemática en términos de sus partes. Es así, como el grupo de álgebra se ha planteado estudiar el proceso de analizar desde el objeto matemático de la divisibilidad en estructuras algebraicas no usuales, partiendos de ejemplos conocidos.

De esta forma es como el presente trabajo surgió, del estudio adelantado en el seminario, de conjuntos de la forma:

$$\mathbb{Z}(k) = \{a + bk \mid a, b, \in \mathbb{Z}; k^2 \in \mathbb{Z} \ \ y \ \ k \notin \mathbb{Z}\}$$

Sobre estas estructuras se definen un par de operaciones y con base en ellas se busca caracterizar los números primos de dicho conjunto. Para ello se establecen ciertos elementos diferenciados o especiales del conjunto, entre los cuales, están aquellos a los que se les denomina primos.

Luego de esto, se plantea el problema de poder descomponer un número que no pertenezca a los elementos diferenciados en producto o suma de números primos de la estructura, con el fin de encontrar un teorema análogo al

teorema fundamental de la aritmética en dicha estructura.

Capítulo 2

Conceptos preliminares

2.1. El conjunto $\mathbb{Z}(\sqrt{2})$

Uno de los objetos de estudio para el seminario de álgebra de la Universidad Pedagógica Nacional se centra en definir algunos elementos de la teoría de números en estructuras algebraicas no usuales; en particular, en el seminario, se estudiaron los conjuntos $\mathbb{Z}(\sqrt{k})$.

Se puede ampliar el conjunto de los números enteros a un conjunto que los incluya y que involucren a $\sqrt{k}$ en nuevos números de la forma

$$z = a + bk$$

donde a y b son números enteros, $k^2 \in \mathbb{Z}$ y $k \notin \mathbb{Z}$, al conjunto de estos elementos se les denotará por $\mathbb{Z}(k)$.

Para encontrar resultados generales sobre las estructuras $\mathbb{Z}(\sqrt{k})$, es importante realizar algunos estudios sobre casos particulares, así, este trabajo busca realizar un estudio detallado sobre el conjunto $\mathbb{Z}(\sqrt{2})$.

El conjunto $\mathbb{Z}(\sqrt{2})$ es el conjunto de los números de la forma:

$$z = a + b\sqrt{2}$$

donde a y b son números enteros, $k^2 = 2 \in \mathbb{Z}$ y $\sqrt{2} \notin \mathbb{Z}$

2.2. Parejas Ordenadas

Para el desarrollo de este trabajo, se denotará el número $a + bk$ mediante la pareja ordenada (a, b), donde la primera componente será la parte entera y la segunda componente será el número entero que acompaña a $k = \sqrt{2}$.

2.3. Igualdad entre números de $\mathbb{Z}(\sqrt{2})$

Definición 2.1 Dos números $z = a + bk$ y $w = c + dk$ son iguales si y sólo si $a = c$ y $b = d$. Reescribiendo esta definición en términos de parejas ordenadas, se tiene que $(a, b) = (c, d)$ si y sólo si $a = c$ y $b = d$.

2.4. Suma en el conjunto de $\mathbb{Z}(\sqrt{2})$

Sea $a + bk$ y $c + dk$ que pertenecen a $\mathbb{Z}(\sqrt{2})$, es natural pensar que la suma de estos elementos se realiza sumando término a término de forma usual, luego:

$$(a + bk) + (c + dk) = (a + c) + (b + d)k$$

así, es conveniente definir la suma en $\mathbb{Z}(\sqrt{2})$ de la siguiente forma:

Definición 2.2 Suma: Sean (a, b) y (c, d) que pertenecen al conjunto $\mathbb{Z}(\sqrt{2})$, la suma de estos números se define como:

$$(a, b) + (c, d) = (a + c, b + d)$$

Es importante realizar una aclaración respecto a la notación usada para definir la suma en $\mathbb{Z}(\sqrt{2})$; el símbolo "+" que está dentro de las parejas ordenadas sí representa la suma usual de los números enteros, sin embargo el simbolo "+" que se encuentra por fuera y entre las parejas ordenadas no tiene el mismo significado que la suma usual de números enteros, este es precisamente el símbolo usado para definir la operación, que por costumbre, también llamamos suma.

2.4.1. Propiedades de la suma en $\mathbb{Z}(\sqrt{2})$

Teorema 2.1 Propiedad conmutativa: Sean (a, b) y (c, d) que pertenecen a $\mathbb{Z}(\sqrt{2})$ se cumple que $(a, b) + (c, d) = (c, d) + (a, b)$.

Demostración: Aplicando la definición de suma en el conjunto de $\mathbb{Z}(\sqrt{2})$, se tiene:

$$(a, b) + (c, d) = (a + c, b + d)$$

por la propiedad conmutativa de la suma en los números enteros:

$$(a, b) + (c, d) = (c + a, d + b)$$

por la definición de suma en el conjunto de $\mathbb{Z}(\sqrt{2})$ se obtiene la siguiente igualdad:

$$(a, b) + (c, d) = (c, d) + (a, b)$$

Por lo tanto se cumple la propiedad conmutativa de la suma en $\mathbb{Z}(\sqrt{2})$

Teorema 2.2 Propiedad asociativa: La suma en el conjunto $\mathbb{Z}(\sqrt{2})$ cumple la propiedad asociativa.

Demostración: Sean (a, b), (c, d) y (e, f) que pertenecen al conjunto $\mathbb{Z}(\sqrt{2})$, luego, por definición de suma en $\mathbb{Z}(\sqrt{2})$ se tiene:

$$((a, b) + (c, d)) + (e, f) = (a + c, b + d) + (e, f)$$

aplicando de nuevo la definición de suma en $\mathbb{Z}(\sqrt{2})$, se tiene la siguiente igualdad:

$$((a, b) + (c, d)) + (e, f) = ((a + c) + e, (b + d) + f)$$

utilizando la propiedad asociativa de la suma de los números enteros:

$$((a, b) + (c, d)) + (e, f) = (a + (c + e), b + (d + f))$$

aplicando dos veces la definición de adición en $\mathbb{Z}(\sqrt{2})$:

$$((a, b) + (c, d)) + (e, f) = (a, b) + (c + e, d + f)$$

$$((a, b) + (c, d)) + (e, f) = (a, b) + ((c, d) + (e, f)).$$

Por lo tanto, se cumple la propiedad asociativa de la suma en $\mathbb{Z}(\sqrt{2})$.

Una vez demostrada la propiedad asociativa de la suma en $\mathbb{Z}(\sqrt{2})$, se procede a verificar si en este conjunto existe elemento neutro o no bajo la suma, para esto, sean (a, b) y (x, y) que pertenecen al conjunto de $\mathbb{Z}(\sqrt{2})$ tal que:

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

por definición de suma en $\mathbb{Z}(\sqrt{2})$ se tiene:

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

por igualdad de parejas ordenadas, se obtiene el siguiente sistema de ecuaciones:

$$a + x = a$$

$$b + y = b$$

resolviendo el anterior sistema de ecuaciones se obtiene que $(x, y) = (0, 0)$ por lo tanto:

$$(a, b) + (0, 0) = (a, b)$$

y por la propiedad conmutativa de la suma en $\mathbb{Z}(\sqrt{2})$ se tiene que:

$$(0, 0) + (a, b) = (a, b)$$

luego $(0, 0)$ es el elemento neutro de la suma en $\mathbb{Z}(\sqrt{2})$

Teorema 2.3 Elemento Neutro: la suma en el conjunto $\mathbb{Z}(\sqrt{2})$ cumple la propiedad de la existencia del elemento neutro.

Demostración: sea $(a, b) \in \mathbb{Z}(\sqrt{2})$, y sea $(0, 0) \in \mathbb{Z}(\sqrt{2})$, luego

$$(a, b) + (0, 0) = (a, b)$$

$$(0, 0) + (a, b) = (a, b)$$

en este caso $(0, 0)$ se denomina elemento neutro.

una vez demostrado que la suma en $\mathbb{Z}(\sqrt{2})$ cumple con la propiedad de la existencia de elemento neutro, ahora se procede a ver si existen elementos inverso, para esto, sean las parejas (a, b) y (x, y) que pertenecen al conjunto de $\mathbb{Z}(\sqrt{2})$ tal que:

$$(a, b) + (x, y) = (0, 0)$$

por definición de suma en $\mathbb{Z}(\sqrt{2})$ se tiene:

$$(a + x, b + y) = (0, 0)$$

por igualdad de parejas ordenadas, se obtiene el siguiente sistema de ecuaciones:

$$a + x = 0$$

$$b + y = 0$$

resolviendo el anterior sistema de ecuaciones se obtiene que $(x, y) = (-a, -b)$ por lo tanto:

$$(a, b) + (-a, -b) = (0, 0)$$

y por la propiedad conmutativa de la suma en $\mathbb{Z}(\sqrt{2})$ se tiene que:

$$(-a, -b) + (a, b) = (0, 0)$$

Teorema 2.4 Elementos inversos: la suma en el conjunto $\mathbb{Z}(\sqrt{2})$ cumple la propiedad de la existencia de elementos inversos.

Demostración: sean (a, b) y $(-a, -b)$ que pertenecen a $\mathbb{Z}(\sqrt{2})$, luego

$$(a, b) + (-a, -b) = (0, 0)$$

$$(-a, -b) + (a, b) = (0, 0)$$

En este caso, a la pareja $(-a, -b)$ se le llama el inverso aditivo de (a, b)

En consecuencia, el conjunto de $\mathbb{Z}(\sqrt{2})$ es un grupo abeliano bajo la suma puesto que cumple con la propiedad conmutativa, la propiedad asociativa, existe un elemento neutro y existen elementos inversos.

2.5. Multiplicación en el conjunto de $\mathbb{Z}(\sqrt{2})$

Análogamente a la suma, para definir la multiplicación en $\mathbb{Z}(\sqrt{2})$ es natural pensar en lo siguiente: Sea $a + bk$ y $c + dk$, entonces la multiplicación de estos dos elementos se realiza de forma usual, utilizando la propiedad distributiva, agrupando términos semejantes y tomando el hecho de que $k^2 = 2$, así:

$$(a + bk)(c + dk) = (ac + 2bd) + (ad + bc)k$$

Por lo tanto, es conveniente definir la multiplicación de la siguiente forma:

Definición 2.3 Multiplicación: Sean (a, b) y (c, d) que pertenecen a $\mathbb{Z}(\sqrt{2})$, se define la multiplicación como:

$$(a, b) * (c, d) = (ac + 2bd, ad + bc)$$

De forma similar a la suma, es importante mencionar que ac, $2bd$, ad y bc representa el producto usual de los números enteros y el símbolo " + " que se encuentra dentro de la pareja ordenada representa la suma usual de los números enteros; sin embargo, el símbolo $*$ no representa el producto usual en los números enteros.

Nota: Por simplicidad, de ahora en adelante, omitiremos el signo $*$ para referirnos a la multiplicación en el conjunto $\mathbb{Z}(\sqrt{2})$, es decir, de ahora en adelante se denotara $(a, b) * (c, d)$ como $(a, b)(c, d)$.

2.5.1. Propiedades de la multiplicación en $\mathbb{Z}(\sqrt{2})$

Teorema 2.5 Propiedad asociativa: Sean (a,b), (c,d) y (e,f) que pertenecen a $\mathbb{Z}(\sqrt{2})$, entonces:

$$((a,b)(c,d))(e,f) = (a,b)((c,d)(e,f))$$

Demostración: Por definición de multiplicación en $\mathbb{Z}(\sqrt{2})$ se tiene:

$$((a,b)(c,d))(e,f) = (ac+2bd, ad+bc)(e,f)$$

$$((a,b)(c,d))(e,f) = ((ac+2bd)e + 2(ad+bc)f, (ac+2bd)f + (ad+bc)e)$$

utilizando la propiedad distributiva en los números enteros:

$$((a,b)(c,d))(e,f) = (ace+2bde+2adf+2bcf, acf+2bdf+ade+bce)$$

utilizando las propiedades conmutativa de la suma y la multiplicación en los números enteros:

$$((a,b)(c,d))(e,f) = (ace+a2df+2bcf+2bde, acf+ade+bce+b2df)$$

aplicando propiedad distributiva en los números enteros:

$$((a,b)(c,d))(e,f) = (a(ce+2df)+2b(cf+de), a(cf+de)+b(ce+2df))$$

utilizando la definición de multiplicación en $\mathbb{Z}(\sqrt{2})$ dos veces:

$$((a,b)(c,d))(e,f) = (a,b)(ce+2df, cf+de)$$

$$((a,b)(c,d))(e,f) = (a,b)((c,d))(e,f))$$

Por lo tanto, la multiplicación en el conjunto $\mathbb{Z}(\sqrt{2})$ cumple la propiedad asociativa.

Teorema 2.6 Propiedad Conmutativa: Sean (a,b) y (c,d) que pertenecen a $\mathbb{Z}(\sqrt{2})$, entonces $(a,b)(c,d) = (c,d)(a,b)$

Demostración: Por definición de multiplicación en $\mathbb{Z}(\sqrt{2})$, se tiene:

$$(a,b)(c,d) = (ac+2bd, ad+bc)$$

aplicando la conmutatividad de la suma y multiplicación de los números enteros:

$$(a,b)(c,d) = (ca+2db, cb+da)$$

usando la definición de multiplicación en $\mathbb{Z}(\sqrt{2})$:

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

Así, la multiplicación en $\mathbb{Z}(\sqrt{2})$ cumple la propiedad conmutativa.

Una vez demostrada la propiedad conmutativa de la multiplicación en $\mathbb{Z}(\sqrt{2})$, se procede a verificar si existe elementos neutros, para esto, sea (a,b) y $(c,d) \in \mathbb{Z}(\sqrt{2})$ tal que

$$(a,b)(c,d) = (ac + 2bd, ad + bc) = (a,b)$$

por igual de parejas ordenadas, se obtiene el siguiente sistema de ecuaciones:

$$\begin{aligned} ac + 2bd &= a \\ ad + bc &= b \end{aligned}$$

Resolviendo el sistema de ecuaciones, se tiene que $c = 1$ y $d = 0$

Teorema 2.7 Propiedad modulativa: la multiplicación en el conjunto $\mathbb{Z}(\sqrt{2})$ cumple la propiedad de la existencia de elemento neutro.

Demostración: Sea $(a,b) \in \mathbb{Z}(\sqrt{2})$, y sea $(1,0) \in \mathbb{Z}(\sqrt{2})$ luego

$$(1,0)(a,b) = (a,b)$$

$$(a,b)(1,0) = (a,b)$$

En este caso, a la pareja $(1,0)$ se le llama el modulo de la multiplicación en $\mathbb{Z}(\sqrt{2})$, así, la multiplicación en el conjunto de $\mathbb{Z}(\sqrt{2})$ cumple la propiedad modulativa.

Observación: Existen parejas (a,b) que no poseen elemento inverso, por ejemplo, sea la pareja $(0,2)$, se debe encontrar la pareja (x,y) tal que $(0,2)(x,y) = (1,0)$, por definición de multiplicación en el conjunto de $\mathbb{Z}(\sqrt{2})$ se obtiene:

$$(2y, x) = (1,0)$$

por igualdad de parejas ordenadas, se construye el siguiente sistema de ecuaciones:

$$\begin{aligned} 2y &= 1 \\ x &= 0 \end{aligned}$$

Este sistema de ecuaciones no tiene solución en el conjunto de los números enteros, por lo tanto, no existe (x, y) tal que $(0, 2)(x, y) = (1, 0) = (x, y)(0, 2)$, así, la multiplicación en $\mathbb{Z}(\sqrt{2})$ no cumple la propiedad de existencia de elementos inversos.

Este hecho es precisamente el que motiva el estudio que se adelantará más adelante, ya que al no haber inversos multiplicativos para todos los elementos, una cuestión inmediata que surge es estudiar aquellos elementos que sí tienen inversos y por eso, adquiere sentido el estudio de la divisibilidad.

2.6. Divisibilidad

Análogo al caso de los números enteros, se define la relación de divisibilidad en el conjunto de $\mathbb{Z}(\sqrt{2})$

Definición 2.4 Sean (a, b) y (c, d) que pertenecen a $\mathbb{Z}(\sqrt{2})$ con (a, b) diferente de $(0, 0)$, se dice que (a, b) divide a (c, d) si y sólo si existe $(x, y) \in \mathbb{Z}(\sqrt{2})$ tal que $(a, b)(x, y) = (c, d)$. En tal caso se denota como $(a, b)|(c, d)$. También se dice que (a, b) es un divisor de (c, d) o que (c, d) es un múltiplo de (a, b).

Para indicar que (a, b) no divide a (c, d) se escribe $(a, b) \nmid (c, d)$.

Nótese que se definió la relación de divisibilidad para $(a, b) \neq (0, 0)$, esto se debe a que si $(a, b) = (0, 0)$, y si $(a, b)|(c, d)$, entonces $(c, d) = (0, 0)$, la justificación de este hecho radica en que para todo $(x, y) \in \mathbb{Z}(\sqrt{2})$, $(0, 0)(x, y) = (0, 0)$, por lo tanto, no tiene mucho sentido estudiar el caso en que $(a, b) = (0, 0)$.

2.6.1. Algunas propiedades de la divisibilidad

Teorema 2.8: Si $(a, b) \neq (0, 0)$ entonces $(a, b)|(0, 0)$

Demostración: Como $(a, b)(0, 0) = (0, 0)$ se tiene que $(a, b)|(0, 0)$

Teorema 2.9: Si $(a, b) \neq (0, 0)$ entonces $(a, b)|(a, b)$

Demostración: Por la propiedad modulativa de la multiplicación en $\mathbb{Z}(\sqrt{2})$ se tiene:

$$(a, b)(1, 0) = (a, b)$$

por lo tanto $(a,b)|(a,b)$

Teorema 2.10: Si $(a,b) \neq (0,0)$ entonces $(-a,-b)|(a,b)$

Demostración: Sea $(-1,0) \in \mathbb{Z}\sqrt{2}$, luego

$$(-a,-b)(-1,0) = (a,b)$$

, así $(-a,-b)|(a,b)$.

Teorema 2.11: Si $(a,b)|(c,d)$ entonces $(a,b)|(c,d)(e,f)$

Demostración: Como $(a,b)|(c,d)$ entonces existe (x,y) tal que:

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

Multiplicando a ambos lados de la igualdad por (e,f) se obtiene:

$$(a,b)(x,y)(e,f) = (c,d)(e,f)$$

por la propiedad asociativa de la multiplicación en $\mathbb{Z}(\sqrt{2})$, se tiene:

$$(a,b)((x,y)(e,f)) = (c,d)(e,f)$$

por tanto $(a,b)|(c,d)(e,f)$

Teorema 2.12 Transitividad: Si $(a,b)|(c,d)$ y si $(c,d)|(e,f)$ entonces $(a,b)|(e,f)$

Demostración: Como $(a,b)|(c,d)$ entonces existe (x,y) tal que:

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

Análogamente como $(c,d)|(e,f)$ entonces existe (w,z) tal que:

$$(c,d)(w,z) = (e,f)$$

reemplazando $(c,d) = (a,b)(x,y)$ en la ecuación $(c,d)(w,z) = (e,f)$ se obtiene:

$$(a,b)(x,y)(w,z) = (e,f)$$

Por la propiedad asociativa de la multiplicación en $\mathbb{Z}(\sqrt{2})$, se obtiene:

$$(a,b)((x,y)(w,z)) = (e,f)$$

por lo tanto, $(a,b)|(e,f)$.

Teorema 2.13 si $(a,b)|(x,y)$ entonces $(-a,-b)|(x,y)$

Demostración: por el teorema 2.10 se tiene que $(-a,-b)|(a,b)$ y como $(a,b)|(x,y)$, entonces por el teorema 2.12 se tiene que $(-a,-b)|(x,y)$

Capítulo 3

Las Unidades en el conjunto $\mathbb{Z}(\sqrt{2})$

3.1. ¿Qué son Unidades?

Como el objetivo de este trabajo de grado es desarrollar algunos elementos de la teoría de números en $\mathbb{Z}(\sqrt{2})$ es importante identificar algunos elementos diferenciados. Para esto, es importante tener como referencia algunas estructuras algebraicas usuales, aquellas que se tienen a la mano son el conjunto de los números enteros y el conjunto de los números naturales.

En el conjunto de los números naturales existe un elemento que es diferente a todos los demás cuya característica principal es tener un único divisor, el único elemento en este conjunto que cumple con esta característica es el número 1 cuyo único divisor es él mismo; no existen otros elementos que pertenezcan a este conjunto y que cumplan con esta condición. Otra forma de identificar este elemento es caracterizar a aquellos que dividen a todos los demás, nótese que en el conjunto de los números Naturales 1 es el único elemento que cumple con esta condición puesto que $1 \mid n$ para todo $n \in \mathbb{N}$.

En el conjunto de los números enteros existen un par de elementos que son diferentes a todos los demás en el sentido de que tienen únicamente dos divisores, los únicos elementos en este conjunto que cumplen con esta condición son el número 1 y -1, dado que los únicos divisores de 1 y -1 son 1 y -1; no existen otros elementos en este conjunto que tengan únicamente dos divisores. Otra forma de identificar estos elementos es caracterizar a aquellos números que dividan a todos los demás, nótese que los únicos números que cumplen con esta condición son el 1 y -1, pues estos dividen a todos los

números que pertenecen al conjunto de los números enteros.

A estos elementos que se diferenciaron en el conjunto de los números naturales y enteros se les denominan unidades. El objetivo de la siguiente sección es identificar estos elementos pero en $\mathbb{Z}(\sqrt{2})$.

3.2. Unidades en el conjunto $\mathbb{Z}(\sqrt{2})$

Tomando como referencia las unidades en el conjunto de los números naturales y el conjunto de los números enteros, se define de forma análoga las unidades en el conjunto de $\mathbb{Z}(\sqrt{2})$

Definición 3.1 Unidad en $\mathbb{Z}(\sqrt{2})$. $(a,b) \in \mathbb{Z}(\sqrt{2})$ se denomina unidad, si y sólo si, para todo $(x,y) \in \mathbb{Z}(\sqrt{2})$, $(a,b) \mid (x,y)$. Así, el conjunto U de las unidades de $\mathbb{Z}(\sqrt{2})$ se define como:

$$U = \Big\{(a,b) \in \mathbb{Z}(\sqrt{2}) : \forall (x,y) \in \mathbb{Z}(\sqrt{2}) \ : \ (a,b)|(x,y)\Big\}$$

Caracterización de las unidades en $\mathbb{Z}(\sqrt{2})$

Una vez planteada la definición de unidad en $\mathbb{Z}(\sqrt{2})$ se procede a buscar y a caracterizar las unidades en este conjunto, para esto, se sospecha que una unidad es la pareja $(1,0)$ por ser el módulo de la multiplicación

Teorema 3.1: El elemento $(1,0)$ es una unidad en el conjunto $\mathbb{Z}(\sqrt{2})$

Demostración: Como $(1,0)$ es el elemento neutro de la multiplicación en $\mathbb{Z}(\sqrt{2})$, se tiene que para todo $(a,b) \in \mathbb{Z}(\sqrt{2})$, $(1,0)(a,b) = (a,b)$, luego por definición de divisibilidad en $\mathbb{Z}(\sqrt{2})$ $(1,0)|(a,b)$, así $(1,0)$ es una unidad.

Para encontrar otras unidades en el conjunto $\mathbb{Z}(\sqrt{2})$, se utiliza la propiedad transitiva de la divisibilidad en $\mathbb{Z}(\sqrt{2})$, pues si $(1,0)|(x,y)$ para todo $(x,y) \in \mathbb{Z}(\sqrt{2})$ y si $(a,b)|(1,0)$ entonces, por propiedad transitiva de la divisibilidad $(a,b)|(x,y)$, esto quiere decir que el conjunto de divisores de la pareja $(1,0)$ son elementos del conjunto U, es decir son elementos del conjunto de las unidades en $\mathbb{Z}(\sqrt{2})$.

Sea $(a,b) \in \mathbb{Z}(\sqrt{2})$ tal que $(a,b)|(1,0)$, luego, por definición de divisibilidad, existe la pareja ordenada (x,y) tal que:

$$(a,b)(x,y) = (1,0)$$

aplicando la definición de multiplicación en $\mathbb{Z}(\sqrt{2})$, se tiene:

$$(ax + 2by, ay + bx) = (0, 1)$$

por definición de igualdad de parejas ordenadas, se obtiene el siguiente sistema de ecuaciones:

$$\begin{aligned} ax + 2by &= 1 \\ bx + ay &= 0 \end{aligned}$$

resolviendo, se obtiene que:

$$x = \frac{a}{a^2 - 2b^2}$$

$$y = -\frac{b}{a^2 - 2b^2}$$

Pero estos elementos deben ser números enteros, ya que como vimos, no todos los elementos de $\mathbb{Z}(\sqrt{2})$ tienen inversos, por tanto, es necesario establecer condiciones para saber cuándo los números anteriores son enteros, para esto, observemos que:

$$x^2 - 2y^2 = \left(\frac{a}{a^2 - 2b^2}\right)^2 - 2\left(\frac{b}{a^2 - 2b^2}\right)^2$$

$$x^2 - 2y^2 = \frac{1}{a^2 - 2b^2}$$

por lo tanto, al suponer x, y enteros, es claro que $x^2 - 2y^2$ es entero, pero por la igualdad anterior, para que se dé este hecho, es necesario que $a^2 - 2b^2 = \pm 1$. Esta es una ecuación de **Pell-Fermat**[1]; así, hemos encontrado que los divisores de la pareja $(1, 0)$ en el conjunto de $\mathbb{Z}(\sqrt{2})$ satisfacen la ecuación de **Pell-Fermat** anterior.

Se ha demostrado que si $(a, b)|(1, 0)$ entonces $a^2 - 2b^2 = \pm 1$, ahora se quiere verificar si el recíproco de este resultado es cierto.

Teorema 3.2: Si $a^2 - 2b^2 = \pm 1$, entonces $(a, b)|(1, 0)$

Demostración: Por definición de multiplicación en $\mathbb{Z}(\sqrt{2})$ Se tiene que

[1]Alanya, S. Fracciones continuas, ecuación de Pell y unidades en el anillo de enteros de los cuerpos cuadráticos (2004). Extraido el 4 de Noviembre de http: //sisbib.unmsm.edu.pe/bibVirtualData/monografias/basic/alanya_ps/cap8.pdf

$(a,b)(a,-b) = (a^2 - 2b^2, 0)$. Como $a^2 - 2b^2 = \pm 1$ entonces $(a,b)(a,-b) = (\pm 1, 0)$, de lo cual se obtienen dos casos

Caso 1: si $(a,b)(a,-b) = (1,0)$ entonces por definición de divisibilidad $(a,b)|(1,0)$

Caso 2: si $(a,b)(a,-b) = (-1,0)$, entonces $(a,b)|(-1,0)$ y como $(-1,0)(-1,0) = (1,0)$ entonces $(-1,0)|(1,0)$ luego por propiedad transitiva de la divisibilidad entonces $(a,b)|(1,0)$

De lo anterior, se tiene entonces que si $(a,b)|(1,0)$ entonces (a,b) es unidad. Por otra parte si $a^2 - 2b^2 = \pm 1$ entonces $(a,b)|(1,0)$ es decir (a,b) es unidad.

Ahora bien, establecidos los resultados anteriores, se quieren buscar las soluciones de la ecuación de **Pell-Fermat** mencionada, para esto, se usó un software[2], con el cual se encontró que algunos divisores de $(1,0)$ son: $(1,1)$, $(3,2)$, $(7,5)$, $(17,12)$, $(41,29)$, $(99,70)$, $(239,169)$. Otra forma de encontrar algunas soluciones de la ecuación $a^2 - 2b^2 = \pm 1$ es a través de las reductas o convergentes de la fracción continua simple de $\sqrt{2}$ donde las reductas son[3]:

Reducta No. 1: $\frac{1}{1}$

Reducta No. 2: $\frac{3}{2}$

Reducta No. 3: $\frac{7}{5}$

Reducta No. 4: $\frac{17}{12}$

[2]Este software fue desarrollado en Pascal por el compañero Nicolás Mahecha, participante del seminario de álgebra.

[3]La fracción continua de $\sqrt{2}$ es:

$$\sqrt{2} = 1 + \cfrac{1}{2 + \cfrac{1}{2 + \cfrac{1}{2 + \cfrac{1}{2 + \cfrac{1}{2 + \cdots}}}}}$$

Reducta No. 5: $\frac{41}{29}$

Reducta No. 6: $\frac{99}{70}$

Reducta No. 7: $\frac{239}{169}$

Observando las reductas se tiene:

$$\{f_n\}_{n=0}^{\infty} = \left\{1, \frac{3}{2}, \frac{7}{5}, \frac{41}{29}, \frac{99}{70}, \frac{239}{169}...\right\}$$

esta sucesión se puede definir por recurrencia como:

$$f_n = \frac{x_n}{y_n}$$

donde $x_0 = 1$, $y_0 = 1$, $x_1 = 3$, $y_1 = 2$, $x_{n+1} = x_n + 2y_n$ y $y_{n+1} = x_n + y_n$, por lo cual, surge el siguiente teorema.

Teorema 3.3: si (x, y) es solución de la ecuación $a^2 - 2b^2 = \pm 1$, entonces $(x + 2y, x + y)$ es solución a la ecuación.

Demostración: considere la siguiente expresión $(x+2y)^2 - 2(x+y)^2$, luego:

$$\begin{aligned}(x + 2y)^2 - 2(x + y)^2 &= x^2 + 4xy + 4y^2 - 2(x^2 + 2xy + y^2) \\ &= -x^2 + 2y^2 \\ &= -(x^2 - 2y^2) \\ &= -(\pm 1) \\ &= \pm 1\end{aligned}$$

Nótese que como (x, y) satisface la ecuación de **Pell-Fermat** entonces $(x, y)|(1, 0)$, por otra parte $(x + 2y, x + y)$ también satisface la ecuación de **Pell-Fermat**, entonces $(x + 2y, x + y)|(1, 0)$.

De lo anterior, se puede concluir que dado una solución podemos obtener más soluciones por recurrencia, es decir que la ecuación de **Pell-Fermat** tiene infinitas soluciones, por lo tanto $(1, 0)$ tiene infinitos divisores y como los divisores de $(1, 0)$ son unidades, entonces existen infinitas unidades.

Por otra parte, como $(1, 0)|(a, b)$ para todo $(a, b) \in \mathbb{Z}(\sqrt{2})$ (por ser unidad) y como $(1, 0)$ tiene infinitos divisores, entonces por la propiedad transitiva de

la divisibilidad, (a, b) tiene también infinitos divisores.

Así se ha presentado un ejemplo de una estructura algebraica donde todos sus elementos tienen infinitos divisores y hay infinitas unidades, muy distinto a lo que pasa en el conjunto de los números naturales y enteros.

3.3. Función N

A continuación se dará una definición muy importante que se utilizarán en algunos resultados posteriores.

Definición 3.2 Función N**:** Sea $N : \mathbb{Z} \times \mathbb{Z} \to \mathbb{N}$ tal que para todo $(a, b) \in \mathbb{Z} \times \mathbb{Z}$,

$$N(a, b) = |a^2 - 2b^2|$$

Nota: $(0, 0)$ es la única pareja en $\mathbb{Z}(\sqrt{2})$ tal que al aplicar la función N su resultado es cero.

3.3.1. Propiedades de la Función N

Teorema 3.4 Sean las parejas ordenadas (a, b) y (c, d) , entonces $N((a, b)(c, d)) = N(a, b)N(c, d)$

Demostración: Por definición de multiplicación en $\mathbb{Z}(\sqrt{2})$, se tiene:

$$(a, b)(c, d) = (ac + 2bd, ad + bc)$$

aplicando la función N, se tiene:

$$\begin{aligned} N((a, b)(c, d)) &= N(ac + 2bd, ad + bc) \\ &= |(ac + 2bd)^2 - 2(ad + bc)^2| \\ &= |a^2c^2 + 4abcd + 4b^2d^2 - 2a^2d^2 - 4abcd - 2b^2c^2| \\ &= |(a^2c^2 - 2a^2d^2) + (4b^2d^2 - 2b^2c^2)| \\ &= |a(c^2 - 2d^2) - 2b^2(c^2 - 2d^2)| \\ &= |(a - 2b^2)||(c^2 - 2d^2)| \\ &= N(a, b)N(c, d) \end{aligned}$$

Teorema 3.5 Si $N(a, b) = 1$ entonces $(a, b)|(1, 0)$

Demostración: Como $N(a, b) = 1$ entonces $|a^2 - 2b^2| = 1$, esto quiere decir que $a^2 - 2b^2 = \pm 1$ que es la ecuación de **Pell-Fermat**, luego aplicando

el teorema 3.2 se tiene que $(a,b)|(1,0)$

Teorema 3.6 Sea $(a,b) \in \mathbb{Z}(\sqrt{2})$ tal que $N(a,b) = 1$, y sea $(c,d) \in \mathbb{Z}(\sqrt{2})$ tal que $(c,d)|(a,b)$ entonces $N(c,d) = 1$.

Demostración: Como $(c,d)|(a,b)$, entonces existe $(x,y) \in \mathbb{Z}(\sqrt{2})$ tal que:

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

luego, aplicando la función N se tiene:

$$N((c,d)(x,y)) = N(a,b)$$

como $N(a,b) = 1$ y aplicando el teorema 3.4

$$N(c,d)N(x,y) = 1$$

luego por definición de la función N se tiene que $N(c,d)$ tiene que ser un número natural, por lo tanto $N(c,d)$ obigatoriamente debe ser igual a 1.

Con este teorema, podemos concluir que si $N(a,b) = 1$ entonces para todo (x,y) que sea divisor de (a,b) se tiene que $N(x,y) = 1$.

Teorema 3.7 Sea $(a,b) \in \mathbb{Z}(\sqrt{2})$, si $N(a,b) = 1$ entonces $(a,b)|(x,y)$ para todo $(x,y) \in \mathbb{Z}(\sqrt{2})$

Demostración: Como $N(a,b) = 1$, entonces por el teorema 3,5, se tiene que $(a,b)|(1,0)$, luego por el teorema 3,1 $(1,0)|(x,y)$ pata todo $(x,y) \in \mathbb{Z}(\sqrt{2})$ y por el teorema 2,15 $(a,b)|(x,y)$, por lo tanto (a,b) es unidad.

Dado el anterior teorema, se puede reescribir el conjunto U de las unidades como:

$$U = \left\{(x,y) \in \mathbb{Z}(\sqrt{2}) \ \mid \ N(x,y) = 1\right\}$$

Así por ejemplo, $(3,2)$ es unidad pues $N(3,2) = |3^2 – 2(2)^2| = |9 – 8| = 1$. Resultado que también puede verificarse utilizando la definición de unidad, dado que $(3,2)(3a-4b, 3b-2a) = (a,b)$, esto quiere decir que $\forall (a,b) \in \mathbb{Z}(\sqrt{2})$ $(3,2)|(a,b)$.

Capítulo 4

Números Primos en el conjunto $\mathbb{Z}(\sqrt{2})$

4.1. ¿Qué es un número primo?

En los casos usuales de los números naturales y enteros, una vez halladas las unidades, rápidamente se caracterizan otros elementos, de los que hemos llamado diferenciados o especiales (como el caso de las unidades) y son precisamente los números que llamamos primos, pero, ¿qué es un número primo?. Como es costumbre, volvamos la mirada de nuevo a los casos conocidos.

En el conjunto de los números naturales, usualmente se dice que un número es primo si y sólo si tiene exactamente dos divisores, el uno y él mismo, esto hace que un número natural sea primo si pertenece al conjunto de aquellos números cuyo número de divisores es exactamente dos.

Por otra parte, en el conjunto de los números enteros, una forma de caracterizar a los números primos es mediante el número de divisores que éste tiene, así, se dirá que un número es primo si y sólo si tiene la segunda menor cantidad de divisores (al igual que en los números naturales).

Aunque estas formas de caracterizar números primos en el conjunto de los números enteros y naturales sean muy comunes, éstas, sin embargo, no permiten generar una definición de número primo para elementos de $\mathbb{Z}(\sqrt{2})$, pues como se demostró en el capítulo anterior, todo elemento que pertenece a $\mathbb{Z}(\sqrt{2})$ tiene infinitos divisores. Por lo tanto, el desarrollar algunos conceptos de teoría de números en este conjunto numérico se torna en un problema un poco más complejo, ya que es claro que las definciones usuales de número

primo resultan difíciles de adaptar para el ejemplo que se está considerando.

Uno de los objetivos que se trabajó en el seminario de álgebra fue llegar a un consenso sobre la definición de unidades y números primos en distintas estructuras algebraicas, donde dicha definición acordada debía funcionar en todas las estructuras, así, la definición a la que se llegó de número primo fue:

Un número es primo si y sólo si es divisible únicamente por las unidades y sus asociados, donde dos números son asociados si y sólo si se dividen entre sí.

Nótese que esta definición funciona para el conjunto de los números naturales y enteros; así, por ejemplo en el conjunto de los números enteros, 2 es primo porque este es divisible por 1, -1, pero además por -2 y por 2. De manera similar, -7 es primo pues sus únicos divisores son 1, -1, 7 y -7. En estos ejemplos se observa además que 7 divide a -7 y -7 divide a 7, de la misma forma, 2 divide a -2 y -2 a 2. En general, aquellos números a y b tales que a divide a b y b a a, decimos que a y b son asociados. Con esta definición, podemos entonces concluir que en $\mathbb{Z}$ un número es primo si y sólo si es divisible exactamente por las unidades y sus asociados.

El objetivo fundamental de éste capítulo es identificar y caracterizar a los número primos en el conjunto $\mathbb{Z}(\sqrt{2})$ partiendo de ésta definición de número primo, para esto es importante definir asociados en $\mathbb{Z}(\sqrt{2})$

Definición 4.1 Asociados en $\mathbb{Z}(\sqrt{2})$: Sean (a,b) y (c,d) que pertenecen a $\mathbb{Z}(\sqrt{2})$, (a,b) y (c,d) son asociados si y sólo si $(a,b)|(c,d)$ y $(c,d)|(a,b)$.

4.2. Números Primos en $\mathbb{Z}(\sqrt{2})$

Definición 4.2 Número primo en $\mathbb{Z}(\sqrt{2})$: Sea $(a,b) \in \mathbb{Z}(\sqrt{2})$ se dice que (a,b) es primo si y sólo si tiene como únicos divisores a los elementos del conjunto U de las unidades de $\mathbb{Z}(\sqrt{2})$ y a los elementos del conjunto $A_{(a,b)}$ formado por los asociados de (a,b), esto es:

$$U = \Big\{(x,y) \in \mathbb{Z}(\sqrt{2}) \ ; \ N(x,y) = 1\Big\}$$

$$A_{(a,b)} = \Big\{(z,w) \in \mathbb{Z}(\sqrt{2}) \ ; \ (a,b)|(z,w) \ \wedge \ (z,w)|(a,b)\Big\}$$

Teorema 4.1 Sean (a,b) y $(c,d) \in \mathbb{Z}(\sqrt{2})$, si (a,b) y (c,d) son asociados,

entonces $N(a,b) = N(c,d)$

Demostración: Como (a,b) y (c,d) son asociados, entonces $(a,b)|(c,d)$ y $(c,d)|(a,b)$, luego por definición de divisibilidad, existen las parejas (x_1,y_1) y (x_2,y_2) tales que

$$(a,b)(x_1,y_1) = (c,d)$$

$$(c,d)(x_2,y_2) = (a,b)$$

al sustituir $(c,d)(x_2,y_2) = (a,b)$ en $(a,b)(x_1,y_1) = (c,d)$ se obtiene:

$$(c,d)(x_2,y_2)(x_1,y_1) = (c,d)$$

al aplicar la función N en ambos lados de la igualdad y aplicando el teorema 3.4, se tiene:

$$N(c,d)N(x_2,y_2)N(x_1,y_1) = N(c,d)$$

$$N(x_2,y_2)N(x_1,y_1) = 1$$

como $N(x_2,y_2)$ y $N(x_1,y_1) \in \mathbb{N}$ entonces $N(x_2,y_2)N(x_1,y_1) \in \mathbb{N}$ Por lo tanto obligatoriamente $N(x_2,y_2) = N(x_1,y_1) = 1$. Así, como $(a,b)(x_1,y_1) = (c,d)$, entonces $N(a,b)N(x_1,y_1) = N(c,d)$, y como $N(x_1,y_1) = 1$ entonces $N(a,b) = N(c,d)$.

Puede pensarse, debido al resultado anterior, que si $N(a,b) = N(c,d)$, entonces (a,b) y (c,d) son asociados, sin embargo, se encontraron varios casos en donde esto no se cumple, por ejemplo: sean las parejas $(3,1)$ y $(-5,4)$, en ambos casos, $N(3,1) = |3^2 - 2(1)^2| = |7| = 7$ y $N(-5,4) = |(-5)^2 - 2(4)^2| = |-7| = 7$, pero $(-5,4)$ no divide a $(3,1)$ pues no existe (x,y) tal que $(-5,4)(x,y) = (3,1)$. Esto demuestra que el recíproco del teorema 4.1 es falso, sin embargo, el siguiente teorema proporciona condiciones necesarias y suficientes para que una proposición similar al recíproco del teorema anterior sea verdadera.

Teorema 4.2 Sean (c,d) y (a,b) que pertenecen a $\mathbb{Z}(\sqrt{2})$ si $(c,d)|(a,b)$ y si $N(c,d) = N(a,b)$ entonces $(a,b)|(c,d)$, es decir, (a,b) y (c,d) son asociados.

Demostración: como $(c,d)|(a,b)$ entonces existe (x_1,y_1) tal que

$$(c,d)(x_1,y_1) = (a,b)$$

por definición de multiplicación en $\mathbb{Z}(\sqrt{2})$

$$(cx_1 + 2dy_1, cy_1 + dx_1) = (a,b)$$

por definición de igualdad de parejas ordenadas

$$a = cx_1 + 2dy_1$$

$$b = cy_1 + dx_1$$

resolviendo este sistema de ecuaciones se obtiene:

$$x_1 = \frac{2bd - ac}{c^2 - 2d^2}$$

$$y_1 = \frac{bc - ad}{c^2 - 2d^2}$$

por otra parte, se debe probar que existe (x_2, y_2) tal que

$$(a, b)(x_2, y_2) = (c, d)$$

por definición de multiplicación en $\mathbb{Z}(\sqrt{2})$ se tiene

$$(ax_2 + 2by_2, ay_2 + bx_2) = (c, d)$$

por definición de igualdad de parejas ordenadas

$$ax_2 + 2by_2 = c$$

$$ay_2 + bx_2 = d$$

resolviendo este sistema de ecuaciones se obtiene:

$$x_2 = \frac{2bd - ac}{a^2 - 2b^2}$$

$$y_2 = \frac{ad - bc}{a^2 - 2b^2}$$

como $(c, d)|(a, b)$, es claro que x_1 y y_1 son números enteros. Por otra parte para que $(a, b)|(c, d)$ se debe probar que x_2 e y_2 pertenecen al conjunto de los números enteros. Como $N(c, d) = N(a, b)$ entonces $|c^2 - 2d^2| = |a^2 - 2b^2|$ de lo cual $c^2 - 2d^2 = a^2 - 2b^2$ ó $c^2 - 2d^2 = -a^2 + 2b^2$

- **Caso 1:** Si $c^2 - 2d^2 = a^2 - 2b^2$ entonces

  $$x_2 = \frac{2bd - ac}{c^2 - 2d^2}$$

  por lo tanto $x_2 = x_1$ y como x_1 es un número entero, entonces x_2 también lo es.

  por otra parte

  $$y_2 = \frac{ad - bc}{c^2 - 2d^2} = \frac{-(bc - ad)}{c^2 - 2d^2} = -y_1$$

  por lo tanto, como y_1 es un número entero, entonces y_2 también lo es

- **Caso 2:** Si $c^2 - 2d^2 = -a^2 + 2b^2$, el desarrollo se hace de forma análoga al caso 1

Así, $(a,b)|(c,d)$ es decir, (a,b) y (c,d) son asociados.

De acuerdo a este teorema, podemos re definir el concepto de número primo como:

Definición 4.3 Sea $(a,b) \in \mathbb{Z}(\sqrt{2})$ se dice que (a,b) es primo si y sólo tiene como únicos divisores a los elementos del conjunto U y el conjunto $A_{(a,b)}$ tales que:

$$U = \Big\{(x,y) \in \mathbb{Z}(\sqrt{2}) \ ; \ N(x,y) = 1\Big\}$$

$$A_{(a,b)} = \Big\{(z,w) \in \mathbb{Z}(\sqrt{2}) \ ; \ N(z,w) = N(a,b) \ \wedge \ (z,w)|(a,b)\Big\}$$

Una vez re definido el concepto de número primo en $\mathbb{Z}(\sqrt{2})$, ahora el objetivo es encontrar algunos primos en nuestro conjunto de estudio, para esto inicialmente se consideran las parejas $(2n,m)$

4.3. Las parejas de la forma $(2n,m)$

Desde el proceso de analizar, es importante realizar estudios para casos particulares, un primer caso que se estudia es el de las parejas de la forma $(2n,m)$ donde $n,m \in \mathbb{Z}$. En el conjunto de los números naturales y enteros se tiene que 2 es un número primo, así y dado que $N(0,1) = 2$ entonces se sospecha que $(0,1)$ es un número primo en $\mathbb{Z}(\sqrt{2})$, por lo tanto, inicialmente se considera una primera exploración sobre esta pareja.

La pareja $(0,1)$

En la siguiente tabla, se muestra algunos divisores de $(0,1)$ donde ambas componentes son positivas, ya que según el teorema (2.13) si (a,b) divide a (x,y), entonces $(-a,-b)$ también divide a (x,y)

Divisores de la Unidad	Divisores de $(0,1)$ donde $N(a,b)=2$
$(1,0)$	$(0,1)$
$(1,1)$	$(2,1)$
$(3,2)$	$(4,3)$
$(7,5)$	$(10,7)$
$(17,12)$	$(24,17)$
$(41,29)$	$(58,41)$
$(99,70)$	$(140,99)$
$(239,169)$	$(338,239)$
$(577,408)$	$(816,577)$
$(1393,985)$	$(1970,1393)$

Cuadro 4.1: Divisores de $(0,1)$

En la tabla 4,1 se han expuesto algunos divisores y estos a su vez se han clasificado en dos grupos, en un primer grupo se encuentran algunos divisores que pertenecen al conjunto U de las unidades y en un segundo grupo se han expuesto algunos divisores de $(0,1)$ tal que $N(0,1)=2$, es importante mencionar que por el teorema 4,2 estos últimos divisores pertenecen al conjunto $A_{(0,1)}$. Por lo tanto, bajo el proceso de analizar, el primer elemento que se encontró que es candidato a ser primo en $\mathbb{Z}(\sqrt{2})$ bajo la definición 4.2 es la pareja $(0,1)$. Demostremos que $(0,1)$ es un número primo en $\mathbb{Z}(\sqrt{2})$, para esto, suponga que $(0,1)$ no es primo, luego debe existir un (x,y) donde $(x,y)|(0,1)$ tal que $(x,y) \notin U$ y que $(x,y) \notin A_{(0,1)}$; por definición de divisibilidad existe (w,z) tal que

$$(x,y)(w,z) = (0,1)$$

aplicando la función N a ambos lados de la igualdad y aplicando el Teorema 3,4 se tiene:

$$N(x,y)N(z,w) = N(0,1)$$

$$N(x,y)N(z,w) = 2$$

por definición de divisibilidad en los números naturales $N(x,y)|2$, pero como en $\mathbb{N}$ los únicos divisores de 2 son el 1 y 2 entonces $N(x,y)=1$ o $N(x,y)=2$ de lo cual surgen dos casos:

- **Caso 1:** Cuando $N(x,y)=1$: Si $N(x,y)=1$ entonces por el teorema 3.7 $(x,y) \in U$ lo cual es una contradicción pues se había supuesto que $(x,y) \notin U$

- **Caso 2:** Cuando $N(x,y) = 2$: Si $N(x,y) = 2$ y como $(x,y)|(0,1)$ entonces por el teorema 4,2 $(x,y) \in A_{(0,1)}$ lo cual es una contradicción pues se había supuesto que $(x,y) \notin A_{(0,1)}$

Por lo tanto $(0,1)$ únicamente tiene dos conjuntos de divisores, el conjunto U y el conjunto $A_{(0,1)}$, así $(0,1)$ es un número primo.

Es importante encontrar un algoritmo que permita identificar cuándo una pareja de la forma $(2n,m)$ es primo o no, sin necesidad de listar los divisores. Para esto, se consideran los siguientes teoremas:

Teorema 4.3 Sean las parejas ordenadas $(0,1)$ y $(2n,m) \in \mathbb{Z}(\sqrt{2})$ entonces $(0,1)|(2n,m)$

Demostración: Como $(0,1)(m,n) = (2n,m)$ entonces $(0,1)|(2n,m)$.

Teorema 4.4 Sean $(0,1)$ y $(2n,m)$ donde n y m son enteros cualesquiera, si $(2n,m)|(0,1)$ entonces $(2n,m)$ tiene exactamente dos conjuntos de divisores, el conjunto U y el conjunto $A_{(2n,m)}$, es decir, $(2n,m)$ es primo.

Demostración: Sea $(a,b) \in \mathbb{Z}(\sqrt{2})$ tal que $(a,b)|(0,1)$, del teorema anterior se tiene que $(0,1)|(2n,m)$, luego, por propiedad transitiva de la divisibilidad se tiene que $(a,b)|(2n,m)$ por lo tanto $(2n,m)$ por lo menos tiene el mismo conjunto de divisores de $(0,1)$, es decir el conjunto U y el conjunto $A_{(0,1)}$. Ahora se debe probar que $(2n,m)$ no tiene otro conjunto de divisores, para esto, sea la pareja $(w,z) \in \mathbb{Z}(\sqrt{2})$ tal que $(w,z)|(2n,m)$, por hipótesis se tiene que $(2n,m)|(0,1)$, luego por propiedad transitiva de la divisibilidad $(w,z)|(0,1)$ por lo tanto (w,z) pertenece al conjunto de divisores de la pareja $(0,1)$ es decir debe pertenecer al conjunto U o al conjunto $A_{(0,1)}$, así, $(2n,m)$ únicamente tiene como divisores el conjunto $A_{(0,1)}$ y el conjunto U. Ahora se debe probar que $A_{(0,1)} = A_{(2n,m)}$, para esto, sea $(p,q) \in A_{(2n,m)}$ luego por definición de asociados se tiene que $(p,q)|(2n,m)$ y $(2n,m)|(p,q)$, por otra parte se tiene que $(2n,m)|(0,1)$ y $(0,1)|(2n,m)$ por propiedad transitiva de la divisibilidad se tiene que $(p,q)|(0,1)$ y que $(0,1)|(p,q)$ por lo tanto $(p,q) \in A_{(0,1)}$ esto quiere decir que todas las parejas que pertenecen a $A_{(2n,m)}$ también pertenecen a $A_{(0,1)}$, de forma análoga se demuestra que todas las parejas que pertenecen a $A_{(0,1)}$ también pertenecen a $A_{(2n,m)}$, por lo tanto $A_{(0,1)} = A_{(2n,m)}$. Así, los únicos conjuntos de divisores de $(2n,m)$ son el conjunto U y el conjunto $A_{(2n,m)}$, por tanto $(2n,m)$ es primo.

Este teorema se constituye en un criterio para saber cuándo un número de

la forma $(2n, m)$ es primo, además, se ha probado también que cualquier elemento de $A_{(0,1)}$ es un número primo, esto es, cualquier asociado a $(0, 1)$ es un número primo. Este hecho también es cierto en el caso de los números enteros, ya que por ejemplo 5 es un número primo en $\mathbb{Z}$ y como $-5 \mid 5$, vemos que -5 también es un número primo.

4.4. Uso de la función N para encontrar números Primos

En esta sección, se hará énfasis en el problema de generar un algoritmo para verificar cuándo un $(a, b) \in \mathbb{Z}(\sqrt{2})$ es primo o no, para esto, se utilizará nuevamente la función N. Debido al estudio anterior, una primera conjetura en relación con la solución al problema es la siguiente: si $N(a, b)$ es un número entero primo, entonces (a, b) es un primo en $\mathbb{Z}(\sqrt{2})$. Al realizar una exploración con algunas parejas ordenadas se obtuvo que efectivamente las parejas con esta condición únicamente tenía como divisores el conjunto U de las unidades y el conjunto $A_{(a,b)}$ de sus asociados, es decir son primos. A continuación una justificación de este resultado:

Teorema 4.5 Si $N(a, b) = |p|$, con p un número entero primo, entonces (a, b) es primo en $\mathbb{Z}(\sqrt{2})$.

Demostración: La demostración se realiza por contradicción, supongamos que (a, b) no es primo, luego debe existir (c, d) tal que $(c, d)|(a, b)$, $N(c, d) \neq 1$ (es decir, no es unidad) y $(a, b) \nmid (c, d)$ (o sea, no es un asociado de (a, b)). Por definición de divisibilidad, existe (x, y) tal que:

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

aplicando la función N en ambos lados de la igualdad y aplicando el teorema 3,4 se tiene:

$$N(c, d)N(x, y) = N(a, b)$$

$$N(c, d)N(x, y) = |p|$$

como $|p|$ es un número primo, entonces, los únicos divisores de $|p|$ son 1 y $|p|$, por lo tanto $N(c, d) = 1$ ó $N(c, d) = |p|$. Si $N(c, d) = 1$ llegamos a una contradicción, pues se había supuesto que $N(c, d) \neq 1$, por otra parte si $N(c, d) = |p|$ entonces $N(c, d) = N(a, b)$ y como $(c, d)|(a, b)$ entonces por el teorema 4.2 se obtiene que $(a, b)|(c, d)$ llegando a una contradicción. Por lo tanto (a, b) es primo.

Es importante mencionar que durante el proceso de exploración, se encontraron parejas (a, b) tales que $N(a, b)$ no son números primos, pero las parejas (a, b) sí son primos bajo la definición 4.2. Para caracterizar a estas parejas es importante indentificar para cuáles números enteros x no existe la pareja (a, b) tal que $N(a, b) = x$, en la siguiente tabla se listan algunos números enteros que cumplen esta condición.

$4n + 1$ con n impar	$4n + 3$ con n par
5	3
13	11
29	19
37	43
53	59
61	67

Cuadro 4.2: Enteros Positivos x para los cuales no existe (a, b) tal que $N(a, b) = x$

A continuación, algunos resultados que permiten justificar las exploraciones asociadas a estas observaciones:

Teorema 4.6 Todo cuadrado perfecto es de la forma $4n$ o $4n + 1$

Demostración: Sea x un cuadrado perfecto, entonces $x = m^2$, donde m puede ser un número par o impar

Caso 1: Si m es par, es de la forma $2k$, por lo tanto:

$$x = (2k)(2k) = 4k^2$$

Si $k^2 = n$, entonces

$$x = 4n$$

Por lo que si x es un cuadrado perfecto, con $\sqrt{x}$ igual a un número par, entonces x es de la forma $4n$.

Caso 2: Si m es impar es de la forma $2k + 1$, por lo tanto:

$$x = (2k + 1)(2k + 1) = 4k^2 + 4k + 1 = 4(k^2 + k) + 1$$

Si $k^2 + k = n$, entonces

$$x = 4n + 1$$

Por lo que si x es un cuadrado perfecto, con $\sqrt{x}$ igual a un número impar, entonces x es de la forma $4n+1$.

Teorema 4.7 Si $4n+1$ es un cuadrado perfecto, entonces n es par.

Demostración: Como $4n+1$ es un número cuadrado, entonces, existe un número natural x tal que $4n+1 = x^2$. Por otro lado, tenemos que $x^2 = 2(2n)+1$, por tanto, x^2 es impar de modo que x es impar, así, $x = 2k+1$, con lo que:

$$4n+1 = (2k+1)^2 = 4k^2+4k+1$$

de donde,

$$4n = 4(k^2+k)$$

y de esto,

$$n = k^2+k$$

en el caso en que k sea un número par, es claro que n es par. En el caso en el que k sea un número impar, k^2 es impar, por tanto, k^2+k es par y por tanto, n es par.

Teorema 4.8 Sea x un número de la forma $4n+3$ con $n \geq 0$ y n par, entonces no existe un $(a,b) \in \mathbb{Z}(\sqrt{2})$ tal que $N(a,b) = x$

Demostración: Por definición de la función N se tiene:

$$N(a,b) = |a^2 - 2b^2|$$

Como n es par, es de la forma $2k$, y suponiendo que el consecuente del enunciado del teorema es falso, resulta:

$$|a^2 - 2b^2| = x = 4n+3$$

para algún $n \geq 1$ y $n = 2k$. Como a^2 y b^2 son cuadrados perfectos (dado que a y b son enteros), entonces son de la forma $4m$ o $4m+1$, de lo cual se obtienen 4 casos:

Caso 1: Si $a^2 = 4m$ y $b^2 = 4p$, entonces

$$|4m - 2(4p)| = 4n+3$$

$$|4(m-2p)| = 4n+3$$

$$4|(m-2p)| = 4n+3$$

Lo cual es falso, ya que el primer término es divisible entre 4 y el segundo término no, y dos números iguales deben tener exactamente los mismos divisores.

Caso 2: Si $a^2 = 4m$ y $b^2 = 4p + 1$, entonces

$$|4m - 2(4p + 1)| = 4n + 3$$

$$|4m - 8p - 2| = 4n + 3$$

$$|2(2m - 4p - 1)| = 4n + 3$$

$$2|(2m - 4p - 1)| = 4n + 3$$

Lo cual es falso, ya que el primer término es un número par y el segundo término es un número impar, ya que la suma de $4n$ que es par con 3 que es impar da un número impar.

Caso 3: Si $a^2 = 4m + 1$ y $b^2 = 4p + 1$, entonces

$$|4m + 1 - 2(4p + 1)| = 4n + 3$$

$$|4m + 1 - 8p - 2| = 4n + 3$$

$$|4(m - 2p) - 1| = 4n + 3$$

si $m - 2p = q$,entonces

$$|4q - 1| = 4n + 3$$

Pero n es par (es lo dado) y m también es par (por el teorema 4.5), entonces $m - 2p$ es par (ya que $2p$ es par, y la sustracción entre números pares da un número par), por ende q es un número par, por definición de valor absoluto, se tiene los siguientes dos casos:

Caso 3.a:

$$4(2l) - 1 = 4(2k) + 3$$

$$8l - 1 = 8k + 3$$

$$8l = 8k + 4$$

$$2l = 2k + 1$$

Lo cual es falso, ya que el primer número es par y el segundo impar.

Caso 3.b:

$$-4(2l) + 1 = 4(2k) + 3$$

$$-8l + 1 = 8k + 3$$
$$-8l = 8k + 2$$
$$-4l = 4k + 1$$

Lo cual es falso, ya que el primer término es divisible entre 4 y el segundo término no, y dos números iguales deben tener exactamente los mismos divisores.

Caso 4: Si $a^2 = 4m + 1$ y $b^2 = 4p$

$$|(4m + 1) - 2(4p)| = 4n + 3$$

por definición de valor absoluto se tienen dos casos:

caso 4.a:

$$(4m + 1) - 2(4p) = 4n + 3$$
$$4m + 1 - 8p = 4n + 3$$
$$4(m - 2p) + 1 = 4n + 3$$

si $m - 2p = q$, entonces

$$4q + 1 = 4n + 3$$
$$4q = 4n + 2$$

Lo cual es falso, ya que el primer término es divisible entre 4 y el segundo término no, y dos números iguales deben tener exactamente los mismos divisores.

Caso 4.b:

$$-(4m + 1) + 2(4p) = 4n + 3$$
$$-4m - 1 + 8p = 4n + 3$$
$$-4m + 8p = 4n + 4$$
$$4(-m + 2p) = 4n + 4$$
$$-4q = 4n + 4$$
$$-q = n + 1$$
$$n + q = -1$$

nótese que $2p$ es un número par y m también es un número par por el teorema 4,7, luego la resta de dos números pares es un número par, por lo tanto q es un número par, luego, como n es par y como q es par, entonces la suma

debe ser un número par, llegando a una contradicción.

Por tanto, no existe un $(a, b) \in \mathbb{Z}(\sqrt{2})$ tal que $N(a, b) = x$.

Teorema 4.9 Sea $(a, b) \in \mathbb{Z}(\sqrt{2})$ con $N(a, b) = |p^2|$ donde p es primo de la forma $4n + 3$, con $n \geq 0$ y n par, entonces (a, b) es primo en $\mathbb{Z}(\sqrt{2})$.

Demostración: La demostración se realizará por contradicción. Supongamos que existe $(x, y) \in \mathbb{Z}(\sqrt{2})$ de modo que $(x, y)|(a, b)$ con $N(x, y) \neq 1$ y $(a, b) \nmid (x, y)$. Por definición de divisibilidad, existe $(w, z) \in \mathbb{Z}(\sqrt{2})$ tal que $(x, y)(w, z) = (a, b)$, aplicando la función N a ambos lados de la igualdad y aplicando el teorema 3,4 se tiene:

$$N(x, y)N(w, z) = N(a, b)$$

por definición de divisibilidad en $\mathbb{Z}$ se tiene que $N(x, y)|N(a, b)$ y como $N(a, b) = |p^2|$ entonces sus únicos divisores en $\mathbb{Z}^+$ son 1, p y p^2, luego, $N(x, y) = 1$ ó $N(x, y) = |p|$ ó $N(x, y) = |p^2|$, si $N(x, y) = 1$ se llega a una contradicción, pues se había supuesto que $N(x, y) \neq 1$. Si $N(x, y) = |p|$ donde p es primo de la forma $4n + 3$, con $n \geq 1$ y n par, entonces por el teorema 4.8 no existe la pareja (x, y) tal que $N(x, y) = |p|$ por lo tanto este caso se descarta. Por último, como $(x, y)|(a, b)$ y como $N(x, y) = |p^2|$ se tiene que $N(x, y) = N(a, b)$, luego por el teorema 4.2 se obtiene que $(a, b)|(x, y)$ llegando a una contradicción, dado que se había supuesto que $(a, b) \nmid (x, y)$, por lo tanto (a, b) es un número primo.

A continuación se realiza un tratamiento similar a lo anterior, pero para los enteros de la forma $4n + 1$:

Teorema 4.10 Sea x un número de la forma $4n + 1$ con $n \geq 1$ y n impar, entonces no existe un (a, b) tal que $N(a, b) = x$.

Demostración: Por definición de la función N se tiene:

$$N(a, b) = |a^2 - 2b^2|$$

Como n es impar, se dice que es de la forma $2k + 1$, y suponiendo que el consecuente del enunciado del teorema es falso, resulta:

$$|a^2 - 2b^2| = x = 4n + 1$$

con $n \geq 1$ y $n = 2k + 1$. Pero como a^2 y b^2 son cuadrados perfectos (dado que a y b son enteros), luego a^2 y b^2 son de la forma $4m$ o $4m + 1$, de lo cual

aparecen 4 casos:

Caso 1: $a^2 = 4m$ y $b^2 = 4p$

$$|4m - 2(4p)| = 4n + 1$$

$$4|(m - 2p)| = 4n + 1$$

sea $m - 2p = q$, luego

$$4|q| = 4n + 1$$

Lo cual es falso, ya que el primer término es divisible entre 4 y el segundo término no, y dos números iguales deben tener exactamente los mismos divisores.

Caso 2: $a^2 = 4m$ y $b^2 = 4p + 1$

$$|4m - 2(4p + 1)| = 4n + 1$$

$$|4m - 8p - 2| = 4n + 1$$

$$2|(2m - 4p - 1)| = 4n + 1$$

sea $2m - 4p - 1 = q$, luego

$$2|q| = 4n + 1$$

Lo cual es falso, ya que el primer término es un número par y el segundo término es un número impar, ya que la suma de $4n$ que es par con 1 que es impar da un número impar.

Caso 3: $a^2 = 4m + 1$ y $b^2 = 4p + 1$

$$|4m + 1 - 2(4p + 1)| = 4n + 1$$

$$|4m + 1 - 8p - 2| = 4n + 1$$

$$|4(m - 2p) - 1| = 4n + 1$$

sea $m - 2p = q$, luego

$$|4q - 1| = 4n + 1$$

por definición de valor absuloto, surgen dos casos:

Caso 3.a

$$4q - 1 = 4n + 1$$

$$4q = 4n + 2$$

Lo cual es falso, ya que el primer término es divisible entre 4 y el segundo término no, y dos números iguales deben tener exactamente los mismos divisores.

Caso 3.b

$$-4q + 1 = 4n + 1$$

$$-4q = 4n$$

nótese que q es par dado que m es un número par por el teorema 4,7 y $2p$ es un número par, y la resta de dos números pares da par, por otro lado, n es un número impar, por lo tanto no es posible tener que la igualdad anterior sea cierta.

Caso 4: $a^2 = 4m + 1$ y $b^2 = 4p$

$$|4m + 1 - 2(4p)| = 4n + 1$$

$$|4m + 1 - 8p| = 4n + 1$$

$$|4(m - 2p) + 1| = 4n + 1$$

sea $m - 2p = q$, luego

$$|4q + 1| = 4n + 1$$

por definición de valor absoluto, surgen 2 casos:

Caso 4.a

$$4q + 1 = 4n + 1$$

Pero n es impar (es lo dado) y m es par, entonces que $m - 2p$ es par (ya que $2p$ es par, y la sustracción entre números pares da un número par), por lo tanto q es un número par, de lo cual:

$$4(2l) + 1 = 4(2k + 1) + 1$$

$$8l + 1 = 8k + 4 + 1$$

$$8l = 8k + 4$$

Lo cual es falso, ya que el primer número es divisible entre 8 y el segundo término no, y dos números iguales deben tener exactamente los mismos divisores.

Caso 4.b

$$-4q - 1 = 4n + 1$$

$$-4q = 4n + 2$$

Lo cual es falso, ya que el primer término es divisible entre 4 y el segundo término no, y dos números iguales deben tener exactamente los mismos divisores.

por lo tanto, no existe (a, b) tal que $N(a, b) = x$ donde x es un número de la forma $4n + 1$ con $n \geq 1$ y n impar.

Teorema 4.11 Sea $(a, b) \in \mathbb{Z}(\sqrt{2})$ con $N(a, b) = |p^2|$ Si p es primo de la forma $4n + 1$, con $n \geq 1$ y n impar, entonces (a, b) es primo.

Demostración: La demostración es análoga al teorema 4.9.

En conclusión y de acuerdo a los teoremas 4.5, 4.9 y 4.11 un algoritmo para verificar si $(a, b) \in \mathbb{Z}(\sqrt{2})$ es primo o no, sin necesidad de elaborar una lista de sus divisores, es aplicando la función N así, si $N(a, b) = x$ donde $x = |p|$ siendo p un número primo ó $x = p^2$ donde p es un número primo de la forma $4n+1$ con n impar ó $x = p^2$ donde p es un número primo de la forma $4n+3$ con n par, entonces (a, b) es primo.

A continuación se presentan algunos teoremas que permiten identificar cuales otros números son primos dado que se tiene un $(a, b) \in \mathbb{Z}(\sqrt{2})$ primo.

Teorema 4.12 Si (p, q) es primo, entonces $(-p, -q)$ es primo.

Demostración: utilizando la función N se tiene que $N(p, q) = |p^2 - 2q^2|$, por otra parte al aplicar la función N a $(-p, -q)$ se tiene que $N(-p, -q) = |(-p)^2 - 2(-q)^2|$, como $(-p)^2 = p^2$ y $(-q)^2 = q^2$, se tiene que $|(-p)^2 - 2(-q)^2| = |p^2 - 2p^2|$, luego $N(p, q) = N(-p, -q)$, por otra parte se tiene que $(p, q)(-1, 0) = (-p, -q)$ por lo tanto $(p, q)|(-p, -q)$ y por el teorema 4.2 $(-p, -q)|(p, q)$ es decir que (p, q) y $(-p, -q)$ son asociados. Sea (w, z) tal que $(w, z)|(-p, -q)$ luego por propiedad transitiva de la divisibilidad $(w, z)|(p, q)$ como (p, q) es primo, entonces (w, z) pertenece al conjunto U de las unidades ó al conjunto $A_{(p,q)}$, esto quiere decir que los únicos conjuntos de divisores de $(-p, -q)$ es el conjunto U y el conjunto $A_{(p,q)}$. Ahora se debe probar que todos los elementos de $A_{(p,q)}$ pertenecen a $A_{(-p,-q)}$, para esto sea $(a, b) \in A_{(p,q)}$, por definición de parejas asociadas $(a, b)|(p, q)$ y $(p, q)|(a, b)$, luego por propiedad transitiva de la divisibilidad $(a, b)|(-p, -q)$ y $(-p, -q)|(a, b)$, luego $(a, b) \in A_{(-p,-q)}$ por lo tanto todos los elementos del conjunto $A_{(p,q)}$ son elementos del conjunto $A_{(-p,-q)}$, así, $(-p, -q)$ únicamente tiene dos conjuntos

de divisores, el conjunto U y el conjunto $A_{(-p,-q)}$.

Teorema 4.13 Si $(-p, q)$ es primo, entonces $(p, -q)$ es primo.

Demostración: análoga al teorema 4.12.

Una vez caracterizados los números primos de la anterior forma,se intuye que no hay más números primos en $\mathbb{Z}(\sqrt{2})$ distintos a los presentados en los teoremas 4.5, 4.9 y 4.11. Para abordar este problema, se estudiará un nuevo conjunto numérico denominado N_2.

4.4.1. El Conjunto N_2

Anteriormente se elaboró un algoritmo para identificar cuando (a, b) es una unidad o un número primo mediante el uso de la función N, ahora, y con base en la función N, se procede a establecer un nuevo conjunto numérico que será de gran utilidad en el capítulo 6, denominado N_2 que se define como:

$$N_2 = \{x \in \mathbb{N} : (\exists (a, b) \in \mathbb{Z}(\sqrt{2}))(N(a, b) = x)\}$$

nótese que $N_2 \subseteq \mathbb{N}$, ahora considere la estructura $(N_2, *)$ donde $*$ es el producto usual en $\mathbb{N}$, para verificar algunas propiedades del producto usual de los números naturales en N_2, primero se debe verificar que $*$ es cerrada en N_2, para esto, sea x y y que pertenecen a N_2, luego existe la pareja (a, b) y (c, d) tal que $N(a, b) = x$ y $N(c, d) = y$, luego

$$x * y = N(a, b)N(c, d)$$

aplicando el teorema 3.4 se tiene:

$$x * y = N((a, b)(c, d))$$

ahora, como $(a, b)(c, d) \in \mathbb{Z}(\sqrt{2})$, entonces $N((a, b)(c, d)) \in N_2$, por lo tanto, $x * y \in N_2$.

Dado que la multiplicación usual de los números naturales en N_2 es una operación cerrada, se procede a mostrar algunas propiedades. Como $N_2 \subseteq \mathbb{N}$, entonces $(N_2, *)$ hereda algunas propiedades de $(\mathbb{N}, *)$ como lo son la propiedad asociativa y la propiedad conmutativa. Además, en el capítulo de Unidades, se mostró que existen parejas (a, b) para los cuales $N(a, b) = 1$, luego $1 \in N_2$, dado que 1 es el elemento neutro de la multiplicación en el conjunto de los números naturales y como $N_2 \subseteq \mathbb{N}$ entonces 1 también es el

elemento neutro de la multiplicación en N_2, por lo tanto, N_2 cumple con la propiedad modulativa bajo el producto usual de los números naturales. Por último, dado que $N(0,1) = 2$ entonces $2 \in N_2$, es evidente que en N_2 no existe un elemento x tal que $2 * x = 1$, por lo tanto en N_2 no se cumple la propiedad de existencia de elementos inversos bajo el producto usual de los números naturales.

Una vez definido el conjunto N_2, ahora se procede a definir algunos elementos diferenciados en N_2. Análogamente al conjunto $\mathbb{Z}(\sqrt{2})$, uno de los primeros elementos diferenciados son las unidades, bajo la misma definición que se ha venido trabajando, se dirá que x es una unidad en N_2 si y sólo si x divide a todos los elementos que pertenecen a N_2, es evidente que el único elemento en N_2 que cumple con la definición de unidad es 1.

El segundo conjunto de elementos diferenciados que se consideran en N_2 son los números primos, donde un número en N_2 es primo si y sólo si es divisible únicamente por las unidades y sus asociados, donde dos números son asociados si y sólo si se dividen entre si. Como se mencionó anteriormente, se tiene que 1 es la única unidad que existe en N_2, por otra parte, se tiene que si dado dos elementos x y y que pertenecen a N_2, entonces $x|y$ y $y|x$ si y sólo si $x = y$, la justificación de este hecho radica en lo siguiente:

Si $x|y$ y si $y|x$, entonces existe w y z que pertenecen a N_2 tales que

$$xw = y$$

$$yz = x$$

luego, $xwyz = xy$, por la propiedad conmutativa de la multiplicación en N_2 se tiene que $xywz = xy$, luego $wz = 1$, así $w = 1$ y $z = 1$, Por lo tanto $x = y$. Por otra parte se tiene que si $x = y$ entonces $x * 1 = y$ y $y * 1 = x$, por lo tanto, $x|y$ y $y|x$.

El anterior hecho implica que si $x \in N_2$, entonces su único asociado es él mismo, así, se puede reescribir la definición de número primo en N_2 como: Un número x es primo en N_2 si y sólo si es divisible por 1 y por si mismo.

Una vez definido número primo en N_2, ahora se procede a caracterizar los números primos en N_2

4.4.2. Caracterización de algunos números primos en N_2

Para caracterizar algunos números primos en N_2, inicialmente se procede a demostrar los siguientes teoremas:

Teorema 4.14 Sea $x \in N_2$, entonces $x^2 \in N_2$

Demostración: Como $x \in N_2$ y como la multiplicación es una operación cerrada en N_2, entonces $x^2 = x * x$ también pertenece a N_2.

Teorema 4.15 Sea $x \notin N_2$, entonces $x^2 \in N_2$

Demostración: Vamos a considerar dos casos:

Caso 1: sea $x = 2n - 1$ con $n \geq 0$, donde $x \notin N_2$, sea $a = (2n - 1)$ y $b = 0$, como $a \in \mathbb{Z}$ y $b \in \mathbb{Z}$, entonces $(2n - 1, 0) \in \mathbb{Z}(\sqrt{2})$, aplicando la función N se tiene:

$$N(2n - 1, 0) = (2n - 1)^2$$

por lo tanto, $x = (2n - 1)^2 \in N_2$.

Caso 2: sea $x = 2n$ con $n \geq 0$, donde $x \notin N_2$, sea $a = (2n)$ y $b = 0$, como $a \in \mathbb{Z}$ y $b \in \mathbb{Z}$, entonces $(2n - 1, 0) \in \mathbb{Z}(\sqrt{2})$, aplicando la función N se tiene:

$$N(2n, 0) = (2n)^2$$

por lo tanto, $x = (2n)^2 \in N_2$.

así, dado los teoremas (4.14) y (4.15), se puede afirmar que todo cuadrado perfecto pertenece a N_2. Ahora, se procede a caracterizar algunos números primos en N_2 mediante los siguientes teoremas:

Teorema 4.16: si p es un número primo en $\mathbb{N}$ y si $p \in N_2$, entonces p también es un número primo en N_2

Demostración: Como $N_2 \subset \mathbb{N}$, y como los único divisores de p en $\mathbb{N}$ son 1 y el mismo, entonces se tiene que los únicos divisores de p en N_2 son el 1 y él mismo, por lo tanto p es un número primo en N_2.

Teorema 4.17 Si $x = p^2$ con p un número primo en $\mathbb{N}$ de la forma $4n + 1$

con $n \geq 1$ y n impar entonces x es un número primo en N_2

Demostración: Sea $x = p^2$, entonces los únicos divisores de x son 1, p y p^2 en $\mathbb{N}$, pero por el teorema (4.10) no existe (a, b) tal que $N(a, b) = p$, por lo tanto, $p \notin N_2$, por otra parte, por el teorema (4.15) p^2 existe en N_2, luego x únicamente tiene como únicos divisores a 1 y a él mismo, por lo tanto x es primo.

Teorema 4.18 Si $x = p^2$ con p un número primo en $\mathbb{N}$ de la forma $4n + 3$ con $n \geq 0$ y n par entonces x es un número primo en N_2.

Demostración: La demostración se realiza de forma análoga al teorema 4.17.

Para comprender un poco mejor los resultados anteriores, considere el siguiente ejemplo.

Ejemplo 4.1 25 efectivamente pertenece a N_2, ya que, $N(5, 0) = 25$, y $(5, 0) \in \mathbb{Z}(\sqrt{2})$, en el conjunto de los números naturales, los divisores de 25 son el 1,5 y 25, pero como 5 no pertenece a N_2 (por el teorema 4.10) , entonces 25 es un número primo en N_2 pues sólo tiene como divisores a la unidad y a él mismo.

Habiendo definido número primo en N_2, se procede a definir números compuestos en N_2, para esto, se utiliza la definición usual de número compuesto en el conjunto de los números naturales, donde un número es compuesto si y sólo tiene como divisores al conjunto de las unidades, el conjunto de sus asociados y además tiene otro conjunto de divisores que no es subconjunto del conjunto de las unidades y de sus asociados, ésta definición es equivalente a decir que un número en N_2 es compuesto si y sólo si tiene tres o más divisores.

Una vez definido los números primos y compuestos en N_2, se sospecha que no hay más primos distintos a los caracterizados anteriormente en N_2, para abarcar este problema, considere los siguientes teoremas:

Teorema 4.19 sea $c \in \mathbb{N}$, c es un cuadrado si y sólo si los exponentes de su factorización prima son pares:

Demostración: Como c es un cuadrado perfecto, entonces $c = x^2$, por el

teorema fundamental de la aritmética en $\mathbb{N}$, se tiene que $x = a_1 * ... * a_k$, así:

$$x^2 = (a_1 * ... * a_k)(a_1 * ... * a_k)$$

$$x^2 = a_1^2 * ... * a_k^2$$

por otra parte, si $c = a_1^2 * ... * a_k^2$, entonces:

$$c = (a_1 * ... * a_k)(a_1 * ... * a_k)$$

sea $x = (a_1 * ... * a_k)$, entonces $c = x^2$, por lo tanto c es un cuadrado perfecto.

Teorema 4.20 Sea c un número compuesto en $\mathbb{N}$ tal que $c \notin N_2$, entonces c^2 es un número compuesto en N_2

Demostración: Como c^2 es un cuadrado perfecto, entonces por el teorema (4.15), se tiene que $c^2 \in N_2$, por otra parte, por el teorema fundamental de la aritmética en $\mathbb{N}$ y por el teorema (4.19) se tiene:

$$c^2 = a_1^2 * ... * a_k^2$$

luego, por los teoremas (4.14) y (4.15) se tiene que $a_1^2 \in N_2$, ..., $a_k^2 \in N_2$, por lo tanto, c^2 es un número compuesto en N_2.

Teorema 4.21 Si $c \notin N_2$ y $d \in N_2$, entonces $cd \notin N_2$

Demostración: Como $d \in N_2$, entonces existe $(a, b) \in \mathbb{Z}(\sqrt{2})$ tal que $N(a, b) = |a^2 - 2b^2| = d$, luego

$$c|a^2 - 2b^2| = cd$$

$$|ca^2 - 2cb^2| = cd$$

ahora, como $c \notin N_2$ entonces c no es un cuadrado perfecto, de lo cual, ca^2 y cb^2 no son cuadrados perfectos y por ende, al no existir x y y tal que $x^2 = ca^2$ y $y^2 = cb^2$ se tiene que $cd \notin N_2$

Teorema 4.22 Sea $z \in \mathbb{N}$ tal que $z = cx^{2k+1}$, $k \geq 0$, donde x es de la forma $4n + 1$ con n impar ó $4n + 3$ con n par con $x \neq c$ y $c \in N_2$ entonces $z \notin N_2$

Demostración: Si $z = cx^{2k+1}$, entonces $z = cx^{2k}x$, de lo cual se tiene dos casos:

Caso 1: Si $x = 4n + 1$ con n impar, entonces $z = c(4n + 1)^{2k}(4n + 1)$, nótese que $(4n+1)^{2k}$ es un cuadrado perfecto, por lo tanto $(4n+1)^{2k} \in N_2$, por otra parte, como $c \in N_2$ entonces por la propiedad clausurativa de la multiplicación $c(4n + 1)^{2k} \in N_2$, ahora, por el teorema (4.10) se tiene que no existe $(a, b) \in \mathbb{Z}(\sqrt{2})$ tal que $N(a, b) = 4n + 1$,así, por el teorema (4.21) $z = cx^{2k+1} \notin N_2$

Caso 2: para $x = 4n + 3$ con n par, mediante el uso del teorema (4.8) y de forma análoga al caso anterior se obtiene que $z = cx^{2k+1} \notin N_2$

Teorema 4.23 si $z = cx^{2k}$ con $k \geq 0$ y $c \in N_2$ entonces $z \in N_2$

Demostración: sea $x^{2k} = (x^k)^2$, luego $x^{2k} \in N_2$ por ser un cuadrado perfecto, como $c \in N_2$, entonces por la propiedad cerrada de la multiplicación $z = cx^{2k} \in N_2$.

Una vez demostrado los teoremas anteriores, se procede a estudiar los elementos que pertenecen a N_2 distintos a los caracterizados en los teoremas (4.16), (4.17) y (4.18), para esto, se divide en tres grupos al conjunto de los números naturales como se muestra en la siguiente figura, nótese que en esta división, no se tiene en cuenta el número 1 puesto que habiamos dicho que 1 es la unidad en el conjunto de los número naturales y también es la unidad en el conjunto N_2:

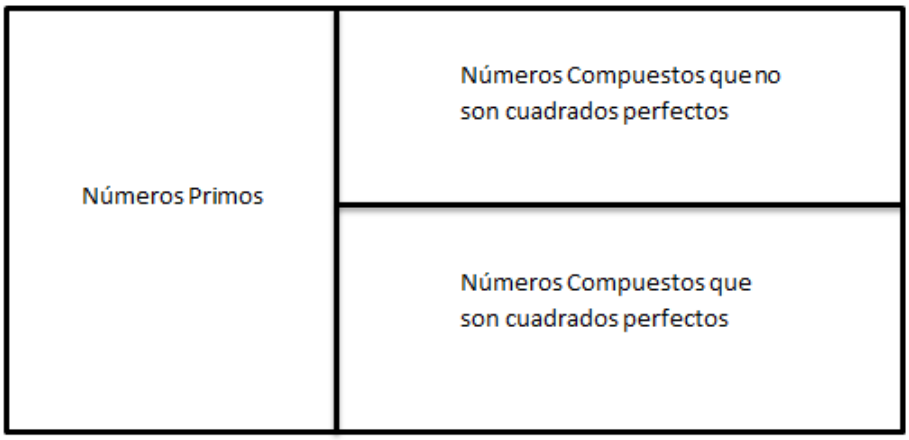

Figura 4.1: Conjunto de los números Naturales

De la figura 4.1, se consideran 3 casos, un primer caso que correponde al conjunto de los números primos en $\mathbb{N}$, un segundo caso que corresponde al

conjunto de los números compuestos que son cuadrados perfectos en $\mathbb{N}$ y un tercer caso que corresponde a los números compuestos que no son cuadrados perfectos en $\mathbb{N}$

Caso 1: Considere todos los números primos en $\mathbb{N}$, de estos números primos, hay algunos que pertenecen a N_2 y otros que no, como únicamente nos interesa el caso en que pertenezcan a N_2, se tiene que si p pertenece a N_2 entonces por el teorema 4.16 se tiene que p es un número primo en N_2.

Caso 2: Considere todos los números compuestos que son cuadrados perfectos, anteriormente se demostró que si un número es un cuadrado perfecto, entonces éste pertenece a N_2, luego, para caracterizar a estos números, se tomaran 4 casos:

Caso 2.1 Sea $(4n)^2$, con $n \geq 0$, nótese que $4n$ es un número compuesto en $\mathbb{N}$, luego si $4n \notin N_2$ entonces por el teorema (4.20) $(4n)^2$ es un número compuesto en N_2. Por otra parte, si $4n \in N_2$ entonces $(4n)^2 = (4n)(4n)$, así $4n|(4n)^2$, por lo tanto $(4n)^2$ es un número compuesto.

Caso 2.2 Sea $(4n+1)^2$, para estos cuadrados perfecto, se toman los siguientes casos:

Caso 2.2.1 si $(4n+1) \in N_2$, entonces $(4n+1)^2 = (4n+1)(4n+1)$, luego $4n+1|(4n+1)^2$, por lo tanto $(4n+1)^2$ es un número compuesto en N_2.

Caso 2.2.2 si $(4n+1) \notin N_2$ con $(4n+1)$ un número compuesto en $\mathbb{N}$, entonces por el teorema (4.20) $(4n+1)^2$ es un número compuesto en N_2

Caso 2.2.3 si $(4n+1) \notin N_2$ con $(4n+1)$ un número primo en $\mathbb{N}$ y n impar, se tiene que $(4n+1)^2$ es un número primo en N_2 como ya se había mencionado anteriormente.

Caso 2.2.4 si $(4n+1) \notin N_2$ con $(4n+1)$ un número primo en $\mathbb{N}$ y n par, se tiene que este caso no se puede dar, puesto que al ser $(4n+1)$ un número primo, este no es múltiplo de ningún número de la forma $4n+1$ con n impar o $4n+3$ con n par, por lo tanto si p es un número primo de la forma $4n+1$ con n par, este siempre va a pertenecer a N_2 y por tanto, se remite al caso

2.2.1.

Caso 2.3 Sea $(4n+2)^2$, con $n \geq 0$, nótese que $4n+2$ es un número compuesto en $\mathbb{N}$ (por ser divisible entre 2), luego si $(4n+2) \notin N_2$ entonces por el teorema (4.20) $(4n+2)^2$ es un número compuesto en N_2. Por otra parte, si $(4n+2) \in N_2$ entonces $(4n+2)^2 = (4n+2)(4n+2)$, así $(4n+2)|(4n+2)^2$, por lo tanto $(4n+2)^2$ es un número compuesto.

Caso 2.4 Sea $(4n+3)^2$, para estos cuadrados perfecto, se toman los siguientes casos:

Caso 2.4.1 si $(4n+3) \in N_2$, entonces $(4n+3)^2 = (4n+3)(4n+3)$, luego $4n+3|(4n+3)^2$, por lo tanto $(4n+3)^2$ es un número compuesto en N_2.

Caso 2.4.2 si $(4n+3) \notin N_2$ con $(4n+3)$ un número compuesto en $\mathbb{N}$, entonces por el teorema (4.20) $(4n+3)^2$ es un número compuesto en N_2

Caso 2.4.3 si $(4n+3) \notin N_2$ con $(4n+3)$ un número primo en $\mathbb{N}$ y n par, se tiene que $(4n+3)^2$ es un número primo en N_2 como ya se había mencionado anteriormente.

Caso 2.4.4 si $(4n+3) \notin N_2$ con $(4n+3)$ un número primo en $\mathbb{N}$ y n impar, se tiene que este caso no se puede dar, puesto que al ser $(4n+3)$ un número primo, este no es múltiplo de ningún número de la forma $4n+1$ con n impar o $4n+3$ con n par, por lo tanto si p es un número primo de la forma $4n+3$ con n par, este siempre va a pertenecer a N_2 y por tanto, se remite al caso 2.4.1.

Nótese que $(4n)^2$ y $(4n+2)^2$ se pueden escribir de la forma $4k$, por otra parte, $(4n+1)^2$ y $(4n+3)^2$ se pueden escribir de la forma $4l+1$ con k y l números enteros positivso, así, por el teorema 4.6 y por los resultados expuestos en el caso 2 se puede concluir que si c es un cuadrado perfecto distinto a los expuestos en los teoremas (4.17) y (4.18) entonces c es un número compuesto en N_2

Caso 3: En este caso, se va cosiderar todos los números compuestos en $\mathbb{N}$ que no son cuadrados perfectos y que pertenecen a N_2, mediante el uso de

un software [1] se realizó una exploración de forma rigorosa, de la cual surgió la siguiente conjetura:

Conjetura 4.1: Si c es un número compuesto en $\mathbb{N}$, tal que c no es un cuadrado perfecto y si c pertenece a N_2, entonces c es un número compuesto en N_2

Una vez estudiados los casos 1,2 y 3 mencionados anteriormente, se tiene entonces como conjetura que no existen otros números primos en N_2 distintos a los caracterizados en los teoremas (4.16), (4.17) y (4.18).

Una vez estudiado el conjunto de los números primos en N_2, se retoma de nuevo el conjunto $\mathbb{Z}(\sqrt{2})$, con el fin de estudiar otros elementos diferenciados que denominaremos números compuestos.

4.4.3. Números Compuestos en el conjunto $\mathbb{Z}(\sqrt{2})$

Continuando con el estudio del conjunto $\mathbb{Z}(\sqrt{2})$, en esta sección se considerarán ahora unos nuevos elementos diferenciados denominados números compuestos. Sea $(a, b) \in \mathbb{Z}(\sqrt{2})$, se dice que (a, b) es un número compuesto si y sólo si tiene como divisores el conjunto U de las unidades, el conjunto $A_{(a,b)}$ de sus asociados y además tiene otro conjunto de divisores $C_{(a,b)}$ donde

$$C_{(a,b)} = \{(x, y) \in \mathbb{Z}(\sqrt{2}) : (x, y)|(a, b) \wedge (x, y) \notin U \wedge (x, y) \notin A_{(a,b)}\}$$

una vez definido números compuestos en $\mathbb{Z}(\sqrt{2})$, se procede a realizar un algoritmo que permita identificar cuando (a, b) es un número compuesto, para esto, se utilizará de nuevo la función N. Mediante múltiples pruebas utilizando un software[2], se llegó a la siguiente conjetura:

Conjetura 4.2 Sea $(a, b) \in \mathbb{Z}(\sqrt{2})$, si $N(a, b)$ es un número compuesto en N_2, entonces (a, b) es un número compuesto en $\mathbb{Z}(\sqrt{2})$

Recordemos que si $N(a, b) = p$ con p un número primo en $\mathbb{N}$ ó si $N(a, b) = p^2$ con p un número primo en $\mathbb{N}$ de la forma $4n + 1$ con n impar ó con p un número primo de la forma $4n+3$ en $\mathbb{N}$ con n par, entonces (a, b) es un número primo en $\mathbb{Z}(\sqrt{2})$, por otra parte, se tiene como conjetura que no existen

[1] Elaborado por el profesor Yeison Sánchez del departamento de matemáticas de la Universidad Pedagógica Nacional

[2] Para el estudio de números compuestos en $\mathbb{Z}(\sqrt{2})$, se utilizó de nuevo el programa elaborado por el estudiante Nicolás Mahecha de la lincenciatura en Matemáticas

números primos en N_2 distintos a los caracterizados en los teoremas (4.16), (4.17) y (4.18), por lo tanto, se intuye que si $N(a,b) = p$ con p un número primo en N_2, entonces (a,b) es un número primo en $\mathbb{Z}(\sqrt{2})$, así, y dado la conjetura 4.2, se tiene:

Conjetura 4.3 No existen números primos en $\mathbb{Z}(\sqrt{2})$ distintos a los caracterizados en los teoremas (4.5), (4.9) y (4.11).

Capítulo 5

Criterios de Divisibilidad en $\mathbb{Z}(\sqrt{2})$

En el capítulo de conceptos preliminares, se definió la relación de divisibilidad en $\mathbb{Z}(\sqrt{2})$ y algunas de sus propiedades; en este capítulo, se exponen algunos criterios de divisibilidad en el conjunto $\mathbb{Z}(\sqrt{2})$. Para esto vamos a considerar seis casos: Caso Cero-Par, caso Par-Par, caso Par-Impar, caso Cero-Impar, caso Impar-par y caso Impar-Impar, los cuales se definen a continuación:

5.1. Caso Cero - Par

En esta sección, se considera inicialmente la pareja $(0, 2n)$ con $n \in \mathbb{Z}$ y $n \neq 0$, ahora, se desea encontrar $(\square, \diamond) \in \mathbb{Z}(\sqrt{2})$ donde $(0, 2n)|(\square, \diamond)$, por definición de divisibilidad existe (x, y) tal que

$$(0, 2n)(x, y) = (\square, \diamond)$$

por definición de multiplicación en $\mathbb{Z}(\sqrt{2})$ se tiene:

$$(4ny, 2nx) = (\square, \diamond)$$

por igualdad de parejas ordenadas se obtiene el siguiente sistema de ecuaciones:

$$4ny = \square$$

$$2nx = \diamond$$

despejando se obtiene que $y = \frac{\square}{4n}$ y $x = \frac{\diamond}{2n}$, como x e y deben pertenecer a $\mathbb{Z}$ entonces $\square = 4nc$ donde $c \in \mathbb{Z}$ y $\diamond = 2nd$ donde $d \in \mathbb{Z}$. Así $x = d$ e $y = c$.

Teorema 5.1 Sea la pareja $(0, 2n) \in \mathbb{Z}(\sqrt{2})$ entonces $(0, 2n)|(4nc, 2nd)$ con $n, c, d \in \mathbb{Z}$

Demostración: Por definición de divisibilidad, debe existir $(x, y) \in \mathbb{Z}(\sqrt{2})$ tal que

$$(0, 2n)(x, y) = (4nc, 2nd)$$

por definición de multiplicación se tiene:

$$(4ny, 2nx) = (4nc, 2nd)$$

por definición de igualdad entre parejas ordenadas se tiene:

$$4ny = 4nc$$

$$2nx = 2nd$$

resolviendo este sistema de ecuaciones se tiene que si $y = c$ y $x = d$, entonces $(0, 2n)|(4nc, 2nd)$.

5.2. Caso Par - Par

Sean las parejas $(2b, 2n)$ y $(\diamond, \square) \in \mathbb{Z}(\sqrt{2})$ tal que $(2b, 2n)|(\diamond, \square)$, por definición de divisibilidad, existe $(x, y) \in \mathbb{Z}(\sqrt{2})$ tal que:

$$(2b, 2n)(x, y) = (\diamond, \square))$$

por definición de multiplicación en $\mathbb{Z}(\sqrt{2})$ se tiene:

$$(2bx + 4ny, 2by + 2nx) = (\diamond, \square)$$

por definición de igualdad de parejas ordenadas se tiene:

$$2bx + 4ny = \diamond \tag{5.1}$$

$$2by + 2nx = \square \tag{5.2}$$

De la ecuación 5.2 se obtiene

$$x = \frac{\square - 2by}{2n}$$

como $x \in \mathbb{Z}$ entonces $\square = 2nc + 2by$, con $c \in \mathbb{Z}$ luego se tiene:

$$x = \frac{2nc + 2by - 2by}{2n}$$

$$x = c$$

Reemplazando $x = c$ en la ecuación 5.1 se obtiene:

$$2bc + 4ny = \diamond$$

$$y = \frac{\diamond - 2bc}{4n}$$

como $y \in \mathbb{Z}$, entonces $\diamond = 4nd + 2bc$ luego

$$y = \frac{4nd + 2bc - 2bc}{4n}$$

$$y = d$$

luego, $\diamond = 4nd + 2bc$ y $\square = 2nc + 2bd$.

Teorema 5.2 Sea la pareja $(2b, 2n) \in \mathbb{Z}(\sqrt{2})$ entonces $(2b, 2n)|(4nd+2bc, 2nc+2bd)$ con $b, n, c, d \in \mathbb{Z}$

Demostración: Por definición de divisibilidad, debe existir $(x, y) \in \mathbb{Z}(\sqrt{2})$ tal que

$$(2b, 2n)(x, y) = (4nd + 2bc, 2nc + 2bd)$$

por definición de multiplicación en $\mathbb{Z}(\sqrt{2})$ se obtiene:

$$(2bx + 4ny, 2by + 2nx) = (4nd + 2bc, 2nc + 2bd)$$

por definición de igualdad entre parejas ordenadas se tiene:

$$2bx + 4ny = 4nd + 2bc$$

$$2by + 2nx = 2nc + 2bd$$

resolviendo este sistema de ecuaciones se tiene que si $x = c$ e $y = d$, entonces $(2b, 2n)|(4nd + 2bc, 2nc + 2bd)$.

5.3. Caso Par - Impar

Sean las parejas $(2b, 2n-1)$ y $(\diamond, \square) \in \mathbb{Z}(\sqrt{2})$ tal que $(2b, 2n-1)|(\diamond, \square)$, por definición de divisibilidad, existe $(x, y) \in \mathbb{Z}(\sqrt{2})$ tal que:

$$(2b, 2n - 1)(x, y) = (\diamond, \square))$$

por definición de multiplicación en $\mathbb{Z}(\sqrt{2})$ se tiene:

$$(2bx + 2(2n - 1)y, 2by + (2n - 1)x) = (\diamond, \square)$$

por definición de igualdad de parejas ordenadas se tiene:

$$2bx + 2(2n-1)y = \diamond \tag{5.3}$$

$$2by + (2n-1)x = \square \tag{5.4}$$

De la ecuación 5.4 se obtiene;

$$x = \frac{\square - 2by}{2n-1}$$

como $x \in \mathbb{Z}$ entonces $\square = (2n-1)c + 2by$, con $c \in \mathbb{Z}$ luego se tiene:

$$x = \frac{(2n-1)c + 2by - 2by}{2n-1}$$

$$x = c$$

Reemplazando $x = c$ en la ecuación 5.3 se obtiene:

$$2bc + 2(2n-1)y = \diamond$$

$$y = \frac{\diamond - 2bc}{2(2n-1)}$$

como $y \in \mathbb{Z}$ entonces $\diamond = 2(2n-1)d + 2bc$ luego

$$y = \frac{2(2n-1)d + 2bc - 2bc}{2(2n-1)}$$

$$y = d$$

luego, $\diamond = 2(2n-1)d + 2bc$ y $\square = (2n-1)c + 2bd$.

Teorema 5.3 Sea la pareja $(2b, 2n-1) \in \mathbb{Z}(\sqrt{2})$ entonces $(2b, 2n-1)|(2(2n-1)d + 2bc, (2n-1)c + 2bd)$ con $b, n, c, d \in \mathbb{Z}$

Demostración: Por definición de divisibilidad, debe existir $(x, y) \in \mathbb{Z}(\sqrt{2})$ tal que

$$(2b, 2n-1)(x, y) = (2(2n-1)d + 2bc, (2n-1)c + 2bd)$$

por definición de multiplicación en $\mathbb{Z}(\sqrt{2})$ se obtiene:

$$(2bx + 2(2n-1)y, 2by + (2n-1)x) = (2(2n-1)d + 2bc, (2n-1)c + 2bd)$$

por definición de igualdad entre parejas ordenadas se tiene:

$$2bx + 2(2n-1)y = 2(2n-1)d + 2bc$$

$$2by + (2n-1)x = (2n-1)c + 2bd)$$

resolviendo este sistema de ecuaciones se obtiene que si $x = c$ e $y = d$ entonces $(2b, 2n-1)|(2(2n-1)d + 2bc, (2n-1)c + 2bd)$

5.4. Caso Cero - Impar

Considere la pareja $(0, 2n-1)$ con $n \in \mathbb{Z}$, sea $(\square, \diamond) \in \mathbb{Z}(\sqrt{2})$ tal que $(0, 2n-1)|(\square, \diamond)$, por definición de divisibilidad existe (x, y) tal que

$$(0, 2n-1)(x, y) = (\square, \diamond)$$

por definición de multiplicación en $\mathbb{Z}(\sqrt{2})$ se tiene:

$$(2(2n-1)y, (2n-1)x) = (\square, \diamond)$$

por igualdad de parejas ordenadas se obtiene el siguiente sistema de ecuaciones:

$$2(2n-1)y = \square$$

$$(2n-1)x = \diamond$$

despejando se obtiene que $y = \frac{\square}{2(2n-1)}$ y $x = \frac{\diamond}{2n-1}$, como x e y deben pertenecer a $\mathbb{Z}$ entonces $\square = 2(2n-1)c$ donde $c \in \mathbb{Z}$ y $\diamond = (2n-1)d$ donde $d \in \mathbb{Z}$. Así $x = d$ e $y = c$.

Teorema 5.4 Sea la pareja $(0, 2n-1) \in \mathbb{Z}(\sqrt{2})$ entonces $(0, 2n-1)|(2(2n-1)c, (2n-1)d)$ con $n, c, d \in \mathbb{Z}$

Demostración: Por definición de divisibilidad, debe existir $(x, y) \in \mathbb{Z}(\sqrt{2})$ tal que

$$(0, 2n-1)(x, y) = (2(2n-1)c, (2n-1)d)$$

por definición de multiplicación se tiene:

$$(2(2n-1)y, (2n-1)x) = (2(2n-1)c, (2n-1)d)$$

por definición de igualdad entre parejas ordenadas se tiene:

$$2(2n-1)y = 2(2n-1)c$$

$$(2n-1)x = (2n-1)d$$

resolviendo este sistema de ecuaciones se tiene que si $y = c$ y $x = d$ entonces $(0, 2n-1)|(2(2n-1)c, (2n-1)d)$

5.5. Caso Impar - Par

Sea las parejas $(2n-1, 2m)$ y $(\square, \diamond)$ que pertenecen a $\mathbb{Z}(\sqrt{2})$ tales que $(2n-1, 2m)|(\square, \diamond)$, por definición de divisibilidad, existe $(x, y) \in \mathbb{Z}(\sqrt{2})$ tal que:

$$(2n-1, 2m)(x, y) = (\square, \diamond)$$

por definición de multiplicación en $\mathbb{Z}(\sqrt{2})$ se tiene:

$$((2n-1)x + 4my, (2n-1)y + 2mx) = (\square, \diamond)$$

por igualdad de parejas ordenadas se obtiene el siguiente sistema de ecuaciones:

$$(2n-1)x + 4my = \square \tag{5.5}$$

$$(2n-1)y + 2mx = \diamond \tag{5.6}$$

de la ecuación 5.6 se obtiene:

$$x = \frac{\diamond - (2n-1)y}{2m}$$

como $x \in \mathbb{Z}$ entonces $\diamond = 2mc + (2n-1)y$ donde $c \in \mathbb{Z}$, luego

$$x = \frac{2mc + (2n-1)y - (2n-1)y}{2m}$$

$$x = c$$

Reemplazando $x = c$ en 5.5 se tiene:

$$(2n-1)c + 4my = \square$$

$$y = \frac{\square - (2n-1)c}{4m}$$

como $y \in \mathbb{Z}$ entonces $\square = 4md + (2n-1)c$, luego

$$y = \frac{4md + (2n-1)c - (2n-1)c}{4m}$$

$$y = d$$

Así, $\square = 4md + (2n-1)c$ y $\diamond = 2mc + (2n-1)d$.

Teorema 5.5 Sea la pareja $(2n-1, 2m) \in \mathbb{Z}(\sqrt{2})$ entonces $(2n-1, 2m)|(4md + (2n-1)c, 2mc + (2n-1)d)$ con $m, n, c, d \in \mathbb{Z}$

Demostración: por definición de divisibilidad, debe existir $(x, y) \in \mathbb{Z}(\sqrt{2})$ tal que $(2n-1, 2m)(x, y) = ((4md+(2n-1)c, 2mc+(2n-1)d)$, por definición de multiplicación en $\mathbb{Z}(\sqrt{2})$ se tiene

$$((2n-1)x + 4my, (2n-1)y + 2mx) = (4md + (2n-1)c, 2mc + (2n-1)d)$$

por definición de igualdad de parejas ordenadas se obtiene el siguiente sistema de ecuaciones

$$(2n-1)x + 4my = 4md + (2n-1)c$$
$$(2n-1)y + 2mx = 2mc + (2n-1)d$$

resolviendo, se obtiene que si $x = c$ e $y = d$ entonces $(2n-1, 2m)|(4md + (2n-1)c, 2mc + (2n-1)d)$.

5.6. Caso Impar - Impar

Sea las parejas $(2n-1, 2m-1)$ y $(\square, \diamond)$ que pertenecen a $\mathbb{Z}(\sqrt{2})$ tales que $(2n-1, 2m-1)|(\square, \diamond)$, por definición de divisibilidad, existe $(x, y) \in \mathbb{Z}(\sqrt{2})$ tal que:

$$(2n-1, 2m-1)(x, y) = (\square, \diamond)$$

por definición de multiplicación en $\mathbb{Z}(\sqrt{2})$ se tiene:

$$((2n-1)x + 2(2m-1)y, (2n-1)y + (2m-1)x) = (\square, \diamond)$$

por igualdad de parejas ordenadas se obtiene el siguiente sistema de ecuaciones:

$$(2n-1)x + 2(2m-1)y = \square \tag{5.7}$$
$$(2n-1)y + (2m-1)x = \diamond \tag{5.8}$$

de la ecuación 5.8 se obtiene:

$$x = \frac{\diamond - (2n-1)y}{2m-1}$$

como $x \in \mathbb{Z}$ entonces $\diamond = (2m-1)c + (2n-1)y$ donde $c \in \mathbb{Z}$, luego

$$x = \frac{(2m-1)c + (2n-1)y - (2n-1)y}{2m-1}$$
$$x = c$$

reemplazando $x = c$ en 5.7 se tiene:

$$(2n-1)c + 2(2m-1)y = \square$$

$$y = \frac{\square - (2n-1)c}{2(2m-1)}$$

como $y \in \mathbb{Z}$ entonces $\square = 2(2m-1)d + (2n-1)c$, luego

$$y = \frac{2(2m-1)d + (2n-1)c - (2n-1)c}{2(2m-1)}$$

$$y = d$$

Así, $\square = 2(2m-1)d + (2n-1)c$ y $\diamond = (2m-1)c + (2n-1)d$.

Teorema 5.5 Sea la pareja $(2n-1, 2m-1) \in \mathbb{Z}(\sqrt{2})$ entonces $(2n-1, 2m-1)|(2(2m-1)d + (2n-1)c, (2m-1)c + (2n-1)d)$ con $m, n, c, d \in \mathbb{Z}$

Demostración: por definición de divisibilidad, debe existir $(x, y) \in \mathbb{Z}(\sqrt{2})$ tal que $(2n-1, 2m-1)(x, y) = (2(2m-1)d+(2n-1)c, (2m-1)c+(2n-1)d)$, por definición de multiplicación en $\mathbb{Z}(\sqrt{2})$ se tiene

$$((2n-1)x+2(2m-1)y, (2n-1)y+(2m-1)x) = (2(2m-1)d+(2n-1)c, (2m-1)c+(2n-1)d)$$

por definición de igualdad de parejas ordenadas se obtiene el siguiente sistema de ecuaciones

$$(2n-1)x + 2(2m-1)y = 2(2m-1)d + (2n-1)c$$

$$(2n-1)y + (2m-1)x = (2m-1)c + (2n-1)d$$

resolviendo, se obtiene que si $x = c$ e $y = d$ entonces $(2n-1, 2m-1)|(2(2m-1)d + (2n-1)c, (2m-1)c + (2n-1)d)$.

Capítulo 6

Acercamiento al teorema homólogo al teorema fundamental de la aritmética en $\mathbb{Z}(\sqrt{2})$

6.1. Acercamiento al teorema homólogo al teorema fundamental de la aritmética en $\mathbb{Z}(\sqrt{2})$

Una vez realizado un estudio sobre las unidades, números primos y compuestos en $\mathbb{Z}(\sqrt{2})$, es natural pensar en elaborar un acercamiento al teorema homólogo al teorema fundamental de la aritmética en $\mathbb{Z}(\sqrt{2})$ utilizando únicamente los números primos caracterizados en el capítulo 4, para esto, se utilizará de nuevo la función N, además, se hará uso de un algoritmo, basado en ecuaciones modulares, que permitirán encontrar (a, b) dado que $N(a, b) = x$

6.1.1. Dado $x \in N_2$, algoritmo para hallar $(a, b) \in \mathbb{Z}(\sqrt{2})$ de modo que $N(a, b) = x$

En esta sección, se hará énfasis en el problema de encontrar un algoritmo que permita encontrar (a, b) dado que $N(a, b) = x$, para esto, se utilizarán ecuaciones modulares.

Sea la pareja (a, b) por definición de la función N:

$$N(a, b) = |a^2 - 2b^2| = x$$

por definición del valor absoluto

$$a^2 - 2b^2 = \pm x$$

luego se obtiene los siguientes dos casos:

- Caso 1:
$$a^2 - 2b^2 = x \tag{6.1}$$
- Caso 2:
$$a^2 - 2b^2 = -x \tag{6.2}$$

Consideremos el caso 1, despejando a en función de b se tiene $a^2 = x + 2b^2$. De lo cual escribimos la ecuación como:

$$a^2 \equiv x \pmod 2$$

el coeficiente independiente de esta ecuación es x dado que este es un valor conocido, si el modulo fuera un número primo mayor que 2, se podría utilizar el criterio de Euler [1], por ende, trabajaremos la primer raíz como $a_1 = x+2t$, que es una solución paramétrica. Gracias a los estudios de Gauss si una ecuación cuadrática mónica (una ecuación cuadrática con una incógnita) admite una raíz, también admitirá como segunda raíz su inversa. La inversa de un número, respecto al módulo, es su complemento. Por ende, la segunda raíz será $a_2 = y + 2t$, donde $x + y \equiv 0 \ (mod\ 2)$.

Como $a^2-2b^2 = x$ es una ecuación con dos incógnitas, si la primera incógnita tiene dos raíces, la segunda también, reemplazando cada una de las soluciones en la ecuación (6,1) y despejando b_i se obtiene:

$$(x + 2t)^2 - 2(b_1)^2 = x \Rightarrow (b_1)^2 = \frac{(x - (x + 2t)^2)}{(-2)} \Rightarrow b_1 = \pm\sqrt{\frac{(x - (x + 2t)^2)}{(-2)}}$$

$$(y + 2t)^2 - 2(b_2)^2 = x \Rightarrow (b_2)^2 = \frac{(x - (y + 2t)^2)}{(-2)} \Rightarrow b_2 = \pm\sqrt{\frac{(x - (y + 2t)^2)}{(-2)}}$$

[1]Parra . R, Restos Cuadráticos Y Ley de Reciprocidad Cuadrática, Disponible en: hojamat.es, Directorio: http://hojamat.es/parra/restocuad.pdf

como b_1 positivo y negativo sirven, lo mismo para b_2, sólo se utilizará el valor positivo, ya que sólo se necesita un resultado.

Como estamos trabajando con un valor de x que pertenece a N_2, debe existir un (a, b) tal que $N(a, b) = x$, para esto, damos valores a t, buscando un cuadrado en a tal que restando x y dividiendo por 2 obtengamos un cuadrado.

Si se desea tomar el segundo caso es decir cuando $a^2 - 2b^2 = -x$, se plantea la ecuación modular $a^2 \equiv -x \pmod 2$ y lo demás se realiza de forma análoga al primer caso (cuando $a^2 - 2b^2 = x$). Es importante mencionar que si se plantea la ecuación modular $a^2 \equiv -x \pmod 2$ se encuentra una pareja distinta al caso de la ecuación modular $a^2 \equiv x \pmod 2$. Para efectos de este capítulo, siempre se utiliza primero el primer caso, si no funciona se remite al segundo caso.

Ejemplo 6.1 Encontrar un (a, b) tal que $N(a, b) = 4$

Solución: $N(a, b) = a^2 - 2b^2 = 4$

$$a^2 \equiv 4 \ (mod\ 2) \Rightarrow \begin{cases} a_1 = 4 + 2t \\ \\ a_2 = 0 + 2t \end{cases}$$

$$(4 + 2t)^2 - 2(b_1)^2 = 4 \Rightarrow (b_1)^2 = \frac{(4 - (4 + 2t)^2)}{(-2)} \Rightarrow b_1 = \sqrt{\frac{(4 - (4 + 2t)^2)}{(-2)}}$$

$$(2t)^2 - 2(b_2)^2 = 4 \Rightarrow (b_2)^2 = \frac{(4 - (2t)^2)}{(-2)} \Rightarrow b_2 = \sqrt{\frac{(4 - (2t)^2)}{(-2)}}$$

Para $t = 1$ se tiene

$a_1 = 4 + 2t = 4 + 2 = 6$ y $b_1 = \sqrt{(6 + 8t + 2t^2)} = \sqrt{(6 + 8 + 2)} = \sqrt{16} = 4$

como ambas soluciones son enteros no necesitamos reemplazar en a_2 y b_2 y la solución es $(6, 4)$.

Ejemplo 6.2 Encontrar un (a, b) tal que $N(a, b) = 3$

Solución: Por el teorema (4.8) no existe un (a, b) tal que $N(a, b) = 3$

Ejemplo 6.3 Encontrar un (a, b) tal que $N(a, b) = 14$

Solución: $N(a, b) = a^2 - 2b^2 = 14$

$$a^2 \equiv 14(mod\ 2) \Rightarrow \begin{cases} a_1 = 14 + 2t \\ \\ a_2 = a_2 = 0 + 2t \end{cases}$$

$$(14+2t)^2-2(b_1)^2 = 14 \Rightarrow (b_1)^2 = \frac{(14-(14+2t)^2)}{(-2)} \Rightarrow b_1 = \sqrt{\frac{(14-(14+2t)^2)}{(-2)}}$$

$$b_1 = \sqrt{(91 + 28t + 2t^2)}$$

$$(2t)^2-2(b_2)^2 = 14 \Rightarrow (b_2)^2 = \frac{(14-(2t)^2)}{(-2)} \Rightarrow b_2 = \sqrt{\frac{(14-(2t)^2)}{(-2)}} = \sqrt{(-7 + 2t^2)}$$

para $t = 1$ se tiene

$a_1 = 14 + 2t = 14 + 2 = 16$ y $b_1 = \sqrt{(91 + 28t + 2t^2)} = \sqrt{(91 + 28 + 2)} = \sqrt{121} = 11$

como ambas soluciones son enteros no necesitamos reemplazar en a_2 y b_2 y la solución es $(16, 11)$.

Ejemplo 6.4 Encontrar un (a, b) tal que $N(a, b) = 7$

Solución: $N(a, b) = a^2 - 2b^2 = 7$

$$a^2 \equiv 7(mod\ 2) \Rightarrow \begin{cases} a_1 = 7 + 2t \\ \\ a_2 = 1 + 2t \end{cases}$$

$$(7 + 2t)^2 - 2(b_1)^2 = 7 \Rightarrow (b_1)^2 = \frac{(7-(7+2t)^2)}{(-2)} \Rightarrow b_1 = \sqrt{\frac{(7-(7+2t)^2)}{(-2)}}$$

$$b_1 = \sqrt{(21 + 14t + 2t^2)}$$

$$(1 + 2t)^2 - 2(b_2)^2 = 7 \Rightarrow (b_2)^2 = \frac{(7-(1+2t)^2)}{(-2)} \Rightarrow b_2 = \sqrt{\frac{(7-(1+2t)^2)}{(-2)}}$$

$$b_2 = \sqrt{(-3 + 2t + 2t^2)}$$

Para $t = 1$ se tiene

$a_1 = 7 + 2t = 7 + 2 = 9$ y $b_1 = \sqrt{(21 + 14t + 2t^2)} = \sqrt{(21 + 14 + 2)} = \sqrt{37}$, como b_1 es un número no entero necesitamos realizar el reemplazo en a_2 y b_2.

$a_2 = 1+2t = 1+2 = 3$ y $b_2 = \sqrt{(-3 + 2t + 2t^2)} = \sqrt{(-3 + 2 + 2)} = \sqrt{1} = 1$

Como ambas soluciones son enteros hemos terminado, la solución es $(3, 1)$.

Ejemplo 6.5 Encontrar un (a, b) tal que $N(a, b) = 9$

Solución: $N(a, b) = a^2 - 2b^2 = 9$

$$a^2 \equiv 9(mod\ 2) \Rightarrow \begin{cases} a_1 = 9 + 2t \\ \\ a_2 = 1 + 2t \end{cases}$$

$$(9 + 2t)^2 - 2(b_1)^2 = 9 \Rightarrow (b_1)^2 = \frac{(9 - (9 + 2t)^2)}{(-2)} \Rightarrow b_1 = \sqrt{\frac{(9 - (9 + 2t)^2)}{(-2)}}$$

$$b_1 = \sqrt{(36 + 18t + 2t^2)}$$

$$(1 + 2t)^2 - 2(b_2)^2 = 9 \Rightarrow (b_2)^2 = \frac{(9 - (1 + 2t)^2)}{(-2)} \Rightarrow b_2 = \sqrt{\frac{(9 - (1 + 2t)^2)}{(-2)}}$$

$$b_2 = \sqrt{(-4 + 2t + 2t^2)}$$

Para $t = 1$ se tiene $a_1 = 9 + 2t = 9 + 2 = 11$ y $b_1 = \sqrt{(36 + 18t + 2t^2)} = \sqrt{(36 + 18 + 2)} = \sqrt{56}$, como b_1 es un número no entero necesitamos realizar el reemplazo en a_2 y b_2.

$a_2 = 1+2t = 1+2 = 3$ y $b_2 = \sqrt{(-4 + 2t + 2t^2)} = \sqrt{(-4 + 2 + 2)} = \sqrt{0} = 0$

Como ambas soluciones son enteros hemos terminado, la solución es $(3, 0)$.

Una vez estudiado el algoritmo para obtener (a, b) dado que se tiene $N(a, b)$, se propone ahora un acercamiento al teorema homólogo al teorema fundamental de la aritmética en $\mathbb{Z}(\sqrt{2})$

6.1.2. Una propuesta del teorema homólogo al teorema fundamental de la aritmética en $\mathbb{Z}(\sqrt{2})$

A continuación se presenta un algoritmo que permite realizar el estudio de descomposición de números en $\mathbb{Z}(\sqrt{2})$ en términos de factores primos que

se caracterizaron en los teoremas (4.5) (4.9) y (4.11), para ello, sea $(a, b) \in \mathbb{Z}(\sqrt{2})$, luego:

1. Aplicar la función N a (a, b)

2. Descomponer en factores primos a $N(a, b)$ teniendo en cuenta los números primos que se caracterizaron en N_2 a través de los teoremas (4.16), (4.17) y (4.18), obteniendo:

$$N(a, b) = N(a_1, b_1)N(a_2, b_2)...N(a_k, b_k)$$

3. Ordenar los factores primos de menor a mayor obteniendo

$$N(a, b) = N(a_{(1)}, b_{(1)})N(a_{(2)}, b_{(2)})...N(a_{(k)}, b_{(k)})$$

   donde $N(a_{(i)}, b_{(i)}) < N(a_{(j)}, b_{(j)})$ para $i < j$

4. Aplicar el algoritmo expuesto en la sección 6.1.1 a $N(a_{(1)}, b_{(1)})$ (es decir, al menor de los factores primos) partiendo de la ecuación modular $a^2 \equiv x \pmod 2$ para obtener (a_1, b_1), y verificar que $(a_1, b_1)|(a, b)$, si en determinado caso $(a_1, b_1) \not|(a, b)$ entonces se aplica el algoritmo 6.1.1 a $N(a_{(1)}, b_{(1)})$ pero esta vez partiendo de la ecuación modular $a^2 \equiv -x \pmod 2$ (ver ejemplo 6.11)

5. Por último, se procede a buscar los otros factores mediante el uso de sistema de ecuaciones.

Se puede observar de forma general que el método para descomponer a (a, b) en factores primos consiste inicialmente en utilizar la función N, esto se hace con el objetivo de no trabajar directamente con el conjunto $\mathbb{Z}(\sqrt{2})$, sino con el conjunto N_2, después, se descompone en factores primos a $N(a, b)$,por último, volvemos de nuevo a $\mathbb{Z}(\sqrt{2})$. Como estamos elaborando un acercamiento a un teorema homólogo al teorema fundamental de la aritmética en $\mathbb{Z}(\sqrt{2})$, es necesario hacer énfasis en la unicidad de la factorización, suponga que no se utiliza el paso 3 y 4 del algortimo descrito, luego, al momento de pasar del conjunto N_2 al conjunto $\mathbb{Z}(\sqrt{2})$, existen múltiples parejas (c, d) tales que $N(c, d) = x$ donde x es un factor primo de $N(a, b)$ y que además $(c, d)|(a, b)$, por lo tanto la factorización en $\mathbb{Z}(\sqrt{2})$ no es única. Para comprender un poco mejor esta afirmación, considere el siguiente ejemplo:

Ejemplo 6.6: Sea $(2, 0)$, al aplicar la función N se tiene que $N(2, 0) = 4$, 4 es un número compuesto en N_2 puesto que $2|4$ y $2 \in N_2$, luego al factorizar

en factores primos a 4 en N_2 se tiene que $4 = (2)(2)$, luego, se deben encontrar a dos elementos (a_1, b_1) y (a_2, b_2) en $\mathbb{Z}(\sqrt{2})$ tales que el producto de estos sea $(2, 0)$ y además que $N(a_1, b_1) = 2$ y $N(a_2, b_2) = 2$. Existen múltiples parejas que cumplen con estas condiciones entre las cuales tenemos: Sea $(0, 1)$, luego $(0, 1)(0, 1) = (2, 0)$, y $N(0, 1) = 2$, por otra parte, sea $(2, 1)$ y $(2, -1)$, luego $(2, 1)(2, -1) = (2, 0)$ y $N(2, 1) = N(2, -1) = 2$. Nótese que como $N(0, 1) = N(2, 1) = N(2, -1) = 2$, entonces por el teorema (4.5) se tiene que $(0, 1)$, $(2, 1)$ y $(2, -1)$ son primos. Así, la factorización prima en $\mathbb{Z}(\sqrt{2})$ no es única.

Aunque la factorización en $\mathbb{Z}(\sqrt{2})$ no es única, una forma de solucionar este inconveniente es mediante los pasos 3 y 4 del algoritmo, pues estos permiten generar una única factorización. A continuación se presentan algunos ejemplos del algoritmo propuesto en la sección 6.1.2

Ejemplo 6.7 Descomponer $(16, 11)$ en factores primos.

Solución: Aplicando la función N se tiene:

$$N(16, 11) = |16^2 - 2(11)^2| = |256 - 2(121)| = |256 - 242| = |14| = 14$$

vemos que 14 es un número compuesto en N_2 luego $14 = (2)(7)$, vemos que 2 y 7 son números primos en N_2, ahora se debe encontrar un (a, b) tal que $N(a, b) = 2$, aplicando el algoritmo anterior se tiene:

$$N(a, b) = a^2 - 2b^2 = 2$$

$$a^2 \equiv 2(mod\ 2) \Rightarrow \begin{cases} a_1 = 2 + 2t \\ \\ a_2 = 2t \end{cases}$$

$$(2 + 2t)^2 - 2(b_1)^2 = 2 \Rightarrow (b_1)^2 = \frac{(2 - (2 + 2t)^2)}{(-2)} \Rightarrow b_1 = \sqrt{\frac{(2 - (2 + 2t)^2)}{(-2)}}$$

$$b_1 = \sqrt{(1 + 4t + 2t^2)}$$

$$(2t)^2 - 2(b_2)^2 = 2 \Rightarrow (b_2)^2 = \frac{(2 - (2t)^2)}{(-2)} \Rightarrow b_2 = \sqrt{\frac{(2 - (2t)^2)}{(-2)}}$$

$$b_2 = \sqrt{(-1 + 2t^2)}$$

Para $t = 1$ se tiene

$a_1 = 2 + 2 = 4$ y $b_1 = \sqrt{1 + 4 + 2} = \sqrt{7}$, como b_1 es un número no entero necesitamos realizar el reemplazo en a_2 y b_2. luego

$a_2 = 2$ y $b_2 = \sqrt{-1 + 2} = \sqrt{1} = 1$

Como ambas soluciones son enteros hemos terminado, la solución es $(2, 1)$.

Ahora se debe encontrar la pareja (x, y) tal que $(16, 11) = (2, 1)(x, y)$ para esto, aplicando la definición de multiplicación en $\mathbb{Z}(\sqrt{2})$ se obtiene:

$$(2x + 2y, 2y + x) = (16, 11)$$

por definición de parejas ordenadas se obtiene el siguiente sistema de ecuaciones

$$2x + 2y = 16$$

$$2y + x = 11$$

resolviendo se obtiene que $x = 5$ e $y = 3$, nótese que $N(5, 3) = 7$, luego la descomposición en factores primos de $(16, 11)$ es:

$$(16, 11) = (2, 1)(5, 3)$$

Ejemplo 6.8 Descomponer $(-7, 3)$ en factores primos:

Solución: Como $N(-7, 3) = |(-7)2 - 2(3)^2| = |49 - (2)(9)| = |49 - 18| = |31| = 31$, como 31 es primo entonces $(-7, 3)$ es un número primo (Teorema 4.5).

Ejemplo 6.9 Descomponer $(2, 4)$ en factores primos.

Solución:

$$N(2, 4) = |2^2 - 2(4)^2| = |4 - 2(16)| = | - 28| = 28$$

como 28 es un número compuesto en N_2, entonces se descompone a 28 como $28 = (2)(2)(7)$, vemos que 2 y 7 son números primos, ahora se debe encontrar un (a, b) tal que $N(a, b) = 2$, el cuál se ha encontrado en el ejemplo 6.6 que es $(2, 1)$, como $(2, 1)|(2, 4)$, entonces existe (x, y) tal que $(2, 1)(x, y) = (2, 4)$, por definición de multiplicación en $\mathbb{Z}(\sqrt{2})$ se obtiene:

$$(2x + 2y, 2y + x) = (2, 4)$$

por definición de igualdad de parejas ordenadas se tiene el siguiente sistema de ecuaciones

$$2x + 2y = 2$$

$$x + 2y = 4$$

resolviendo este sistema de ecuaciones se obtiene $x = -2$ e $y = 3$, luego

$$(2, 4) = (2, 1)(-2, 3)$$

nótese que $N(-2, 3) = 14 = (2)(7)$, entonces ahora se debe descomponer $(-2, 3)$ en factores primos, luego del ejemplo 6.6 se tiene que $N(2, 1) = 2$, así se debe encontrar (w, z) tal que $(2, 1)(w, z) = (-2, 3)$, por definición de multiplicación en $\mathbb{Z}(\sqrt{2})$ se tiene

$$(2w + 2z, 2z + w) = (-2, 3)$$

por igualdad de parejas ordenadas se obtiene el siguiente sistema de ecuaciones

$$2w + 2z = -2$$

$$w + 2z = 3$$

resolviendo se obtiene que $(w, z) = (-5, 4)$, además $N(-5, 4) = 7$ por lo tanto, al descomponer $(2, 4)$ en factores primos se obtiene

$$(2, 4) = (2, 1)(2, 1)(-5, 4)$$

Ejemplo 6.10 Descomponer $(5, 4)$ en factores primos:

Solución: Como $N(5, 4) = |(5)2 - 2(4)^2| = |25 - (2)(16)| = |25 - 32| = |31| = 7$, como 7 es primo entonces $(5, 4)$ es un número primo (teorema 4.5).

Ejemplo 6.11 Descomponer $(33, 24)$ en factores primos

Solución: $N(33, 24) = |33^2 - 2(24)^2| = |1089 - 1152| = | - 63| = 63$, como 63 es un número compuesto en N_2 se puede expresar como factores primos de la forma $63 = (7)(9)$, donde 9 y 7 son números primos en N_2, se debe encontrar una pareja (a, b) tal que $N(a, b) = 7$, aplicando el algoritmo se encuentra que la pareja es $(3, 1)$, ahora se debe encontrar (x, y) tal que $(3, 1)(x, y) = (33, 24)$, por definición de multiplicación en $\mathbb{Z}(\sqrt{2})$ se tiene

$$(3x + 2y, 3y + x) = (33, 24)$$

por igualdad de parejas ordenadas

$$3x + 2y = 33$$

$$3y + x = 24$$

este sistema de ecuaciones no tiene solución, esto quiere decir que a pesar de que $N(3,1)|N(33,24)$ no necesariamente $(3,1)|(33,24)$. Sin embargo, el algoritmo que se utilizó para encontrar la pareja $(3,1)$ fue utilizando la ecuación modular $a^2 \equiv 7(mod\ 2)$, como no funcionó, entonces se utiliza el segundo caso del algoritmo que es utilizar la ecuación modular $a^2 \equiv -7(mod\ 2)$, al aplicar el algoritmo se obtiene la pareja $(-5,4)$ donde $N(-5,4) = 7$ y de forma análoga a los ejemplos anteriores se encuentra que:

$$(33,24) = (-5,4)(51,39)$$

nótese que $N(51,39) = 9$

Capítulo 7

Horizontes del trabajo

En este capítulo se expone algunos trabajos a futuro que se pueden realizar tomando como base lo que se desarrolló en los capítulos anteriores.

- En el capítulo 4, fue necesario realizar un estudio sobre un conjunto numérico denominado N_2, donde a través de los teoremas (4.14) y (4.15) se demostró que todos elementos que pertenezca a $\mathbb{N}$ y que además son cuadrados perfectos, pertenecen a N_2. Por otra parte, por medio de los teoremas (4.21) y (4.22) se caracterizaron algunos elementos que no existen en N_2. Así, para enriquecer estos resultados, se propone realizar un estudio detallado sobre N_2 con el objetivo de caracterizar absolutamente a todos los elementos que pertenecen a dicho conjunto.

- Continuando con el conjunto N_2, en este trabajo se lograron caracterizar algunos números primos en N_2 por medio de los teoremas (4.16), (4.17) y (4.18), aunque se tiene como conjetura que no existen números primos en N_2 distintos a los caracterizados en estos teoremas, se propone como tema de estudio caracterizar a todos los números primos en N_2.

- En cuanto al estudio del conjunto $\mathbb{Z}(\sqrt{2})$, a través de los teoremas (4.5), (4.9) y (4.11), se lograron caracterizar algunos números primos, análogamente al ítem anterior y como se expuso en este trabajo, se intuye que no existen otros números primos distintos a los caracterizados en estos teoremas, así, se propone como tema de estudio caracterizar a todos los números primos en $\mathbb{Z}(\sqrt{2})$.

- En el capítulo 6 de este trabajo, se propone un acercamiento al teorema homólogo al teorema fundamental de la aritmética en $\mathbb{Z}(\sqrt{2})$ en términos de factores primos que se lograron caracterizar, así y dado el

ítem anterior, se propone para trabajos posteriores elaborar un teorema homólogo al teorema fundamental de la aritmética en $\mathbb{Z}(\sqrt{2})$.

En el seminario de álgebra de la universidad Pedagógica Nacional, se ha venido estudiando casos particulares del conjunto $\mathbb{Z}(k)$ que se define como:

$$\mathbb{Z}(\sqrt{k}) = \{a + bk \mid a, b, \in \mathbb{Z}; k^2 \in \mathbb{Z} \ \ y \ \ k \notin \mathbb{Z}\}$$

Así, una vez estudiados varios casos particulares, se propone los siguientes temas de estudio:

- De forma análoga a como se definió N_2, definir N_k y realizar un estudio general sobre este conjunto, donde se caractericen números primos.
- Realizar un estudio de forma general sobre $\mathbb{Z}(\sqrt{k})$ caracterizando números primos y elaborar un teorema homólogo al teorema fundamental de la aritmética.

Capítulo 8

Conclusiones

- La principal característica del conjunto $\mathbb{Z}(\sqrt{2})$ radica en que todos sus elementos tienen infinitos divisores, diferente a lo que sucede en el conjunto de los números naturales y enteros. Lo cual representa un cambio en torno a la noción que se tenía respecto a las unidades, números primos y números compuestos.

- Una forma que permite encontrar unidades en $\mathbb{Z}(\sqrt{2})$ es mediante el uso de la ecuación de **Pell-Fermat** $a^2 - 2b^2 = \pm 1$, donde hay infinitas soluciones, así, se tiene que en $\mathbb{Z}(\sqrt{2})$ hay infinitas unidades muy distinto a lo que se sucede en el conjunto de los números naturales y enteros.

- Un algoritmo que permite identificar si una pareja de la forma $(2n, m)$ es primo o no es verificando que $(2n, m)|(0, 1)$, si $(2n, m)|(0, 1)$ entonces $(2n, m)$ es primo.

- Se encontró que un algoritmo para identificar si $(a, b) \in \mathbb{Z}(\sqrt{2})$ es primo o no, sin necesidad de elaborar una lista de sus divisores, es aplicando la función N así, si $N(a, b) = x$ donde $x = |p|$ siendo p un número primo ó $x = p^2$ donde p es un número primo de la forma $4n + 1$ con n impar ó $x = p^2$ donde p es un número primo de la forma $4n + 3$ con n par, entonces (a, b) es primo.

- En N_2, bajo la definición usual de unidad, se tiene que análogamente al conjunto de los números naturales, 1 es la unidad.

- En N_2, a pesar de ser un subconjunto de los números naturales, existen elementos que son primos en este conjunto y que a su vez no son números primos en los naturales.

- En el conjunto $\mathbb{Z}(\sqrt{2})$ se pueden establecer criterios de divisibilidad.
- Se encontró una forma de descomponer a un elemento en $\mathbb{Z}(\sqrt{2})$ en términos de factores primos que se lograron caracterizar.
- Como futuros profesores de matemáticas, es importante reflexionar en torno a la noción que se tiene de unidad, número primo y número compuesto, por lo tanto, las definiciones usuales que se presentan sobre estos elementos diferenciados no siempre funcionan.

Bibliografía

[1] Entero Gaussiano. Disponible en: es.wikipedia.org, Directorio: wiki, File: Entero_gaussiano.

[2] Jiménez L., Gordillo J. & Rubiano G. (2004). Teoría de números (para principiantes). Bogotá: Universidad Nacional de Colombia, Sede Bogotá. Facultad de Ciencias.

[3] Lefèvre V. (1993). Entiers de Gauss. Disponible en: www.vinc17.org, Directorio: math, File: entgauss.pdf.

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

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

[6] Parra R. ECUACION PELL. Disponible en: hojamat.es, Directorio: parra, File: pell.pdf

[7] Pettofrezzo A. & Byrkit D. (1972). INTRODUCCION A LA TEORIA DE LOS NUMEROS. España: Ediciones del Castillo, S. A.