Estudio de los números gaussianos-dobles desde la teoría de números

Johana Olarte Pataquiva

199240030

Carlos Augusto Montes Fajardo

199240028

Universidad Pedagógica Nacional

Facultad de Ciencia y Tecnología

Departamento de Matemáticas

Bogotá, D.C.

2006

Estudio de los números gaussianos-dobles desde la teoría de números

Johana Olarte Pataquiva

Carlos Augusto Montes Fajardo

Trabajo de grado presentado como

requisito parcial para optar al

título de Licenciado en Matemáticas

Asesor

Carlos Julio Luque Arias

Docente Universidad Pedagógica Nacional

Universidad Pedagógica Nacional

Facultad de Ciencia y Tecnología

Departamento de Matemáticas

Bogotá, D.C.

2006

A mis padres,
que con su esfuerzo y dedicación han contribuido en mi
desarrollo profesional.

Johana Olarte

A mi madre,
que con su incondicional apoyo me ha motivado
a cumplir con mis metas.

Carlos Montes

En especial a nuestro gran amigo Helbert Rodriguez,
que la falta de razonamiento de algunos
terminaron con su existencia.

Johana y Carlos

Tabla de contenido

Introducción **i**

Objetivos **iv**

1 El anillo de los números Dobles **1**

1.1 El anillo de los números gaussianos-dobles 2

1.1.1 Elemento inverso de la multiplicación 4

1.2 El conjugado de un número gaussiano-doble 10

1.3 La σ-norma de un número gaussiano-doble 12

1.4 Algoritmo de división de los números gaussianos-dobles 15

1.5 Divisibilidad en $Z[\sigma]$ 17

1.6 Unidades de $Z[\sigma]$ 26

1.7 Números asociados en $Z[\sigma]$ 28

1.8 Teorema de descomposición de la $Z[\sigma]$-aritmética 29

1.9 Números primos en $Z[\sigma]$ 31

1.10 Criterios de divisibilidad en $Z[\sigma]$ 58

1.11 Máximo común divisor 65

1.12 Algoritmo de Euclides en $Z[\sigma]$ 67

1.13 Ecuaciones diofánticas gaussianas-dobles 74

1.14 Teoría de congruencias 78

1.15 Ideales en $Z[\sigma]$ 83

Anexos **86**

Bibliografía **93**

Introducción

Día a día la educación nos sugiere ir creando nuevas experiencias que reconstruyan los procesos de enseñanza y aprendizaje de una forma más dinámica, puesto que el mismo contexto se ha ido transformando. Esto se debe a que frente a la serie de inquietudes que se presentan actualmente es necesario que nosotros como maestros, seres artífices de conocimiento matemático, desarrollemos habilidades dentro de este campo, con el fin de fortalecer nuestro desempeño académico, profesional y personal.

De esta forma en el desarrollo de este trabajo haremos diferentes actividades que nos permitan articular procesos de creación, discusión, proposición de algoritmos, manejo de teorías, formulación de conjeturas, formulación y demostración de teoremas y en general, dichas actividades son características del trabajo matemático el cual resulta motivante porque brinda la posibilidad de investigar y formular proposiciones con propiedad o grado de generalidad, lo que permite que los docentes contemos con fundamentos sólidos

en el hacer y quehacer matemático y así mismo generar interés y motivación en nuestros estudiantes hacia el aprendizaje de las matemáticas.

Es así que para llegar a este fin se propuso y desarrollo este estudio titulado "Estudio de los números gaussianos-dobles desde la teoría de números".

Inicialmente, teniendo en cuenta la estructura de los números de Minkowski o números dobles construimos un conjunto de números que los denominamos *Números gaussianos-dobles*, este es un anillo conmutativo con unidad (1, 0), y con divisores de cero. Como en el anillo de los números gaussianos-dobles no todos los números poseen inversos entonces, buscamos cuáles si tiene inversos y los definimos como unidades. Seguidamente determinamos el conjugado de un número gaussiano-doble, para luego definir una función llamada σ-norma, se denomina de esta forma puesto que la función no cumple todas las condiciones necesarias para ser una norma euclidiana.

Estudiamos la divisibilidad dentro de este conjunto, así como también se determinaron criterios de divisibilidad.

Teniendo en cuenta la definición de números primos en los números enteros se encontraron números gaussianos-dobles distintos de cero y de las unidades que son divisibles únicamente por las unidades y sus asociados los cuales llamamos números primos gaussianos-dobles. Generalizamos una forma de encontrarlos y realizamos un programa escrito en lenguaje de programación python que además de determinar números primos, determina la σ-norma y realiza la multiplicación de dos números gaussianos-dobles.

Así mismo a los números distintos de las unidades y los números primos gaussianos-dobles los llamamos números compuestos y generalizamos la descomposición de ellos.

Determinamos un algoritmo para realizar la división de números dentro de este conjunto, así como un procedimiento para hallar el máximo común divisor.

Analizamos que ocurre con el algoritmo de euclides en este anillo. Y a partir de este análisis planteamos la resolución de ecuaciones diofánticas.

También se desarrollaron algunos teoremas sobre teoría de congruencias dentro de este conjunto. A partir de las conjeturas formuladas a lo largo de este trabajo se definen y demuestran los teoremas.

Para el desarrollo de este proyecto fue necesario realizar el estudio de las estructura de los números dobles, los números gaussianos y los números duales, de igual manera profundizar en el conocimiento de la teoría de números, teoría de anillos y algebra moderna.

Llegados a este punto fue necesario, de la manera más precisa y concreta posible sistematizar cada uno de los resultados en cuanto a lo que se puede y se debe hacer y que sea lógicamente coherente con todo lo planteado.

Finalmente será necesario producir la capacidad propositiva y que los docentes permitan compartir con otras personas lo aprendido, ya que vale la pena dedicar un tiempo importante a esto, con el fin de no limitar los procesos de aprendizaje, sino enriquecerlos y así pensar y transformar nuestra propia práctica.

Los autores.

Objetivos

- Elaboración de un documento donde se recopile el estudio de la teoría de los Números *Gaussianos-Dobles* teniendo en cuenta, estudios previos sobre Teoría de Números.

- Efectuar actividad matemática como parte fundamental de nuestra formación profesional, con el fin de desarrollar habilidad en el análisis y redacción de conjeturas matemáticas.

Resumen Analítico - RAES

Tipo de documento: Tesis de Grado

Acceso al documento: Universidad Pedagógica Nacional

Titulo del documento: Estudio de los números gaussianos-dobles desde la teoría de números.

Autor(s): OLARTE PATAQUIVA, Johana

MONTES FAJARDO, Carlos Augusto

Palabras Claves: gaussianos-dobles, anillo, unidades, asociados, primos, σ-norma, divisibilidad, algoritmo.

Descripción:

Teniendo en cuenta la estructura de dos conjuntos de números, los números dobles y los números gaussianos, sus operaciones, propiedades, relaciones y características se define un subconjunto de los números dobles llamado "*números gaussianos dobles*". En este documento se analiza su estructura teniendo en cuenta estudios anteriores en teoría de números y teoría de anillos.

Fuentes:

Las fuentes consultadas para la elaboración del documento son de carácter teórico donde se desarrollan temas tales como teoría de números, teoría de grupos, teoría de anillos y algebra moderna.

Contenidos:

Los temas desarrollados en el documento son:

El anillo de los números Dobles, se define este conjunto con sus operaciones y propiedades fundamentales.

El anillo de los números gaussianos-dobles, se define como un subanillo del conjunto de los números dobles.

El conjugado de un número gaussiano-doble, se define las caracteristicas de este número y se enuncian algunos teoremas.

La σ-norma de un número gaussiano-doble, se define la función σ-norma, y se enuncian algunos teoremas.

Algoritmo de división de los números gaussianos-dobles, Se define el procedimiento para dividir dos números gaussianos-dobles.

Divisibilidad en $Z[\sigma]$, se explica que condiciones debe cumplir un número gaussiano-doble para que divida a otro.

Unidades de $Z[\sigma]$, se encuentran las unidades, de este conjunto.

Teorema de descomposición de la $Z[\sigma]$-aritmética, muestra que no todos los números pueden descomponerse en factores primos en este conjunto.

Números primos en $Z[\sigma]$, se determinan los números primos y algunas formas de hallarlos.

Máximo común divisor, se explica el procedimiento para hallar el máximo común divisor de dos números gaussianos-dobles.

Teoría de congruencias, se definen algunos teoremas de congruencias.

Fecha Elaboración resumen Día 15 Mes 05 Año 2006

CAPÍTULO 1

El anillo de los números Dobles

El conjunto $\mathbb{R}^2$, donde $\mathbb{R}$ es el conjunto de los números reales con la suma definida componente a componente y el producto dado por

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

forma un anillo conmutativo con unidad $(1,\, 0)$, inverso multiplicativo de $(a,\, b)$

$$z^{-1} = \frac{1}{a^2 - b^2}(a,\, -b),$$

con $a^2 \neq b^2$ y con divisores de cero, es decir no es un dominio de integridad, conocido como el anillo de los *números dobles*[1] o de *Minkowski*, que notaremos M.

[1] Yaglom, I. *A simple non Euclidean Geometry and its Physical basis.* Springer. 1979, p. 265.

Igualdad de los números dobles

Dos números dobles $z = (a,\, b)$ y $w = (c,\, d)$ son iguales si y sólo si $a = c$ y $b = d$.

Propiedad distributiva de la multiplicación respecto a la adición de números dobles

Para todo $z = (a,\, b)$, $w = (c,\, d)$ y $v = (e,\, f)$ en M, se cumple que

$$z(w + v) = z\,w + z\,v$$

Prueba:

$$\begin{aligned}
z(w+v) &= (a,\, b)\,\big((c,\, d) + (e,\, f)\big) \\
&= (a,\, b)\,(c+e,\, d+f) && \text{Definición de adición} \\
&= \big(a(c+e) + b(d+f),\, b(c+e) + a(d+f)\big) && \text{Definición de multiplicación} \\
&= \big((ac+ae) + (bd+bf),\, (bc+be) + (ad+af)\big) && \text{Propiedad distributiva de la} \\
&&& \text{multiplicación respecto a la} \\
&&& \text{adición de los enteros} \\
&= \big((ac+bd) + (ae+bf),\, (bc+ad) + (be+af)\big) && \text{Propiedad conmutativa y} \\
&&& \text{asociativa de los enteros} \\
&= (ac+bd,\, bc+ad) + (ae+bf,\, be+af) && \text{Definición de adición} \\
&= (a,\, b)\,(c,\, d) + (a,\, b)\,(e,\, f) && \text{Definición de multiplicación} \\
&= z\,w + z\,v && \square
\end{aligned}$$

1.1 El anillo de los números gaussianos-dobles

Consideremos el subconjunto de M,

$$Z[\sigma] = \{(a,\, b) \in M \ \text{ tal que } \ a, b \in \mathbb{Z}\}$$

donde $\mathbb{Z}$ es el conjunto de los números enteros, a es la parte entera y b es la parte *gaussiana-doble*[2].

$Z[\sigma]$ es un subanillo de M ya que cumple las siguientes propiedades.

i) $(0,\,0) \in Z[\sigma]$;

ii) $(z - w) \in Z[\sigma]$ para todo $z,\, w \in Z[\sigma]$;

iii) $z\,w \in Z[\sigma]$ para todo $z,\, w \in Z[\sigma]$.

Consideremos el subconjunto de $Z[\sigma]$ dado por

$$A = \{(a,\,0) \in Z[\sigma] \text{ tal que } a \in \mathbb{Z}\}.$$

Veamos que la aplicación $f((a,\,0)) = a$ define un *isomorfismo*[3] entre el anillo A y el anillo de los números enteros ya que

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

y

$$f((a,\,0)\,(b,\,0)) = f((a\,b,\,0)) = a\,b.$$

Veamos si $Z[\sigma]$ es un *dominio de integridad*, para esto verifiquemos si es válida la *ley de simplificación (propiedad cancelativa)*[4].

[2]El símbolo σ aparece porque la pareja $(a,\,b)$ se puede escribir $(a,\,b) = a(1,\,0) + b(0,\,1)$ identificamos a $(1,\,0) = 1$, $(0,\,1) = \sigma$ con $\sigma^2 = 1$ y $\sigma \neq \pm 1$. En analogía con los números gaussianos $Z[i]$.

[3]Dados dos anillos A, A', una función biyectiva $f : A \to A'$ se dice un isomorfismo de anillos si para todo par de elementos r, s de A se tiene que

$$f(r + s) = f(r) + f(s), \qquad f(rs) = f(r)\,f(s).$$

(Dorronsoro, J. *Números grupos y anillos*. Madrid: Addison-Wesley; 1996. 202 p.)

[4]La ley de simplificación para la multiplicación es válida sobre un anillo, para todo elemento no nulo, si y sólo si, el producto de dos elementos diferentes de cero es distinto de cero. (Lentin A, Rivaud J. *Algebra moderna*. Madrid: Aguilar; 1967. 78 p.)

En $Z[\sigma]$, existen elementos diferentes de cero tales que su producto es cero llamados *divisores de cero*, estos elementos son de la forma;

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

con $a \neq 0$.

Ya que la ley de simplificación no se cumple, entonces $Z[\sigma]$ no es un dominio de integridad.

Sin embargo existen números, de hecho casi todos, en $Z[\sigma]$ que si cumplen la propiedad cancelativa, estos números son de la forma $(a,\, b)$ donde $|a| \neq |b|$.

Consideremos el subconjunto de $Z[\sigma]$ que llamaremos $Z'[\sigma]$ donde

$$Z'[\sigma] = \{(a,\, b) \in Z[\sigma] \text{ tal que } |a| \neq |b| \text{ con } a \times b \neq 0\}.$$

El conjunto $Z'[\sigma]$ tiene estructura de monoide para la operación multiplicación, además es conmutativa, cumple la propiedad cancelativa y no tiene divisores de cero.

1.1.1 Elemento inverso de la multiplicación

Busquemos que elementos $(a,\, b) \in Z[\sigma]$ tiene inverso multiplicativo, para ello debemos encontrar un número $(x,\, y)$ en $Z[\sigma]$, tal que cumpla la siguiente igualdad

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

de aquí

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

$$a\,x + b\,y = 1 \tag{1.1}$$

$$a\,y + b\,x = 0. \tag{1.2}$$

Multiplicando (1.1) por $-b$ y (1.2) por a se tiene

$$-bax - b^2\, y = -b$$

$$a^2\, y + abx = 0$$

sumando las igualdades obtenemos:

$$(a^2 - b^2)\, y = -b$$

Por otro lado, multiplicando (1.1) por a y (1.2) por $-b$ se tiene

$$a^2x + aby = a$$

$$-bay - b^2x = 0$$

sumando las igualdades obtenemos

$$(a^2 - b^2)\, x = a.$$

Es decir,

$$(a^2 - b^2)\, x = a$$

$$(a^2 - b^2)\, y = -b$$

Para que x e y sean números enteros, es necesario que ocurra por lo menos una de las siguientes condiciones:

i) $a^2 - b^2 = \pm 1$

ii) $a^2 - b^2 | a \quad$ y $\quad a^2 - b^2 | b$

Veamos para cuáles números a y $b \in \mathbb{Z}$ se cumple la condición:

i) $a^2 - b^2 = \pm 1$.

Esta ecuación es un caso particular de la ecuación de *Pell*[5] $x^2 - dy^2 = N$ donde N y d son números enteros.

Con $d > 0$, si d es un cuadrado entonces esta ecuación puede escribirse como

$$x^2 - (d'y)^2 = 1$$

y como los únicos dos cuadrados cuya diferencia es 1 son 0 y 1, las únicas soluciones en este caso son[6] $x = \pm 1$ e $y = 0$. Igualmente para la ecuación $x^2 - y^2 = -1$, se tiene las soluciones; $x = 0$ e $y = \pm 1$.

Se puede encontrar las soluciones de esta ecuación de la siguiente forma:

$$a^2 - b^2 = \pm 1$$

$$(a - b)(a + b) = \pm 1$$

de aquí, un caso es

$$a - b = 1$$

[5]Realmente esta ecuación nunca fue considerada por Pell $(1610 - 1685)$, puesto que el no fue ni el primero en tratarla ni el primero en resolverla. Hankel supuso que la ecuación fue llamada así debido a que la solución fue reproducida por Pell de una edición inglesa que hizo en 1668 de la obra de Thomas Brouncker. La atribución de la solución de Pell fue erróneamente dado por Euler probablemente debido a la lectura rápida que hizo del segundo volumen de la *Opera* de Wallis en la cual aparece la ecuación $ax^2 + 1 = y^2$, así corno los trabajos hechos por Pell en análisis indeterminado. Los primeros matemáticos griegos e hindúes consideraron casos especiales, pero Fermat fue el primero en tratarla sistemáticamente. Este dijo que había demostrado, en el caso especial en que $N = 1$ y $d > 0$ no es un cuadrado perfecto, que existe una infinidad de soluciones enteras x, y; pero como ya es usual, no dio una demostración. La primera demostración publicada fue dada por Lagrange, quien usó la teoría de las fracciones continuadas. Anterior a esta, Euler demostró que existe una infinidad de soluciones si es que existe una. (Leveque, W. *Elementary theory of numbers.* New york: Dover publications; 1962. 111 p.)

[6]*Ibíd.*, 112-113 pp.

$$a + b = 1$$

entonces

$$\begin{bmatrix} 1 & -1 \\ 1 & 1 \end{bmatrix} \begin{bmatrix} a \\ b \end{bmatrix} = \begin{bmatrix} 1 \\ 1 \end{bmatrix}$$

luego

$$\begin{bmatrix} a \\ b \end{bmatrix} = \frac{1}{2} \begin{bmatrix} 1 & 1 \\ -1 & 1 \end{bmatrix} \begin{bmatrix} 1 \\ 1 \end{bmatrix} = \begin{bmatrix} 1 \\ 0 \end{bmatrix}$$

$$a = 1 \quad \text{y} \quad b = 0$$

Para los casos restantes es análogo el procedimiento para hallar las siguientes soluciones:

$$a = 1 \qquad \text{y} \qquad b = 0$$

$$a = -1 \quad \text{y} \qquad b = 0$$

$$a = 0 \qquad \text{y} \qquad b = 1$$

$$a = 0 \qquad \text{y} \qquad b = -1.$$

Veamos para cuáles números a y $b \in \mathbb{Z}$ se cumple la condición:

ii) $a^2 - b^2 | a \quad \text{y} \quad a^2 - b^2 | b.$

Por definición de divisibilidad, existen p, $q \in \mathbb{Z}$ tales que;

$$a = (a^2 - b^2)\, p \tag{1.3}$$

$$b = (a^2 - b^2)\, q. \tag{1.4}$$

Multiplicando las anteriores igualdades por b y $-a$, respectivamente tenemos;

$$ba = b\,(a^2 - b^2)\, p \tag{1.5}$$

$$-ab = -a\,(a^2 - b^2)\, q \tag{1.6}$$

sumando las igualdades (1.5) y (1.6):

$$0 = (a^2 - b^2)(pb - qa).$$

Luego

$$a^2 - b^2 = 0 \qquad \text{ó} \qquad pb - qa = 0$$

pero, $a^2 - b^2$ tiene que ser distinto de cero, ya que si fuera igual a cero se tendría que

$$0|a \quad \text{y} \quad 0|b$$

lo que es imposible.

Luego debe ocurrir que

$$pb - qa = 0$$

es decir;

$$pb = qa. \tag{1.7}$$

De esta igualdad podemos tomar dos caminos:

(a) si

$$b = \frac{qa}{p} \tag{1.8}$$

$b \in \mathbb{Z}$, ya que por (1.3) se tiene que $p|a$, entonces $p|aq$.

Remplazando (1.8) en (1.3), se tiene:

$$a = \left(a^2 - \frac{q^2a^2}{p^2}\right)p$$

$$a = a^2\, p\left(1 - \frac{q^2}{p^2}\right)$$

$$1 = a\, p\left(1 - \frac{q^2}{p^2}\right).$$

Entonces

$$ap = \pm 1 \qquad \text{y} \qquad 1 - \frac{q^2}{p^2} = \pm 1$$

como $ap = \pm 1$, entonces a es el inverso multiplicativo de p o, p es el inverso multiplicativo de a, pero como a y $p \in \mathbb{Z}$, entonces $a = \pm 1$ y $p = \pm 1$.

Como

$$1 - \frac{q^2}{p^2} = \pm 1$$

remplazando $p = \pm 1$, se tiene

$$1 - \frac{q^2}{(\pm 1)^2} = \pm 1$$

$$1 - \frac{q^2}{1} = \pm 1$$

$$1 - q^2 = \pm 1$$

$$1 \pm 1 = q^2$$

$$1 + 1 = q^2 \qquad \text{ó} \qquad 1 - 1 = q^2$$

$$2 = q^2 \qquad \text{ó} \qquad 0 = q^2$$

pero como $q \in \mathbb{Z}$, entonces $q = 0$.

Remplazando a, p y q en (1.7) se tiene

$$\pm 1\, b = 0 \pm 1$$

$$b = 0,$$

luego, $a = \pm 1$ y $b = 0$.

(b) O si

$$a = \frac{pb}{q}.$$

La demostración es análoga a la del caso anterior, para obtener las siguientes soluciones:

$$a = 0 \text{ y } \quad b = \pm 1.$$

Entonces los números a y $b \in \mathbb{Z}$, que cumplen la condición *ii)* son:

$$a = 1 \qquad \text{y} \qquad b = 0$$

$$a = -1 \quad \text{y} \qquad b = 0$$

$$a = 0 \qquad \text{y} \qquad b = 1$$

$$a = 0 \qquad \text{y} \qquad b = -1$$

es decir para estos números las ecuaciones (1.1) y (1.2) tienen soluciones en los números enteros.

Por tanto, los únicos números gaussianos-dobles que tienen inverso multiplicativo son:

$$(1,\, 0) \quad (-1,\, 0) \quad (0,\, 1) \quad (0,\, -1).$$

De la condición i), podemos enunciar el siguiente teorema.

Teorema 1.

Los únicos números enteros a y b que cumplen

$$a^2 - b^2 = \pm 1$$

son

$$\begin{aligned} a &= 1 \quad && y \quad && b = 0, \\ a &= -1 \quad && y \quad && b = 0, \\ a &= 0 \quad && y \quad && b = 1, \\ a &= 0 \quad && y \quad && b = -1. \end{aligned}$$

1.2 El conjugado de un número gaussiano-doble

Llamaremos el *conjugado* de un número gaussiano-doble $z = (a,\, b)$ al número

$$\overline{z} = (a,\, -b).$$

Teorema 2.

Para todo $z \in Z[\sigma]$ se cumple que $z = \overline{z}$ si y sólo si z es un número entero.

Teorema 3.

Para todo $z,\, w \in Z[\sigma]$ se cumple que

$$\overline{z + w} = \overline{z} + \overline{w}.$$

Prueba:

Si $z = (a,\, b)$, $w = (c,\, d)$, entonces $\overline{z} = (a,\, -b)$ y $\overline{w} = (c,\, -d)$ entonces

$$\begin{aligned}
\overline{z + w} &= \overline{(a,\, b) + (c,\, d)} \\
&= \overline{(a + c,\, b + d)} && \text{Definición de adición} \\
&= (a + c,\, -b - d) && \text{Definición de conjugado} \\
&= (a,\, -b) + (c,\, -d) && \text{Definición de adición} \\
&= \overline{z} + \overline{w} && \square
\end{aligned}$$

Teorema 4.

Para todo z, $w \in Z[\sigma]$ se cumple que

$$\overline{z \times w} = \overline{z} \times \overline{w}.$$

Prueba:

Sea $z = (a,\, b)$, $w = (c,\, d)$, entonces $\overline{z} = (a,\, -b)$ y $\overline{w} = (c,\, -d)$ entonces

$$\begin{aligned}
\overline{z \times w} &= \overline{(a,\, b)\,(c,\, d)} \\
&= \overline{(ac + bd,\, bc + ad)} && \text{Definición de multiplicación} \\
&= (ac + bd,\, -bc - ad) && \text{Definición de conjugado} \\
&= (a,\, -b)\,(c,\, -d) && \text{Definición de multiplicación} \\
&= \overline{z} \times \overline{w} && \square
\end{aligned}$$

Teorema 5.

Para todo número natural $n \geq 2$ y todo número gaussiano-doble z, se tiene que

$$\overline{z^n} = (\overline{z})^n.$$

Prueba:

Por inducción sobre n:

Primero verificamos para $n = 2$; que es consecuencia inmediata del teorema 4.

Ahora supongamos que se cumple para algún $n = k$; es decir que,

$$\overline{z^k} = (\overline{z})^k$$

debemos probar que

$$\overline{z^{k+1}} = (\overline{z})^{k+1}$$

Entonces

$$\begin{aligned}
\overline{z^{k+1}} &= (\overline{z^k \times z}) \\
&= (\overline{z^k} \times \overline{z}) && \text{Por el teorema 4} \\
&= (\overline{z}^k \times \overline{z}) && \text{Por la hipótesis de inducción} \\
&= (\overline{z})^{k+1}
\end{aligned}$$

Por tanto el teorema es válido para todo número natural n. □

1.3 La σ-norma de un número gaussiano-doble

Para que $Z[\sigma]$ sea un *Anillo euclidiano*[7], entonces debe determinarse una función

$$\boldsymbol{N} : Z[\sigma] - \{0\} \to \mathbb{N},$$

la *función grado*, tal que:

i) $\boldsymbol{N}(z) \leq \boldsymbol{N}(z\,w)$ para todo $z,\ w \in Z[\sigma]$ con $z,\ w \neq 0$.

ii) Para todo $w,\ z \in Z[\sigma]$ con $w \neq 0$, existen $k,\ p \in Z[\sigma]$ tales que

$$z = k\,w + r$$

donde $\boldsymbol{N}(r) = 0$ o bien $\boldsymbol{N}(r) < \boldsymbol{N}(w)$.

[7]Perez, E. *Estructuras algebraicas.* Bogotá. Universidad Pedagógica Nacional, 2005. 48 p.

Si la función grado $\boldsymbol{N}$ es multiplicativa:

$$\boldsymbol{N}(z\,w) = \boldsymbol{N}(z)\ \boldsymbol{N}(w)$$

se llama *norma euclídiana*.

Definamos una función en $Z[\sigma]$ como sigue:

Si multiplicamos un número gaussiano-doble $z = (a,\, b)$ por su conjugado $\overline{z}$ obtenemos

$$z \times \overline{z} = a^2 - b^2$$

como esta multiplicación no siempre es positiva entonces la función queda definida así:

$$\boldsymbol{N}(z) = \begin{cases} a^2 - b^2 & \text{si} \quad a^2 \geq b^2 \\ b^2 - a^2 & \text{si} \quad b^2 > a^2 \end{cases}$$

Esta función no es una función grado ya que no cumple la condiciíon *i)*, puesto que existen elementos en $Z[\sigma]$ que no cumplen la desigualdad. Por ejmplo;

$$\boldsymbol{N}(4,\, -3) \nleq \boldsymbol{N}((4,\, -3)(3,\, 3))$$
$$7 \nleq 0.$$

Sin embargo la propiedad *i)* si se cumple para los elementos de $Z'[\sigma]$.

La función cumple la propiedad *ii)* para todos los elementos de $Z[\sigma]$. (La demostración la realizaremos en la siguiente sección.)

Como la función cumple la propiedad *i)* para todos los elementos de $Z'[\sigma]$ y *ii)* para todos los elementos de $Z[\sigma]$ llamaremos a esta función, *función σ-grado*.

Ya que la función σ-grado cumple el siguiente teorema

Teorema 6.

Para todo z, $w \in Z[\sigma]$ se tiene que

$$\boldsymbol{N}(z\,w) = \boldsymbol{N}(z)\ \boldsymbol{N}(w).$$

Prueba:

Por la definición de la función σ-grado, esta prueba debe hacerse por casos, pero realmente los casos no difieren uno de otros, la única diferencia es en lo algebraico por ello se demostrara solamente para un caso.

Sean $z = (a,\, b)$, $w = (c,\, d) \in Z[\sigma]$, entonces:

Si $a^2 \geq b^2$, y $\ c^2 \geq d^2$

$$\begin{aligned}
\boldsymbol{N}(z)\ \boldsymbol{N}(w) &= (a^2 - b^2)\,(c^2 - d^2) \\
&= (ac)^2 + (bd)^2 - (ad)^2 - (bc)^2 \\
&= (ac)^2 + 2acbd + (bd)^2 - (ad)^2 - 2adbc - (bc)^2 \\
&= (ac + bd)^2 - (ad + bc)^2 \\
&= \boldsymbol{N}(ac + bd,\, ad + bc) \\
&= \boldsymbol{N}\big((a,\, b)\,(c,\, d)\big) \\
&= \boldsymbol{N}(z\,w).
\end{aligned}$$

Análogamente en los demás casos. □

Entonces la función σ-grado la llamaremos *σ-norma euclídiana* o simplemnte *σ-norma*. La notaremos $\boldsymbol{N}(z)$ o $\boldsymbol{N}z$.

Observamos que el anillo $Z[\sigma]$ no es un anillo euclídiano con la función grado $\boldsymbol{N}$. Sin embargo, trabajeremos con la σ-norma definida.

Teorema 7.

Para todo $z \in Z[\sigma]$ se tiene que

$$\boldsymbol{N}z = \boldsymbol{N}\overline{z}.$$

Prueba:

Sea $z = (a,\, b)$, entonces

i) Si $a^2 \geq b^2$ entonces

$$\begin{aligned}\boldsymbol{N}z &= \boldsymbol{N}(a,\, b)\\ &= a^2 - b^2\\ &= a^2 - (-b^2)\\ &= \boldsymbol{N}(a,\, -b)\\ &= \boldsymbol{N}\,\overline{z}.\end{aligned}$$

ii) Si $b^2 > a^2$ entonces

$$\begin{aligned}\boldsymbol{N}z &= \boldsymbol{N}(a,\, b)\\ &= b^2 - a^2\\ &= (-b^2) - a^2\\ &= \boldsymbol{N}(a,\, -b)\\ &= \boldsymbol{N}\,\overline{z}. \quad \square\end{aligned}$$

1.4 Algoritmo de división de los números gaussianos-dobles

Teorema 8.

Si $z, w \in Z[\sigma]$ y $\boldsymbol{N}w > 0$, entonces existen k y $p \in Z[\sigma]$ tales que

$$z = w\,k + p \quad con \quad \boldsymbol{N}p < \boldsymbol{N}w$$

Prueba:

Sea $z = (a,\, b)$, $w = (c,\, d)$ y $\boldsymbol{N}w > 0$, podemos escribir

$$\frac{z}{w} = \frac{(a,\, b)}{(c,\, d)} = \frac{(a,\, b)\,(c,\, -d)}{(c,\, d)\,(c,\, -d)} = \frac{(a,\, b)\,(c,\, -d)}{c^2 - d^2} = (A,\, B)$$

donde A y B son números racionales, no necesariamente enteros.

Sean x y y los enteros más cercanos a A y B, respectivamente, entonces

$$|A - x| < \frac{3}{4},$$

$$|B - y| \leq \frac{1}{2}$$

entonces,

$$\begin{aligned}\boldsymbol{N}\Big(\frac{z}{w} - (x,\, y)\Big) &= \boldsymbol{N}\big((A - x),\, (B - y)\big) \\ &= \big((A - x)^2 - (B - y)^2\big) \leq \Big(\frac{9}{16} - \frac{1}{4}\Big) < 1.\end{aligned}$$

Por tanto, si hacemos

$$(x,\, y) = k, \qquad z - w\,k = p$$

y, k, $p \in Z[\sigma]$. Entonces

$$\begin{aligned}\boldsymbol{N}p &= \boldsymbol{N}(z - w\,k) \\ &= \boldsymbol{N}w\Big(\frac{z}{w} - k\Big) \\ &= \boldsymbol{N}w\ \boldsymbol{N}\Big(\frac{z}{w} - k\Big) < \boldsymbol{N}w. \quad \square\end{aligned}$$

Ejemplo

Dividamos $z = (6,\, 5)$ entre $w = (3,\, 1)$ se tiene;

$$\frac{z}{w} = \frac{(6,\, 5)}{(3,\, 1)} = \frac{(6,\, 5)}{(3,\, 1)}\frac{(3,\, -1)}{(3,\, -1)} = \frac{(13,\, 9)}{8} = (1,\, 1) + \frac{(5,\, 1)}{8}$$

$$\underbrace{(6,\,5)}_{z} = \underbrace{(1,\,1)}_{k}\,\underbrace{(3,\,1)}_{w} + \underbrace{\frac{(5,\,1)}{(3,\,-1)}}_{p}$$

como

$$p = \frac{(5,\,-1)}{(3,\,-1)} = \frac{(5,\,1)}{(3,\,1)}\,\frac{(3,\,-1)}{(3,\,1)} = \frac{(16,\,8)}{8} = (2,\,1)$$

entonces existen $k = (1,\,1)$ y $p = (2,\,1) \in Z[\sigma]$ tales que

$$\begin{aligned} z &= w\,k + p && \text{con} && \boldsymbol{N}p < \boldsymbol{N}w \\ (6,\,5) &= (3,\,1)\,(1,\,1) + (2,\,1) && \text{con} && \boldsymbol{N}(2,\,1) < \boldsymbol{N}(3,\,1) \\ & && && 3 < 8 \end{aligned}$$

Nota 1.

En el anillo $Z[\sigma]$ el cociente y el residuo no son únicos.

Ejemplo

$$\begin{aligned} (8,\,7) &= (5,\,3)\,(1,\,0) + (3,\,4) && \text{con} && \boldsymbol{N}(3,\,4) < \boldsymbol{N}(5,\,3) \\ & && && 7 < 16 \\ (8,\,7) &= (5,\,3)\,(2,\,0) + (-2,\,1) && \text{con} && \boldsymbol{N}(-2,\,1) < \boldsymbol{N}(5,\,3) \\ & && && 3 < 16. \end{aligned}$$

1.5 Divisibilidad en $Z[\sigma]$

Los Griegos [600 a.c - 300 d.c] hicieron de la aritmética, la parte de las matemáticas destinada al estudio de las propiedades de los número como tales. Pitágoras, Platón, Euclides, Arquímedes y Diofanto escribieron sobre teoría de divisibilidad. Posteriormente Fermat, Pascal, Euler, Langrange y Gauss fueron quienes principalmente lo desarrollaron creando la moderna aritmética superior. En los *Elementos de Euclides* se recopilan los principales resultados obtenidos por los griegos al respecto. Legrende en el siglo XVIII

publicó su *Teoría de Números*, en donde se recogen nuevos aportes en este campo, pero fue Gauss que en 1801 apoyándose en los resultados conocidos hasta el momento sobre divisibilidad, demostró el teorema fundamental de la aritmética, piedra angular sobre la cual descansa la aritmética superior.

Si z y w son dos números gaussianos-dobles, decimos que w divide a z (se escribe $w \mid z$) si existe un elemento $p \in Z[\sigma]$ tal que

$$z = w\,p.$$

En este caso decimos que w *es un divisor de* z, o que z *un múltiplo de* w.

Si w no divide a z se escribe $w \nmid z$.

Teorema 9.

Para todo $z \in Z[\sigma]$, *entonces* $z|z$.
Prueba:

Sean $z = (a,\, b)$ y $w = (1,\, 0)$, entonces

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

$$z = z\,w$$

por tanto

$$z|z. \quad \square$$

Teorema 10.

Sean z, $w \;\; y \;\; v \in Z[\sigma]$, *si* $z \mid w \;\; y \;\; w \mid v$ *entonces* $z \mid v$.

Prueba:

Como $z \mid w \;\; \text{y} \;\; w \mid v$, entonces existen $p \;\; \text{y} \;\; r \in Z[\sigma]$ tal que:

$$w = z\,p \tag{1.9}$$

$$v = w\,r. \tag{1.10}$$

remplazando (1.9) en (1.10) obtenemos:

$$v = (z\,p)\,r$$

aplicando la propiedad asociativa de la multiplicación de números gaussianos-dobles, tenemos;

$$v = z\,(p\,r)$$

lo que significa que $z \mid v$, que es lo que se quería demostrar. □

Luego por los teoremas 9 y 10, la relación de divisibilidad es reflexiva y transitiva.

Nota 2.

Para todo $z \in Z[\sigma]$, se tiene que $z \mid (0,\,0)$, pero $(0,\,0)$ solo divide a él mismo porque $(0,\,0)\,z = (0,\,0)$.

Teorema 11.

Sean z, w, $v \in Z[\sigma]$, si $z \mid w$ y $z \mid v$ entonces z divide cualquier combinación lineal de w y v.

Prueba:

Como $z \mid w$ y $z \mid v$, entonces existen p y $r \in Z[\sigma]$ tal que:

$$w = z\,p \tag{1.11}$$

$$v = z\,r. \tag{1.12}$$

Multiplicando (1.11) por $s \in Z[\sigma]$ y (1.12) por $t \in Z[\sigma]$ respectivamente, tenemos

$$s\,w = s\,(z\,p) \tag{1.13}$$

$$t\,v = t\,(z\,r) \tag{1.14}$$

sumando (1.13) y (1.14) obtenemos:

$$\begin{aligned} s\,w + t\,v =& s\,(z\,p) + t\,(z\,r) \\ =& s\,z\,p + t\,z\,r \\ =& z\,(s\,p + t\,r). \end{aligned}$$

Luego por definición de divisibilidad

$$z \mid (s\,w + t\,v).$$

Lo que significa que z divide a la combinación lineal de w y v, en particular divide a $w + v$. □

Teorema 12.

Sean z, w *y* $v \in Z[\sigma]$, *si* $z \mid w$ *y* $z \mid v$ *entonces* $z \mid (w\,v)$.

Prueba:

Como $z \mid w$ y $z \mid v$, entonces existen p y $r \in Z[\sigma]$ tal que:

$$w = z\,p \tag{1.15}$$

$$v = z\,r. \tag{1.16}$$

Multiplicando (1.15) y (1.16) obtenemos:

$$\begin{aligned} w\,v &= z\,p\,z\,r \\ &= z\,(p\,z\,r) \end{aligned}$$

lo que significa que $z \mid (w\,v)$, que es lo que se quería demostrar. □

Teorema 13.

Sean z, w *y* $v \in Z[\sigma]$, *si* $z \mid w$ *entonces* $(v\,z) \mid (v\,w)$.

Prueba:

Como $z \mid w$ entonces existe $p \in Z[\sigma]$ tal que:

$$w = z\,p$$

multiplicando a ambos lados de la igualdad por v

$$v\,w = v\,(z\,p)$$
$$v\,w = (v\,z)\,p$$

Luego

$$(v\,z) \mid (v\,w). \quad \square$$

Nota 3.

El recíproco del teorema 13 no se cumple, puesto que el conjunto de los números gaussianos-dobles no cumple la propiedad cancelativa.

Ejemplo

Sean $z = (1,\ 7)$, $v = (3,\ 3)$ *y* $w = (3,\ -3) \in Z[\sigma]$, *entonces*

$$(3,\ 3)\,(1,\ 7) \,\big|\, (3,\ 3)\,(3,\ -3)$$

ya que existe $(0,\ 0) \in Z[\sigma]$ *tal que:*

$$(3,\ 3)\,(3,\ -3) = (3,\ 3)\,(1,\ 7)\,(0,\ 0)$$
$$(0,\ 0) = (0,\ 0).$$

Veamos que

$$(1,\, 7) \nmid (3,\, -3)$$

ya que si lo dividiera existiría $(x,\, y) \in Z[\sigma]$ *tal que*

$$\begin{aligned}(3,\, -3) &= (1,\, 7)\,(x,\, y)\\ &= (x + 7y,\, 7x + y).\end{aligned}$$

es decir,

$$x + 7y = 3 \tag{1.17}$$

$$7x + y = -3 \tag{1.18}$$

Multiplicando (1.17) por -7 *y sumandola con (1.18) obtenemos,*

$$-48y = 18$$

y esta ecuacion no tiene solución en el conjunto de los números enteros.

Sin embargo el recíproco del teorema 13 se cumple para el conjunto $Z'[\sigma]$.

Teorema 14.

Sean $z,\, w\ y\ v \in Z'[\sigma]$, *si* $(v\, z) \mid (v\, w)$ *entonces* $z \mid w$.

Prueba:

Como $(v\, z) \mid (v\, w)$ entonces existe $p \in Z'[\sigma]$ tal que:

$$\begin{aligned}v\, w &= (v\, z)\, p\\ v\, w &= v\, (z\, p)\end{aligned}$$

aplicando la propiedad cancelativa

$$w = z\, p.$$

Luego

$$z \mid w. \quad \square$$

Teorema 15.

Para todo $z,\ w \in Z[\sigma]$ *se tiene que*

$$si\ z \mid w\ \ entonces\ \ \boldsymbol{N}z \mid \boldsymbol{N}w.$$

Prueba:

Por la definición de la σ-norma de números gaussianos-dobles, esta prueba debe hacerse por casos.

Sea $z = (a,\ b)$, $w = (c,\ d) \in Z[\sigma]$ entonces

i) Si $a^2 \geq b^2$ y $c^2 \geq d^2$, entoces, por hipótesis $z \mid w$, es decir $(a,\ b) \mid (c,\ d)$.

Por definición de divisibilidad, existe $(x,\ y) \in Z[\sigma]$ tal que

$$(c,\ d) = (a,\ b)\,(x,\ y)$$
$$(c,\ d) = (ax + by,\ ay + bx).$$

Calculando la σ-norma a ambos lados de la igualdad se tiene que;

$$c^2 - d^2 = (ax + by)^2 - (ay + bx)^2$$
$$c^2 - d^2 = (ax)^2 + 2axby + (by)^2 - (ay)^2 - 2aybx - (bx)^2$$
$$c^2 - d^2 = (ax)^2 + (by)^2 - (ay)^2 - (bx)^2$$
$$c^2 - d^2 = x^2(a^2 - b^2) - y^2(a^2 - b^2)$$
$$c^2 - d^2 = (a^2 - b^2)\,(x^2 - y^2)$$
$$\boldsymbol{N}(c,\ d) = \boldsymbol{N}(a,\ b)\ \boldsymbol{N}(x,\ y)$$

luego

$$\boldsymbol{N}(a,\, b) \mid \boldsymbol{N}(c,\, d)$$

$$\boldsymbol{N}z \mid \boldsymbol{N}w.$$

ii) De forma análoga se demuestran los otros casos. □

Teorema 16.

Sea $z = (a,\, b)$ *y* $w = (c,\, d)$ *números gaussianos-dobles, si* $z \mid w$ *entonces*

$$\boldsymbol{N}z \mid \overline{z}\, w.$$

Prueba:

Como $z \mid w$ entonces por definición de divisibilidad existe un $p \in Z[\sigma]$, tal que:

$$w = z\, p$$

multiplicando por el conjugado de z a ambos lados de la igualdad

$$\overline{z}\, w = \overline{z}\, z\, p$$

$$\overline{z}\, w = (a^2 - b^2)\, p$$

y de nuevo por la definición de divisibilidad en $Z[\sigma]$

$$(a^2 - b^2) \mid \overline{z}\, w,$$

$$\boldsymbol{N}z \mid \overline{z}\, w. \quad \square$$

Teorema 17.

Sea $z = (a,\, b)$ *y* $w = (c,\, d) \in Z'[\sigma]$, *si* $\boldsymbol{N}z \mid \overline{z}\, w$ *si y sólo si* $z \mid w$.

Prueba:

i) Como $\boldsymbol{N}z \mid \overline{z}\,w$ entonces por definición de divisibilidad existe un $p \in Z[\sigma]$, tal que:

$$\overline{z}\,w = \boldsymbol{N}z\,p$$

por la propiedad cancelativa se tiene

$$w = z\,p$$

es decir;

$$z \mid w.$$

ii) La demostración es evidente del teorema 16. □

Nota 4.

Sea $z \in Z[\sigma]$ entonces

$$\boldsymbol{N}z \nmid z.$$

Ejemplo

Sea $z = (3,\, 1)$, entonces

$$\boldsymbol{N}z = 8.$$

Luego $8 \nmid (3,\, 1)$, ya que si lo divide, existe $(x,\, y) \in Z[\sigma]$ tal que;

$$(3,\, 1) = (8,\, 0)\,(x,\, y)$$

$$(3,\, 1) = (8x,\, 8y).$$

es decir,

$$8x = 3$$

$$8y = 1$$

y este sistema no tiene solución en el conjunto de los números enteros. Por tanto $\boldsymbol{N}z \nmid z$.

1.6 Unidades de $Z[\sigma]$

Existen ciertos gaussianos-dobles que dividen a todos los números gaussianos-dobles, a estos números los llamaremos *unidades de* $Z[\sigma]$.

En particular, una unidad debe dividir a $(1,\,0)$. Sea $e = (a,\,b) \in Z[\sigma]$, si $e \mid (1,\,0)$, entonces e es una unidad.

Por definición de divisibilidad, existe $p \in Z[\sigma]$ tal que;

$$(1,\,0) = p\,e.$$

Para todo $z \in Z[\sigma]$, podemos escribir $z = z\,(1,\,0) = (z\,p)\,e$ de donde $e \mid z$. Por lo que podemos determinar las unidades de $Z[\sigma]$ simplemente determinando los divisores de $(1,\,0)$.

Ahora, si $e \mid (1,\,0)$ entonces, por el teorema 15, $\boldsymbol{N}e \mid \boldsymbol{N}(1,\,0)$, por lo que $\boldsymbol{N}e = 1$.

Por el teorema 1, las únicas soluciones de la ecuación $a^2 - b^2 = \pm 1$ en $\mathbb{Z}$ son:

$$\begin{array}{lll} a = 1 & \text{y} & b = 0 \\ a = -1 & \text{y} & b = 0 \\ a = 0 & \text{y} & b = 1 \\ a = 0 & \text{y} & b = -1. \end{array}$$

Y por tanto las únicas unidades de $Z[\sigma]$ son:

$$(1,\,0) \quad (-1,\,0) \quad (0,\,1) \quad (0,\,-1).$$

Teorema 18.

Sea $z = (a,\,b) \in Z[\sigma]$, $\boldsymbol{N}z = 1$ *si y sólo si* z *es una unidad.*

Prueba:

i) Si $\boldsymbol{N}z = 1$ *entonces* z *es unidad.*

Como $\boldsymbol{N}z = 1$ entonces, por definición de σ-norma

$$a^2 - b^2 = 1 \quad \text{ó} \quad a^2 - b^2 = -1$$

es decir;

$$a^2 - b^2 = \pm 1$$

por el teorema 1, los únicos números enteros a y b que cumplen esta igualdad son:

$$\begin{array}{lll} a = 1 & \text{y} & b = 0 \\ a = -1 & \text{y} & b = 0 \\ a = 0 & \text{y} & b = 1 \\ a = 0 & \text{y} & b = -1 \end{array}$$

De aquí los números gaussianos-dobles cuya $\boldsymbol{N}z = 1$ son:

$$(1,\, 0),\ (-1,\, 0),\ (0,\, 1),\ (0,\, -1)$$

es decir, las unidades.

ii) Si z *es una unidad entonces* $\boldsymbol{N}z = 1$.

Como z es una unidad entonces, z es uno de los siguientes números gaussianos-dobles; $(1,\, 0)$, $(-1,\, 0)$, $(0,\, 1)$, $(0,\, -1)$.

Si $z = (1,\, 0)$, entonces $\boldsymbol{N}z = \boldsymbol{N}(1,\, 0) = 1$.

Si $z = (-1,\, 0)$, entonces $\boldsymbol{N}z = \boldsymbol{N}(-1,\, 0) = 1$.

Si $z = (0,\, 1)$, entonces $\boldsymbol{N}z = \boldsymbol{N}(0,\, 1) = 1$.

Si $z = (0,\, -1)$, entonces $\boldsymbol{N}z = \boldsymbol{N}(0,\, -1) = 1$.

Por tanto, si z es una unidad entonces $\boldsymbol{N}z = 1$. □

1.7 Números asociados en $Z[\sigma]$

Dos números z y w son *asociados* en $Z[\sigma]$, si $z \mid w$ y $w \mid z$ y se denota como $z \sim w$.

Sea $z = (a,\, b) \in Z[\sigma]$ los asociados de z se consiguen al multiplicar z por las unidades de $Z[\sigma]$, esto es

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

luego los asociados de z (denotado como $\widetilde{z}$) son:

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

Para todo z, w y $t \in Z[\sigma]$, se tiene:

i) Reflexiva: $z \sim z$, ya que por el teorema 9, $z \mid z$.

ii) Simétrica: $z \sim w$ y $w \sim z$, ya que por definición de asociados en $Z[\sigma]$, $z \mid w$ y $w \mid z$.

iii) Transitiva: $z \sim w$ y $w \sim t$, entonces $z \sim t$. Como $z \sim w$ entonces $z \mid w$ y como $w \sim t$ entonces $w \mid t$, luego por el teorema 10, $z \mid t$, además $t \mid w$ y $w \mid z$ por el teorema 10, $t \mid z$ queda así probado que $z \sim t$.

La relación $\sim$ es una relación de equivalencia ya que es reflexiva, simétrica y transitiva.

Teorema 19.

Para todo $z \in Z[\sigma],\ \boldsymbol{N}z = \boldsymbol{N}\ \widetilde{z}$.

Prueba:

Sea $z = (a,\, b) \in Z[\sigma]$, como $a^2 \geq b^2$, se tiene que

$$\boldsymbol{N}z = a^2 - b^2.$$

Sea $(b,\, a) \in Z[\sigma]$, como $a^2 \geq b^2$, se tiene que

$$\boldsymbol{N}(b,\, a) = a^2 - b^2 = \boldsymbol{N}z.$$

Sea $(-a,\, -b) \in Z[\sigma]$, como $(-a)^2 \geq (-b)^2$, se tiene que

$$\boldsymbol{N}(-a,\, -b) = (-a)^2 - (-b)^2 = a^2 - b^2 = \boldsymbol{N}z.$$

Sea $(-b,\, -a) \in Z[\sigma]$, como $(-a)^2 \geq (-b)^2$, se tiene que

$$\boldsymbol{N}(-b,\, -a) = (-b)^2 - (-a)^2 = a^2 - b^2 = \boldsymbol{N}z.$$

Luego con $a^2 \geq b^2$, $\boldsymbol{N}z = \boldsymbol{N}\ \widetilde{z}$. Los demás casos son análogos. □

Nota 5.

Si dos números gaussianos-dobles tienen la misma norma, no necesariamente son asociados, por ejemplo; $(3,\, 1)$ *tiene la misma norma de* $(3,\, -1)$*, pero estos números gaussianos-dobles no son asociados.*

1.8 Teorema de descomposición de la $Z[\sigma]$-aritmética

Como el conjunto $Z[\sigma]$ no es un dominio de integridad, entonces existen elementos $h \in Z[\sigma]$ distintos de $(0,\, 0)$ que no se pueden descomponer como producto finito de primos de $Z[\sigma]$, para estos elementos $\boldsymbol{N}h = 0$, con $h \neq 0$, por esto $Z[\sigma]$ no es un *dominio de factorización*[8].

[8]Dorronsoro J, Hernandez E. *op.cit.*, 241 p.

Veamos que $Z'[\sigma]$, aunque no es un dominio, sus elementos se pueden descomponer como producto finito de primos de $Z'[\sigma]$.

Teorema 20.

Todo número $z = (a, b) \in Z'[\sigma]$, tal que $\boldsymbol{N}z > 1$, puede ser expresado como producto finito de factores primos en $Z'[\sigma]$.

Prueba:

Sea $z \in Z'[\sigma]$ y $\boldsymbol{N}z > 1$, si z es primo la demostración termina. Si z es un número compuesto tiene un factor primo $z_1 \in Z'[\sigma]$ esto es,

$$z = z_1\, z_2 \qquad \text{para algún} \quad z_2 \in Z'[\sigma], \;\; \boldsymbol{N}z_2 > 1.$$

Si z_2 es primo la factorización de z se ha logrado. Si z_2 es un número compuesto entonces tiene un factor primo $z_3 \in Z'[\sigma]$ esto es,

$$z_2 = z_3\, z_4 \qquad \text{para algún} \quad z_4 \in Z'[\sigma], \;\; \boldsymbol{N}z_4 > 1.$$

Si z_4 es primo la factorización se ha logrado para z_2; de aquí obtenemos que $z = z_1\, z_2\, z_4$, si z_4 no es primo podemos continuar con el procedimiento aplicado a z y z_2 y así obtener un tercer factor primo $z_5 \in Z'[\sigma]$, esto es:

$$z = z_1\, z_3\, z_5\, z_6 \qquad \text{con} \quad z_6 \in Z'[\sigma], \;\; \boldsymbol{N}z_6 > 1.$$

En general, después de k pasos tenemos

$$z = z_1\, z_3\, z_5\, \cdots z_{2k-1}\, z_{2k}$$

donde z_1, z_3, z_5, $\cdots z_{2k-1}$ son números primos y $z_{2k} \in Z'[\sigma]$ y $\boldsymbol{N}z_{2k} > 1$.

Por teorema 6 se tiene

$$\boldsymbol{N}z = \boldsymbol{N}z_1\; \boldsymbol{N}z_3\; \boldsymbol{N}z_5\; \cdots\; \boldsymbol{N}z_{2k-1}\; \boldsymbol{N}z_{2k}$$

entonces

$$\boldsymbol{N}z > \boldsymbol{N}z_1 > \boldsymbol{N}z_3 > \cdots > \boldsymbol{N}z_{2k-1} > \boldsymbol{N}z_{2k} > 1$$

y solo existe un número finito de enteros en $Z'[\sigma]$ cuyas σ-normas son menores que la de z. El proceso debe terminar, es decir z_{2k} es primo para algún k.

En conclusión cualquier número $z \in Z'[\sigma]$ con $\boldsymbol{N}z > 1$, puede ser expresado como producto de factores primos en $Z'[\sigma]$. □

Nota 6.

En el conjunto $Z'[\sigma]$ existen elementos que tienen más de una descomposición distinta en factores primos.

Ejemplo

$$(8,\, 0) = (2,\, 0)(2,\, 0)(2,\, 0)$$
$$(8,\, 0) = (-1,\, 3)(1,\, 3).$$

1.9 Números primos en $Z[\sigma]$

En $Z[\sigma]$ definiremos los números primos de la siguiente manera:

> *Sea $p \in Z[\sigma]$ distinto de cero y de las unidades, p es un número primo gaussiano-doble si no tiene más divisores que sus asociados y las unidades, es decir, si p es primo solo se puede expresar como el producto:*
>
> $$p = z\, w$$
>
> *donde uno de ellos es unidad.*

Un número gaussiano-doble que posee divisores diferentes de las unidades y sus asociados se llama *compuesto gaussiano-doble*.

Los números gaussianos-dobles se clasifican en tres clases que se excluyen entre sí:

1. Las unidades
2. Los números primos gaussianos-dobles
3. Los números compuestos gaussianos-dobles.

Ejemplos

1. Sea $z = (3,\ 1) \in Z[\sigma]$, veamos si es un número primo gaussiano-doble:

   Supongamos que $(3,\ 1)$ no es número primo gaussiano-doble. Entonces existe $\alpha = (a,\ b) \in Z[\sigma]$ distinto de las unidades y los asociados de $(3,\ 1)$, tal que

   $$\alpha \mid (3,\ 1)$$

   entonces, por el teorema 15

   $$\boldsymbol{N}\alpha \mid \boldsymbol{N}(3,\ 1)$$
   $$\boldsymbol{N}\alpha \mid 8$$

   como α no es unidad, entonces $\boldsymbol{N}\alpha$ debe ser distinto de uno, pero $\boldsymbol{N}\alpha \neq 8$, ya que los únicos números gausianos-dobles cuya norma es ocho son $(3,\ 1)$ y sus asociados pero como α no es asociado de $(3,\ 1)$ no puede ser estos números, y $(3,\ -1)$ y sus asociados, pero si α fuera estos números gaussianos-dobles se tendría que:

   $$(3,\ -1) \mid (3,\ 1)$$

   entonces

   $$\begin{aligned}(3,\ 1) &= (3,\ -1)\,(x,\ y)\\ &= (3x - y,\ -x + 3y)\end{aligned}$$

$$3x - y = 3 \tag{1.19}$$

$$-x + 3y = 1 \tag{1.20}$$

multiplicando la ecuación (1.20) por 3 y sumandola con (1.19) obtenemos;

$$8y = 6$$

y esta ecuación no tiene solución en los enteros. Es análogo con los otros asociados de $(3, -1)$. Luego α no puede ser $(3, 1)$ ni sus asociados. Por esto la $\boldsymbol{N}\alpha \neq 8$.

Entonces la $\boldsymbol{N}\alpha$ debe ser igual a 2 o igual a 4. Si $\boldsymbol{N}\alpha = 2$ entonces

$$a^2 - b^2 = 2$$

pero esta ecuación no tiene solución en $\mathbb{Z}$.

Luego $\boldsymbol{N}\alpha$ debe ser igual a 4, es decir

$$a^2 - b^2 = 4$$

entonces las soluciones de esta ecuación son $a = \pm 2$ y $b = 0$.

Por tanto $\alpha = (\pm 2, 0)$. Como $\alpha \mid (3, 1)$, entoces existe $(x, y) \in Z[\sigma]$ tal que

$$(3, 1) = (\pm 2, 0)\,(x, y)$$

$$(3, 1) = (\pm 2x, \pm 2y)$$

$$\pm 2x = 3$$

$$\pm 2y = 1.$$

Pero este sistema no tiene solución en $\mathbb{Z}$.

Luego $\boldsymbol{N}\alpha \neq 4$, es decir, $(3, 1)$ no se puede descomponer en factores distintos de las unidades y sus asociados.

Por tanto $(3, 1)$ es un número primo gaussiano-doble.

2. (2, 0) es un número primo gaussiano-doble.

   Supongamos que (2, 0) no es un número primo gaussiano-doble. Entonces existe $\alpha = (a, b) \in Z[\sigma]$ que no es unidad ni asociado de (2, 0), tal que

   $$\alpha \mid (2, 0)$$

   entonces, por el teorema 15

   $$\boldsymbol{N}\alpha \mid 4$$

   como α no es unidad, $\boldsymbol{N}\alpha$ debe ser distinto de uno, además $\boldsymbol{N}\alpha \neq 4$, los únicos números gausianos-dobles cuya norma es cuatro son (2, 0) y sus asociados pero α no puede ser estos números.

   Luego $\boldsymbol{N}\alpha = 2$, es decir

   $$a^2 - b^2 = 2$$

   pero esta ecuación no tiene solución en $\mathbb{Z}$. Luego (2, 0) es un número primo gaussiano-doble.

3. (2, 1) es un número primo gaussiano-doble.

   Supongamos que (2, 1) no es número primo gaussiano-doble. Entonces existe $\alpha \in Z[\sigma]$ que no es unidad ni asociado, tal que

   $$\alpha \mid (2, 1)$$

   entonces, por el teorema 15

   $$\boldsymbol{N}\alpha \mid \boldsymbol{N}(2, 1)$$
   $$\boldsymbol{N}\alpha \mid 3$$

   como α no es unidad, $\boldsymbol{N}\alpha$ debe ser distinto de uno, además $\boldsymbol{N}\alpha \neq 3$, ya que los únicos números gausianos-dobles cuya norma es tres son (2, 1) y sus asociados

pero α no puede ser estos números, y $(2,\,-1)$ y sus asociados, pero si α fuera estos números gaussianos-dobles se tendría que:

$$(2,\,-1) \mid (2,\,1)$$

entonces

$$\begin{aligned}(2,\,1) &= (2,\,-1)\,(x,\,y)\\ &= (2x-y,\,-x+2y)\end{aligned}$$

$$2x - y = 2 \tag{1.21}$$

$$-x + 2y = 1 \tag{1.22}$$

multiplicando la ecuación (1.21) por 2 y sumando con (1.22) obtenemos;

$$3y = 4,$$

y esta ecuación no tiene solución en los enteros. Es análogo con los demás asociados de $(2,\,-1)$. Luego α no puede ser $(2,\,-1)$ ni sus asociados. Por esto la $\boldsymbol{N}\alpha \neq 3$.

Luego como $\boldsymbol{N}\alpha$ debe ser distinto de uno y de tres, no se puede descomponer en factores primos.

Por tanto $(2,\,1)$ es un número primo gaussiano-doble.

4. $(2,\,-1)$ es un número primo gaussiano-doble. La verificación es análoga a la anterior.

No todos los números primos p en $\mathbb{Z}$ son primos gaussianos-dobles $(p,\,0)$ en $Z[\sigma]$

5. El número gaussiano-doble $(3,\,0)$ se descompone en factores primos, en $Z[\sigma]$, así

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

y por tanto no es primo gaussiano-doble.

Nota 7.

En los ejemplos anteriores, para verificar que un número gaussiano-doble es primo gaussiano-doble se supone que existe $\alpha \in Z[\sigma]$ que lo divide, distinto de las unidades y los asociados de z, es decir;

$$\alpha \mid z$$

Por el teorema 15

$$\boldsymbol{N}\alpha \mid \boldsymbol{N}z$$

Como α es distinto de las unidades entonces $\boldsymbol{N}\alpha$ debe ser distinto de uno. Pero $\boldsymbol{N}\alpha \neq \boldsymbol{N}z$, porque los únicos números α para los cuales $\boldsymbol{N}\alpha = \boldsymbol{N}z$ son:

$$\widetilde{z}, \qquad \widetilde{\overline{z}}$$

Como α no es asociado de z entonces $\alpha \neq \widetilde{z}$. Si $\alpha = \widetilde{\overline{z}}$, en particular $\alpha = \overline{z}$, entonces

$$\overline{z} \mid z,$$

por definición de divisibilidad, existe $w \in Z[\sigma]$ tal que

$$z = w\,\overline{z}$$

calculando la norma se tiene

$$\boldsymbol{N}z = \boldsymbol{N}(w\,\overline{z})$$

por teorma 6

$$\boldsymbol{N}z = \boldsymbol{N}w\ \boldsymbol{N}\overline{z}$$

por teorema 7

$$1 = \boldsymbol{N}w.$$

Por teorema 18, w debe ser unidad. Pero si w fuera unidad, z sería un número primo gaussiano-doble lo que es una contradicción. De forma análoga se verifica para $\widetilde{\overline{z}}$, entonces $\alpha \neq \widetilde{\overline{z}}$. Por tanto $\boldsymbol{N}\alpha \neq \boldsymbol{N}\,\widetilde{\overline{z}}$. En general $\boldsymbol{N}\alpha \neq \boldsymbol{N}z$.

En conclusión, sin importar el número gaussiano-doble z, σ-norma de α debe ser distinto de las unidades y σ-norma de z.

Teorema 21.

Para todo $z \in Z[\sigma]$, z es primo gaussiano-doble si y sólo si $\widetilde{z}$, son primos gaussianos-dobles.

Teorema 22.

Para todo $z \in Z[\sigma]$ es un número primo gaussiano-doble si y sólo si $\overline{z}$ es un número primo gaussiano-doble.

Prueba:

i) Si $z \in Z[\sigma]$, es un número primo gaussiano-doble entonces $\overline{z}$ es un número primo gaussiano-doble.

Como z es primo gaussiano-doble entonces

$$z = \alpha\,\beta$$

donde α es unidad o asociado o, β es unidad o asociado.

Calculando la σ-norma a ambos lados de la igualdad tenemos

$$\boldsymbol{N}z = \boldsymbol{N}(\alpha\,\beta)$$

por el teorema 6

$$\boldsymbol{N}z = \boldsymbol{N}\alpha\ \boldsymbol{N}\beta$$

por el teorema 7

$$\boldsymbol{N}z = \boldsymbol{N}\overline{z} = \boldsymbol{N}\alpha\ \boldsymbol{N}\beta$$

$$\boldsymbol{N}\overline{z} = \boldsymbol{N}\alpha\ \boldsymbol{N}\beta.$$

Supongamos que α es unidad, entonces por el teorema 18

$$\boldsymbol{N}\overline{z} = 1\ \boldsymbol{N}\beta$$

luego β es asociado de $\overline{z}$, entonces

$$\overline{z} = \alpha\,\beta$$

Luego $\overline{z}$ es un número primo gaussiano-doble.

ii) Si $\overline{z} \in Z[\sigma]$, es un número primo gaussiano-doble entonces z es un número primo gaussiano-doble.

La demostración de la recíproca es análoga a la anterior. □

Teorema 23.

Para todo $z \in Z[\sigma]$ es un número compuesto gaussiano-doble si y sólo si su conjugado $\overline{z}$ es un número compuesto gaussiano-doble.

Prueba:

i) Si $z \in Z[\sigma]$, es un número compuesto gaussiano-doble entonces $\overline{z}$ es un número compuesto gaussiano-doble.

La demostracción la realizaremos por contradicción. Supongamos que $\overline{z}$ es primo gaussiano-doble, entonces por el teorema 22, z es primo gaussiano-doble. Lo que es una contradicción.

Luego $\overline{z}$ es un número compuesto gaussiano-doble en $Z[\sigma]$.

ii) Si $\overline{z} \in Z[\sigma]$, es un número compuesto gaussiano-doble entonces z es un número compuesto gaussiano-doble.

La demostración de la recíproca es análoga a la anterior. □

Teorema 24.

Todos los números enteros mayores que dos, son números compuestos gaussianos-dobles.

Prueba:

Esta demostración la haremos por casos.

i) Si z es un entero impar, entonces puede descomponerse en $Z[\sigma]$ de la forma:

$$\begin{aligned}(2n+1,\,0) &= (n+1,\,n)\,(n+1,-n)\\ &= ((n+1)^2-n^2,\,0).\end{aligned}$$

ii) Si z es un entero par distinto de dos, entonces puede descomponerse en $Z[\sigma]$ de la forma:

$$(2n,\,0) = (2,\,0)\,(n,\,0) \qquad con \quad n \neq 1. \quad \square$$

A partir del teorema 24, podemos enunciar el siguiente corolario:

Corolario 1.

Todo número primo impar entero, no es primo gaussiano-doble.

Consideremos los siguientes números gaussianos-dobles con su σ-norma, con el fin de buscar números primos[9] en $Z[\sigma]$.

Caso	z	$\boldsymbol{N}z$	
i	$(n+1,\,n)$	$(n+1)^2-n^2 =$	$2(n+1)$
ii	$(n+2,\,n)$	$(n+2)^2-n^2 =$	$2^2(n+1)$

[9]Esto requiere operaciones que pueden resultar tediosas, para evitar esto podemos recurrir a los software, por esta razón hemos incluido un programa llamado "*G-D*" que esta escrito la plataforma *PYTHON*.

iii	$(n+3,\, n)$	$(n+3)^2 - n^2 =$	$3(2n+3)$
iv	$(n+4,\, n)$	$(n+4)^2 - n^2 =$	$2^3(n+2)$
v	$(n+5,\, n)$	$(n+5)^2 - n^2 =$	$5(2n+5)$
$\vdots$	$\vdots$	$\vdots$	$\vdots$
k	$(n+k,\, n)$	$(n+k)^2 - n^2 =$	$k(2n+k)$

Veamos por aparte cada uno de los casos

Caso i. Sea $z = (n+1,\, n)$ y $\boldsymbol{N}z = 2(n+1)$ entonces,

n	z	$\boldsymbol{N}z$
0	(1, 0)	1
1	(2, 1)	3
2	(3, 2)	5
3	(4, 3)	7
4	(5, 4) = (2, 1)(2, 1)	9
5	(6, 5)	11
6	(7, 6)	13
7	(8, 7) = (2, 1)(3, 2)	15
8	(9, 8)	17
9	(10, 9)	19
10	(11, 10) = (2, 1)(4, 3)	21

De aquí vemos que los números cuya σ-norma es prima no se pueden descomponer en factores, es decir, son números primos gaussianos-dobles.

Teorema 25.

Sea $z \in Z[\sigma]$ si $\boldsymbol{N}z = p$, donde p es un número primo entero entonces z es un número primo gaussiano-doble.

Prueba:

La demostracción la realizaremos por contradicción. Supongamos que z no es número primo gaussiano-doble. Entonces existe $\alpha \in Z[\sigma]$ que no es unidad ni asociado de z, tal que

$$\alpha \mid z$$

entonces, por el teorema 15

$$\boldsymbol{N}\alpha \mid \boldsymbol{N}z$$

$$\boldsymbol{N}\alpha \mid p$$

como α no es unidad $\boldsymbol{N}\alpha \neq 1$. Como α no es asociado de z y como vimos en la nota 7, $\boldsymbol{N}\alpha \neq p$. Lo cual es una contradicción ya que los únicos divisores de p son las unidades y sus asociados. □

Nota 8.

El recíproco del teorema anterior no es cierto, es decir, si $z = (a, b) \in Z[\sigma]$ es un número primo gaussiano-doble entonces $\boldsymbol{N}z$ es igual a un número primo.

Ejemplo

Sea $z = (3, 1) \in Z[\sigma]$ un número primo gaussiano-doble, luego

$$\boldsymbol{N}(3, 1) = 8$$

pero 8 no es un número primo.

Veamos de que forma son los números primos gaussianos-dobles que cumplen el teorema 25, para esto bastaría resolver la siguiente ecuación:

$$a^2 - b^2 = p \tag{1.23}$$

donde a, b, $p \in \mathbb{Z}$ y p es un número primo.

Tratemos de encontrar una solución general para la ecuación (1.23).

Entonces

$$a^2 - b^2 = p$$

$$(a-b)(a+b) = p$$

de aquí $(a-b)$ es unidad o $(a+b)$ es unidad.

Si $a - b = \pm 1$ entonces

$$a = \pm 1 + b,$$

si $a + b = \pm 1$ entonces

$$a = \pm 1 - b.$$

Luego los números primos gaussianos-dobles son de la forma $(b \pm 1,\, b)$ y $(\pm 1 - b,\, b)$, pero estas soluciones estan relacionadas ya que son conjugados entre si o son asociados, y por los teoremas 21 y 22, podemos escribir la solución como

$$(b+1,\, b)$$

donde $$(b+1)^2 - b^2 = p,$$

$$2b + 1 = p.$$

Es decir, para hallar algunos números primos gaussianos-dobles basta con encontrar el valor de b donde $2b + 1$ sea un número primo.

En la teoría de números enteros existe un teorema denominado *Teorema de los cuadrados de Fermat*[10] que dice; *Un primo impar p es la suma de dos cuadrados,* $p = a^2 + b^2$ *donde a y b son enteros si, y sólo si* $p \equiv 1$ *mód* 4, al resolver el problema de encontrar números primos gaussianos-dobles, se verifica el siguiente teorema en los números enteros.

[10]Perez, E. *op. cit.*, 51 p.

Teorema 26.

Todo número primo impar $p \in \mathbb{Z}$, es la difierencia de dos cuadrados:

$$x^2 - y^2 = p \qquad \textit{con } x,\ y \in \mathbb{Z}.$$

Prueba:

Las soluciones de la ecuación $x^2 - y^2 = p$, son $x = \dfrac{p+1}{2}$, $y = \dfrac{p-1}{2}$ con p un número primo impar entero, ya que;

$$\left(\frac{p+1}{2}\right)^2 - \left(\frac{p-1}{2}\right)^2 = \frac{p^2+2p+1}{4} - \frac{p^2-2p+1}{4}$$
$$= \frac{4p}{4} = p. \quad \square$$

Caso *ii*. Sea $z = (n+2,\ n)$ y $\boldsymbol{N}z = 2^2(n+1)$ entonces,

n	z	$\boldsymbol{N}z$
0	(2, 0)	$4 = 2^2$
1	(3, 1)	$8 = 2^3$
2	(4, 2) = (2, 0)(2, 1)	12
3	(5, 3)	$16 = 2^4$
4	(6, 4) = (2, 0)(3, 2)	20
5	(7, 5) = (3, 1)(2, 1)	24
6	(8, 6) = (2, 0)(4, 3)	28
7	(9, 7)	$32 = 2^5$
8	(10, 8) = (2, 0)(5, 4)	36
9	(11, 9) = (3, 1)(3, 2)	40
10	(12, 10) = (2, 0)(6, 5)	44

De aquí vemos que los números cuya σ-norma es una potencia de 2 no se pueden descomponer en factores, es decir, son números primos gaussianos-dobles.

Si n es un número par entonces $n = 2t$, y el número gaussiano-doble

$$z = (n + 2,\, n) = (2t + 2,\, 2t) = (2,\, 0)(t + 1,\, t).$$

A excepción de $(2,\, 0)$, todo número de la forma $(2t + 2,\, 2t)$, es compuesto gaussiano-doble.

Si n es un número impar entonces $n = 2t + 1$, y el número gaussiano-doble

$$z = (n + 2,\, n) = (2t + 3,\, 2t + 1)$$

calculando la σ-norma tenemos que

$$\begin{aligned} \boldsymbol{N}(2t + 3,\, 2t + 1) &= (2t + 3)^2 - (2t + 1)^2 \\ &= 4t^2 + 12t + 9 - 4t^2 - 4t - 1 \\ &= 8t + 8 \\ &= 2^3(t + 1). \end{aligned}$$

Entonces para que la σ-norma de z sea una potencia de dos, $t + 1 = 2^r$.

Además como $n = 2t + 1$, entonces

$$t = \frac{n - 1}{2}. \tag{1.24}$$

Como $t + 1 = 2^r$, remplazando t de la ecuación (1.24) se tiene

$$\begin{aligned} \frac{n - 1}{2} + 1 &= 2^r \\ \frac{n + 1}{2} &= 2^r \\ n + 1 &= 2^{r+1} \\ n &= 2^{r+1} - 1. \end{aligned}$$

Entonces como

$$z = (n+2,\, n)$$
$$z = (2^{r+1}+1,\, 2^{r+1}-1).$$

De aqui podemos enunciar el siguiente teorema.

Teorema 27.

Para todo $z = (n+2,\, n) \in Z[\sigma]$, z *es un número primo-gaussiano doble si es de la forma* $z = (2^{r+1}+1,\, 2^{r+1}-1)$, *con* $r \in \mathbb{Z}$, *y* $r \geq 0$.

Prueba:

Supongamos que el número z no es un número primo gaussiano-doble, entonces existen $(a,\, b)$, $(c,\, d) \in Z[\sigma]$ que no son ni unidades ni asociados de $(2^{r+1}+1,\, 2^{r+1}-1)$, tal que

$$\begin{aligned}
(2^{r+1}+1,\, 2^{r+1}-1) &= (a,\, b)\,(c,\, d)\\
(2^{r+1}+1,\, 2^{r+1}-1) &= (ac+bd,\, bc+ad)\\
\boldsymbol{N}(2^{r+1}+1,\, 2^{r+1}-1) &= \boldsymbol{N}(ac+bd,\, bc+ad)\\
(2^{r+1}+1)^2-(2^{r+1}-1)^2 &= (ac+bd)^2-(bc+ad)^2\\
(2^{r+1})^2+2(2^{r+1})+1-(2^{r+1})^2+2(2^{r+1})-1 &= (ac)^2+(bd)^2-(bc)^2-(ad)^2\\
2^{r+3} &= a^2(c^2-d^2)-b^2(c^2-d^2)\\
2^{r+3} &= (a^2-b^2)\,(c^2-d^2).
\end{aligned}$$

Sean p y $q \in \mathbb{N}$ tal que $p+q = r+3$, entonces

$$2^{r+3} = \underbrace{(c^2-d^2)}_{2^p}\ \underbrace{(a^2-b^2)}_{2^q}$$

es decir

$$2^{r+3} = 2^p\, 2^q.$$

Supongamos que r es par, entonces $r = 2j$ con $j \in \mathbb{N} + \{0\}$, luego

$$2j + 3 = p + q$$

Consideremos los valores que puede tomar p y q

p	q
$2j+3$	0
$2j+2$	1
$2j+1$	2
$2j$	3
$2j-1$	4
$2j-2$	5
$2j-3$	6
$\vdots$	$\vdots$
$j+2$	$j+1$

Si $q = 0$, entonces $2^q = 2^0 = 1 = a^2 - b^2$, y los únicos números para los cuales se tiene esta igualdad son $a = 1$ y $b = 0$, entonces (a, b) es unidad, lo que contradice la hipótesis, por ello $q \neq 0$.

Si $q = 1$, entonces $2^q = 2^1 = 2 = a^2 - b^2$, pero esta ecuación no tiene solución en los $\mathbb{Z}$, por lo que $q \neq 0$.

Si q es un número par entonces $q = 2s$, con $s \in \mathbb{N}$.

La solución de la euación

$$2^{2s} = a^2 - b^2$$

es $a = 2^s$ y $b = 0$, es decir

$$(a, b) = (2^s, 0).$$

Luego

$$(2^s,\, 0)\,(c,\, d)$$

debe ser de la forma $(n+2,\, n)$, es decir

$$(2^s c,\, 2^s d) = (n+2,\, n) \tag{1.25}$$

de esta ecuación se tiene que, como $2^s d = n$, entonces

$$2^s c = 2^s d + 2$$

luego

$$2^s c - 2^s d = 2$$

$$2^s (c-d) = 2$$

$$c - d = \frac{2}{2^s}$$

$$c - d = 2^{1-s}$$

Como $c - d \in \mathbb{Z}$ entonces $2^{1-s} \in \mathbb{N} + \{0\}$. Luego $s = 0$ o $s = 1$, pero si $s = 0$ entonces $q = 0$ y ya vimos que $q \neq 0$.

Si $s = 1$

$$(a,\, b) = (2,\, 0)$$

entonces

$$(2,\, 0)\,(c,\, d) = (n+2,\, n)$$

$$(2c,\, 2d) = (n+2,\, n)$$

de esta ecuación se tiene que, como $2d = n$, entonces

$$2c = 2d + 2$$

$$2c - 2d = 2$$

$$c - d = 1.$$

Existen finitos números c y d que cunplen esta ecuacón, podemos escribir $d = c - 1$, tenemos que;

$$\begin{aligned}(c^2 - d^2) &= c^2 - (c-1)^2 \\ &= c^2 - c^2 + 2c - 1 \\ &= 2c - 1;\end{aligned}$$

pero este número no es una potencia de dos, lo que contradice la hipótesis, por tanto $s \neq 1$.

Luego no existe ningún s que cumpla la ecuación (1.25). Por tanto q no puede ser un número par.

Supongamos que q es un número impar, entonces $q = 2m + 1$ con $m \geq 1$. Luego la solución de la ecuación

$$2^{m+1} = a^2 - b^2$$

es $a = 3(2^{m-1})$ y $b = 2^{m-1}$ ya que

$$\begin{aligned}a^2 - b^2 &= (3 \cdot 2^{m-1})^2 - (2^{m-1})^2 \\ &= 3^2 \cdot 2^{2(m-1)} - 2^{2(m-1)} \\ &= 2^{2(m-1)}(3^2 - 1) \\ &= 2^{2(m-1)} \cdot 2^3 \\ &= 2^{2m+1}.\end{aligned}$$

Entonces

$$(a,\, b) = (3 \cdot 2^{m-1},\, 2^{m-1}).$$

Luego

$$(3 \cdot 2^{m-1},\, 2^{m-1})\,(c,\, d)$$

debe ser de la forma $(n + 2,\, n)$, es decir

$$(3 \cdot 2^{m-1}c + 2^{m-1}d,\, 2^{m-1}c + 3 \cdot 2^{m-1}d) = (n + 2,\, n) \tag{1.26}$$

de esta ecuación se tiene que, como $2^{m-1}c + 3 \cdot 2^{m-1}d = n$, entonces

$$\begin{aligned}
3 \cdot 2^{m-1}c + 2^{m-1}d &= 2^{m-1}c + 3 \cdot 2^{m-1}d + 2 \\
3 \cdot 2^{m-1}c - 2^{m-1}c &= 3 \cdot 2^{m-1}d - 2^{m-1}d + 2 \\
2^{m-1}c(3-1) &= 2^{m-1}d(3-1) + 2 \\
2^{m-1}c2 &= 2^{m-1}cd2 + 2 \\
2^{m-1}c &= 2^m d + 2 \\
2^m c - 2^m d &= 2 \\
c - d &= \frac{2}{2^m} \\
c - d &= 2^{1-m}
\end{aligned}$$

Como $c - d \in \mathbb{Z}$ entonces $2^{1-m} \in \mathbb{N} + \{0\}$. Luego $m = 0$ o $m = 1$, pero si $m = 0$ entonces $q = 1$ y ya vimos que $q \neq 1$.

Si $m = 1$

$$(a,\, b) = (3,\, 1)$$

entonces

$$(3,\, 1)\,(c,\, d) = (n + 2,\, n)$$

$$(3c + d,\, c + 3d) = (n + 2,\, n)$$

de esta ecuación se tiene que, como $c + 3d = n$, entonces

$$\begin{aligned}
3c + d &= c + 3d + 2 \\
3c - c + d - 3d &= 2 \\
2c - 2d &= 2 \\
c - d &= 1.
\end{aligned}$$

Existen finitos números c y d que cunplen esta ecuacón, podemos escribir $d = c - 1$, tenemos que;

$$\begin{aligned}(c^2 - d^2) &= c^2 - (c-1)^2 \\ &= c^2 - c^2 + 2c - 1 \\ &= 2c - 1;\end{aligned}$$

pero este número no es una potencia de dos, lo que contradice la hipótesis, por tanto $m \neq 1$.

Luego no existe ningún m que cumpla la ecuación (1.26). En consecuencia q no puede ser un número impar.

Por tanto no existe ningún r par, ni exsten números gaussianos-dobles $(a,\, b)$, $(c,\, d)$ distintos de las unidades y sus asociados que que cumpla la ecuación

$$(2^{r+1} + 1,\, 2^{r+1} - 1) = (a,\, b)\,(c,\, d).$$

La demostración es análoga para r impar.

Por tanto no existen $(a,\, b)$, $(c,\, d) \in Z[\sigma]$ que no son ni unidades ni asociados de $(2^{r+1} + 1,\, 2^{r+1} - 1)$, tal que

$$(2^{r+1} + 1,\, 2^{r+1} - 1) = (a,\, b)\,(c,\, d).$$

es decir el número $(2^{r+1} + 1,\, 2^{r+1} - 1)$ es un número primo gaussiano-doble. □

Veamos que en los siguientes casos no existen números primos gaussianos-dobles, ya que todos estos números se pueden descomponer en factores.

Caso *iii*. Sea $z = (n+3,\, n)$ y $\boldsymbol{N}z = 3(2n+3)$ entonces,

n	z	$\boldsymbol{N}z$
0	$(3,\, 0) = (-1,\, 2)(1,\, 2)$	9
1	$(4,\, 1) = (-1,\, 2)(2,\, 3)$	15
2	$(5,\, 2) = (-1,\, 2)(3,\, 4)$	21
3	$(6,\, 3) = (-1,\, 2)(4,\, 5)$	27
4	$(7,\, 4) = (-1,\, 2)(5,\, 6)$	33
5	$(8,\, 5) = (-1,\, 2)(6,\, 7)$	39
6	$(9,\, 6) = (-1,\, 2)(7,\, 8)$	45
7	$(10,\, 7) = (-1,\, 2)(8,\, 9)$	51
8	$(11,\, 8) = (-1,\, 2)(9,\, 10)$	57
9	$(12,\, 9) = (-1,\, 2)(10,\, 11)$	63
10	$(13,\, 10) = (-1,\, 2)(11,\, 12)$	69

Caso *iv*. Sea $z = (n+4,\, n)$ y $\boldsymbol{N}z = 2^3(n+2)$ entonces,

n	z	$\boldsymbol{N}z$
0	$(4,\, 0) = (2,\, 0)(2,\, 0)$	16
1	$(5,\, 1) = (-1,\, 3)(1,\, 2)$	24
2	$(6,\, 2) = (2,\, 0)(3,\, 1)$	32
3	$(7,\, 3) = (-1,\, 3)(2,\, 3)$	40
4	$(8,\, 4) = (2,\, 0)(4,\, 2)$	48
5	$(9,\, 5) = (-1,\, 3)(3,\, 4)$	56
6	$(10,\, 6) = (2,\, 0)(5,\, 3)$	64
7	$(11,\, 7) = (-1,\, 3)(4,\, 5)$	72
8	$(12,\, 8) = (2,\, 0)(6,\, 4)$	80
9	$(13,\, 9) = (-1,\, 3)(5,\, 6)$	88
10	$(14,\, 10) = (2,\, 0)(7,\, 5)$	96

Caso *v*. Sea $z = (n+5,\ n)$ y $\boldsymbol{N}z = 5(2n+5)$ entonces,

n	z	$\boldsymbol{N}z$
0	$(5,\ 0) = (-2,\ 3)(2,\ 3)$	25
1	$(6,\ 1) = (-2,\ 3)(3,\ 4)$	35
2	$(7,\ 2) = (-2,\ 3)(4,\ 5)$	45
3	$(8,\ 3) = (-2,\ 3)(5,\ 6)$	55
4	$(9,\ 4) = (-2,\ 3)(6,\ 7)$	65
5	$(10,\ 5) = (-2,\ 3)(7,\ 8)$	75
6	$(11,\ 6) = (-2,\ 3)(8,\ 9)$	85
7	$(12,\ 7) = (-2,\ 3)(9,\ 10)$	95
8	$(13,\ 8) = (-2,\ 3)(10,\ 11)$	105
9	$(14,\ 9) = (-2,\ 3)(11,\ 12)$	115
10	$(15,\ 10) = (-2,\ 3)(12,\ 13)$	125

Caso *vi*. Sea $z = (n+6,\ n)$ y $\boldsymbol{N}z = 6(2n+6)$ entonces,

n	z	$\boldsymbol{N}z$
0	$(6,\ 0) = (2,\ 0)(3,\ 0)$	36
1	$(7,\ 1) = (-1,\ 2)(3,\ 5)$	48
2	$(8,\ 2) = (2,\ 0)(4,\ 1)$	60
3	$(9,\ 3) = (-1,\ 2)(5,\ 7)$	72
4	$(10,\ 4) = (2,\ 0)(5,\ 2)$	84
5	$(11,\ 5) = (-1,\ 2)(7,\ 9)$	96
6	$(12,\ 6) = (2,\ 0)(6,\ 3)$	108
7	$(13,\ 7) = (-1,\ 2)(9,\ 11)$	120
8	$(14,\ 8) = (2,\ 0)(7,\ 4)$	132
9	$(15,\ 9) = (-1,\ 2)(11,\ 13)$	144
10	$(16,\ 10) = (2,\ 0)(8,\ 5)$	156

Caso *vii*. Sea $z = (n+7,\, n)$ y $\boldsymbol{N}z = 7(2n+7)$ entonces,

n	z	$\boldsymbol{N}z$
0	$(7,\, 0) = (-3,\, 4)(3,\, 4)$	49
1	$(8,\, 1) = (-3,\, 4)(4,\, 5)$	63
2	$(9,\, 2) = (-3,\, 4)(5,\, 6)$	77
3	$(10,\, 3) = (-3,\, 4)(6,\, 7)$	91
4	$(11,\, 4) = (-3,\, 4)(7,\, 8)$	105
5	$(12,\, 5) = (-3,\, 4)(8,\, 9)$	119
6	$(13,\, 6) = (-3,\, 4)(9,\, 10)$	133
7	$(14,\, 7) = (-3,\, 4)(10,\, 11)$	147
8	$(15,\, 8) = (-3,\, 4)(11,\, 12)$	161
9	$(16,\, 9) = (-3,\, 4)(12,\, 13)$	175
10	$(17,\, 10) = (-3,\, 4)(13,\, 14)$	189

Caso *viii*. Sea $z = (n+8,\, n)$ y $\boldsymbol{N}z = 2^4(n+4)$ entonces,

n	z	$\boldsymbol{N}z$
0	$(8,\, 0) = (2,\, 0)(4,\, 0)$	64
1	$(9,\, 1) = (-3,\, 5)(2,\, 3)$	80
2	$(10,\, 2) = (2,\, 0)(5,\, 1)$	96
3	$(11,\, 3) = (-3,\, 5)(3,\, 4)$	112
4	$(12,\, 4) = (2,\, 0)(6,\, 2)$	128
5	$(13,\, 5) = (-3,\, 5)(4,\, 5)$	144
6	$(14,\, 6) = (2,\, 0)(7,\, 3)$	160
7	$(15,\, 7) = (-3,\, 5)(5,\, 6)$	176
8	$(16,\, 8) = (2,\, 0)(8,\, 4)$	192
9	$(17,\, 9) = (-3,\, 5)(6,\, 7)$	208
10	$(18,\, 10) = (2,\, 0)(9,\, 5)$	224

Caso *ix*. Sea $z = (n+9,\, n)$ y $\boldsymbol{N}z = 9(2n+9)$ entonces,

n	z	$\boldsymbol{N}z$
0	$(9,\, 0) = (-4,\, 5)(4,\, 5)$	81
1	$(10,\, 1) = (-4,\, 5)(5,\, 6)$	99
2	$(11,\, 2) = (-4,\, 5)(6,\, 7)$	117
3	$(12,\, 3) = (-4,\, 5)(7,\, 8)$	135
4	$(13,\, 4) = (-4,\, 5)(8,\, 9)$	153
5	$(14,\, 5) = (-4,\, 5)(9,\, 10)$	171
6	$(15,\, 6) = (-4,\, 5)(10,\, 11)$	189
7	$(16,\, 7) = (-4,\, 5)(11,\, 12)$	207
8	$(17,\, 8) = (-4,\, 5)(12,\, 13)$	225
9	$(18,\, 9) = (-4,\, 5)(13,\, 14)$	243
10	$(19,\, 10) = (-4,\, 5)(14,\, 15)$	261

Caso *x*. Sea $z = (n+10,\, n)$ y $\boldsymbol{N}z = 2^2\,(5n+25)$ entonces,

n	z	$\boldsymbol{N}z$
0	$(10,\, 0) = (2,\, 0)(5,\, 0)$	100
1	$(11,\, 1) = (-2,\, 3)(5,\, 7)$	120
2	$(12,\, 2) = (2,\, 0)(6,\, 1)$	140
3	$(13,\, 3) = (-2,\, 3)(7,\, 9)$	160
4	$(14,\, 4) = (2,\, 0)(7,\, 2)$	180
5	$(15,\, 5) = (-2,\, 3)(9,\, 11)$	200
6	$(16,\, 6) = (2,\, 0)(8,\, 3)$	220
7	$(17,\, 7) = (-2,\, 3)(11,\, 13)$	240
8	$(18,\, 8) = (2,\, 0)(9,\, 4)$	260
9	$(19,\, 9) = (-2,\, 3)(13,\, 15)$	280
10	$(20,\, 10) = (2,\, 0)(10,\, 5)$	300

De los casos anteriores como conclusión podemos generalizar la descomposición con los siguientes teoremas.

Todo número gaussiano-doble, se puede expresar de la forma $(n+k,\, n)$, entonces:

Si n es cualquiera y $k = 2j+1$ con $j \neq 0$ entonces,

Teorema 28.

Todo número gaussiano-doble de la forma $(n+(2j+1),\, n) \in Z[\sigma]$*, con* $j \neq 0$ *se puede descomponer en* $Z[\sigma]$*.*

Prueba:

Sea el número $(n+(2j+1),\, n) \in Z[\sigma]$, entonces la descomposición en factores distintos de las unidades y de sus asociados, es

$$(n+(2j+1),\, n) = (-j,\, j+1)\,(n+j, n+j+1)$$

ya que

$$\begin{aligned}(n+(2j+1),\, n) &= (-j,\, j+1)\,(n+j, n+j+1)\\ &= (-j(n+j)+(j+1)(n+j+1),\, (j+1)(n+j)-j(n+j+1))\\ &= (-jn-j^2+jn+j^2+j+n+j+1,\, jn+j^2+n+j-jn-j^2-j)\\ &= (n+2j+1,\, n). \quad \square\end{aligned}$$

Si n es cualquiera y $k = 2(2j)$ con $j \neq 0$ entonces,

Teorema 29.

Todo número gaussiano-doble de la forma $(n+4j,\, n) \in Z[\sigma]$ *con* $j \neq 0$*, se puede descomponer en* $Z[\sigma]$*.*

Prueba:

Sea el número $(n+4j,\, n) \in Z[\sigma]$ con $j \neq 0$, entonces la descomposición en factores distintos de las unidades y de sus asociados, es

i) Si n es par entonces

$$(n+4j,\, n) = \left(\frac{n+4j}{2},\, \frac{n}{2}\right)(2,\, 0)$$

ya que

$$\begin{aligned}(n+4j,\, n) &= \left(\frac{n+4j}{2},\, \frac{n}{2}\right)(2,\, 0) \\ &= \left(\frac{2(n+4j)}{2},\, \frac{2n}{2}\right) \\ &= (n+4j,\, n).\end{aligned}$$

ii) Si n es impar entonces

$$(n+4j,\, n) = \left(\frac{n+2j-1}{2},\, \frac{n+2j+1}{2}\right)(-2j+1,\, 2j+1)$$

ya que

$$\begin{aligned}(n+4j,\, n) &= \left(\frac{n+2j-1}{2},\, \frac{n+2j+1}{2}\right)(-2j+1,\, 2j+1) \\ &= \left(\frac{n+2j-1}{2}(-2j+1) + \frac{n+2j+1}{2}(2j+1),\right. \\ &\qquad \left. \frac{n+2j+1}{2}(-2j+1) + \frac{n+2j-1}{2}(2j+1)\right)\end{aligned}$$

$$= \left(\frac{-2jn - 4j^2 + 2j + n + 2j - 1}{2} + \frac{2jn + 4j^2 + 2j + n + 2j + 1}{2}, \right.$$
$$\left. \frac{-2jn - 4j^2 - 2j + n + 2j + 1}{2} + \frac{2jn + 4j^2 - 2j + n + 2j - 1}{2} \right)$$
$$= \left(\frac{8j + 2n}{2}, \frac{2n}{2} \right)$$
$$= (n + 4j,\ n). \quad \square$$

Si n es cualquiera y $k = 2(2j + 1)$ entonces,

Teorema 30.

Todo número gaussiano-doble de la forma $(n+2(2j+1),\ n) \in Z[\sigma]$, *se puede descomponer en* $Z[\sigma]$.

Prueba:

Sea el número $(n+2(2j+1),\ n) \in Z[\sigma]$, entonces la descomposición en factores distintos de las unidades y de sus asociados, es

$$(n + 2(2j + 1),\ n) = (-j,\ j + 1)\,(n + 2j, n + 2j + 2)$$

ya que

$$(n + 2(2j + 1),\ n) = (-j,\ j + 1)\,(n + 2j, n + 2j + 2)$$
$$= (-j(n + 2j) + (j + 1)(n + 2j + 2),\ (j + 1)(n + 2j) - j(n + 2j + 2))$$
$$= (-jn - 2j^2 + jn + 2j^2 + 2j + n + 2j + 2,\ jn + 2j^2 + n + 2j - jn - 2j^2 - 2j)$$
$$= (n + 4j + 2,\ n)$$
$$= (n + 2(2j + 1),\ n). \quad \square$$

Para el caso donde $k = 0$, entonces el número gaussiano-doble $(n,\, n)$ no tiene descomposición en $Z[\sigma]$, puesto que es el producto de sí mismo por otro número

$$(n,\, n) = (n,\, n)\,(a,\, 1 - a),$$

para cualquier a. Es decir, no se puede descomponer como producto finito de elementos primos.

1.10 Criterios de divisibilidad en $Z[\sigma]$

Ya que conocemos los números primos gaussianos-dobles, a partir de ellos definimos criterios de divisibilidad, esto lo haremos sacando algunos múltiplos de cada número para poder generalizar las regularidades.

Algunos múltiplos de $(2,\, 0)$

$$\begin{aligned}
(2,\, 0)\,(2,\, 0) &= (4,\, 0)\\
(2,\, 0)\,(2,\, 1) &= (4,\, 2)\\
(2,\, 0)\,(3,\, 1) &= (6,\, 2)\\
(2,\, 0)\,(3,\, 2) &= (6,\, 4)\\
(2,\, 0)\,(4,\, 3) &= (8,\, 6)\\
(2,\, 0)\,(5,\, 3) &= (10,\, 6)\\
&\vdots
\end{aligned}$$

De la lista podemos observar que todos los múltiplos de $(2,\, 0)$, tanto como la parte entera como la parte gaussiana-doble es divisible por 2.

Teorema 31.

Sea $z = (a,\, b) \in Z[\sigma]$, $(a,\, b)$ *es divisible por los asociados de* $(2,\, 0)$ *si* $2 \mid a$ *y* $2 \mid b$.

Prueba:

Como $(a,\, b)$ es divisible por $(2,\, 0)$, entonces existe $(c,\, d) \in Z[\sigma]$ tal que

$$\begin{aligned}(a,\, b) &= (2,\, 0)\,(c,\, d)\\ &= (2c,\, 2d)\end{aligned}$$

entonces $$a = 2c$$

y $$b = 2d,$$

luego $$2 \mid a \quad y \quad 2 \mid b.$$

La demostración para los asociados de $(2,\, 0)$, es análoga. □

Algunos múltiplos de $(2,\, 1)$

$$\begin{aligned}(2,\, 1)\,(2,\, 0) &= (4,\, 2)\\ (2,\, 1)\,(2,\, 1) &= (5,\, 4)\\ (2,\, 1)\,(3,\, 1) &= (7,\, 5)\\ (2,\, 1)\,(3,\, 2) &= (8,\, 7)\\ (2,\, 1)\,(4,\, 3) &= (11,\, 10)\\ (2,\, 1)\,(5,\, 3) &= (13,\, 11)\\ &\vdots\end{aligned}$$

Teorema 32.

Sea $z = (a,\, b) \in Z[\sigma]$, $(a,\, b)$ *es divisible por los asociados de* $(2,\, 1)$ *si* $3 \mid a + b$.

Prueba:

Como $(a,\, b)$ es divisible por $(2,\, 1)$, entonces existe $(c,\, d) \in Z[\sigma]$ tal que

$$\begin{aligned}(a,\, b) &= (2,\, 1)\,(c,\, d)\\ &= (2c + d,\, c + 2d)\end{aligned}$$

entonces

$$2c + d = a \tag{1.27}$$

$$c + 2d = b \tag{1.28}$$

luego sumando (1.27) y (1.28) se tiene

$$3c + 3d = a + b$$

$$3(c + d) = a + b$$

luego

$$3 \mid a + b.$$

La demostración para los asociados de (2, 1), es análoga. □

Algunos múltiplos de (3, 2)

$$(3,\, 2)\,(2,\, 0) = (6,\, 4)$$

$$(3,\, 2)\,(2,\, 1) = (8,\, 7)$$

$$(3,\, 2)\,(3,\, 1) = (11,\, 9)$$

$$(3,\, 2)\,(3,\, 2) = (12,\, 13)$$

$$(3,\, 2)\,(4,\, 3) = (18,\, 17)$$

$$(3,\, 2)\,(5,\, 3) = (21,\, 19)$$

$$\vdots$$

Teorema 33.

Sea $z = (a,\, b) \in Z[\sigma]$, $(a,\, b)$ *es divisible por los asociados de* $(3,\, 2)$ *si* $5 \mid a + b$.

Prueba:

Como $(a,\, b)$ es divisible por $(3,\, 2)$, entonces existe $(c,\, d) \in Z[\sigma]$ tal que

$$\begin{aligned}(a,\, b) &= (3,\, 2)\,(c,\, d)\\ &= (3c + 2d,\, 2c + 3d)\end{aligned}$$

entonces

$$3c + 2d = a \tag{1.29}$$

$$2c + 3d = b \tag{1.30}$$

luego sumando (1.29) y (1.30) se tiene

$$5c + 5d = a + b$$

$$5(c + d) = a + b$$

luego

$$5 \mid a + b.$$

La demostración para los asociados de (3, 2), es análoga. □

Algunos múltiplos de (4, 3)

$$(4,\, 3)\,(2,\, 0) = (8,\, 6)$$

$$(4,\, 3)\,(2,\, 1) = (11,\, 10)$$

$$(4,\, 3)\,(3,\, 1) = (15,\, 13)$$

$$(4,\, 3)\,(3,\, 2) = (18,\, 17)$$

$$(4,\, 3)\,(4,\, 3) = (25,\, 24)$$

$$(4,\, 3)\,(5,\, 3) = (29,\, 27)$$

$$\vdots$$

Teorema 34.

Sea $z = (a,\, b) \in Z[\sigma]$, $(a,\, b)$ *es divisible por los asociados de* $(4,\, 3)$ *si* $7 \mid a + b$.

Prueba:

Como $(a,\, b)$ es divisible por $(4,\, 3)$, entonces existe $(c,\, d) \in Z[\sigma]$ tal que

$$\begin{aligned}(a,\, b) &= (4,\, 3)\,(c,\, d)\\ &= (4c + 3d,\, 3c + 4d)\end{aligned}$$

entonces

$$4c + 3d = a \tag{1.31}$$

$$3c + 4d = b \tag{1.32}$$

luego sumando (1.31) y (1.32) se tiene

$$\begin{aligned}4c + 3d &= a + b\\ 7(c + d) &= a + b\end{aligned}$$

luego

$$7 \mid a + b.$$

La demostración para los asociados de $(4,\, 3)$, es análoga. □

En general, se tiene:

Teorema 35.

Sea $z = (a,\, b) \in Z[\sigma]$, $(a,\, b)$ es divisible por $p = (t,\, q)$ y sus asociados donde $\boldsymbol{N}p$ es un número primo entero, si $(t + q) \mid (a + b)$.

Prueba:

Como $(a,\, b)$ es divisible por $(t,\, q)$, entonces existe $(c,\, d) \in Z[\sigma]$ tal que

$$\begin{aligned}(a,\, b) &= (t,\, q)\,(c,\, d)\\ &= (tc + qd,\, qc + td)\end{aligned}$$

entonces

$$tc + qd = a \tag{1.33}$$

$$qc + td = b \tag{1.34}$$

luego sumando (1.33) y (1.34) se tiene

$$(t + q)c + (q + t)d = a + b$$

$$(t + q)(c + d) = a + b$$

luego

$$(t + q) \mid (a + b).$$

La demostración para los asociados de $(t,\, q)$, es análoga. □

Hemos omitido en los criterios de divisibilidad los números primos gaussianos-dobles de la forma $(2^{r+1} + 1,\, 2^{r+1} - 1)$, porque algunos múltiplos de estos números tiene más de una factorización. En general

Teorema 36.

Los números de la forma $(2^{l+3},\, 0)$ *tienen más de una descomposición prima en* $Z[\sigma]$.

Prueba:

Una factorización es

$$(2^{r+3},\, 0) = (2,\, 0)\,(2,\, 0)\,(2^{r+1},\, 0).$$

Otra factorización es

$$\begin{aligned}(2^{r+3},\, 0) &= (2^{r+1} + 1,\, 2^{r+1} - 1)\,(2^{r+1} + 1,\, -2^{r+1} + 1)\\ &= ((2^{r+1} + 1)\,(2^{r+1} + 1) + (2^{r+1} - 1)\,(-2^{r+1} + 1),\\ &\qquad (2^{r+1} - 1)\,(2^{r+1} + 1) + (2^{r+1} + 1)\,(-2^{r+1} + 1))\end{aligned}$$

$$= (2^{2(r+1)} + 2^{r+2} + 1 + 2^{r+1} - 2^{2(r+1)} + 2^{r+1} - 1,$$
$$2^{2(r+1)} + 2^{r+1} - 2^{r+1} - 1 + 2^{r+1} - 2^{2(r+1)} + 1 - 2^{r+1})$$
$$= (2^{r+2} + 2^{r+1} + 2^{r+1},\, 0)$$
$$= (2^{r+3},\, 0). \quad \square$$

Teorema 37.

Los números de la forma $(2^{l+3} + 2,\, 2^{l+3} - 2)$*, tienen más de una descomposición prima en* $Z[\sigma]$*.*

Prueba:

Una factorización es

$$(2^{l+3} + 2,\, 2^{l+3} - 2) = (2,\, 0)\,(2^{l+2} + 1,\, 2^{l+2} - 1).$$

Otra factorización es

$$\begin{aligned}(2^{l+3} + 2,\, 2^{l+3} - 2) &= (2^{r+1} + 1,\, 2^{r+1} - 1)\,(2^{h+1} + 1,\, 2^{h+1} - 1)\\ &= ((2^{r+1} + 1)\,(2^{h+1} + 1) + (2^{r+1} - 1)\,(2^{h+1} - 1),\\ &\qquad (2^{r+1} - 1)\,(2^{h+1} + 1) + (2^{r+1} + 1)\,(2^{h+1} - 1))\\ &= (2^{r+1}2^{h+1} + 2^{r+1} + 2^{h+1} + 1 + 2^{r+1}2^{h+1} - 2^{r+1} - 2^{h+1} + 1,\\ &\qquad 2^{r+1}2^{h+1} + 2^{r+1} - 2^{h+1} - 1 + 2^{r+1}2^{h+1} - 2^{r+1} + 2^{h+1} - 1)\\ &= (2(2^{r+h+2}) + 2,\, 2(2^{r+h+2}) - 2)\\ &= (2^{r+h+3} + 2,\, 2^{r+h+3} - 2)\end{aligned}$$

si $l = r + h$, entonces

$$= (2^{l+3} + 2,\, 2^{l+3} - 2). \quad \square$$

Además, debemos tener en cuenta que los múltiplos de $(2^{l+3},\, 0)$ y $(2^{l+3} + 2,\, 2^{l+3} - 2)$ también tienen más de una descomposición prima.

1.11 Máximo común divisor

Sean z y w números gaussianos-dobles, distintos de cero (por lo menos uno), entonces existe $\alpha \in Z[\sigma]$ con las siguientes propiedades[11]:

i) $\alpha \mid z \quad \text{y} \quad \alpha \mid w$.

ii) Si α' está en $\in Z[\sigma]$, $\alpha' \mid z \quad \text{y} \quad \alpha' \mid w$, entonces $\alpha' \mid \alpha$.

Un número gaussiano-doble α que tiene estas propiedades se le llama un *Máximo común divisor* de z y w y, se denota $\boldsymbol{MCD}[z, w] = \alpha$.

Demostremos la unicidad de α excepto por el producto por unidades. Supongamos que α y α' son dos números gaussianos-dobles que tienen las propiedades *i)* y *ii)*. Entonces, como $\alpha \mid z$ y $\alpha \mid w$, $\alpha' \mid z$ y $\alpha' \mid w$ entonces por *ii)* se tiene que $\alpha \mid \alpha'$. Por simetría tenemos que $\alpha' \mid \alpha$. Por tanto, α y α' son asociados. Luego α' pertenece a $[\alpha]$, donde $[\alpha]$ es la clase de equivalencia de los asociados a α. Por tanto α es único excepto por el producto por unidades.

Ejemplo

1. Determinar el máximo común divisor de $z = (10,\ 2)$ y $w = (7,\ 3)$.

   Para determinar el máximo común divisor entre $(10,\ 2)$ y $(7,\ 3)$ se descompone cada número gaussiano-doble en sus factores primos.

   $$z = (10,\ 2) = (10,\ 2)\,(1,\ 2)\,(-1,\ 3)$$
   $$w = (7,\ 3) = (2,\ 3)\,(-1,\ 3)$$

   El número $\alpha \in Z[\sigma]$, tal que $\alpha \mid (10,\ 2) \quad \text{y} \quad \alpha \mid (7,\ 3)$, es $\alpha = (-1,\ 3)$. Como no existe otro número gaussiano-doble que sea divisor común de $z = (10,\ 2)$ y $w = (7,\ 3)$, entonces el $\boldsymbol{MCD}[(10,\ 2),\ (7,\ 3)] = (-1,\ 3)$.

[11] Se dice que α es un *divisor común* o un *factor común* de z y w.

2. Determinar el máximo común divisor de $z = (17,\ 13)$ y $w = (37,\ 33)$.

   Para determinar el máximo común divisor entre $(17,\ 13)$ y $(37,\ 33)$ se descompone cada número gaussiano-doble en sus factores primos.

$$z = (17,\ 13) = (2,\ 1)\,(2,\ 3)\,(-1,\ 3)$$
$$w = (37,\ 33) = (2,\ 3)\,(-1,\ 3)\,(4,\ 3)$$

   Los divisores comunes de $(17,\ 13)$ y $(37,\ 33)$ son

$$\alpha_1 = (2,\ 3), \quad \alpha_2 = (-1,\ 3) \quad \text{y} \quad \alpha_3 = (2,\ 3)\,(-1,\ 3) = (7,\ 3).$$

   Luego el $\boldsymbol{MCD}[(17,\ 13),\ (37,\ 33)]$ es $\alpha_3 = (7,\ 3)$ porque

$$\alpha_1 \mid \alpha_3 \quad \text{y} \quad \alpha_2 \mid \alpha_3.$$

3. Para los números mencionados en los teoremas 36, 37 no se puede determinar el máximo común divisor.

   Por ejemplo, supongamos que queremos determinar el $\boldsymbol{MCD}[(18,\ 14)\,(34,\ 30)]$.

   Para hallar el máximo común divisor entre $(18,\ 14)$ y $(34,\ 30)$ se descompone cada número gaussiano-doble en sus factores primos.

$$(18,\ 14) = (2,\ 0)\,(9,\ 7)$$
$$(18,\ 14) = (3,\ 1)\,(5,\ 3).$$

   Además

$$(34,\ 30) = (2,\ 0)\,(17,\ 15)$$
$$(34,\ 30) = (3,\ 1)\,(9,\ 7)$$
$$(34,\ 30) = (5,\ 3)\,(5,\ 3)$$

   Los divisores comunes de $(18,\ 14)$ y $(34,\ 30)$ son

$$(2,\ 0), \quad (3,\ 1), \quad (5,\ 3) \quad \text{y} \quad (9,\ 7).$$

Pero la condición *ii*) no se cumple, por tanto no es posible determinar el máximo común divisor.

Si el máximo común divisor entre dos números gaussianos-dobles es una unidad entonces son *primos gaussianos-dobles relativos*.

Por ejemplo, (9, 4) y (11, 5) son primos gaussianos-dobles relativos.

1.12 Algoritmo de Euclides en $Z[\sigma]$

Como el conjunto $Z[\sigma]$ no es un anillo euclídiano, es posible que el algoritmo de Euclides no sea una un procedimiento eficaz para obtener el máximo común divisor de dos elementos[12] de $Z[\sigma]$, sin embargo veamos algo en detalle sobre este tema.

Sean z y $w \in Z[\sigma]$ y $\boldsymbol{N}w > 0$, entonces por el teorema 8 existen k y $p \in Z[\sigma]$ tales que;

$$z = w\,k_1 + p_1, \qquad\qquad \boldsymbol{N}p_1 < \boldsymbol{N}w.$$

Si $\boldsymbol{N}p_1 = 0$ entonces $p_1 = (a,\, b)$ donde $|a| = |b|$, de aquí tenemos dos posibilidades, que $p_1 = (0,\, 0)$, entonces $w \mid z$; o que $p_1 \neq (0,\, 0)$, de aquí $w \nmid z$ y el proceso aquí termina.

Si $\boldsymbol{N}p_1 \neq 0$ aplicamos nuevamente el algoritmo para obtener

$$w = p_1\,k_2 + p_2, \qquad\qquad \boldsymbol{N}p_2 < \boldsymbol{N}p_1.$$

Si $\boldsymbol{N}p_2 = 0$ entonces $p_2 = (a,\, b)$ donde $|a| = |b|$, de aquí tenemos dos posibilidades, que $p_2 = (0,\, 0)$, entonces $p_1 \mid w$, y $p_1 \mid z$; o que $p_2 \neq (0,\, 0)$, de aquí $p_1 \nmid w$ y el proceso aquí termina.

[12]Dorronsoro J, Hernandez E. *op.cit.*, 257 p.

Si $\boldsymbol{N}p_2 \neq 0$, repetimos el proceso, hasta llegar a un residuo cuya σ-norma sea igual a cero; obteniendo las siguientes ecuaciones:

$$\begin{aligned}
z &= w\,k_1 + p_1, & \boldsymbol{N}p_1 &< \boldsymbol{N}w,\\
w &= p_1\,k_2 + p_2, & \boldsymbol{N}p_2 &< \boldsymbol{N}p_1,\\
p_1 &= p_2\,k_3 + p_3, & \boldsymbol{N}p_3 &< \boldsymbol{N}p_2,\\
p_2 &= p_3\,k_4 + p_4, & \boldsymbol{N}p_4 &< \boldsymbol{N}p_3,\\
&\vdots & &\\
p_{k-3} &= p_{k-2}\,k_{k-1} + p_{k-1}, & \boldsymbol{N}p_{k-1} &< \boldsymbol{N}p_{k-2},\\
p_{k-2} &= p_{k-1}\,k_k + p_k, & \boldsymbol{N}p_k &< \boldsymbol{N}p_{k-1},\\
p_{k-1} &= p_k\,k_{k+1} + p_{k+1}, & \boldsymbol{N}p_{k+1} &= 0.
\end{aligned}$$

Esta secuencia de ecuaciones termina, porque $\boldsymbol{N}w$, $\boldsymbol{N}p_1$, $\boldsymbol{N}p_2, \ldots$ es una secuencia decreciente de números enteros no negativos.

Si la $\boldsymbol{N}p_{k+1} = 0$ con $p_{k+1} \neq (0,\,0)$ entonces este algoritmo no determina divisores comunes de z y w.

Si consideramos que al desarrollar este algoritmo el último residuo $p_{k+1} = (0,\,0)$, podemos demostrar que p_k, último residuo que no se anula, es un divisor de z y w:

De la última ecuación tenemos que

$$p_k \mid p_{k-1}$$

sustituyendo p_{k-1} en la penúltima ecuación,

$$\begin{aligned}
p_{k-2} &= p_k\,k_{k+1}\,k_k + p_k\\
&= (k_{k+1}\,k_k + 1)\,p_k.
\end{aligned}$$

Por tanto, $p_k \mid p_{k-2}$. Sustituyendo p_{k-2} y p_{k-1} en la antepenúltima ecuación,

$$\begin{aligned} p_{k-3} &= [(k_{k+1}\, k_k + 1)\, p_k]\, k_{k-1} + p_k\, k_{k+1} \\ &= (k_{k-1} k_{k+1}\, k_k + k_{k-1} + k_{k+1})\, p_k. \end{aligned}$$

Por tanto, $p_k \mid p_{k-3}$. Continuando en forma análoga tenemos que;

$$p_k \mid w \ \text{ y } \ p_k \mid z$$

luego p_k es un común divisor de z y w.

Probemos ahora que todo divisor común de z y w divide a p_k.

Consideremos d como cualquier divisor común de z y w. De la primera ecuación $d \mid p_1$, de la segunda $d \mid p_2$, etc.; y finalmente, de la penúltima ecuación, $d \mid p_k$.

Luego todo divisor de z y w también divide a p_k.

Por tanto p_k es un número gaussiano-doble que tiene todas las propiedades para ser un máximo común divisor de z y w.

Ejemplos

1. Apliquemos el algoritmo de euclides a los números gaussianos-dobles $z = (3,\, 2)$ y $w = (2,\, 5)$

   $$\frac{z}{w} = \frac{(2,\, 5)}{(3,\, 2)} = \frac{(2,\, 5)}{(3,\, 2)}\frac{(3,\, -2)}{(3,\, -2)} = \frac{(-4,\, 11)}{5} = (0,\, 2) + \frac{(-4,\, 1)}{5}$$

   por lo que

   $$\underbrace{(2,\, 5)}_{z} = \underbrace{(3,\, 2)}_{w}\ \underbrace{(0,\, 2)}_{k_1} + \underbrace{\frac{(-4,\, 1)}{(3,\, -2)}}_{p_1}$$

   como

   $$p_1 = \frac{(-4,\, 1)}{(3,\, -2)} = \frac{(-4,\, 1)}{(3,\, -2)}\frac{(3,\, 2)}{(3,\, 2)} = \frac{(-10,\, -5)}{5} = (-2,\, -1)$$

entonces

$$\begin{aligned} z = w\,k_1 + p_1 \qquad & \text{con} \qquad \boldsymbol{N}p_1 < \boldsymbol{N}w \\ (2,\,5) = (3,\,2)\,(0,\,2) + (-2,\,-1) \qquad & \text{con} \qquad \boldsymbol{N}(-2,\,-1) < \boldsymbol{N}(3,\,2) \\ & \qquad\qquad 3 < 9 \end{aligned}$$

En forma similar,

$$\frac{w}{p_1} = \frac{(3,\,2)}{(-2,\,-1)} = \frac{(3,\,2)}{(-2,\,-1)}\frac{(-2,\,1)}{(-2,\,1)} = \frac{(-4,\,-1)}{3} = (-1,\,0) + \frac{(-1,\,-1)}{3}$$

$$\underbrace{(3,\,2)}_{w} = \underbrace{(-2,\,-1)}_{p_1}\,\underbrace{(-1,\,0)}_{k_2} + \underbrace{\frac{(-1,\,-1)}{(-2,\,1)}}_{p_2}$$

como

$$p_2 = \frac{(-1,\,-1)}{(-2,\,1)} = \frac{(-1,\,-1)}{(-2,\,1)}\frac{(-2,\,-1)}{(-2,\,-1)} = (1,\,1)$$

entonces

$$\begin{aligned} w = p_1\,k_2 + p_2 \qquad & \text{con} \qquad \boldsymbol{N}p_2 < \boldsymbol{N}p_1 \\ (3,\,2) = (-2,\,-1)\,(-1,\,0) + (1,\,1) \qquad & \text{con} \qquad \boldsymbol{N}(1,\,1) < \boldsymbol{N}(-2,\,-1) \\ & \qquad\qquad 0 < 3 \end{aligned}$$

pero este proceso aquí termina, puesto que $\boldsymbol{N}(1,\,1) = 0$ y la división $\dfrac{p_1}{p_2} = \dfrac{(-2,\,-1)}{(1,\,1)}$, no está definida.

2. Determinar el máximo común divisor de $z = (10,\,2)$ y $w = (7,\,3)$.

   Tenemos

$$\frac{z}{w} = \frac{(10,\,2)}{(7,\,3)} = \frac{(10,\,2)\,(7,\,-3)}{(7,\,3)\,(7,\,-3)} = \frac{(64,\,-16)}{40} = (1,\,0) + \frac{(24,\,-16)}{40}$$

por lo que

$$\underbrace{(10,\,2)}_{z} = \underbrace{(7,\,3)}_{w}\,\underbrace{(1,\,0)}_{k_1} + \underbrace{\frac{(24,\,-16)}{(7,\,-3)}}_{p_1}$$

como

$$p_1 = \frac{(24,\,-16)}{(7,\,-3)} = \frac{(24,\,-16)\,(7,\,3)}{(7,\,-3)\,(7,\,3)} = \frac{(120,\,-40)}{40} = (3,\,-1)$$

entonces

$$\begin{aligned} z = w\,k_1 + p_1 \qquad & \text{con} \qquad \boldsymbol{N}p_1 < \boldsymbol{N}w \\ (10,\,2) = (7,\,3)\,(1,\,0) + (3,\,-1) \qquad & \text{con} \qquad \boldsymbol{N}(3,\,-1) < \boldsymbol{N}(7,\,3) \\ & \qquad\qquad 8 < 40. \end{aligned}$$

En forma similar,

$$\frac{w}{p_1} = \frac{(7,\,3)}{(3,\,-1)} = \frac{(7,\,3)\,(3,\,1)}{(3,\,-1)\,(3,\,1)} = \frac{(24,\,16)}{8} = (3,\,2)$$

entonces

$$w = p_1\,k_2$$

$$(7,\,3) = (3,\,-1)\,(3,\,2).$$

Por tanto el $\boldsymbol{MCD}[(10,\,2),\,(7,\,3)] = (3,\,-1)$.

3. Verifiquemos por el algoritmo de Euclides que el $\boldsymbol{MCD}[(9,\,4)\,(11,\,5)]$, es $(1,\,0)$.

   Tenemos

$$\frac{z}{w} = \frac{(11,\,5)}{(9,\,4)} = \frac{(11,\,5)\,(9,\,-4)}{(9,\,4)\,(9,\,-4)} = \frac{(79,\,1)}{65} = (1,\,0) + \frac{(14,\,1)}{65}$$

   por lo que

$$\underbrace{(11,\,5)}_{z} = \underbrace{(9,\,4)}_{w}\,\underbrace{(1,\,0)}_{k_1} + \underbrace{\frac{(14,\,1)}{(9,\,-4)}}_{p_1}$$

como

$$p_1 = \frac{(14,\ 1)}{(9,\ -4)} = \frac{(14,\ 1)\,(9,\ 4)}{(9,\ -4)\,(9,\ 4)} = \frac{(130,\ 65)}{65} = (2,\ 1)$$

entonces

$$(11,\ 5) = (9,\ 4)\,(1,\ 0) + (2,\ 1) \qquad \text{con} \qquad \boldsymbol{N}(2,\ 1) < \boldsymbol{N}(9,\ 4)$$
$$3 < 65.$$

En forma similar,

$$\frac{w}{p_1} = \frac{(9,\ 4)}{(2,\ 1)} = \frac{(9,\ 4)\,(2,\ -1)}{(2,\ 1)\,(2,\ -1)} = \frac{(14,\ -1)}{3} = (4,\ 0) + \frac{(2,\ -1)}{3}$$

por lo que

$$\underbrace{(9,\ 4)}_{w} = \underbrace{(2,\ 1)}_{p_1}\ \underbrace{(4,\ 0)}_{k_2} + \underbrace{\frac{(2,\ -1)}{(2,\ -1)}}_{p_2}$$

entonces

$$(9,\ 4) = (2,\ 1)\,(4,\ 0) + (1,\ 0) \qquad \text{con} \qquad \boldsymbol{N}(1,\ 0) < \boldsymbol{N}(2,\ 1)$$
$$1 < 3.$$

entonces

$$(2,\ 1) = (1,\ 0)\,(2,\ 1).$$

Por tanto el $\boldsymbol{MCD}[(9,\ 4),\ (11,\ 5)] = (1,\ 0)$.

En adelante se consideraran únicamente los números gaussianos-dobles para los que el algortimo de euclides si determina el máximo común divisor.

Teorema 38.

Sean z y $w \in Z[\sigma]$, $\boldsymbol{N}w \neq 0$, entonces el $\boldsymbol{MCD}[z,\ w]$ puede ser expresado en la forma

$$\boldsymbol{MCD}[z,\ w] = zx + wy,$$

donde x e y son gaussianos-dobles.

Prueba:

Supongamos que el $\boldsymbol{MCD}[z, w] = p_k$, de acuerdo con los resultados obtenidos en la descripción del algoritmo de Euclides, podemos expresar los sucesivos restos p_i, en terminos de z y w:

$$\begin{aligned} p_1 &= z + (-k_1)\, w \\ p_2 &= w + (-k_2)\, p_1 = (-k_2)\, z + (1 + k_1 k_2)\, w \\ p_3 &= p_1 + (-k_3)\, p_2 = (1 + k_3 k_2)\, z + (-k_1 - k_3 - k_1 k_2 k_3)\, w \\ &\vdots \end{aligned}$$

Eventualmente se obtendrá p_k como una combinación lineal de z y w. □

Ejemplo

Encontrar $\boldsymbol{MCD}[(1,\, 8)\,(2,\, 5)]$ y expresarlo como combinación lineal de $(1,\, 8)$ $(2,\, 5)$.

Entonces por el algoritmo de Euclides,

$$\begin{aligned} \underbrace{(1,\, 8)}_{z} &= \underbrace{(2,\, 5)}_{w}\, \underbrace{(1,\, 0)}_{k_1} + \underbrace{(-1,\, 3)}_{p_1} \\ \underbrace{(2,\, 5)}_{w} &= \underbrace{(-1,\, 3)}_{p_1}\, \underbrace{(2,\, 1)}_{k_2} + \underbrace{(1,\, 0)}_{p_2} \\ \underbrace{(-1,\, 3)}_{p_1} &= \underbrace{(1,\, 0)}_{p_2}\, \underbrace{(-1,\, 3)}_{k_3}. \end{aligned}$$

Entonces,

$$\boldsymbol{MCD}[(1,\, 8)\,(2,\, 5)] = (1,\, 0).$$

Además,

$$\underbrace{(-1,\,3)}_{p_1} = \underbrace{(1,\,8)}_{z} + \underbrace{(-1,\,0)}_{-k_1}\,\underbrace{(2,\,5)}_{w}, \qquad \text{y}$$

$$\underbrace{(1,\,0)}_{p_2} = \underbrace{(2,\,5)}_{w} + \underbrace{(-2,\,-1)}_{-k_2}\,\underbrace{(-1,\,3)}_{p_1}$$

$$\underbrace{(1,\,0)}_{p_2} = \underbrace{(2,\,5)}_{w} + \underbrace{(-2,\,-1)}_{-k_2}\,\underbrace{\left[(1,\,8) + (-1,\,0)\,(2,\,5)\right]}_{p_1}$$

$$(1,\,0) = \underbrace{(1,\,8)}_{z}\,\underbrace{(-2,\,-1)}_{x} + \underbrace{(2,\,5)}_{w}\,\underbrace{(3,\,1)}_{y}$$

esto es

$$\boldsymbol{MCD}[(1,\,8)\,(2,\,5)] = (1,\,8)\,(-2,\,-1) + (2,\,5)\,(3,\,1)$$

El teorema 38 nos permite encontrar soluciones de la ecuación $zx + wy = \boldsymbol{MCD}[z,\,w]$, en general se puede estudiar si la ecuación $zx + wy = v$ tiene o no soluciones que sean números gaussianos-dobles, entonces recibe el nombre de ecuaciones *diofanticas gaussianas-dobles*.

1.13 Ecuaciones diofánticas gaussianas-dobles

Sean z, w y v números gaussianos-dobles, $\boldsymbol{N}z \neq 0$ y $\boldsymbol{N}w \neq 0$, toda ecuación lineal de la forma:

$$zx + wy = v,$$

donde x e y estan restringuidos al conjunto $Z[\sigma]$, se dice una *ecuación diofantica en dos variables*.

Ejemplo

Consideremos la ecuación diofántica gaussiana-doble

$$(2,\,5)\,(a,\,b) + (1,\,8)\,(c,\,d) = (51,\,31)$$

Sea $z = (1,\, 8)$ y $w = (2,\, 5)$. Entonces por el algoritmo de euclides,

$$(1,\, 8) = (1,\, 0)\,(2,\, 5) + (-1,\, 3)$$

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

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

Por tanto $(1,\, 8)$ y $(2,\, 5)$ son primos gaussianos-dobles relativos. Por el teorema 38 es posible escribir $(1,\, 0)$ como una combinación lineal de $(1,\, 8)$ y $(2,\, 5)$:

$$(-1,\, 3) = (1,\, 8) + (-1,\, 0)\,(2,\, 5) \qquad \text{y}$$

$$(1,\, 0) = (1,\, 8)\,(-2,\, -1) + (2,\, 5)\,(3,\, 1).$$

Como $(-2,\, -1)\,(1,\, 8) + (3,\, 1)\,(2,\, 5) = (1,\, 0)$, entonces

$$(51,\, 31)\,(-2,\, -1)\,(1,\, 8) + (51,\, 31)\,(3,\, 1)\,(2,\, 5) = (51,\, 31)\,(1,\, 0)$$

$$(-133,\, -113)\,(1,\, 8) + (184,\, 144)\,(2,\, 5) = (51,\, 31)$$

De aquí que una *solución particular* de ecuación diofántica gaussiana-doble

$$(2,\, 5)\,(a,\, b) + (1,\, 8)\,(c,\, d) = (51,\, 31)$$

está dada por

$$(a,\, b) = (-133,\, -113) \qquad \text{y} \qquad (c,\, d) = (184,\, 144)$$

Una *solución general* de la ecuación diofántica gaussiana-doble está dada por

$$(a,\, b) = (184,\, 144) + (1,\, 8)\,t \qquad \text{y} \qquad (c,\, d) = (-133,\, -113) + (-2,\, -5)\,t$$

Teorema 39.

Sean z, w y $v \in Z[\sigma]$ con $\boldsymbol{MCD}[z,\, w] = v$*, la ecuación;*

$$zx + wy = c$$

tiene soluciones gaussianas-dobles si y sólo si

$$v \mid c.$$

Prueba:

i) Si la ecuación $zx + wy = c$ tiene soluciones en los números gaussianos-dobles, entonces existen t y $r \in Z[\sigma]$ tales que

$$zt + wr = c.$$

Como v es un divisor común de z y w, tenemos que

$$z = vp \qquad \text{y} \qquad w = vq$$

con p y $q \in Z[\sigma]$.

Por tanto

$$\begin{aligned} c &= zt + wr \\ &= vpt + vqr \\ &= v(pt + qr) \end{aligned}$$

Luego

$$v \mid c.$$

ii) Supongamos que v divide a c es decir, existe un $k \in Z[\sigma]$ tal que

$$c = kv,$$

por el teorema 38, existen t y $r \in Z[\sigma]$ tales que

$$zt + wr = v.$$

Multiplicando por k a ambos lados de esta ecuación se obtiene:

$$ztk + wrk = vk$$

$$z(tk) + w(rk) = c.$$

Por tanto $x = tk$ y $y = rk$, es una solución de la ecuación

$$zx + wy = c. \quad \square$$

Teorema 40.

Dos números z y $w \in Z[\sigma]$, $\boldsymbol{N}z$ y $\boldsymbol{N}w \neq 0$, son primos gaussianos-dobles relativos si y sólo si existen x e $y \in Z[\sigma]$ tales que,

$$zx + wy = (1,\, 0).$$

Prueba:

i) Si el $\boldsymbol{MCD}[z,\, w] = (1,\, 0)$, entonces por el teorema 38 existen números gaussianos-dobles x e y yales que;

$$zx + wy = (1,\, 0).$$

ii) Por otra parte, si $zx + wy = (1,\, 0)$ y r es un divisor común de z y w, se tiene que

$$z = pr \qquad \text{y} \qquad w = qr$$

y por lo tanto

$$(pr)x + (qr)y = (1,\, 0)$$

$$r(xp + yq) = (1,\, 0),$$

Así pues $r \mid (1,\, 0)$ y en consecuencia $\boldsymbol{MCD}[z,\, w] = (1,\, 0)$. □

Teorema 41.

Es posible encontrar x, y e $z \in Z[\sigma]$, que cumplan la siguiente ecuación

$$x^2 + y^2 = z^2.$$

Prueba:

Sean $x = (2a{+}1,\, 2b)$, $y = \big(2(a^2{+}a{+}b^2),\, 2(2ab{+}b)\big)$ y $z = \big(2(a^2{+}a{+}b^2){+}1,\, 2(2ab{+}b)\big)$,

entonces

$$\begin{aligned}
x^2 + y^2 &= \big(2a+1,\, 2b\big)^2 + \big(2(a^2+a+b^2),\, 2(2ab+b)\big)^2 \\
&= \Big((2a+1)^2 + 4b^2,\, 4b(2a+1)\Big) + \Big(4(a^2+a+b^2)^2 + 4b^2(2a+1), \\
&\qquad\qquad 8b(a^2+a+b^2)(2a+1)\Big) \\
&= \Big(4a^4 + 8a^3 + 8a^2(3b^2+1) + a(24b^2+4) + 4b^4 + 8b^2 + 1, \\
&\qquad\qquad 4b(2a+1)(2a^2+2a+2b^2+1)\Big) \\
&= (2a^2+2a+2b^2+1,\, 4ab+2b)^2 \\
&= \big(2(a^2+a+b^2)+1,\, 2(2ab+b)\big)^2 \\
&= z^2 \quad \square
\end{aligned}$$

1.14 Teoría de congruencias

Sean z, w y n números gaussianos dobles. Si $n \mid (z-w)$ decimos que z y w son *congruentes módulo* n y escribimos

$$z \equiv w \ (\text{mód}\ \ n).$$

Si z no es congruente con w módulo n, escribimos

$$z \not\equiv w \ (\text{mód}\ \ n).$$

Ejemplos

1. $(3,\, 4) \equiv (7,\, 2)\ (\text{mód}\ \ (-4,\, 2))$.

2. $(5,\, 2) \equiv (3,\, 1)\ (\text{mód}\ \ (2,\, 1))$.

3. Para todo par de números gaussianos dobles z y w, tenemos;

$$z \equiv w \text{ (mód } (1, 0))$$
$$z \equiv w \text{ (mód } (-1, 0))$$
$$z \equiv w \text{ (mód } (0, 1))$$
$$z \equiv w \text{ (mód } (0, -1))$$

4. $(7, 9) \not\equiv (13, 3)$ (mód $(9, 2)$).

Teorema 42.

Sean z, w, n y d números gaussianos-dobles si $d \mid n$ y $z \equiv w$ (mód n) entonces $z \equiv w$ (mód d).

Prueba:

Como $d \mid n$ entonces existe $p \in Z[\sigma]$ tal que

$$n = dp. \tag{1.35}$$

Además, como $z \equiv w$ (mód n), se tiene que

$$n \mid (z - w),$$

entonces existe $q \in Z[\sigma]$ tal que

$$(z - w) = qn$$

remplazando por (1.35) se tiene

$$(z - w) = q(dp)$$
$$(z - w) = (qp)d$$

es decir,

$$d \mid (z - w),$$

lo que significa que $z \equiv w \pmod{d}$. □

Teorema 43.

La congruencia módulo n es una relación de equivalencia sobre $Z[\sigma]$.

Prueba:

i) Reflexiva: Para cualquier número gaussiano-doble z

$$n \mid (z - z)$$
$$n \mid 0$$

es decir, $z \equiv z \pmod{n}$.

ii) Simétrica: Si $z \equiv w \pmod{n}$ entoces $n \mid (z - w)$ y por tanto

$$n \mid -(z - w)$$
$$n \mid (-z + w)$$
$$n \mid (w - z)$$

Luego $w \equiv z \pmod{n}$.

iii) Transitiva: Si $z \equiv w \pmod{n}$ y Si $w \equiv v \pmod{n}$ entonces $n \mid (z - w)$ y $n \mid (w - v)$, por tanto

$$n \mid (z - w) + (w - v)$$
$$n \mid (z - v)$$

es decir, $z \equiv v \pmod{n}$. □

Teorema 44.

Dos números gaussianos-dobles z y w son congruentes módulo n si y sólo tienen el mismo residuo al dividirlos por n.

Prueba:

Supongamos $z \equiv w$ (mód n) y sea r el residuo de dividir w por n, entonces existe un $k \in Z[\sigma]$ tal que $z - w = k\,n$ y además $w = q\,n + r$ con $\boldsymbol{N}r < \boldsymbol{N}n$. En consecuencia

$$\begin{aligned} z &= w + k\,n = (q\,n + r) + k\,n \\ &= (q + k)\,n + r. \end{aligned}$$

Como $q+k$ es un número gaussiano-doble observamos que z y w tiene el mismo residuo al dividirlos por n.

Recíprocamente, supongamos que z y w tienen el mismo residuo al dividirlos por n. Tenemos entonces que

$$z = q\,n + r,$$

$$w = p\,n + r,$$

con $\boldsymbol{N}r < \boldsymbol{N}n$.

En consecuencia, restando término a término tenemos $z - w = (q - p)\,n$ es decir, $z \equiv w$ (mód n).

Nota 9.

Veamos la siguiente situación

$$(8,\, 7) \equiv (4,\, 2)\ (\mathit{mód}\ (4,\, 5))$$

entonces

$$(8,\,7) = (4,\,5)\,(0,\,1) + (3,\,3) \qquad con \quad \boldsymbol{N}(3,\,3) < \boldsymbol{N}(4,\,5)$$
$$0 < 9$$
$$(4,\,2) = (4,\,5)\,(0,\,1) + (-1,\,-2) \qquad con \quad \boldsymbol{N}(-1,\,-2) < \boldsymbol{N}(4,\,5)$$
$$3 < 9.$$

Esto no significa que el teorema 44 no se cumpla. Puesto que ya vimos en la nota 1, el cociente y el residuo en la división no son únicos entonces existe otro cociente y otro residuo para la división de $(8,\,7)$ *entre* $(4,\,5)$.

$$(8,\,7) = (4,\,5)\,(1,\,1) + (-1,\,-2) \qquad con \quad \boldsymbol{N}(-1,\,-2) < \boldsymbol{N}(4,\,5)$$
$$3 < 9.$$

Teorema 45.

Sean z, w, u *y* $v \in Z[\sigma]$, *si* $z \equiv w \ (mód\ n)$ *y* $u \equiv v \ (mód\ n)$ *entonces:*

1. *Para todo par de números gaussianos-dobles* r *y* s, $zr + us \equiv wr + vs \ (mód\ n)$.
2. $zu \equiv wv \ (mód\ n)$.

Prueba:

1. Por hipótesis se tiene que $n \mid (z - w)$ y $n \mid (u - v)$, luego por el teorema 11 tenemos que

$$n \mid r(z - w) + s(u - v)$$
$$n \mid rz - rw + su - sv)$$
$$n \mid (zr + us) - (wr + vs)$$

y por tanto

$$zr + us \equiv wr + vs \text{ (mód } n).$$

En particular se tiene que:

$$z + u \equiv w + v \text{ (mód } n)$$

$$z - u \equiv w - v \text{ (mód } n)$$

$$zr \equiv wr \text{ (mód } n).$$

2. Por hipótesis se tiene que $n \mid (z - w)$ y $n \mid (u - v)$, entonces existen k y $j \in Z[\sigma]$ tales que

$$z - w = nk \qquad u - v = nj$$

$$z = nk + w \qquad u = nj + v$$

$$zu = (nk + w)(nj + u)$$

$$zu = nknj + nkv + wnj + wv$$

$$zu = n(knj + kv + wj) + wv$$

$$zu - wv = n(knj + kv + wj)$$

como $knj + kv + wj \in Z[\sigma]$, por la definición de congruencia tenemos

$$zu \equiv wv \text{ (mód } n). \quad \square$$

1.15 Ideales en $Z[\sigma]$

Un *ideal* en el dominio $Z[\sigma]$ es un conjunto $I \subset Z[\sigma]$ que cumpla las propiedades siguientes:

i) $(0, 0) \in I$,

ii) Si z y $w \in I$, entonces $z - w \in I$,

iii) Si $z \in Z[\sigma]$ y $w \in I$, entonces $z\,w \in I$.

El anillo $Z[\sigma]$ tiene al menos dos ideales, a saber, $\{(0,\,0)\}$ ya que $z\,(0,\,0) = (0,\,0)\,z = (0,\,0)$ para todo $z \in Z[\sigma]$ y el propio $Z[\sigma]$. A estos ideales se les llama *ideales impropios*. El ideal $\{(0,\,0)\}$ es el ideal *trivial*.

Nota 10.

$Z[\sigma]$ es un anillo con unidad $(1,\,0)$ y I es un ideal de $Z[\sigma]$ tal que $(1,\,0) \in I$, se tiene que $I = Z[\sigma]$, en efecto para todo $z \in Z[\sigma]$, $z = z\,(1,\,0) \in I$.

Un ideal del dominio $Z[\sigma]$ es *principal* si está generado por un solo elemento, es decir, si es de la forma $(z) = z\,Z[\sigma] = \{z\,w$ tal que $w \in Z[\sigma]\}$.

Ejemplos

1. $I = \{(a,\,a)\}$, es un ideal de $Z[\sigma]$ puesto que:

   i) $(0,\,0) \in I$,

   ii) $(a,\,a) - (b,\,b) = (a - b,\,a - b) \in I$,

   iii) $(c,\,d)(a,\,a) = (ca + da,\,da + ca) \in I$.

   El ideal I es principal porque está generado por el elemento $(1,\,1)$.

2. $I = \{(a,\,-a)\}$, es un ideal de $Z[\sigma]$ puesto que:

   i) $(0,\,0) \in I$,

   ii) $(a,\,-a) - (b,\,-b) = (a - b,\,-(a - b)) \in I$,

   iii) $(c,\,d)(a,\,-a) = (ca - da,\,da - ca) \in I$.

El ideal I es principal porque está generado por el elemento $(1, -1)$.

3. $I = \{(na, nb)\}$, es un ideal de $Z[\sigma]$ puesto que:

   i) $(0, 0) \in I$,

   ii) $(na, nb) - (ne, nf) = (n(a-e), n(b-f)) \in I$,

   iii) $(c, d)(na, nb) = (cna + dnb, dna + cnb) = (n(ca + db), n(da + cb)) \in I$.

   El ideal I es principal porque está generado por el elemento $(n, 0)$.

4. $I = \{(a, 0)\}$, no es un ideal de $Z[\sigma]$ puesto que:

   iii) $(c, d)(a, 0) = (ca, da) \notin I$.

5. $I = \{(0, b)\}$, no es un ideal de $Z[\sigma]$ puesto que:

   iii) $(c, d)(0, b) = (db, cb) \notin I$.

Anexos

Algunos primos gaussianos-dobles

(2, 1)	(3, 1)	(3, 2)	(4, 3)	(5, 3)
(6, 5)	(7, 6)	(9, 7)	(9, 8)	(10, 9)
(12, 11)	(15, 14)	(16, 15)	(17, 15)	(19, 18)
(21, 20)	(22, 21)	(24, 23)	(27, 26)	(30, 29)
(31, 30)	(33, 31)	(34, 33)	(36, 35)	(37, 36)
(40, 39)	(42, 41)	(45, 44)	(49, 48)	(51, 50)
(52, 51)	(54, 53)	(55, 54)	(57, 56)	(64, 63)
(65, 63)	(66, 65)	(69, 68)	(70, 69)	(75, 74)
(76, 75)	(79, 78)	(82, 81)	(84, 83)	(87, 86)
(90, 89)	(91, 90)	(96, 95)	(97, 96)	(99, 98)

(100, 99)	(106, 105)	(112, 111)	(114, 113)	(115, 114)
(117, 116)	(120, 119)	(121, 120)	(126, 125)	(129, 127)
(129, 128)	(132, 131)	(135, 134)	(136, 135)	(139, 138)
(141, 140)	(142, 141)	(147, 146)	(154, 153)	(156, 155)
(157, 156)	(159, 158)	(166, 165)	(169, 168)	(174, 173)
(175, 174)	(177, 176)	(180, 179)	(184, 183)	(187, 186)
(190, 189)	(192, 191)	(195, 194)	(199, 198)	(201, 200)
(205, 204)	(210, 209)	(211, 210)	(216, 215)	(217, 216)
(220, 219)	(222, 221)	(225, 224)	(229, 228)	(231, 230)
(232, 231)	(234, 233)	(240, 239)	(244, 243)	(246, 245)
(250, 249)	(252, 251)	(255, 254)	(257, 255)	(261, 260)
(262, 261)	(271, 270)	(274, 273)	(279, 278)	(282, 281)
(285, 284)	(286, 285)	(289, 288)	(294, 293)	(297, 296)
(300, 299)	(301, 300)	(304, 303)	(307, 306)	(309, 308)
(310, 309)	(316, 315)	(321, 320)	(322, 321)	(324, 323)
(327, 326)	(330, 329)	(331, 330)	(337, 336)	(339, 338)
(342, 341)	(346, 345)	(351, 350)	(355, 354)	(360, 359)
(364, 363)	(367, 366)	(370, 369)	(372, 371)	(376, 375)
(379, 378)	(381, 380)	(385, 384)	(387, 386)	(394, 393)
(399, 398)	(405, 404)	(406, 405)	(411, 410)	(412, 411)
(414, 413)	(415, 414)	(420, 419)	(427, 426)	(429, 428)
(430, 429)	(432, 431)	(439, 438)	(441, 440)	(442, 441)

Programa "*G-D*"

```
# -*- coding: UTF-8 -*-
def espera():
    a=raw_input("Presione cualquier tecla para continuar ...\n")
    return

def opciones():
    opcion=''
    print u"Escoge una opción:"
    print u'a) Realiza la multiplicación de dos números gaussianos
                                                          -dobles.'
    print u'b) Determina la sigma-norma de un número gaussiano-doble.'
    print u'c) Determina si un número es primo gaussiano-doble o no.'
    print u'd) salir\n'
    t='Teclea a, b, c o d y pulsa enter: '
    opcion = raw_input(t)
    return opcion

def multiplicacion():
    a1 = int(raw_input(u'Digite la primera componente del primer
                                                        número ':))
    a2 = int(raw_input(u'Digite la segunda componente del primer
                                                        número ':))
    a3 = int(raw_input(u'Digite la primera componente del segundo
```

```
                                                          número '))
    a4 = int(raw_input(u'Digite la segunda componente del segundo
                                                          número '))
    multi1=(a1*a3)+(a2*a4)
    multi2=(a2*a3)+(a1*a4)
    print 'La multiplicacion (%d , %d)(%d , %d)=(%d , %d)\n'
                                        %  (a1,a2,a3,a4,multi1,multi2)


def norma():
     z = int(raw_input('Digite la primera componente '))
     v = int(raw_input('Digite la segunda componente '))
     norma = abs((z**2)-(v**2))
     print 'La sigma-norma de (%d , %d) es %d\n' % (z, v, norma)
def primos():
    z = int(raw_input('Digite la primera componente '))
    v = int(raw_input('Digite la segunda componente '))
    norma = abs((z**2)-(v**2))
    restos_no_nulos = 0
    for divisor in range(2, norma):
        if norma %divisor != 0:
            restos_no_nulos += 1

    if restos_no_nulos == norma -2:
        print u'El número (%d , %d) es primo gaussiano-doble \n'
                                                          % (z, v)
    else:
        if (abs(z)-abs(v))==2:
            u = 1
```

```
            while (u!=norma) and (u<norma):
                u=2*u
            if (u==norma):
                print u'El número (%d , %d) es primo gaussiano-doble \n'
                                                                % (z, v)
            else:
                print u'El número (%d , %d) no es primo gaussiano-doble
                                                          \n' % (z, v)
        else:
            if norma==1:
                print u'El número (%d , %d) es una unidad\n' % (z, v)
            else:
                print u'El número (%d , %d) no es primo gaussiano-doble
                                                        \n' % (z, v)


        #Menu principal
def operaciones():
    opcion=opciones()
    while opcion != 'd':
        if opcion == 'a':
            multiplicacion()
            espera()
            opcion=opciones()
            continue
        elif opcion == 'b':
            norma()
            espera()
            opcion=opciones()
```

```
            continue

        elif opcion == 'c':
            primos()
            espera()
            opcion=opciones()
            continue

        else:
            print 'Solo hay cuatro opciones: a, b, c o d.'
            print 'Usted tecleo', opcion,"\n"
            espera()
            opcion=opciones()
            continue
    return

operaciones()
```

Bibliografía

[1] Apostol, T. *Introducción a la teoría de números*. Barcelona: Reverté; 1980.

[2] Ayres, F. *Algebra moderna*. México: McGraw-Hill; 1991.

[3] Baker, A. *Breve introducción a la teoría de números*. Madrid: Alianza; 1986.

[4] Burton, J. *Teoría de los números*. México: Trillas; 1969.

[5] Campos M, Garzón M, Perez J, Rodriguez G. *Fundamentos de algebra abstracta*. Bogotá: Universidad Nacional de Colombia; 1990.

[6] Castro, I. *Temas de teoría de cuerpos, teoría de anillos y números algebraicos*. Bogotá: Universidad Nacional de Colombia; 1986.

[7] Cilleruelo J, Cordoba A. *La teoría de los números*, Madrid: Biblioteca Mondadory; 1992.

[8] Dorronsoro J, Hernandez E. *Números, grupos y anillos*. España: Addison-Wesley; 1996.

[9] Fraleigh, J. *A first course in abstract algebra*. 2 ed. Masachusetts: Addison-Wesley; 1976.

[10] Grosswald, E. *Topics form the theory of numbers*. 1978.

[11] Hartley B, Awkes T. *Rings, modules and linear algebra*. New york: Chapman and hall; 1970.

[12] Jimenez R, Gordillo E, Rubiano G. *Teoría de números para principiantes*. Bogotá: Universidad Nacional de Colombia; 1999.

[13] LeVeque, W. *Teoría elemental de los números*. México: Herrera Hermanos; 1968.

[14] Lezama O, De Villamarín G. *Anillos, modúlos y categorías*. Bogotá: Universidad Nacional de Colombia; 1994.

[15] Luque C, Mora L, Torres J. *Actividades matemáticas para el desarrollo de procesos lógicos clasificar medir e invertir*. Bogotá: Universidad Pedagógica Nacional; 2005.

[16] Muñoz, J. *Introducción a la teoría de conjuntos*. 4 ed. Bogotá: Universidad Nacional de Colombia; 2002.

[17] Niven, I, *Introducción a la teoría de números*. Limusa. 1969.

[18] Perez, E. *Estructuras algebraicas*. Bogotá. Universidad Pedagógica Nacional, 2005.

[19] Pettofrezzo A, Byrkit D. *Introducción a la teoría de números*. Prentice/Hall. 1972.

[20] Yaglom, I. *A simple non Euclidean geometry and its physical basis*. New York: Springer-Verlag; 1979.