"FUNCIONES D-ARITMÉTICAS DE LOS NÚMEROS G-PRIMOS DUALES"

Jiwell Enrique Munévar Peña

Asesor

Carlos Julio Luque Arias

Docente Universidad Pedagógica Nacional

Universidad Pedagógica Nacional

Facultad de Ciencia y Tecnología

Departamento de Matemáticas

Bogotá, D. C.

Abril de 2014

“FUNCIONES D-ARITMÉTICAS DE LOS NÚMEROS G-PRIMOS DUALES”
”

Jiwell Enrique Munévar Peña

Trabajo de grado presentado como requisito parcial para optar al título de licenciado en matemáticas

Asesor
Carlos Julio Luque Arias
Docente Universidad Pedagógica Nacional

Modalidad: Interés Personal de los Estudiantes

Universidad Pedagógica Nacional
Facultad de Ciencia y Tecnología
Departamento de Matemáticas Bogotá, D. C.

Abril de 2014

RESUMEN ANALÍTICO EN EDUCACIÓN

UNIVERSIDAD PEDAGOGICA NACIONAL	FORMATO
	RESUMEN ANALÍTICO EN EDUCACIÓN - RAE
Código: FOR020GIB	Versión: 01
Fecha de Aprobación: 10-10-2012	Página 3 de 75

1. Información General	
Tipo de documento	Trabajo de grado
Acceso al documento	Universidad Pedagógica Nacional. Biblioteca Central
Titulo del documento	Funciones D-Aritméticas de los números G-primos duales.
Autor(es)	Munévar Peña, Jiwell Enrique.
Director	Carlos Julio Luque Arias.
Publicación	Bogotá, 2014. Universidad Pedagògica Nacional. 75 Páginas.
Unidad Patrocinante	Universidad Pedagógica Nacional.
Palabras Claves	Naturales gaussianos duales, semianillo, asociados, G-naturales duales, funciones D-aritméticas, G-primos duales, divisibilidad, Espiral de Ulam.

2. Descripción
Los números naturales gaussianos duales D_g^+ son un subconjunto del plano, donde sus elementos son parejas ordenadas $(a,b) \in \mathbb{Z}^+ \times \mathbb{Z}$ tal que la suma está definida componente a componente y la multiplicación por $(a,b) \otimes (c,d) = (ac, ad+bc)$. El conjunto de los números naturales gaussianos duales junto con estas operaciones es un semianillo conmutativo cancelativo con unidad. En este conjunto se define una relación de divisibilidad y se pasa al cociente a partir de otra relación basada en la divisibilidad del conjunto D_g^+. En el conjunto cociente, se definen operaciones D-aritméticas y se estudia la distribución de las

clases de equivalencia de los números primos de D_g^+.

3. Fuentes

Se consultaron algunos textos que abordan la teoría analítica de números, algebra abstracta y algunos contenidos de la web relacionados a la espiral de Ulam en los números enteros.

dual.

4. Contenidos

El presente trabajo tiene 4 capítulos: el capítulo 1 trata de los números naturales gaussianos duales, donde se define una suma y una multiplicación que le dan una estructura de semianillo, además se estudian la divisibilidad, el orden y algunos teoremas de divisibilidad que son análogos a los que se trabajan con los números enteros. En el capítulo 2, se trabaja lo mismo que se desarrolló en el capítulo 1 pero con el conjunto cociente que se obtiene con la relación que se define a partir de la divisibilidad de D_g^+. En el capítulo 3 se estudian las funciones D-aritméticas que allí se definen. Además, se demuestran y conjeturan algunos resultados que se desprenden de las funciones. Finalmente, en el capítulo 4 se estudia la distribución de los números G-primos duales y se conjetura el teorema de los números primos para los números G-naturales duales, finalizando con imágenes de la espiral de Ulam.

5. Metodología

Para realizar este trabajo de grado se llevó a cabo una hora semanal de asesoría por parte del profesor Carlos Julio Luque Arias, a quién se le llevaron avances del trabajo con el fin de recibir aportes y críticas constructivas que enriquecieran el trabajo y el aprendizaje del estudiante. Para este trabajo se vio necesario el estudio de algunos momentos claves de la historia de la matemáticas (como por ejemplo la solución dada para el problema de Basilea), además de estudiar los fundamentos de la teoría de números, teoría de grupos y anillos, análisis y el manejo de algunos software que fueron importantes para algunos resultados que aquí se presentan.

6. Conclusiones

Conclusiones:

- El orden que se define en el conjunto cociente es un orden total.
- En el semianillo de los números naturales gaussianos duales se puede definir el algoritmo de la división con el cociente y el residuo únicos.
- Usando el algoritmo de Euclides es posible calcular la función indicatriz de Euler para los G-naturales duales y junto a la función de elementos comparables, se pueden obtener varios resultados que son esenciales en el presente trabajo.
- El teorema de los números G-primos duales es verdadero para los primeros 499999500000 números G-naturales duales.
- No fue posible hacer un estudio riguroso a la espiral de Ulam, debido a que el software donde se construyó imposibilitaba el dibujo de rectas sobre la espiral. Esto a su vez impedía realizar un estudio de la distribución de los G-primos duales, análogo a como se hace en los números enteros.
- No se cumple con los objetivos propuestos en el anteproyecto del trabajo, pero si los que se modifican y colocan en el trabajo.

Elaborado por:	Jiwell Munevar Peña.
Revisado por:	Carlos Julio Luque Arias.

Fecha de elaboración del Resumen:	10	06	2014

"A mi hijo, mi madre y mi esposa quiénes con su sonrisa y su existencia, hacen de mi vida una alegría, que opaca la maldad de este mundo ignorante"

AGRADECIMIENTOS

Agradezco a mi hijo y mi esposa, pues son ellos los que me levantan de mis más profundas tristezas y generan mis más grandes alegrías.

A mis padres y hermanos, quienes con su aprecio, apoyo y concejo hicieron más llevadera esta dura pero bella vida académica.

Al profesor *Carlos Julio Luque*, ya que fue él, quién me orientó y apoyó en muchos de mis procesos académicos y me indico el camino correcto para estudiar y enseñar las matemáticas.

A mi amiga *Yuli Andrea Medina* porque sin ella este sueño no hubiese sido realidad.

A mis amigos de colegio *Andrés Ramos* y *Vanesa Orrego* porque con su confianza y apoyo contribuyeron en mi crecimiento personal y me permitieron sobrepasar obstáculos.

A la familia *Rojas Macías* que me ayudaron en los momentos más difíciles de la carrera.

Contenido

INTRODUCCIÓN

El presente trabajo de grado es el resultado de un interés personal por *"aprender a estudiar y comprender la matemática",* siendo éste el inicio de un proceso de formación investigativa que será continuo y permitirá fortalecer algunos conocimientos de varias áreas de las matemáticas.

Además, la construcción de varios conceptos matemáticos, no solo afianzaron los conocimientos matemáticos, sino que además implicaron el desarrollo de procesos de conjeturación, representación, argumentación y formulación de teoremas o conjeturas que evidencian un trabajo de análisis y exploración numérica que siempre han sido el quehacer de alguien que intenta estudiar matemáticas.

Por otro lado, el trabajo se empieza atendiendo el estudio de la Función zeta de Riemman y de las series numéricas*,* haciendo recorridos históricos que van desde la Paradoja de Zenón hasta los resultados de Euler y Riemman relacionados con el Problema de Basilea y la Función Zeta de Riemman respectivamente; esto con el fin de estudiar a fondo el concepto de serie y concretar la forma en que se iba a desarrollar una versión dual del teorema de los números primos y de otros conceptos que hacen parte de la *teoría analítica de números.*

Por consiguiente, se decide definir el conjunto de los números naturales gaussianos duales con el fin de formular varias definiciones y conjeturas, que son análogas a los conceptos y resultados que se encuentran en un texto de teoría de números, y en el mejor de los casos se demuestran.

En el primer capítulo se describe la estructura algebraica del conjunto de los números naturales gaussianos duales (se deja de un lado los números enteros y se concibe como conocimiento previo), se estudia el orden que es análogo al de los números naturales, la relación de divisibilidad, los asociados, números primos naturales duales, máximo común divisor, algoritmo de Euclides y de la división así como algunas propiedades de divisibilidad que hacen parte fundamental del trabajo.

En el segundo capítulo, se trabaja con el conjunto cociente que se obtiene a partir de una relación de equivalencia basada en la divisibilidad de los números naturales gaussianos duales, se define un orden análogo al orden lexicográfico del plano que en este caso es total, y se define de nuevo todos los conceptos básicos de la teoría de números.

En el tercer capítulo se definen funciones D-aritméticas (análogas a las funciones aritméticas definidas sobre $\mathbb{Z}$) y se enuncian resultados producidos por procesos de cálculo que se apoyan en software como Excel y Visual Basic, sin embargo, pese a los intentos algunos de ellos no pasaron de ser sola una conjetura.

En el cuarto y último capítulo se enuncia el resultado más importante del presente trabajo y es el Teorema de los números G-primos duales, un resultado análogo al teorema del número primo y que para su formulación se necesitaron más de un millón de cálculos que en su momento fueron apoyados por hojas de cálculos y otros software de matemáticas. Aunque el teorema no se logró demostrar se muestran algunos resultados gráficos como la Espiral de Ulam para este conjunto, que evidencian la relación conjeturada.

Finalmente, para realizar este trabajo se hizo necesario el estudio de parte de la teoría de números, la teoría analítica de números, los números duales, la historia de las series, el álgebra abstracta e inclusive el estudio del lenguaje de programación Visual Basic para la estructuración de macros en Excel. Sin embargo, aunque el objetivo de demostrar el teorema de números G-primos duales con ayuda de la función zeta de Riemman no se cumplió, este trabajo queda como una gran apertura para seguir haciendo teoría de números en este conjunto y porque no en un futuro demostrar todo lo que en este trabajo quedo sin justificar.

JUSTIFICACIÓN

Como ya se mencionó, este trabajo se realizó con el interés de aprender a estudiar matemáticas, buscando verificar si la distribución de los números G-primos duales tiene algún resultado análogo al que se demuestra para los números primos enteros y si además se puede probar de forma analítica como se hace en los enteros con la función zeta de Riemann.

OBJETIVOS

Objetivo general

- Estudiar funciones D-aritméticas en el conjunto de los números G-naturales duales y conjeturar algunos resultados análogos a los existentes en la teoría de números enteros.

Objetivos específicos

- Recolectar información relacionada con la función Zeta de Riemann y su relación con los números primos.
- Definir funciones aritméticas para los números gaussianos duales y estudiar algunas de sus propiedades.
- Realizar conjeturas acerca de las funciones D-aritméticas y los números primos gaussianos duales, así como algunas de sus demostraciones.
- Sistematizar todo el estudio y la información recolectada para ser presentada como trabajo de grado.

Capítulo 1.

LOS NÚMEROS GAUSSIANOS DUALES

1.1. El conjunto de los números duales

Algebra dual

Sea D el plano $\mathbb{R}^2$ con la suma definida componente a componente y la multiplicación definida como:

$$(x,y)(u,t) = (xu, xt + yu), \text{para todo } (x,y), (u,t) \epsilon\, \mathbb{R}^2$$

Con ese par de operaciones el conjunto D de los números duales[1] es un anillo conmutativo con unidad $(1,0)$ y Los elementos $(0,y)$ son nilpotentes, es decir son elementos divisores de cero. El inverso multiplicativo de (x,y) en D es:

$$(x,y)^{-1} = (x^{-1}, -yx^{-2}) \text{ si } x \neq 0$$

1.2. Los números naturales gaussianos duales

Con la información anterior es posible definir un conjunto de números que se denomina el conjunto de números naturales gaussianos duales D_g^+, donde sus elementos son de la forma $z = (a,b)$ con $a \in \mathbb{Z}^+, b \in \mathbb{Z}$:

$$D_g^+ = \{(x,y) \epsilon\, \mathbb{Z}^+ \times \mathbb{Z}\}\text{, donde } \mathbb{Z}^+ = \{k\ \epsilon\ \mathbb{Z} : k > 0\}$$

[1] Operaciones basadas en el trabajo del profesor Carlos Julio Luque que se cita a continuación. LUQUE, C. (1993). "*El anillo de los números duales y la derivada de funciones reales".* Bogotá: Universidad Pedagógica Nacional.

A continuación se presenta una representación gráfica de algunos elementos de D_g^+,

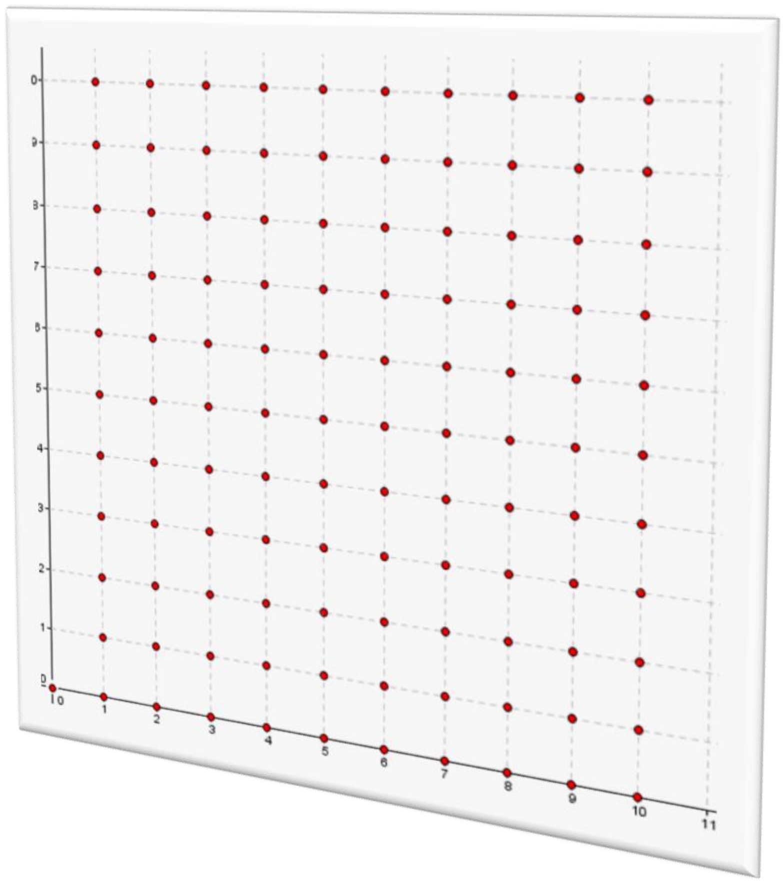


Figura 1 Algunos elementos de D_g^+.

1.2.1. *Estructura algebraica del conjunto de los números naturales gaussianos duales*

Sea $D_g^+ \subseteq \mathbb{R}^2$, en este conjunto de parejas ordenadas se define la ***suma*** componente a componente, es decir

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

Y la ***multiplicación*** como

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

Operaciones definidas para todo $(a, b), (c, d) \epsilon\, D_g^+$.

Con este par de operaciones la tripla $\left(D_g^+, \oplus, \otimes\right)$ se dota de una estructura de semianillo abeliano[2]. Además, el semianillo es cancelativo[3] ya que se cumplen las siguientes propiedades:

Teorema 1.2.1.1. Propiedad asociativa de $\oplus$ en $\boldsymbol{D_g^+}$

Si $(a,b),(c,d),(e,f) \in D_g^+$ entonces $[(a,b)\oplus(c,d)]\oplus(e,f) = (a,b)\oplus[(c,d)\oplus(e,f)]$.

Teorema 1.2.1.2. Propiedad conmutativa de $\oplus$ en $\boldsymbol{D_g^+}$

Si $(a,b),(c,d) \in D_g^+$ entonces $(a,b)\oplus(c,d) = (c,d)\oplus(a,b)$.

Teorema 1.2.1.3. Propiedad asociativa de $\otimes$ en $\boldsymbol{D_g^+}$

Si $(a,b),(c,d),(e,f) \in D_g^+$ entonces $[(a,b)\otimes(c,d)]\otimes(e,f) = (a,b)\otimes[(c,d)\otimes(e,f)]$

Teorema 1.2.1.4. Propiedad conmutativa de $\otimes$ en $\boldsymbol{D_g^+}$

Si $(a,b),(c,d) \in D_g^+$ entonces $(a,b)\otimes(c,d) = (c,d)\otimes(a,b)$

Teorema 1.2.1.5. Propiedad distributiva de $\otimes$ con respecto a $\oplus$ en $\boldsymbol{D_g^+}$

Para todo $(a,b),(c,d),(e,f) \in D_g^+$ se cumple que $(a,b)\otimes[(c,d)\oplus(e,f)] = [(a,b)\otimes(c,d)]\oplus[(a,b)\otimes(e,f)]$ y $[(a,b)\oplus(c,d)]\otimes(e,f) = [(a,b)\otimes(e,f)]\oplus[(c,d)\otimes(e,f)]$

---

[2] *Sea $S \neq \emptyset$ un conjunto y $+,\cdot$ dos operaciones binarias definidas en S , llamadas adición y multiplicación. Entonces la tripla $(S,+,\cdot)$ es denominada un* ***<u>semianillo</u>*** *si satisface las siguientes condiciones:*

1) *$(S,+)$ es un semigrupo abeliano.*
2) *$(S,\cdot)$ es un semigrupo.*
3) *Ambas operaciones están conectadas por la ley distributiva $a\cdot(b+c) = a\cdot b + a\cdot c$ y $(a+b)\cdot c = a\cdot c + b\cdot c$ para todo $a,b,c \in S$.*

En particular, un semianillo $(S,+,\cdot)$ se dice que es abeliano si $(S,\cdot)$ es abeliano. (Hebisch & Weinert, 1992)

[3] *Un semianillo $(S,+,\cdot)$ es cancelativo si el semigrupo $(S,+)$ es cancelativo.* (Hebisch & Weinert, 1992)

Teorema 1.2.1.6. Propiedad cancelativa de $\oplus$,

Para todo $(a,b),(c,d),(x,y) \in D_g^+$, si $(a,b)\oplus(x,y) = (c,d)\oplus(x,y)$ entonces $(a,b) = (c,d)$ (***La demostración de este teorema se realiza después de definir el orden para $\mathbf{D_g^+}$***).

Además de todas las propiedades que cumple $(D_g^+,\oplus,\otimes)$, se tiene un elemento neutro para la adición y uno para la multiplicación como se muestran a continuación:

Teorema 1.2.1.7. Existencia del elemento idéntico para la suma

Para todo $(a,b) \epsilon D_g^+$ se tiene que

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

Teorema 1.2.1.8. Existencia del elemento idéntico de la multiplicación

Para todo $(a,b) \epsilon D_g^+$ se cumple que

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

1.3. Orden en los Números Naturales Gaussianos Duales

Un número natural dual (a,b) es menor o igual a otro (c,d) si existe un número natural gaussiano dual (x,y) tal que:

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

En cuyo caso se escribe que $(a,b) \preccurlyeq (c,d)$ o $(c,d) \succcurlyeq (a,b)$ y si $(a,b) = (c,d)$ entonces $a = c$ y $b = d$.

Además, $(a,b) \prec (c,d)$ si y sólo si $(x,y) \neq (0,0)$.

Con esta relación D_g^+ es un conjunto parcialmente ordenado[4] pues se tiene las siguientes propiedades:

En este momento es necesario realizar la demostración de la propiedad cancelativa de la suma, ya que esta es necesaria para la demostración de la antisimetría de $\prec$.

Teorema 1.2.1.6. Propiedad cancelativa de $\oplus$,

Para todo $(a,b),(c,d),(x,y) \in D_g^+$, si $(a,b)\oplus(x,y) = (c,d)\oplus(x,y)$ entonces $(a,b) = (c,d)$

Demostración

Dado que $(a,b)\oplus(x,y) = (c,d)\oplus(x,y)$, entonces por la definición de suma se tiene que

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

Luego, por la igualdad de elementos de D_g^+ se tiene el siguiente par de ecuaciones

$$a + x = c + x$$

$$b + y = d + y$$

Y como a, b, c, d, x e y son números enteros, la propiedad cancelativa de $+$ permite concluir que

$$a = c$$

$$b = d$$

---

[4] Un orden parcial sobre un conjunto $P \neq \emptyset$, es una relación binaria $\leq$ sobre P que es reflexiva, anti simétrica y transitiva, específicamente, para todo $x, y, z \in P$.

1) (reflexiva)

$$x \leq x$$

2) (anti simétrica)

$$x \leq y, \quad y \leq x \implies x = y$$

3) (transitiva)

$$x \leq y, \quad y \leq z \implies x \leq z$$

La pareja $(P, \leq)$ es llamada un conjunto parcialmente ordenado. Roman, S. (2008). *Lattices and Ordered Sets.* New York: Springer. Pág. 2.

Y en consecuencia

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

Teorema 1.3.1.1. Propiedad reflexiva

Para todo $z = (a,b) \in D_g^+, z \preccurlyeq z$

Demostración

Por la definición de elemento idéntico de la suma en D_g^+

$$(a,b) \oplus (0,0) = (a+0, b+0), \quad \text{para todo } (a,b) \in D_g^+$$

Y por la existencia de elemeto neutro en $\mathbb{Z}^+$

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

Por lo tanto, $(a,b) \preccurlyeq (a,b)$

Teorema 1.3.1.2. Propiedad antisimétrica

Para todo $z = (a,b)$, y $w = (c,d) \in D_g^+$,

$$\text{Si } (a,b) \preccurlyeq (c,d) \text{ y } (c,d) \preccurlyeq (a,b) \text{ entonces } (a,b) = (c,d)$$

Demostración

Si $(a,b) \preccurlyeq (c,d) \quad \wedge \quad (c,d) \preccurlyeq (a,b)$ entonces existen $(x,y),(w,z) \in D_g^+$, tal que

$$(a,b) \oplus (x,y) = (c,d) \ (\mathbf{1}) \quad \text{y} \quad (c,d) \oplus (w,z) = (a,b) \ (\mathbf{2})$$

Sustituimos $(\mathbf{1})$en $(\mathbf{2})$

$$[(a,b) \oplus (x,y)] \oplus (w,z) = (a,b)$$

$$(a,b) \oplus [(x,y) \oplus (w,z)] = (a,b) \oplus (0,0), \text{Propiedad asociativa de } \oplus$$

$$(x,y) \oplus (w,z) = (0,0), \text{Propiedad cancelativa de } \oplus$$

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

Luego,

$$x + w = 0 \ \ y \ \ y + z = 0$$

Pero como $x, w \epsilon\ \mathbb{Z}^+$ y $y, z\ \epsilon\ \mathbb{Z}$ entonces las igualdades anteriores solo se cumplen si

$$x = w = 0 \ \ y \ \ y = z = 0$$

O también si

$$x = w = 0 \;\; y \;\; y = -z$$

Sin embargo, esta última opción no es válida ya que $(0, y) \notin D_g^+$, por lo tanto, la opción verdadera es

$$x = w = 0 \wedge y = z = 0$$

Ello permite concluir que

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

Quedando demostrada la antisimetría.

Teorema 1.3.1.3. Propiedad transitiva

Para todo $z = (a, b), w = (c, d), \; v = (e, f) \in D_g^+$,

Si $(a, b) \preccurlyeq (c, d) \quad \wedge \quad (c, d) \preccurlyeq (e, f)$ entonces $(a, b) \preccurlyeq (e, f)$.

Demostración

Si $(a, b) \preccurlyeq (c, d) \quad \wedge \quad (c, d) \preccurlyeq (e, f)$ entonces existen $(g, h), (p, q) \in D_g^+$, tal que

$$(a, b) \oplus (g, h) = (c, d) \qquad y \qquad (c, d) \oplus (p, q) = (e, f)$$

Se sustituye (c, d) por $(a, b) \oplus (g, h)$ en la segunda igualdad por lo que

$$(a, b) \oplus (g, h) \oplus (p, q) = (e, f)$$

Luego,

$$(a, b) \oplus (g + p, h + q) = (e, f)$$

Como $(g + p, h + q) \in D_g^+$ entonces se concluye que

$$(a, b) \preccurlyeq (e, f)$$

Compatibilidad de $\preccurlyeq$ con $\oplus$ y $\otimes$

Teorema 1.3.1.4.

Para cualesquiera números naturales duales $(a, b), (c, d), (x, y) \epsilon D_g^+$, se cumple que si $(a, b) \preccurlyeq (c, d)$ entonces $(a, b) \oplus (x, y) \preccurlyeq (c, d) \oplus (x, y)$.

Demostración

Si $(a,b) \preccurlyeq (c,d)$, significa que existe $(w,z)\epsilon\ D_g^+$ tal que

$$(a,b)\oplus(w,z) = (c,d)$$

Luego,

$$(c,d)\oplus(x,y) = [(a,b)\oplus(w,z)]\oplus(x,y)$$

$$= (a,b)\oplus[(w,z)\oplus(x,y)] \quad \text{Por la asociatividad de } \oplus$$

$$= (a,b)\oplus[(x,y)\oplus(w,z)] \text{ Propiedad conmutativa de } \oplus$$

$$= [(a,b)\oplus(x,y)]\oplus(w,z) \quad \text{Por la asociatividad de } \oplus$$

En consecuencia,

$$(c,d)\oplus(x,y) = [(a,b)\oplus(x,y)]\oplus(w,z) \quad (\mathbf{1})$$

Además, por la relación de orden en D_g^+se tiene

$$(a,b)\oplus(x,y) \preccurlyeq [(a,b)\oplus(x,y)]\oplus(w,z) \quad (\mathbf{2})$$

De $(\mathbf{1})$ y $(\mathbf{2})$ se concluye que

$$(a,b)\oplus(x,y) \preccurlyeq (c,d)\oplus(x,y)$$

Teorema 1.3.1.5.

Dados los números naturales duales $(a,b),(c,d),(x,y)\ \epsilon\ D_g^+$, se cumple que si $(a,b) \preccurlyeq (c,d)$ entonces $(a,b)\otimes(x,y) \preccurlyeq (c,d)\otimes(x,y)$.

Demostración

Si $(a,b) \preccurlyeq (c,d)$, significa que existe $(w,z)\epsilon\ D_g^+$ tal que

$$(a,b)\oplus(w,z) = (c,d)$$

Luego,

$$(c,d)\otimes(x,y) = [(a,b)\oplus(w,z)]\otimes(x,y) \quad (\mathbf{1})$$

$$= [(a,b)\otimes(x,y)]\oplus[(w,z)\otimes(x,y)] \quad \text{Propiedad distributiva de } \otimes \text{ con respecto a } \oplus$$

Por el orden definido en D_g^+ se tiene que

$$(a,b)\otimes(x,y) \preccurlyeq [(a,b)\otimes(x,y)]\oplus[(w,z)\otimes(x,y)]\ (\mathbf{2})$$

Luego, de $(\mathbf{1})$ y $(\mathbf{2})$

$$(a, b) \otimes (x, y) \preccurlyeq (c, d) \otimes (x, y).$$

Teorema 1.3.1.6.

Si $(a, b) \preccurlyeq (c, d)$ entonces $a < c$.

Demostración

Dado que $(a, b) \preccurlyeq (c, d)$, entonces existe $(x, y) \in D_g^+$ tal que

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

Por definición de suma en los naturales gaussianos duales

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

En consecuencia,

$$a + x = c$$

Y como $a, x, c \in \mathbb{Z}^+$, entonces por la relación de orden[5] del conjunto de los enteros positivos $a < c$.

1.4. Divisibilidad en los números Gaussianos Duales

Si $z_1 = (a, b)$, $z_2 = (c, d) \in D_g^+$ con $z_2 \neq (0,0)$, se define la relación de divisibilidad $|$ como sigue:

$$z_1 | z_2 \text{ si y sólo si existe un } y \in D_g^+, \text{tal que } z_2 = z_1 \otimes y$$

Esta relación es un preorden[6] en el conjunto $D_g^+ - \{(0,0)\}$.

---

[5]En el conjunto de los números enteros positivos se define el orden $a \leq b$ si y solo si existe un entero positivo c tal que $a + c = b$. Luque, C., Jiménez, H., & Ángel, J. (2009). *Representar estucturas algebraicas finitas y enumerables.* Bogotá: Javegraf.

[6] Un preorden o cuasiorden sobre un conjunto no vacío P es una relación binaria que es reflexiva y simétrica. Roman, S. (2008). *Lattices and Ordered Sets.* New York: Springer. Pág. 3.

Teorema 1.4.1.1. Propiedad reflexiva

Para todo $z = (a, b) \in D_g^+ - \{(0,0)\}, z|z$

Demostración

Existe (1,0) tal que $(a, b) \otimes (1,0) = (a \cdot 1, b \cdot 1 + a \cdot 0) = (a, b)$, por lo tanto $z|z$.

Teorema 1.4.1.2. Propiedad transitiva

Para $z = (a, b), w = (c, d), \ v = (e, f) \in D_g^+ - \{(0,0)\}$,

$$\text{Si } (a, b)|(c, d) \ \text{ y } \ (c, d)|(e, f) \ \text{ entonces } (a, b)|(e, f)$$

Demostración

Si $(a, b)|(c, d)$ y $(c, d)|(e, f)$ entonces existen $(g, h), (p, q) \in D_g^+$, tal que

$$(a, b) \otimes (g, h) = (c, d) \qquad \text{y} \qquad (c, d) \otimes (p, q) = (e, f)$$

Se sustituye (c, d) por $(a, b) \otimes (g, h)$ en la segunda igualdad por lo que

$$[(a, b) \otimes (g, h)] \otimes (p, q) = (e, f)$$

$$(a, b) \otimes [(g, h) \otimes (p, q)] = (e, f)$$

Luego,

$$(a, b) \otimes (g \cdot p, h \cdot p + g \cdot q) = (e, f)$$

Por lo tanto, existe $(g \cdot p, h \cdot p + g \cdot q) \in D_g^+ - \{(0,0)\}$, lo que permite concluir que:

$$(a, b)|(e, f)$$

A continuación, se define otra relación sobre el conjunto $D_g^+ \times D_g^+$:

$$(a, b) \sim (c, d) \text{ si y solo si } (a, b)|(c, d) \text{ y } (c, d)|(a, b) \text{ , con } (a, b), (c, d) \in D_g^+$$

Si $(a, b) \sim (c, d)$ diremos que (a, b) y (c, d) son **asociados.**

La relación $\sim$ es una relación de equivalencia:

Teorema 1.4.1.3. *(Reflexibilidad)*

$(a,b) \sim (a,b)$ Para todas las $(a,b) \in D_g^+$

Demostración

$(a,b) \sim (a,b)$ Puesto que $(a,b)|(a,b)$ porque existe $(1,0)$ tal que $(a,b) \otimes (1,0) = (a.b)$.

Teorema 1.4.1.4. *(Simetría)*

Si $(a,b) \sim (c,d)$ entonces $(c,d) \sim (a,b)$

Demostración

Como $(a,b) \sim (c,d)$, $(a,b)|(c,d)$ y $(c,d)|(a,b)$ de ahí que

$(c,d)|(a,b)$ y $(a,b)|(c,d)$ y, por tanto $(c,d)|(a,b)$.

Teorema 1.4.1.5. *(Transitividad)*

Si $(a,b) \sim (c,d)$ y $(c,d) \sim (e,f)$, entonces $(a,b) \sim (e,f)$.

Demostración

Si $(a,b) \sim (c,d)$ y $(c,d) \sim (e,f)$, entonces $(a,b)|(c,d)$ y $(c,d)|(e,f)$. Además de la misma definición de $\sim$ se tiene que $(c,d)|(a,b), (e,f)|(c,d)$. Luego por la propiedad transitiva de la relación de divisibilidad, se tiene que:

$$(a,b)|(e,f) \text{ y } (e,f)|(a,b)$$

En consecuencia $(a,b) \sim (e,f)$.

1.4.2. Algunos teoremas de la divisibilidad en los duales

Teorema 1.4.2.1.

Para todo número natural gaussiano dual z diferente de $(0,0)$, $z|(0,0)$

Demostración

Supóngase que para algún $(c,d) \in D_g^+$ se cumple que

$$(a,b) \otimes (c,d) = (0,0)$$

Por definición de multiplicación

$$(ac, ad + bc) = (0,0)$$

Luego,

$$ac = 0 \quad \text{y} \quad ad + bc = 0$$

Y como $b \neq 0$, entonces

$$c = 0$$

Sustituyendo en $ad + bc = 0$ se tiene que,

$$ad = 0$$

Finalmente, como $a \neq 0$,

$$d = 0.$$

Por lo tanto, existe $(0,0) \in D_g^+$ tal que

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

Y por definición de divisibilidad

$$(a,b)|(0,0)$$

Para todo $z = (a,b) \in D_g^+$.

Teorema 1.4.2.2.

Sean $(a,b), (c,d), (e,f) \in D_g^+$, si $(a,b)|(c,d)$ y $(a,b)|(e,f)$ entonces $(a,b)|[(c,d) \otimes (x,y) \oplus (e,f) \otimes (w,v)]$ donde (x,y) y (w,v) son números naturales gaussianos duales.

Demostración

Como $(a,b)|(c,d)$ y $(a,b)|(e,f)$, entonces por definición de $|$ existen (c',d') y (e',f') tal que

$$(a,b) \otimes (c',d') = (c,d)$$

$$(a,b) \otimes (e',f') = (e,f)$$

Por la compatibilidad del orden dual con la multiplicación de los números naturales gaussianos duales, multiplicamos las igualdades anteriores por (x, y) y (w, v) respectivamente

$$(a, b) \otimes [(c', d') \otimes (x, y)] = (c, d) \otimes (x, y) \ \ (\mathbf{3})$$
$$(a, b) \otimes [(e', f') \otimes (w, v)] = (e, f) \otimes (w, v) \ \ (\mathbf{4})$$

En consecuencia $(a, b)|(c, d) \otimes (x, y)$ y $(a, b)|(e, f) \otimes (w, v)$

Luego, la suma

$$(c, d) \otimes (x, y) \oplus (e, f) \otimes (w, v)$$

Es igual a

$$= \langle (a, b) \otimes [(c', d') \otimes (x, y)] \rangle \oplus \langle (a, b) \otimes [(e', f') \otimes (w, v)] \ \rangle$$

Y por la propiedad distributiva lo anterior se convierte en

$$= (a, b) \otimes \langle [(c', d') \otimes (x, y)] \oplus [(e', f') \otimes (w, v)] \rangle$$

Entonces

$$(a, b)|[(c, d) \otimes (x, y) \oplus (e, f) \otimes (w, v)]$$

Teorema 1.4.2.3.

Sean $(a, b), (c, d), (e, f) \in D_g^+$, si $(a, b)|(c, d)$ y $(a, b)|(c, d) \oplus (e, f)$ entonces $(a, b)|(e, f)$

Demostración

$(a, b)|(c, d)$ Implica que existe (x, y) tal que

$$(a, b) \otimes (x, y) = (c, d) \ (\mathbf{1})$$

Además como $(a, b)|(c, d) \oplus (e, f)$, se tiene que

$$(a, b) \otimes (s, t) = (c, d) \oplus (e, f) \ \ (\mathbf{2}), \qquad \text{para algún } (s, t) \in D_g^+$$

Sustituyendo $(\mathbf{1})$ en $(\mathbf{2})$

$$(a, b) \otimes (s, t) = [(a, b) \otimes (x, y)] \oplus (e, f)$$

Desarrollando los productos y la suma,

$$(as, bs + at) = (ax + e, bx + ay + f)$$

Igualando,

$$as = ax + e$$

$$bs + at = bx + ay + f$$

Como todos los números anteriores son enteros se tiene que:

$$as - ax = a(s - x) = e \quad (\mathbf{3})$$

$$bs - bx + at - ay = b(s - x) + a(t - y) = f \quad (\mathbf{4})$$

De $(\mathbf{3})$ y $(\mathbf{4})$**,** se tiene que existe $(\ s - x, t - y)$ tal que

$$(a, b) \otimes (\ s - x, t - y) = (e, f)$$

Y en conclusión $(a, b)|(e, f)$.

Teorema 1.4.2.4.

Si $(a, b)|(c, d)$ entonces $(a, b)\otimes(x, y)|(c, d)\otimes(x, y)$ para cualquier $(x, y) \neq (0,0)$ arbitrario, que pertenezca a los números naturales gaussianos duales.

Demostración

Por la definición de | se tiene de $(a, b)|(c, d)$, que existe $(s, t) \in D_g^+$ tal que

$$(a, b)\otimes(s, t) = (c, d)$$

Por la compatibilidad del orden dual con la multiplicación de los duales se obtiene

$$(a, b)\otimes[(s, t)\otimes(x, y)] = (c, d)\otimes(x, y)$$

Y por lo tanto

$$(a, b)\otimes(x, y)|(c, d)\otimes(x, y)$$

Teorema 1.4.2.5.

Para todo número natural gaussiano dual z, $(1,0)|z$

Demostración

Si $z = (a, b)$, entonces por definición de elemento idéntico para la multiplicación se obtiene

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

En conclusión

$$(1,0)|(a, b) = z.$$

Teorema 1.4.2.6.

Si $(a, b)|(x, y)$ en D_g^+ entonces $a|x$ en $\mathbb{Z}$

Demostración

Como $(a, b)|(x, y)$, por definición de la relación de divisibilidad en D_g^+ existe (c, d)tal que

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

Luego,

$$(a, b)\otimes(c, d) = (ac, bc + ad) = (x, y)$$

Por lo tanto,

$$ac = x$$

Y por definición de divisibilidad en $\mathbb{Z}$

$$a|x.$$

Teorema 1.4.2.7.

Para todo $(a, b) \in D_g^+$ con $a = 2k, k \in \mathbb{Z}^+$, se cumple una de las siguientes relaciones: $(2,0)|(a, b)$ ó $(2,1)|(a, b)$.

Demostración

Como $(a, b) = (2k, b)$, se tiene que la primera componente es par, luego b tiene dos opciones o es par o es impar en $\mathbb{Z}$.

Si b es par:

$$(a, b) = (2k, 2t), \qquad t \in \mathbb{Z}^+$$

Y por lo tanto, se puede reescribir el segundo término de la igualdad como

$$(2k, 2t) = (2k, 2t + 0k)$$

Luego, por definición de multiplicación,

$$(2k, 2t) = (2,0) \otimes (k, t)$$

Y en conclusión $(2,0)|(a, b)$, sin embargo b no puede ser impar en $\mathbb{Z}$, pues si se supone que es impar, se tiene que $b = 2t + 1$, $t \in \mathbb{Z}^+$, en consecuencia:

$$(a, b) = (2k, 2t + 1) \ \ (\mathbf{1}), \qquad t \in \mathbb{Z}^+$$

Y como,

$$(2,0) \otimes (x, y) = (2x, 2y) \ (\mathbf{2}), \text{para todo } (x, y) \in D_g^+$$

Entonces de $(\mathbf{1})$ y $(\mathbf{2})$ se establece la siguiente ecuación: $2t + 1 = 2y$, pero esta no tiene solución para $t, y \in \mathbb{Z}^+$. En conclusión b debe ser par.

Ahora, si b es impar, existe $(k, y) \in D_g^+$ tal que

$$(2,1) \otimes (k, y) = (2k, k + 2y)$$

Y la ecuación $2t + 1 = k + 2y$ tiene solución en los enteros positivos siempre y cuando k sea un número impar.

1.4.3. Definición de un número primo

Si $p = (a, b) \in D_g^+$, $a > 1$, se dice que p es un numero primo natural gaussiano dual, si y sólo si sus únicos divisores son $(a, ak + b)$ y $(1, e)$ con $k, e \in \mathbb{Z}^+$. Es decir, un numero p es primo si sus divisores son sus asociados y los asociados al (1,0).

Diremos que p es un número compuesto, si $p \succ (1,0)$ y p no es primo.

Teorema 1.4.3.1.

Si $z = (p, f) \in D_g^+$, donde p es un entero primo, entonces z es un entero primo en D_g^+

Demostración

Si $z = (p, f) \in D_g^+$ no es primo entonces existe $(a, b), (c, d) \in D_g^+$ tal que

$$(a,b)\otimes(c,d) = (p,f)$$

Con $a \neq 1, a \neq p, c \neq 1$ y $c \neq p$, por tanto

$$(ac, ad + bc) = (p,f)$$

Luego $ac = p$ y $ad + bc = f$, pero p es un número primo en $\mathbb{Z}^+$, y no admite una factorización diferente a $p = p \cdot 1$, en consecuencia $a = 1$ y $c = p$ o $a = p$ y $c = 1$, lo que es una contradicción y en conclusión $z = (p,f)$ es primo.

Teorema 1.4.3.2.

Si $z = (p^k, f) \in D_g^+$, donde p es un entero primo no par, $k \in \mathbb{N}$, $k > 1, p \nmid f$ entonces z es un entero primo en D_g^+.

Demostración

Si $z = (p^k, f) \in D_g^+$ no es un número primo natural gaussiano dual, entonces existen $(a,b),(c,d) \in D_g^+$ tal que

$$(a,b)\otimes(c,d) = (p^k, f)$$

Luego,

$$(ac, ad + bc) = (p^k, f)$$

De ahí se tiene que

$$ac = p^k,$$

Lo que implica que

$$a = p^h \quad \text{y} \quad c = p^i,$$

Por lo tanto,

$$ac = p^h p^i = p^{h+i} = p^k$$

Además $ad + bc = f$, sustituyendo la información anterior en esta nueva igualdad,

$$ad + bc = p^h d + b p^i = f$$

De modo que $p|p^h$ y $p|p^i$ luego $p|p^h d + b p^i = f$, lo que es una contradicción, en conclusión $z = (p^k, f)$ es un número primo.

1.4.4. Máximo común divisor en $\mathbf{D}_g^+$

Si un número natural guassiano dual (g, h) divide a dos números $(a, b), (c, d) \in D_g^+$, entonces (g, h) se llama divisor común de (a, b) y (c, d), Así pues, (1,0) es un divisor común de todo par de números naturales gaussianos duales. A continuación se presenta una definición de máximo común divisor para D_g^+.

Teorema 1.4.4.1.

Dados $(a, b), (c, d) \in D_g^+$, existe un único (g, h) tal que:

I. (g, h) es un gaussiano natural dual con $0 \leq h < g$

II. $(g, h)|(a, b) \;\wedge\; (g, h)|(c, d)$ $\big((g, h)$ es un divisor común de (a, b) y $(c, d)\big)$

III. Si $(k, m)|(a, b) \;\wedge\; (k, m)|(c, d)$ y $0 \leq m < k$, entonces $(k, m)|(g, h)$

Demostración

$$S = \{(x, y) \succ (0,0): (x, y) \text{ es un divisor común de } (a, b), (c, d) \in D_g^+ \}$$

Por el teorema ***1.4.2.5.*** existe por lo menos un elemento de D_g^+ que es divisor común de $(a, b), (c, d) \in D_g^+$. Por lo tanto $S \neq \emptyset$.

Caso i.

Primero se supone que el máximo común divisor de $(a, c) = 1$ en $\mathbb{Z}$.

Luego, si $(x, y) \in S$ entonces

$$(x, y)|(a, b) \quad \text{y} \quad (x, y)|(c, d)$$

Del teorema ***1.4.2.6.*** se tiene que

$$x|a \quad \text{y} \quad x|c$$

Pero como estos dos números son primos relativos en $\mathbb{Z}$ se concluye que $x = 1$.

Por lo tanto, se obtiene que

$$S = \{(1, y): y \in \mathbb{Z}\}$$

Y el único elemento de este conjunto que cumple *I.* es (1,0). Además cumple *II.* por el teorema ***1.4.2.5.*** y la demostración de que (1,0) cumple *III.* es inmediata pues todos los divisores comunes de S son asociados a (1,0).

En otras palabras para este caso, existe (1,0) tal que cumple *I. II. y III.*

Caso ii.
Como segundo, se supone que el máximo común divisor de $(a, c) = k$ en $\mathbb{Z}$.
Luego, si $(x, y) \in S$ entonces

$$(x, y)|(a, b) \quad \text{y} \quad (x, y)|(c, d)$$

Del teorema ***1.4.2.6.*** se tiene que

$$x|a \quad \text{y} \quad x|c$$

Por lo tanto, por la definición de máximo común divisor en $\mathbb{Z}$, x divide a k en los números enteros. En otros términos

$$k = xt \ , t \in \mathbb{Z}^+$$

Y como $x \in \mathbb{Z}^+$, x se puede escribir como $\frac{k}{t}$, con $t < k < a$ y $t < k < c$
Luego,

$$S = \left\{ \left(\frac{k}{t}, y\right) \succ (0,0) : \left(\frac{k}{t}, y\right) \text{ es un divisor común de } (a, b), (c, d) \in D_g^+ \right\}$$

Es un conjunto de divisores comunes de (a, b) y (c, d) en D_g^+, en el cuál por cada t que divida a k solo se eligen los elementos $\left(\frac{k}{t}, y\right)$ tal que $y < \frac{k}{t}$ de ahí que existen elementos de S que cumplen *I.* y *II.* e inmediatamente cumplen *III.* ya que los demás elementos de S son asociados a los elementos escogidos.

Definición.
El número (g, h) del teorema ***1.4.4.1.*** *se llama máximo común divisor*[7] de (a, b) y (c, d) y se nota como $\boldsymbol{mcd}\ \{(a, b), (c, d)\}$.

Teorema 1.4.4.2.

El *máximo común divisor* de dos números naturales gaussianos duales es único

Demostración

Supongamos $g = \boldsymbol{mcd}\ \{(a, b), (c, d)\}$ y $g' = \boldsymbol{mcd}\ \{(a, b), (c, d)\}$

Entonces por definición de máximo común divisor parte III, se tiene que

$$g|g' \quad \wedge \quad g'|g$$

---

[7] Algunas definiciones como la de primo y máximo común divisor, así como sus respectivos teoremas son idea original de la tesis titulada "Estudio de congruencias en números naturales Duales" escrita por Diana Brausin y Ana Peréz, egresadas de la licenciatura en matemáticas de la Universidad Pedagógica Nacional de Colombia.

Por lo tanto $g \sim g'$. Ahora, si $g' = (x_1, y_1)$, y $g = (x_2, y_2)$, por la definición de la relación$\sim$, $(x_1, y_1)|(x_2, y_2)$ y $(x_2, y_2)|(x_1, y_1)$, Luego por el teorema ***1.4.2.6,*** $x_1|x_2$ y $x_2|x_1$ en los enteros, de ahí que $x_1 = x_2$. Además, $0 \leq y_1 < x_1$, y , $0 \leq y_2 < x_2 = x_1$ entonces $y_1 = y_2$, esto permite concluir que $g = g'$.

Definición de primos relativos

Cuando el ***mcd***{(*a, b*), (*c, d*)}= (1, 0) diremos que (*a, b*) y (*c, d*) son ***primos relativos.***

Teorema 1.4.4.3. Algoritmo de la división

Dados dos números naturales gaussianos duales $z = (z_1, z_2) \succ (0,0)$, $w = (w_1, w_2) \succ (0,0)$, $(z_1, z_2) \succcurlyeq (w_1, w_2)$ existe un único par de números duales $q = (q_1, q_2) \in D_g^+$ y $r = (r_1, r_2) \in D_g^+ \cup \{(0, y): y \in \mathbb{Z}\}$ tales que

$$(z_1, z_2) = (w_1, w_2)(q_1, q_2) \oplus (r_1, r_2)\text{, con } 0 \leq r_1 < w_1 \quad y \quad 0 \leq r_2 < w_1$$

Además, $(r_1, r_2) = (0,0)$ si, y sólo si $w|z$

Demostración:

Sea el conjunto S de números naturales duales dado por

$$S = \{(x, y) \succcurlyeq (0,0): (x, y) = (z_1 - w_1 d_1, z_2 - w_2 d_1 - w_1 d_2)\ ;\ (d_1, d_2) \in D_g^+\}$$

Es un conjunto no vacío de números naturales duales puesto que la primera componente es positiva en $\mathbb{Z}$, $z_1 - w_1 * d_2 > 0$, por lo tanto estas primeras componentes admiten un mínimo, que designaremos $r_1 = z_1 - w_1 q_1$. Sea $(r_1, r_2) = (z_1 - w_1 q_1, z_2 - w_2 q_1 - w_1 q_2)$, con $q_2 \in \mathbb{Z}$. De ahí que $r_1 = z_1 - w_1 q_1$ y $r_2 = z_2 - w_2 q_1 - w_1 q_2$, en consecuencia $z_1 = r_1 + w_1 q_1$ y $z_2 = r_2 + w_2 q_1 + w_1 q_2$ Luego $(z_1, z_2) = (r_1 + w_1 q_1,\ r_2 + w_2 q_1 + w_1 q_2)$ que se puede reescribir en términos de las operaciones duales como sigue $(z_1, z_2) = (r_1, r_2) \oplus (w_1, w_2) \otimes (q_1, q_2)$ y finalmente por la conmutativa de $\oplus$ se tiene que $(z_1, z_2) = (w_1, w_2) \otimes (q_1, q_2) \oplus (r_1, r_2), r_1 \geq 0$. Ahora se muestra que $r_1 < w1$; Supóngase que $r_1 \geq w_1$. Entonces $0 \leq r_1 - w_1 < r_1$. Pero $x = r_1 - w_1 \in S$ ya que $r_1 - w_1 = z_1 - w_1(q_1 + 1)$. Por lo tanto $r_1 - w_1$ es la primera componente de un elemento de S menor que su elemento mínimo r_1. Esto es una contradicción, por lo tanto $r_1 < w1$. Ahora para mostrar la existencia, falta verificar que $0 \leq r_2 < w_1$ pero por lo anterior $r_2 = z_2 - w_2 d_1 - w_1 d_2$, y es posible que este número no sea positivo en $\mathbb{Z}$, pero podemos asociar al par (r_1, r_2) un número (r_1, s_1) a partir de $\sim$ de tal modo que

$$(r_1, r_2) \sim (r_1, r_1 k - r_2)$$

Con $r_1 > s_1 = r_1 * k - r_2 \geq 0$ para algún $k \in \mathbb{Z}^+$, de modo que ya tenemos un asociado que cumple el Algoritmo de la división pues $w_1 \geq r_1 > s_1 \geq 0$.

A continuación, demostraremos su unicidad, supóngase que existen $p = (p_1, p_2)$ y o $= (o_1, o_2)$, tal que

$$(z_1, z_2) = (w_1, w_2) \otimes (p_1, p_2) \oplus (o_1, o_2)$$

Por lo tanto, tenemos que

$$(w_1, w_2) \otimes (p_1, p_2) + (o_1, o_2) = (z_1, z_2) = (w_1, w_2) \otimes (q_1, q_2) + (r_1, r_2)$$

Que es equivalente a:

$$(w_1 * p_1 + o_1, w_2 * p_1 + w_1\, p_2 + \ o_2) = (w_1 * q_1 + r_1, w_2 * q_1 + w_1\, q_2 + \ r_2)$$

Para que sean iguales se compara componente a componente

$$w_1 p_1 + o_1 = w_1 q_1 + r_1 = z_1 \quad (\mathbf{1})$$

$$w_2 p_1 + w_1\, p_2 + \ o_2 = w_2 q_1 + w_1\, q_2 + \ r_2 = z_2 \qquad (\mathbf{2})$$

De $(\mathbf{1})$ tenemos que $w_1(p_1 - q_1) = r_1 - o_1$, luego $w_1 | (r_1 - o_1)$ en $\mathbb{Z}$. Si $r_1 - o_1 \neq 0$ implica que $w_1 \leq |r_1 - o_1|$, que es una contradicción. Por lo tanto, $r_1 = o_1$ y $p_1 = q_1$. Ahora utilizando esa información en $(\mathbf{2})$ $w_2 p_1 + w_1\, p_2 + \ o_2 = w_2 q_1 + w_1\, q_2 + r_2$tenemos

$$w_1\, p_2 + \ o_2 = w_1\, q_2 + \ r_2$$

Y utilizando un razonamiento análogo al anterior deducimos que, $r_2 = o_2$ y $p_2 = q_2$, quedando demostrando la unicidad y en general el algoritmo de la división para los números naturales Gaussianos Duales.

Teorema 1.4.4.4.. Algoritmo de Euclides

Sean $z = (z_1, z_2) \succcurlyeq (0{,}0)$, $w = (w_1, w_2) \succ (0{,}0) \in D_g^+$ tal que $z_2, w_2 \geq 0$, donde $z_2 < z_1$ y $w_2 < w_1$. Y aplicando el algoritmo de la división repetidamente para los números naturales Gaussianos Duales, se obtienen los siguientes resultados:

$$(z_1, z_2) = (w_1, w_2)(p_1, q_1) \oplus (r_1, s_1), \quad 0 \leq r_1 < w_1 \quad y \quad 0 \leq s_1 < w_1$$

$$(w_1, w_2) = (r_1, s_1)(p_2, q_2) \oplus (r_2, s_2), \quad 0 \leq r_2 < r_1 \quad y \quad 0 \leq s_2 < r_1$$

.

.

.

$$(r_{n-1}, s_{n-1}) = (r_n, s_n)(p_{n+1}, q_{n+1})$$

Entonces el número natural gaussiano dual (g, h) asociado con (r_n, s_n), con $0 \leq h < g$, es el máximo común divisor del par de números z, w, en el caso en que $r_n = 0$ se dice que los números z, w son primos relativos en D_g^+.

Demostración

La sucesión de números $r_1, r_2, \ \ldots \ , r_n$ es una secuencia decreciente de enteros no negativos, además existe un número finito de enteros menores que w_1 y mayores que 0, por lo tanto el proceso debe ser finito y en algún momento debe terminar.

De la última igualdad se tiene que

$$(r_n, s_n)|(r_{n-1}, s_{n-1})$$

Se sustituye (r_{n-1}, s_{n-1}) en la penúltima igualdad

$$(r_{n-2}, s_{n-2}) = (r_n, s_n)\otimes(p_{n+1}, q_{n+1})\otimes(p_n, q_n)\oplus(r_n, s_n)$$

$$(r_{n-2}, s_{n-2}) = (r_n, s_n)[(p_{n+1}, q_{n+1})\otimes(p_n, q_n)\oplus(1,0)]$$

Luego,

$$(r_n, s_n)|(r_{n-2}, s_{n-2})$$

Se aplica de nuevo una sustitución, (r_{n-1}, s_{n-1}) y (r_{n-2}, s_{n-2}) en la penúltima ecuación, y se obtiene que

$$(r_n, s_n)|(r_{n-3}, s_{n-3})$$

Y si se aplica un procedimiento análogo al anterior varias veces, se consigue que

$$(r_n, s_n)|(w_1, w_2) \text{ y } (r_n, s_n)|(z_1, z_2)$$

Ahora, se supone que existe $(x, y) \in D_g^+$ tal que $(x, y)|(w_1, w_2)$ y $(x, y)|(z_1, z_2)$.

Como

$$(z_1, z_2) = (w_1, w_2)\otimes(p_1, q_1)\oplus(r_1, s_1)$$

Entonces

$$(x,y)|(r_1,s_1) \ \ \wedge \ \ (x,y)|(w_1,w_2)(p_1,q_1)$$

Además

$$(w_1,w_2) = (r_1,s_1)\otimes(p_2,q_2)\oplus(r_2,s_2)$$

Luego

$$(x,y)|(r_2,s_2) \ \ \wedge \ \ (x,y)|(r_1,s_1)(p_2,q_2)$$

Y continuando con el procedimiento se llega a

$$(x,y)|(r_n,s_n)$$

Por lo tanto, (r_n,s_n) cumple las condiciones II y III de máximo común divisor.

Finalmente, a partir de la relación $\sim$ es posible encontrar un número natural gaussiano dual (g,h) tal que (g,h) es un asociado de (r_n,s_n) con $0 \leq h < g$ y por la definición de máximo común divisor en los naturales gaussianos duales el

$$\mathbf{mcd}\{(z_1,z_2),(w_1,w_2)\} = (g,h)\ .$$

CAPITULO 2

EL CONJUNTO DE LOS NÚMEROS G-NATURALES

2.1. Clases generadas en $\frac{D_g^+}{\sim}$

Las clases de equivalencia que se generan con la relación $\sim$ sobre el conjunto D_g^+ son:

$$\langle z\rangle = \{y \in D_g^+ - \{(0,0)\}: z\sim y\}$$

Veamos a continuación algunos ejemplos de las clases de equivalencia que se forman:

$$\langle(1,0)\rangle = \{(1,-2),(1,-1),(1,1),(1,2),\dots\} = \{(1,k): k \in \mathbb{Z}\}$$

$$\langle(2,0)\rangle = \{(2,2),(2,4),(2,6),(2,8),\dots\} = \{(2,2k): k \in \mathbb{Z}\}$$

$$\langle(2,1)\rangle = \{(2,-3),(2,-1),(2,3),(2,5),\dots\} = \{(2,2k+1): k \in \mathbb{Z}\}$$

$$\langle(3,0)\rangle = \{(3,-3),(3,3),(3,6),(3,9),\dots\} = \{(3,3k): k \in \mathbb{Z}\}$$

$$\langle(3,1)\rangle = \{(3,-2),(3,4),(3,7),(3,10),\dots\} = \{(3,3k+1): k \in \mathbb{Z}\}$$

$$\langle(3,2)\rangle = \{(3,-1),(3,5),(3,8),(3,11),\dots\} = \{(3,3k+2): k \in \mathbb{Z}\}$$

En general

$$\langle(a,b)\rangle = \left\{(a,ak+b) \in D_g^+: k \in \mathbb{Z}\right\}$$

Además se define

$$\langle(0,0)\rangle = \{(0,0)\}.$$

Y

$$\langle(0,0)\rangle = \{(0,y): y \in \mathbb{Z}\}$$

Estas dos últimas clases se traen a colación, por su participación en algunos teoremas claves en el desarrollo de algunos contenidos.

Gráficamente, los elementos de cada clase se representan por un mismo color:

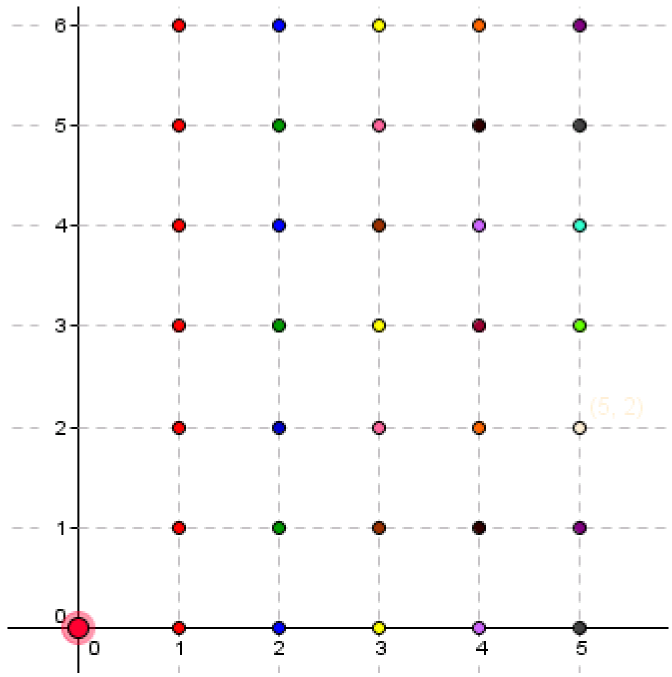


Figura 2

Se observa que cuando la primera componente de un número natural gaussiano dual es 2, se obtienen dos clases de equivalencia, cuando la primera componente es 3, se obtienen tres clases de equivalencia y en general cuando la primera componente es a, se obtienen a clases de equivalencia, resultado sencillo pero muy importante para futuras definiciones.

Además, por cada clase de equivalencia, se sabe que se puede elegir como representante cualquier elemento del conjunto de la clase. Sin embargo, por conveniencia solo se trabaja con los representantes de la forma:

$$\langle (a,b) \rangle, \text{con } a \in \mathbb{Z}^{+} \text{ y } 0 \leq b < a$$

A menos que se indique lo contrario.

Sea $\frac{D_g^+}{\sim}$ el conjunto cociente. Se define

$$H = \frac{D_g^+}{\sim} = \{\langle (a,b) \rangle \colon\ (a,b) \in D_g^+ \ \wedge\ 0 \leq b < a\} \cup \{(0,0)\}$$

Como la unión del conjunto cociente, con el conjunto con único elemento (0,0).

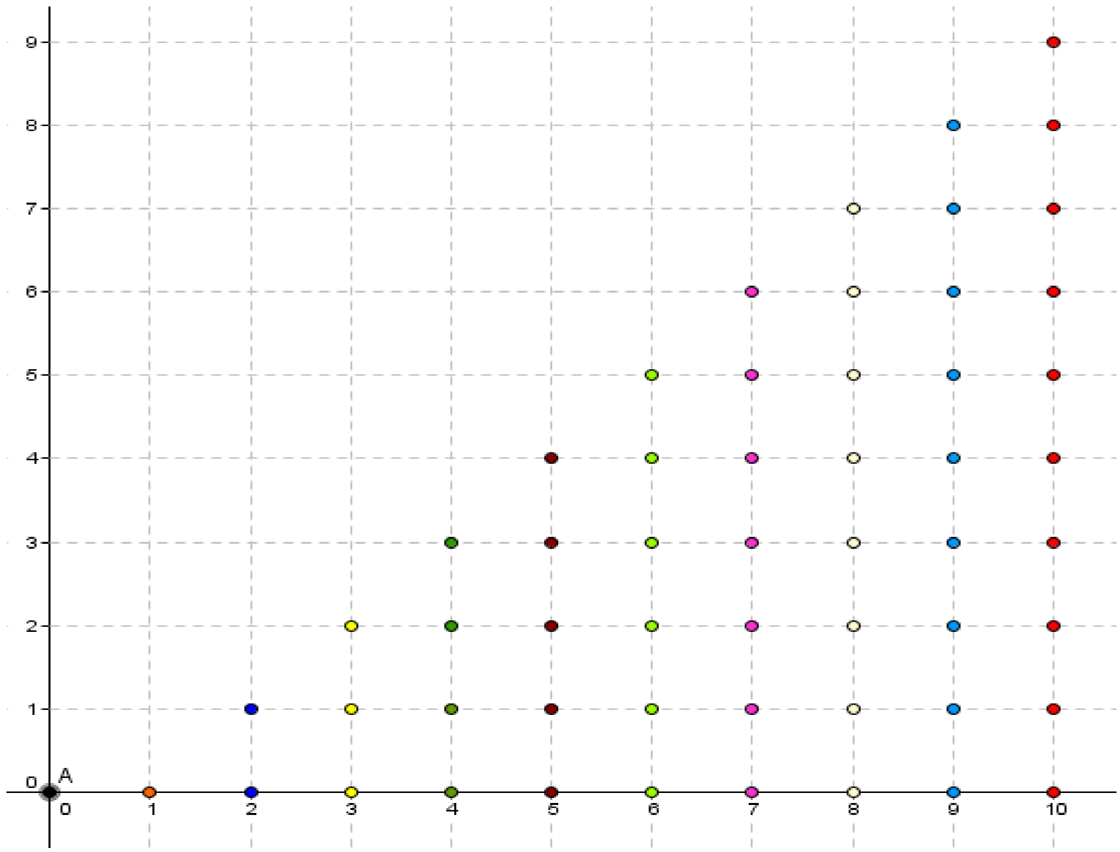


Figura 3. Algunos elementos del conjunto *H* pintados por fibras[8] (es decir los que tengan igual la primera componente)

Este nuevo conjunto se denominará el conjunto de los números G-naturales y en él se define las siguientes relaciones:

Si $z_1 = (a, b),\ z_2 = (c, d)$, entonces

$$\langle z_1 \rangle \oplus \langle z_2 \rangle = \langle a + c, b + d \rangle$$

$$\langle z_1 \rangle \odot \langle z_2 \rangle = \langle ac, ad + bc \rangle$$

Cabe anotar que las clases de equivalencia que se generan no son independientes del representante para la suma. Es decir, no siempre se cumple que si $\langle z_1 \rangle =$

[8] Se define fibra, como el conjunto de elementos de D_g^+ que tienen igual la primera componente, en otros términos una fibra f de componente a es el conjunto definido como sigue:

$$f(a) = \{(x, y) \in D_g^+ : x = a\}$$

$\langle z_2 \rangle$ y $\langle z_3 \rangle = \langle z_4 \rangle$ entonces $\langle z_1 \rangle \oplus \langle z_3 \rangle = \langle z_2 \rangle \oplus \langle z_4 \rangle$:

Por ejemplo:

$$\langle (3,2) \rangle = \langle (3,5) \rangle \quad \text{y} \quad \langle (4,1) \rangle = \langle (4,13) \rangle$$

Luego,

$$\langle (3,2) \rangle \oplus \langle (4,1) \rangle = \langle (7,3) \rangle$$

$$\langle (3,5) \rangle \oplus \langle (4,13) \rangle = \langle (7,18) \rangle$$

$$\text{y} \quad \langle (7,3) \rangle \neq \langle (7,18) \rangle$$

Y al igual que en la suma, en la multiplicación las clases de equivalencia tampoco son independientes del representante, pues

$$\langle (3,2) \rangle = \langle (3,5) \rangle \quad \text{y} \quad \langle (4,1) \rangle = \langle (4,13) \rangle$$

Luego,

$$\langle (3,2) \rangle \otimes \langle (4,1) \rangle = \langle (12,11) \rangle$$

$$\langle (3,5) \rangle \otimes \langle (4,13) \rangle = \langle (12,69) \rangle$$

$$\text{y} \quad \langle (12,11) \rangle \neq \langle (12,69) \rangle$$

Pero esta no independencia, no impide desarrollar la teoría de números para este nuevo conjunto, ya que la condición impuesta a los representantes de las clases en H evita que aparezcan elementos como $\langle (4,13) \rangle$ pues para que sean elementos de H, la primera componente debe ser mayor que la segunda y la clase anterior no lo cumple, en consecuencia $\langle (4,13) \rangle \in H$.

2.2. Estructura algebraica del conjunto de los números G-naturales duales

Ahora se observa que la estructura algebraica de la tripla $(H, \oplus, \otimes)$, es también un semianillo abeliano cancelativo pues:

$(H, \oplus)$ Es un semigrupo abeliano cancelativo.

$(H, \otimes)$ Es un semigrupo abeliano.

$\otimes$ Distribuye con respecto a $\oplus$ en H.

La prueba de que $\oplus$ y $\otimes$ cumplen sus respectivas propiedades es una variación en las demostraciones que se hacen para D_g^+.

El elemento neutro de H para la suma es el elemento $\langle(0,0)\rangle$ y para la multiplicación es la clase del elemento (1,0).

2.3. Orden en los Números G-Naturales Duales

Un número G-natural dual $\langle(a,b)\rangle$ es menor o igual a otro $\langle(c,d)\rangle$ si existe un número natural gaussiano dual $(x,y) \in D_g^+$ tal que

$$\langle(a,b)\rangle \oplus \langle(x,y)\rangle = \langle(c,d)\rangle$$

En cuyo caso se sigue escribiendo que $\langle(a,b)\rangle \ll= \langle(c,d)\rangle$.

Si $\langle(a,b)\rangle = \langle(c,d)\rangle$ entonces $a = c$ y $b = d$.

Además, $\langle(a,b)\rangle \ll \langle(c,d)\rangle$ si y sólo si $\langle(x,y)\rangle \neq (0,0)$.

Con esta relación de orden H es un conjunto parcialmente ordenado pues la relación de orden $\ll$ es reflexiva, anti simétrica y transitiva, pero no es total pues dos elementos que tengan su primera componente igual no son comparables.

Sin embargo, a continuación se establece un orden lexicográfico:

$\langle(a,b)\rangle \ll \langle(c,d)\rangle$ Si existe $(x,y) \in D_g^+$ tal que

$\langle(a,b)\rangle \oplus \langle(x,y)\rangle = \langle(c,d)\rangle$, esto si $a \neq c$

Para el caso en que $a = c$ tenemos que:

$$\langle(a,b)\rangle \ll \langle(c,d)\rangle \text{ si } b < d$$

Este orden es total ya que esta última condición permite comparar todos los elementos de H y sigue siendo compatible con las operaciones $\oplus$ y $\otimes$ que se definieron en el conjunto de los números G-naturales.

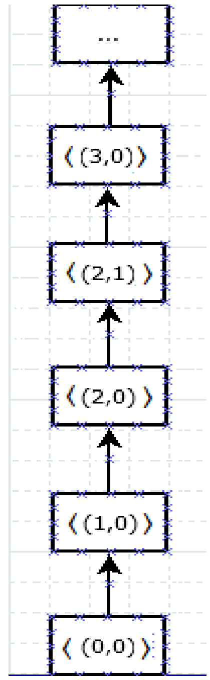


Figura 4. Diagrama de Hasse para $(H,\ll)$.

Teorema 2.3.1.1. Propiedad reflexiva

Para todo $\langle(a,b)\rangle \in H, \langle(a,b)\rangle \ll= \langle(a,b)\rangle$

Demostración

Existe $\langle(0,0)\rangle \in H$ tal que

$\langle(a,b)\rangle \oplus \langle(a,b)\rangle = \langle(a+0,b+0)\rangle = \langle(a,b)\rangle$Por la existencia de elemeto neutro en H

Luego, $\langle(a,b)\rangle \ll= \langle(a,b)\rangle$

Teorema 2.3.1.2. Propiedad antisimétrica

Sean $\langle(a,b)\rangle$, y $\langle(c,d)\rangle \in H$,

Si $\langle(a,b)\rangle \ll= \langle(c,d)\rangle \;\;\wedge\;\; \langle(c,d)\rangle \ll= \langle(a,b)\rangle$ entonces $\langle(a,b)\rangle = \langle(c,d)\rangle$

Demostración

Caso 1. $a \neq c$

Si $\langle(a,b)\rangle \ll= \langle(c,d)\rangle \;\;\wedge\;\; \langle(c,d)\rangle \ll= \langle(a,b)\rangle$ entonces existen $(x,y),(w,z) \in D_g^+$, tal que

$$\langle(a,b)\rangle \oplus \langle(x,y)\rangle = \langle(c,d)\rangle \ \ (\mathbf{1}) \quad \wedge \quad \langle(c,d)\rangle \oplus \langle(w,z)\rangle = \langle(a,b)\rangle \ (\mathbf{2})$$

Sustituimos $(\mathbf{1})$ en $(\mathbf{2})$

$$[\langle(a,b)\rangle \oplus \langle(x,y)\rangle] \oplus \langle(w,z)\rangle = \langle(a,b)\rangle$$

Por la propiedad asociativa de $\oplus$ en H y la existencia del elemento neutro se tiene que

$$\langle(a,b)\rangle \oplus [\langle(x,y)\rangle \oplus \langle(w,z)\rangle] = \langle(a,b)\rangle \oplus \langle(0,0)\rangle,$$

Luego, por la propiedad cancelativa de $\oplus$ en H y la definición de suma se tiene que

$$\langle(x,y)\rangle \oplus \langle(w,z)\rangle = \langle(0,0)\rangle$$

$$\langle(x+w, y+z)\rangle = \langle(0,0)\rangle$$

Por tanto,

$$x + w = 0 \ \wedge \ y + z = 0$$

Pero como $x, w \in \mathbb{Z}^+$ y $y, z \in \mathbb{Z}$ entonces las igualdades anteriores solo se cumplen si

$$x = w = 0 \ \wedge \ y = z = 0$$

O también si

$$x = w = 0 \ \wedge \ y = -z$$

Sin embargo, esta última opción no es válida ya que los elementos de la forma $(0, y) \notin H$, por tanto la opción verdadera es

$$x = w = 0 \ \wedge \ y = z = 0$$

Ello permite concluir que

$$\langle(a,b)\rangle = \langle(c,d)\rangle$$

Caso 2. $a = c$

Si $\langle(a,b)\rangle \ll= \langle(c,d)\rangle \ \wedge \ \langle(c,d)\rangle \ll= \langle(a,b)\rangle$ entonces $b \leq d$ y $d \leq b$ en $\mathbb{Z}$, luego por la anti simetría del orden de los enteros $b = d$ y en consecuencia $\langle(a,b)\rangle = \langle(c,d)\rangle$.

Teorema 2.3.1.3. Propiedad transitiva

Dados $\langle(a,b)\rangle, \langle(c,d)\rangle, \ \langle(e,f)\rangle \in H$,

$$\text{Si } \langle(a,b)\rangle \lll= \langle(c,d)\rangle \quad \wedge \quad \langle(c,d)\rangle \lll= \langle(e,f)\rangle \quad \text{entonces } \langle(a,b)\rangle \lll= \langle(e,f)\rangle$$

Demostración

Caso 1. $a \neq c \neq e$

Si $\langle(a,b)\rangle \lll= \langle(c,d)\rangle \ \wedge \ \langle(c,d)\rangle \lll= \langle(e,f)\rangle$ entonces existen $(g,h),(p,q) \in D_g^+$, tal que

$$\langle(a,b)\rangle \oplus \langle(g,h)\rangle = \langle(c,d)\rangle \qquad \wedge \qquad \langle(c,d)\rangle \oplus \langle(p,q)\rangle = \langle(e,f)\rangle$$

Se sustituye $\langle(c,d)\rangle$ por $\langle(a,b)\rangle \oplus \langle(g,h)\rangle$ en la segunda igualdad y se tiene que

$$\langle(a,b)\rangle \oplus \langle(g,h)\rangle \oplus \langle(p,q)\rangle = \langle(e,f)\rangle$$

Luego,

$$\langle(a,b)\rangle \oplus \langle(g+p,h+q)\rangle = \langle(e,f)\rangle$$

Como $(g+p,h+q) \in D_g^+$ entonces se concluye que

$$\langle(a,b)\rangle \lll= \langle(e,f)\rangle$$

Caso 2. $a \neq c$ y $c = e$

Si $\langle(a,b)\rangle \lll= \langle(c,d)\rangle$ entonces existe $(g,h) \in D_g^+$, tal que

$$\langle(a,b)\rangle \oplus \langle(g,h)\rangle = \langle(c,d)\rangle$$

Además como $\langle(c,d)\rangle \lll= \langle(e,f)\rangle$ $(\mathbf{1})$, se tiene que $d < f$. Luego si se sustituye $\langle(c,d)\rangle$ por $\langle(a,b)\rangle \oplus \langle(g,h)\rangle$ en $(\mathbf{1})$

$$\langle(a,b)\rangle \oplus \langle(g,h)\rangle \lll= \langle(e,f)\rangle$$

En consecuencia,

$$\langle(a,b)\rangle \lll= \langle(e,f)\rangle$$

Caso 3. $a = c$ y $c \neq e$

Si $\langle(c,d)\rangle \lll= \langle(e,f)\rangle$ entonces existe $(p,q) \in D_g^+$, tal que

$$\langle(c,d)\rangle \oplus \langle(p,q)\rangle = \langle(e,f)\rangle$$

Además como $\langle(a,b)\rangle \ll= \langle(c,d)\rangle$ (**1**), se tiene que $b \leq d$. Luego, por la compatibilidad de <<= con $\oplus$

$$\langle(a,b)\rangle \oplus \langle(p,q)\rangle \ll= \langle(c,d)\rangle \oplus \langle(p,q)\rangle$$

Por lo tanto,

$$\langle(a,b)\rangle \oplus \langle(p,q)\rangle \ll= \langle(e,f)\rangle$$

Finalmente se concluye que,

$$\langle(a,b)\rangle \ll= \langle(e,f)\rangle$$

Caso 4. $a = c = e$

Si $\langle(a,b)\rangle \ll= \langle(c,d)\rangle \;\wedge\; \langle(c,d)\rangle \ll= \langle(e,f)\rangle$ entonces $b \leq d$ y $d \leq f$, y por la transitividad del orden de los enteros $b \leq f$, y aplicando el orden lexicográfico $\langle(a,b)\rangle \ll= \langle(e,f)\rangle$.

Cabe dar una demostración de la propiedad cancelativa de la suma, pues su veracidad no es tan clara por la no dependencia de los representantes:

Compatibilidad de $\ll=$ ***con*** $\oplus$ ***y*** $\otimes$

Teorema 2.3.1.4.

Para cualesquiera G-naturales duales $\langle(a,b)\rangle, \langle(c,d)\rangle, \langle(x,y)\rangle \in H$, se cumple que si $\langle(a,b)\rangle \ll= \langle(c,d)\rangle$, entonces $\langle(a,b)\rangle \oplus \langle(x,y)\rangle \ll= \langle(c,d)\rangle \oplus \langle(x,y)\rangle$.

Demostración

Caso 1. $a \neq c$

Si $\langle(a,b)\rangle \ll= \langle(c,d)\rangle$ significa que existe $(w,z) \in D_g^+$ tal que

$$\langle(a,b)\rangle \oplus \langle(w,z)\rangle = \langle(c,d)\rangle$$

Luego,

$$\langle(c,d)\rangle \oplus \langle(x,y)\rangle = [\langle(a,b)\rangle \oplus \langle(w,z)\rangle] \oplus \langle(x,y)\rangle$$

Por la asociatividad de $\oplus$ en H

$$= \langle(a,b)\rangle \oplus [\langle(w,z)\rangle \oplus \langle(x,y)\rangle]$$

Por la propiedad conmutativa de $\oplus$ en H

$$= \langle(a,b)\rangle \oplus [\langle(x,y)\rangle \oplus \langle(w,z)\rangle]$$

$$= [\langle(a,b)\rangle \oplus \langle(x,y)\rangle] \oplus \langle(w,z)\rangle$$

En consecuencia,

$$\langle(c,d)\rangle \oplus \langle(x,y)\rangle = [\langle(a,b)\rangle \oplus \langle(x,y)\rangle] \oplus \langle(w,z)\rangle \quad (\mathbf{1})$$

Además, por la relación de orden en H se tiene

$$\langle(a,b)\rangle \oplus \langle(x,y)\rangle \ll [\langle(a,b)\rangle \oplus \langle(x,y)\rangle] \oplus \langle(w,z)\rangle \qquad (\mathbf{2})$$

De $(\mathbf{1})$ y $(\mathbf{2})$ se concluye que

$$\langle(a,b)\rangle \oplus \langle(x,y)\rangle \ll= \langle(c,d)\rangle \oplus \langle(x,y)\rangle.$$

Caso 2. $a = c$

Si $\langle(a,b)\rangle \ll= \langle(c,d)\rangle$ entonces $b \leq d$, y por la compatibilidad de la relación de orden en los enteros con la suma entonces $b + y \leq d + y$, además $a + x = c + x$por lo tanto, aplicando la definición de orden en H

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

Que es equivalente a

$$\langle(a,b)\rangle \oplus \langle(x,y)\rangle \ll= \langle(c,d)\rangle \oplus \langle(x,y)\rangle.$$

Teorema 2.3.1.5.

Dados los siguientes números $\langle(a,b)\rangle, \langle(c,d)\rangle, \langle(x,y)\rangle \in H$, se cumple que si $\langle(a,b)\rangle \ll= \langle(c,d)\rangle$, entonces$\langle(a,b)\rangle \otimes \langle(x,y)\rangle \ll= \langle(c,d)\rangle \otimes \langle(x,y)\rangle$

Demostración

Caso 1. $a \neq c$

Si $\langle(a,b)\rangle \ll= \langle(c,d)\rangle$ significa que existe $(w,z) \in D_g^+$ tal que

$$\langle(a,b)\rangle \oplus \langle(w,z)\rangle = \langle(c,d)\rangle$$

Luego,

$$\langle(c,d)\rangle \otimes \langle(x,y)\rangle = [\langle(a,b)\rangle \oplus \langle(w,z)\rangle] \otimes \langle(x,y)\rangle$$

Por la propiedad distributiva de $\oplus$ en H

$$\langle(c,d)\rangle \otimes \langle(x,y)\rangle = [\langle(a,b)\rangle \otimes \langle(x,y)\rangle] \oplus [\langle(w,z)\rangle \otimes \langle(x,y)\rangle] \ (\mathbf{1})$$

Por la relación de orden de H se tiene que

$$\langle(a,b)\rangle \otimes \langle(x,y)\rangle \ll= [\langle(a,b)\rangle \otimes \langle(x,y)\rangle] \oplus [\langle(w,z)\rangle \otimes \langle(x,y)\rangle] \ (\mathbf{2})$$

Y sustituyendo $(\mathbf{1})$ y $(\mathbf{2})$

$$\langle(a,b)\rangle \otimes \langle(x,y)\rangle \ll= \langle(c,d)\rangle \otimes \langle(x,y)\rangle$$

Caso 2. $a = c$

Si $\langle(a,b)\rangle \ll= \langle(c,d)\rangle$ entonces $b \leq d$, y por la compatibilidad de la relación de orden en los enteros con la suma y la multiplicación entonces $bx \leq dx$, luego $ay + bx \leq ay + dx$ y como $ay = cy$ se tiene que $ay + bx \leq cy + dx$. Finalmente, $ax = cx$ y aplicando la definición de orden en H se tiene que

$$\langle(ax, ay + bx)\rangle \ll= \langle(cx, cy + dx)\rangle$$

Que en otros términos es lo que se quería demostrar:

$$\langle(a,b)\rangle \otimes \langle(x,y)\rangle \ll= \langle(c,d)\rangle \oplus \langle(x,y)\rangle.$$

2.4. Divisibilidad en los números G-naturales Duales

Si $\langle(a,b)\rangle, \langle(c,d)\rangle \in H$ con $(c,d) \neq (0,0)$, se define la relación de divisibilidad $||$ como sigue:

$\langle(a,b)\rangle || \langle(c,d)\rangle$ si y sólo si existe un $(x,y) \in D_g^+$, tal que $\langle(c,d)\rangle = \langle(a,b)\rangle \otimes \langle(x,y)\rangle$

Esta relación es un pre orden en el conjunto $D_g^+ - \{(0,0)\}$.

Teorema 2.4.1.1. Propiedad reflexiva

Para todo $\langle(x,y)\rangle \in H - \{\langle(0,0)\rangle\}$, $\langle(x,y)\rangle || \langle(x,y)\rangle$

Demostración

Existe $\langle(1,0)\rangle$ tal que $\langle(x,y)\rangle \otimes (\langle 1,0)\rangle = \langle(x \cdot 1, y \cdot 1 + x \cdot 0)\rangle = \langle(x,y)\rangle$, por lo tanto $\langle(x,y)\rangle || \langle(x,y)\rangle$.

Teorema 2.4.1.2. Propiedad antisimétrica

Sean $\langle(a,b)\rangle, \langle(c,d)\rangle \in H$, si $\langle(a,b)\rangle || \langle(c,d)\rangle$ y $\langle(c,d)\rangle || \langle(a,b)\rangle$ entonces $\langle(a,b)\rangle = \langle(c,d)\rangle$

Demostración

Como $\langle(a,b)\rangle || \langle(c,d)\rangle$ y $\langle(c,d)\rangle || \langle(a,b)\rangle$ entonces existen $\langle(x,y)\rangle, \langle(x_1,y_1)\rangle \in H$ tal que

$$\langle(c,d)\rangle = \langle(a,b)\rangle \otimes \langle(x,y)\rangle \quad \text{y} \quad \langle(a,b)\rangle = \langle(c,d)\rangle \otimes \langle(x_1,y_1)\rangle$$

Sustituyendo $\langle(c,d)\rangle$ por $\langle(a,b)\rangle \otimes \langle(x,y)\rangle$ en la segunda igualdad se tiene que:

$$\langle(a,b)\rangle = \langle(a,b)\rangle \otimes \langle(x,y)\rangle \otimes \langle(x_1,y_1)\rangle$$

Realizando los productos

$$\langle(a,b)\rangle = \langle(axx_1, ax_1y + axy_1b + bxx_1)\rangle$$

De ahí que,

$$a = axx_1 \ (\mathbf{1})$$

$$b = ax_1y + axy_1 + bxx_1 \ (\mathbf{2})$$

De $(\mathbf{1})$ como $a, x, x_1 \in \mathbb{Z}^+$, entonces $xx_1 = 1$, luego $x = 1$ y $x_1 = 1$ se sustituye esos resultados en $(\mathbf{2})$,

$$b = ay + ay_1 + b$$

Por la propiedad cancelativa de la suma en los enteros:

$$0 = ay + ay_1$$

Se recuerda que $a \neq 0$ y $0 \leq y < x, 0 \leq y_1 < x_1$ porque así se definieron los elementos de *H,* por tanto

$$0 = y + y_1$$

De ahí que

$$y = y_1 = 0$$

En conclusión

$$\langle(x,y)\rangle = \langle(x_1,y_1)\rangle = \langle(1,0)\rangle$$

Y esto demuestra el teorema.

Teorema 2.4.1.3. Propiedad transitiva

Para $\langle(a,b)\rangle, \langle(c,d)\rangle, \ \langle(e,f)\rangle \in H - \{\langle(0,0)\rangle\}$,

$$\text{Si } \langle(a,b)\rangle || \langle(c,d)\rangle \quad \wedge \quad \langle(c,d)\rangle || \langle(e,f)\rangle \quad \text{entonces } \langle(a,b)\rangle | \langle(e,f)\rangle$$

Demostración

Si $\langle(a,b)\rangle || \langle(c,d)\rangle \quad \wedge \quad \langle(c,d)\rangle || \langle(e,f)\rangle$ entonces existen $\langle(g,h)\rangle, \langle(p,q)\rangle \in H$, tal que

$$\langle(a,b)\rangle \otimes \langle(g,h)\rangle = \langle(c,d)\rangle \qquad \wedge \qquad \langle(c,d)\rangle \otimes \langle(p,q)\rangle = \langle(e,f)\rangle$$

Se sustituye $\langle(c,d)\rangle$ por $\langle(a,b)\rangle \otimes \langle(g,h)\rangle$ en la segunda igualdad por lo que

$$[\langle(a,b)\rangle \otimes \langle(g,h)\rangle] \otimes \langle(p,q)\rangle = \langle(e,f)\rangle$$

$$\langle(a,b)\rangle \otimes [(g,h) \otimes \langle(p,q)\rangle] = \langle(e,f)\rangle$$

Luego,

$$\langle(a,b)\rangle \otimes \langle(g \cdot p, h \cdot p + g \cdot q)\rangle = \langle(e,f)\rangle$$

Por lo tanto, existe $\langle(g \cdot p, h \cdot p + g \cdot q)\rangle \in H - \{\langle(0,0)\rangle\}$, lo que permite concluir que:

$$\langle(a,b)\rangle || \langle(e,f)\rangle$$

Los teoremas de divisibilidad que se cumplen en D_g^+ también se cumplen en H y las demostraciones son análogas a las hechas en los números naturales gaussianos duales.

2.4.2. Definición de un número G-primo dual

Si $\langle(p,q)\rangle \in H$, se dice que $\langle(p,q)\rangle$ es un numero primo, si y sólo si sus únicos divisores son el mismo $\langle(p,q)\rangle$ y $\langle(1,0)\rangle$.

Diremos que p es un número compuesto, si $\langle(p,q)\rangle \gg \langle(1,0)\rangle$ y $\langle(p,q)\rangle$ no es primo.

Teorema 2.4.2.1.

Si $\langle(p,q)\rangle \in H$, donde p es un entero primo en los enteros, entonces $\langle(p,q)\rangle$ es un entero primo en H.

Demostración

Si $\langle(p,q)\rangle \in H$ no es primo entonces existe $\langle(a,b)\rangle, \langle(c,d)\rangle \in H$ tal que

$$\langle(a,b)\rangle \otimes \langle(c,d)\rangle = \langle(p,q)\rangle$$

Con $a \neq 1, a \neq p, c \neq 1$ y $c \neq p$, por tanto

$$\langle(ac, ad+bc)\rangle = \langle(p,q)\rangle$$

Luego $ac = p$, pero p es un número primo en $\mathbb{Z}^+$, y no admite una factorización diferente a $p = p \cdot 1$, en conclusión $\langle(p,q)\rangle$es un número primo en H.

Teorema 2.4.2.2.

Si $\langle(p^k,q)\rangle \in H$, donde p es un entero primo no par, $k \in \mathbb{N}$, $k > 1$, $p \nmid q$ en los enteros, entonces $\langle(p^k,q)\rangle$ es un número primo en H.

Demostración

Si $\langle(p^k,q)\rangle \in H$ no es un número G-primo dual, entonces existen $\langle(a,b)\rangle, \langle(c,d)\rangle \in H$ tal que

$$\langle(a,b)\rangle \otimes \langle(c,d)\rangle = \langle(p^k,q)\rangle$$

$$\langle(ac, ad+bc)\rangle = \langle(p^k,q)\rangle$$

De ahí se tiene que $ac = p^k$, lo que implica que $a = p^h$ y $c = p^i$, por tanto

$$ac = p^h p^i = p^{h+i} = p^k$$

Además, $ad + bc = q$, sustituyendo la información anterior en esta nueva igualdad,

$$ad + bc = p^h d + bp^i = q$$

De modo que $p|p^h$ y $p|p^i$ luego $p|p^h d + bp^i = q$, lo que es una contradicción, en conclusión $\langle(p^k,q)\rangle$ es un número G- primo dual.

2.4.3. Definición de máximo común divisor en H

Teorema 2.4.3.0.

Para toda pareja $\langle(a,b)\rangle, \langle(c,d)\rangle \in H$, existe[9] $\langle(g,h)\rangle$ tal que:

I. $\langle(g,h)\rangle$ es un G-natural dual

II. $\langle(g,h)\rangle \,||\langle(a,b)\rangle \;\wedge\; \langle(g,h)\rangle \,||\langle(c,d)\rangle$

III. Si $\langle(k,m)\rangle||\langle(a,b)\rangle \;\wedge\; \langle(k,m)\rangle||\langle(c,d)\rangle$, entonces $\langle(k,m)\rangle||\langle(g,h)\rangle$

Notaremos el máximo común divisor de $\langle(a,b)\rangle$ y $\langle(c,d)\rangle$ como ***mcd*** $\{\langle(a,b)\rangle, \langle(c,d)\rangle\}$

Teorema 2.4.3.1.

El *máximo común divisor* de dos G-naturales duales es único

Demostración

Supongamos $\langle(g,h)\rangle = \boldsymbol{mcd}\,\{\langle(a,b)\rangle, \langle(c,d)\rangle\}$ y $\langle(g',h')\rangle = \boldsymbol{mcd}\,\{\langle(a,b)\rangle, \langle(c,d)\rangle\}$

Entonces por definición de máximo común divisor (*iii*) tenemos que

$\langle(g,h)\rangle||\,\langle(g',h')\rangle \quad \wedge \quad \langle(g',h')\rangle||\,\langle(g,h)\rangle$

Y por la anti simetría de la relación de divisibilidad $\langle(g,h)\rangle||\,\langle(g',h')\rangle$

Definición de primos relativos

Cuando el $\boldsymbol{mcd}\,\{\langle(a,b)\rangle, \langle(c,d)\rangle\} = \langle(1,0)\rangle$ se dice que $\langle(a,b)\rangle$ y $\langle(c,d)\rangle$ son ***primos relativos.***

El algoritmo de la división y el algoritmo de Euclides solo se dejan mencionados, debido a que las demostraciones son análogas a las realizadas para D_g^+ .

Teorema 2.4.3.2. Algoritmo de la división

Dados dos números G-naturales duales $\langle(z_1,z_2)\rangle \gg \langle(0,0)\rangle$, $\langle(w_1,w_2)\rangle \gg \langle(0,0)\rangle$,

[9] La demostración de la existencia de este número es análoga a la realiza en el teorema ***1.4.4.1.***

existe un único par números duales $\langle(q_1, q_2)\rangle \in H$ y $(r_1, r_2) \in D_g^+ \cup \{(0, y): y \in \mathbb{Z}\}$ tales que

$$\langle(z_1, z_2)\rangle = \langle(w_1, w_2)\rangle \langle(q_1, q_2)\rangle + \langle(r_1, r_2)\rangle, \text{con } 0 \leq r_1 < w_1 \quad y \ 0 \leq r_2 < w_1$$

Además, $(r_1, r_2) = (0,0)$ si, y sólo si , $\langle(w_1, w_2)\rangle || \langle(z_1, z_2)\rangle$

Teorema 2.4.3.2. .Algoritmo de Euclides

Sean dos números G-naturales duales $\langle(z_1, z_2)\rangle \gg \langle(0,0)\rangle$, $\langle(w_1, w_2)\rangle \gg \langle(0,0)\rangle$. Aplicando el algoritmo de la división para los números G-naturales Duales varias veces, se obtienen los siguientes resultados:

$$\langle(z_1, z_2)\rangle = \langle(w_1, w_2)\rangle \langle(p_1, q_1)\rangle + \langle(r_1, s_1)\rangle, \quad 0 \leq r_1 < w_1 \quad y \quad 0 \leq s_1 < w_1$$

$$\langle(w_1, w_2)\rangle = \langle(r_1, s_1)\rangle \langle(p_2, q_2)\rangle + \langle(r_2, s_2)\rangle, \quad 0 \leq r_2 < r_1 \quad y \quad 0 \leq s_2 < r_1$$

.

.

.

$$\langle(r_{n-1}, s_{n-1})\rangle = \langle(r_n, s_n)\rangle \langle(p_{n+1}, q_{n+2})\rangle$$

Entonces el número G-natural gaussiano dual $\langle(r_{n-1}, s_{n-1})\rangle$, es el máximo común divisor del par de números $\langle(z_1, z_2)\rangle, \langle(w_1, w_2)\rangle$. En el caso en que $r_n = 0$ se dice que los números z, w son primos relativos en D_g^+.

Capítulo 3.

FUNCIONES *D*-ARITMETICAS

Una función $f: H \rightarrow \mathbb{Z}^{+}$ se llama función *D*-aritmética y análogamente a como se hace en la teoría de números enteros, se estudiarán algunas de ellas y sus propiedades.

Cabe anotar, que los elementos de H se notarán de la forma (a, b) y no con la notación anterior $\langle(a, b)\rangle$, esto sin olvidar que $a, b \in \mathbb{Z}^{+}$, con $0 \leq b < a$, es decir son clases de equivalencia que representan los números G-naturales duales.

3.1. FUNCIÓN NÚMERO DE ELEMENTOS COMPARABLES

Se define la función número de elementos comparables como sigue:

$$\tau(z) = |\{x \in H : (0,0) << x << z\}|$$

Donde | | indica la cantidad de elementos del conjunto que cumple la condición.

Teorema 3.1.1.1.

Para todo $(a, b) \in H$,

$$\tau(z) = \frac{a(a-1)}{2}$$

Demostración

En el segundo capítulo de este trabajo se indicó que la primera componente de un número G-natural dual indica el número de clases de equivalencia que hay por cada fibra según la relación de equivalencia $\sim$. Es decir por la fibra que tenga primera componente a hay a representantes por esa fibra, por la fibra de primera componente $a-1$ hay $a-1$ representantes y asi sucesivamente hasta la fibra del (1,0) donde solo hay un representante.

Por lo tanto, para hallar $\tau(z)$, se debe sumar en $\mathbb{Z}^{+}$ los números menores que a y mayores de 0, en otros términos:

$$\tau(z) = 1 + 2 + 3 + 4 + \cdots + a - 1$$

Que en la teoría de números enteros representa los números triangulares, y se definen por la expresión:

$$1+2+3+4+\cdots+(a-1)=\frac{a(a-1)}{2}$$

En conclusión,

$$\tau(z)=\frac{a(a-1)}{2}$$

3.2. LA FUNCIÓN INDICATRIZ DE EULER PARA LOS ENTEROS GAUSSIANOS DUALES

3.2.1 Definición

Si $z \in H$, se define la función $\varphi: H \rightarrow \mathbb{Z}^{+}$ como la cantidad de enteros gaussianos duales que son primos relativos con z, en otros términos

$$\varphi(z)=|\{x \epsilon H:(1,0) \lll= x \ll z \wedge \operatorname{mcd}(z, k)=(1,0)\}|$$

Obsérvese que x debe ser comparable con z y el máximo común divisor es el que se define en el capítulo anterior.

Aquí se presenta una tabla con algunos valores de la función indicatriz evaluada en los enteros gaussianos duales:

z	(2,3)	(3,4)	(6,10)	(12,9)	(7,1)	(18,1)
$\varphi(z)$	2	3	11	56	21	116

Para calcular $\varphi(z)$, se necesita el algoritmo de Euclides de los números gaussianos duales y analizar el máximo común divisor de todos los números que sean menores que z, y contar cuántos de ellos son primos relativos con z, además se debe analizar únicamente un representante de las clases de equivalencia que se generan a partir de $\sim$, sin embargo este proceso es bastante tedioso para números gaussianos con parte real muy grande. Por consiguiente se muestran a continuación algunos teoremas que facilitaran el cálculo de la función indicatriz para cualquier número G-natural dual.

Teorema *3.2.1.1.*

Si $z=(p, f)$ es número primo en H entonces

$$\varphi(z) = \sum_{i=1}^{p-1} i = \frac{p(p-1)}{2}$$

Prueba

Primero se demuestra que para cualquier $w = (x, y)$ con $x \neq p, x < p$ y $x \neq 1$, el $inf\{(p, f), (x, y)\}$ es (1,0).

Si $z = (p, f)$ es número primo en H, entonces sus únicos divisores son el mismo y (1,0), por lo tanto si $w = (x, y)$ con $x \neq p, x < p$ y $x \neq 1$, aplicando el algoritmo de Euclides existen $(p_0, q_0) \epsilon\, H$ y $(r_0, s_0) \in D_g^+ \cup \{(0, y): y \in \mathbb{Z}\}$ tal que

$$(p, f) = (x, y)\,(p_0, q_0) + (r_0, s_0)$$

Aplicando varias veces el algoritmo, con el fin de obtener el $mcd\{(p, f), (x, y)\}$, se tiene

$$(x, y) = (r, s)(p_1, q_1) + (r_1, s_1), \quad 0 \leq r_1 < r_0 \;\; y \;\; 0 \leq s_1 < r_0$$

$$(r, s) = (r_1, s_1)(p_2, q_2) + (r_2, s_2), \quad 0 \leq r_2 < r_1 \;\; y \;\; 0 \leq s_2 < r_1$$

.

.

.

$$(r_{n-1}, s_{n-1}) = (r_n, s_n)(p_{n+1}, q_{n+1})$$

Por tanto $mcd\{(p, f), (x, y)\} = (g, h)$ donde (g, h) es un número G-natural dualasociado con (r_n, s_n) . Ahora por definición de máximo común divisor $(g, h)|(p, f)$ y como (p, f)es un número G-natural dual, entonces (g, h) o es un asociado o es una unidad, sin embargo (g, h) no es un asociado a (p, f)ya que si lo fuera $g = p$ y $(p, h)|(x, y)$ es decir que

$$(x, y) = (p, h)(m, n) = (pm, pn + hm)$$

Pero $x < p$ lo cual contradice que $x = pm$ ya que $1 \leq m$, en consecuencia $(g, h) = (1, e)$ es decir el máximo común divisor es (1,0).

Ahora, falta contar la cantidad de números (x, y) que cumplen la condición de ser primos relativos con (p, f)como vimos cualquier (x, y) es primo relativo con (p, f)si $x < p$, entonces contaremos los (x, y) menores que (p, f)tal que $1 < x < p$ y $0 \leq y < x$, , esto con el fin de tomar un representante de cada clase de equivalencia que genera $\sim$, como $p \epsilon \mathbb{Z}^+$, hacemos las posibles combinaciones de x cuando

$x = p - 1$: $(p-1{,}0), (p-1{,}1), \dots (p-1, p-3), (p, p-2)$, es decir hay $a - 1$ combinaciones para este caso, para el caso $x = p - 2$ hay $p - 2$ combinaciones, y en general hay x combinaciones para cada valor de x entonces la cantidad de números gaussianos duales menores que (p, f), contando la unidad es

$1{+}2 + 3 + 4 + 5 + 6 + \cdots + (p-2) + (p-1) = \frac{p(p-1)}{2}$

Teorema ***3.2.1.2.***

Si $z \epsilon H$ y $z = (p^2, f)$, p un numero primo en $\mathbb{Z}$ y $p|f$, entonces

$$\varphi(z) = p^2 * \sum_{i=1}^{p-1} i = \frac{p^3(p-1)}{2}$$

Demostración

Como la cantidad de números naturales gaussianos duales menores que z viene dado por la expresión:

$$\frac{p^2(p^2-1)}{2}$$

Al valor de esta expresión se le debe restar la cantidad de números naturales gaussianos duales que no sean primos relativos con z.

Para encontrar dicha cantidad se debe simplemente eliminar los números gaussianos duales que sean divisibles por $(p, k). k \in \mathbb{Z}^+, k < p$, es decir, se deben suprimir aquellos números que tengan su primera componente un múltiplo de p y que sean menores que p^2, a continuación se listan dichos valores:

$$(p, k), k \in \mathbb{Z}^+, k < p$$

$$(2p, k), k \in \mathbb{Z}^+, k < p * 2$$

$$(3p, k), k \in \mathbb{Z}^+, k < p * 3$$

$$\vdots$$

$$((p-1)p, k), k \in \mathbb{Z}^+, k < p * (p-1)$$

Este término final, es el último que cumple que su primera componente es múltiplo de p y que es menor que p^2 en $\mathbb{Z}^+$.

Luego, como la primera componente indica el número de elementos representantes que hay por cada fibra, solo se debe sumar estos valores para obtener la cantidad solicitada, en otras palabras:

$$p + 2p + 3p + 4p \dots + (p-1)p = p \cdot \frac{p(p-1)}{2} = \frac{p^2(p-1)}{2}$$

Es la cantidad de números gaussianos duales que no son primos relativos con z.

Ahora se obtiene la diferencia:

$$\frac{p^2(p^2-1)}{2} - \frac{p^2(p-1)}{2} = \frac{p^2(p-1)}{2}(p-1+1) = \frac{p^3(p-1)}{2}$$

Y se concluye que:

$$\varphi(z = (p^2, f)) = p^2 * \sum_{i=1}^{p-1} i = \frac{p^3(p-1)}{2}$$

Teorema ***3.2.1.3.***

Si $z \in H$,$z = (a, b)$ con $a = 2p$, con p un número primo en $\mathbb{Z}^+$, entonces

$$\varphi(z) = \frac{3p^2 - p - 2}{2}$$

Demostración

Como a es un número par, el primer grupo de números primos relativos con z son todos aquellos números en los que su primera componente es impar, luego esa cantidad de primos relativos está dado por la siguiente expresión:

$$1 + 3 + 5 + 7 \dots + (2p-1) = p^2$$

Sin embargo, a esa cantidad debemos eliminar al número dual $y = (p, f), 0 \leq f < p$, tal que $(p, f)|z = (a, b)$ pues para (2,0) o para (2,1), se debe cumplir alguno de los siguientes casos $(p, f)\otimes(2,0) = (2p, 2f) = (a, b)$ ó $(p, f)\otimes(2,1) = (2p, 2f' + p) = (a, b)$, no se debe cumplir los dos al mismo tiempo pues eso implicaría que $2f = 2f' + p = b$, pero eso es una contradicción ya que $2f' + p$ es un número impar por ser p un número primo impar.

Luego, la primera cantidad de números primos relativos con z es $p^2 - 1$.

Ahora, el segundo grupo de primos relativos con z, son aquellos números G-naturales duales de primera componente par y que no sean divisibles por (2,0) si $(2,0)|(a,b)$ ó que sean divisibles por (2,1) si $(2,1)|(a,b)$, según sea el caso, es decir por cada fibra de primera componente par solo la mitad de números van a ser primos relativos con z, en términos numéricos la cantidad de este grupo es:

$$\frac{2}{2}+\frac{4}{2}+\frac{6}{2}+\cdots+\frac{2p}{2}=\frac{\frac{2p}{2}(\frac{2p}{2}-1)}{2}$$

Por lo tanto, el número de primos relativos es:

$$p^2-1+\frac{p(p-1)}{2}=\frac{3p^2-p-2}{2}$$

Conjetura 1 (Para ver algunos resultados que ejemplifican la siguiente conjetura, diríjase a los anexos y verifique los números con color de fuente roja)

Sea $z=(a,b)$ un número G-natural dual con $a=p_1^{\alpha_1}*p_2^{\alpha_2}*p_3^{\alpha_3}*\ldots*p_k^{\alpha_k}$ en $\mathbb{Z}^+$ con $p_k=2$ para algún $k\in\mathbb{Z}^+$, si z es un número compuesto en H y $\alpha_1=\alpha_2=\cdots=\alpha_k=1$, entonces

$$\sum_{d|z=(a,b)}\varphi(d)=\frac{a(a-1)}{2}+2$$

En el caso en que z sea un número primo, la ecuación anterior se convierte en

$$\sum_{d|z=(a,b)}\varphi(d)=\frac{a(a-1)}{2}+1$$

Donde d recorre todos los divisores de z en H.

Conjetura 2 (Para ver algunos resultados que ejemplifican la siguiente conjetura, diríjase a los anexos y verifique los números con color de fuente verde)

Sea $z=(a,b)$ un número G-natural dual con $a=p_1^{\alpha_1}*p_2^{\alpha_2}*p_3^{\alpha_1}*\ldots*p_k^{\alpha_k}$ en $\mathbb{Z}^+$ con $p_k\neq 2$ para todo $k\in\mathbb{Z}^+$, si z es un número compuesto en H y $\alpha_1=\alpha_2=\cdots=\alpha_k=1$, entonces

$$\sum_{d|z=(a,b)}\varphi(d)=\frac{a(a-1)}{2}+1$$

Conjetura 3

Sea $z = (a, b)$ un número G-natural dual con $a = p^{\alpha}$ con p un número primo no par en $\mathbb{Z}^{+}$. Si z es un número compuesto en H , entonces

$$\sum_{d|z=(a,b)} \varphi(d) = \frac{a(a-1)}{2} + 1$$

Conjetura 4 (Para ver algunos resultados que ejemplifican la siguiente conjetura, diríjase a los anexos y verifique los números con color de fuente azul**)**

Sea $z = (a, b)$ un número G-natural dual con $a = 2^{\alpha}$ con α un número par en $\mathbb{Z}^{+}$ y $2^{\alpha-2}\,|b$. Si z es un número compuesto en H, entonces

$$\sum_{d|z=(a,b)} \varphi(d) = \frac{a^2}{2} + 1$$

Conjetura 5

Sea $z = (a, b)$ un número G-natural dual con $a = p_1^{\alpha_1} * p_2^{\alpha_2} * p_3^{\alpha_1} * \ldots * p_k^{\alpha_k}$ en $\mathbb{Z}^{+}$, si z es un número compuesto en H y $\alpha_1 = \alpha_2 = \cdots = \alpha_k = 1$, entonces

$$\varphi(a, b) \cong 0 \; mod \; (\, \sigma_1(a) - 1)$$

Donde $\sigma_1(x)$ es la función suma de divisores definida para los números enteros positivos.

Capítulo 4.

FUNCIÓN NÚMERO DE PRIMOS MENORES QUE UN DUAL DADO

Para investigar la distribución de los números G-primos duales se debe empezar con una lista. A continuación, se escriben los primeros 98 números primos menores que los números G-naturales duales con primera componente 20:

(2,0)	(2,1)	(3,0)	(3,1)	(3,2)	(4,1)	(4,3)
(5,0)	(5,1)	(5,2)	(5,3)	(5,4)	(7,0)	(7,1)
(7,2)	(7,3)	(7,4)	(7,5)	(7,6)	(8,1)	(8,3)
(8,5)	(8,7)	(9,1)	(9,2)	(9,4)	(9,5)	(9,7)
(9,8)	(11,0)	(11,1)	(11,1)	(11,2)	(11,3)	(11,4)
(11,5)	(11,6)	(11,7)	(11,8)	(11,9)	(11,10)	(13,0)
(13,1)	(13,2)	(13,3)	(13,4)	(13,5)	(13,6)	(13,7)
(13,8)	(13,9)	(13,10)	(13,11)	(13,12)	(16,1)	(16,3)
(16,5)	(16,7)	(16,9)	(16,11)	(16,13)	(16,15)	(17,0)
(17,1)	(17,2)	(17,3)	(17,4)	(17,5)	(17,6)	(17,7)
(17,8)	(17,9)	(17,10)	(17,11)	(17,12)	(17,13)	(17,14)
(17,15)	(17,16)	(19,0)	(19,1)	(19,2)	(19,3)	(19,4)
(19,5)	(19,6)	(19,7)	(19,8)	(19,9)	(19,10)	(19,11)
(19,12)	(19,13)	(19,14)	(19,15)	(19,16)	(19,17)	(19,18)

No se observa ningún patrón claro y ni siquiera se cumple que las primeras componentes de estos números primos sean impares como pasa en los enteros. Por supuesto, se puede verificar que por cada fibra de primera componente p un número primo, hay una cantidad de p números primos gaussianos duales. También, si la primera componente del número gaussianos dual k es par, entonces hay una cantidad de $\frac{k}{2}$ números primos gaussianos duales por esa fibra. Además, para la fibra de primera componente 9 se observa que hay 6 números G-primos duales, no se olvide que la primera componente de los números G-primos duales o es un entero primo, o es una potencia de un entero primo en los enteros, con ello se puede afirmar que por cada fibra con primera componente no prima p^k, p entero primo hay una cantidad de $p^k - p$ números primos gaussianos duales por cada fibra de esas características.

Si se sigue con el mismo análisis a otros números G-primos duales que no están en la tabla, se encuentra que la afirmación anterior se sigue cumpliendo y la prueba de esta no es más que una consecuencia del ***Teorema 1.4.1.2.*** y la relación $\backsim$.

Por otra parte, aunque la información anterior no afirma nada acerca de la distribución de los números G-primos duales, si es una herramienta que posteriormente permitirá analizar algunos resultados.

Para encontrar alguna relación matemática en este tipo de números se recurre a la definición de la siguiente función D-aritmetica:

Se define $\pi: H \to \mathbb{Z}^{+}$ como el número de primos duales menores que un número natural dual dado:

$$\pi(z) = |\{x \in H: x \ll= z \quad \wedge \quad x \ \ es\ número\ G - primo\ dual\}|$$

A continuación se presenta una tabla que nos presenta varios valores de esta nueva función:

z	(2,1)	(3,0)	(6,4)	(12,9)	(20,1)	(18,1)
$\pi(z)$	1	3	10	40	97	78

Para empezar el estudio se analizan algunas tablas que muestran el comportamiento de la función anterior:

Primera componente de $z = (a, b)$	***k*** $= \frac{a(a-1)}{2}$	***π(z)***	***π(z)/k***	***k/π(z)***
10	45	29	0.644444444	1.551724137931030
100	4950	1262	0.254949495	3.922345483359750
1000	499500	81447	0.163057057	6.132822571733770
10000	49995000	5835684	0.116725353	8.567119124339150
100000	4999950000	456884965	0.091377907	10.943564317114300
1000000	5E+11	37617010825	0.075234097	13.291845604800300

En esta tabla se calculan diferentes valores de la función *π(z)* , en donde los valores *z,* tienen su primera componente una potencia de 10, y también se hallan algunas razones de la misma función con el número $\boldsymbol{k} = \frac{a(a-1)}{2}$. Aquí se toma el valor $\boldsymbol{k}$ y no las potencias de 10, porque el comportamiento de la distribución de los números G-naturales duales se basa en en la cantidad de representantes de cada fibra que se dan a partir de la relación de equivalencia$\sim$.

¿Qué patrones están claros en la tabla? Está claro que cuando z aumenta, la proporción de números G-primos duales menores o iguales a z disminuye (examínese la cuarta columna). En otras palabras, los números G-primos duales se hacen proporcionalmente más escasos cuando nos desplazamos a los números mayores. Este fenómeno que también sucede en los números enteros, tiene una explicación sencilla, pues, después de todo para que un número sea primo no debe ser divisible por ningún número menor. Por ejemplo para saber si el gaussiano dual $(4,3)$ que tienen pocos predecesores es primo, solo se necesita saber que no es divisible por $(2,0), (2,1), (3,0), (3,1), (3,2)$, y es fácil de verificar. Pero para que (313,0) sea primo, no puede ser divisible por $(2,0), (2,1), (3,0), (3,1), (3,2), \dots (312,0), (312,1), \dots (312,311)$, volviéndose más tedioso saber si (313,0) es un primo gaussiano dual.

Para continuar con la observación de la distribución de los primos gaussianos duales, se observa la siguiente tabla con algunos datos nuevos:

Primera componente de $z = (a, b)$	$k = \dfrac{a(a-1)}{2}$	***k/π(z)***	***e^k/π(z)***
10	45	1.551724137931030	4.719600414
100	4950	3.922345483359750	50.51879692
1000	499500	6.132822571733770	460.7347841
10000	49995000	8.567119124339150	5255.966173
100000	4999950000	10.943564317114300	56588.68413
1000000	5E+11	13.291845604800300	592345.6459

La tabla anterior aunque no muestra una regularidad perfecta, se observa que si se desplaza hacia abajo, cada número que se obtiene de la expresión $e^{\frac{k}{\pi(z)}}$, parece ser 10 veces más grande que el valor de arriba. Es decir, al aumentar en un factor de 10 la primera componente de z, también el valor de $e^{\frac{k}{\pi(z)}}$, aumenta aproximadamente en un factor de 10.

En términos matemáticos se tiene que:

$$e^{\frac{50a^2-5a}{\pi(10*a,b)}} \approx 10e^{\frac{\frac{a(a-1)}{2}}{\pi(z=(a,b))}}$$

Que es equivalente a:

$$e^{\frac{10k}{\pi(10a,b)}} \approx 10e^{\frac{\boldsymbol{k}}{\pi(z=(a,b))}}, \quad \text{para un } z \text{ grande}$$

La expresión simplemente afirma que al aumentar la primera componente de
z a $10a$, el resultado, $e^{\frac{10k}{\pi(z=(10a,b))}}$ será unas diez veces más grande que el resultado, $e^{\frac{\boldsymbol{k}}{\pi(z=(a,b))}}$.

Para justificar las expresiones algebraicas anteriores debemos utilizar los siguientes hechos

$$\ln e^{x} = x\,, \qquad e^{\ln x} = x$$

De ahí que,

$$e^{\ln(10*\boldsymbol{a})} = 10 * \boldsymbol{a} = 10e^{\ln(\boldsymbol{a})}$$

Que junto a la relación

$$e^{\frac{10k}{\pi(10a,b)}} \approx 10e^{\frac{\boldsymbol{k}}{\pi(z=(a,b))}}$$

Los patrones son idénticos y sin modo de cometerse una imprudencia: $\frac{\boldsymbol{k}}{\pi(z=(a,b))} \approx \ln a$, para un z grande.

Además si se establece que:

$$2 * \ln a \approx \ln(k)$$

La hipótesis en cuestión se convierte en:

$$\frac{\boldsymbol{k}}{\pi(z=(a,b))} \approx \frac{\ln k}{2}$$

Finalmente, si se toman los inversos a cada lado de la igualdad se obtiene

$$\frac{\pi\big(z=(a,b)\big)}{k} \approx \frac{2}{\ln k}$$

Que da forma al teorema de los números primos gaussianos duales:

$$\frac{\pi\big(z=(a,b)\big)}{k} \approx \frac{2}{\ln k}$$

En la siguiente tabla se observa el patrón numérico:

Primera componente de z	***k***	***π(z)***	***π(z)/k***	***2/Ln(k)***
10	45	29	0.644444444	0.525394622
100	4950	1262	0.254949495	0.235096558
1000	499500	81447	0.163057057	0.152423191
10000	49995000	5835684	0.116725353	0.112819489
100000	4999950000	456884965	0.091377907	0.089554803
1000000	5E+11	37617010825	0.075234097	0.074244912

Y si se replantea el teorema:

$$\pi\big(z = (a, b)\big) \approx \frac{2k}{\ln k}$$

Primera componente de z	***k***	***π(z)***	***2k/Ln(k)***
10	45	29	23.64275799
100	4950	1262	1163.72796
1000	499500	81447	76135.3839
10000	49995000	5835684	5640410.366
100000	4999950000	456884965	447769539.7
1000000	5E+11	37617010825	37122418774

ESPIRAL DE ULAM PARA NÚMEROS G-NATURALES DUALES

A continuación se define la función $\boldsymbol{U} : \boldsymbol{H} \longrightarrow \mathbb{Z}^{+}$, tal que a cada elemento de $\boldsymbol{H}$ le corresponde un entero positivo de la siguiente forma:

$$(\boldsymbol{a}, \boldsymbol{b}) \longrightarrow \boldsymbol{n}$$

$$(\mathbf{1}, \mathbf{0}) \longrightarrow \mathbf{1}$$

$$(\mathbf{2}, \mathbf{0}) \longrightarrow \mathbf{2}$$

$$(\mathbf{2}, \mathbf{1}) \longrightarrow \mathbf{3}$$

$$(\mathbf{3}, \mathbf{0}) \longrightarrow \mathbf{4}$$

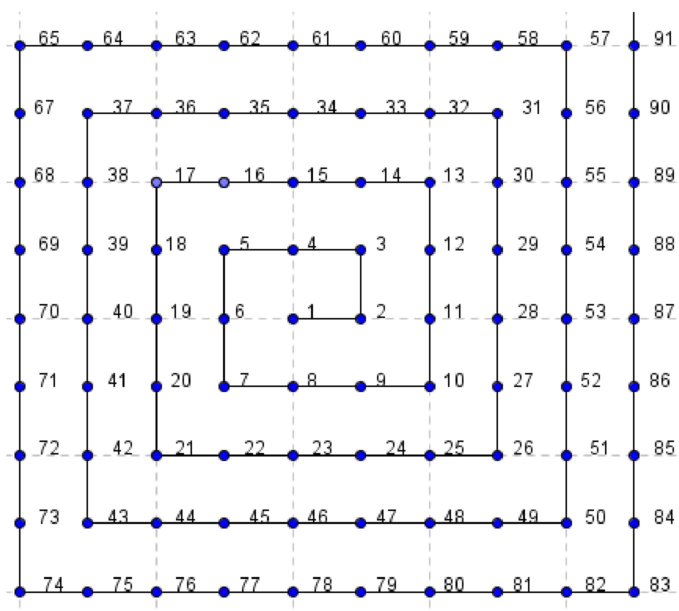
$$(\mathbf{3}, \mathbf{1}) \longrightarrow \mathbf{5}$$

$$(\mathbf{3}, \mathbf{2}) \longrightarrow \mathbf{6}$$

$$(\mathbf{4}, \mathbf{0}) \longrightarrow \mathbf{7}$$

$$\vdots$$

Ahora dibujamos una espiral cuadrada y en ella, ubicamos los números enteros positivos como sigue:



Para pintar una espiral para los números G-primos duales, se realiza lo siguiente:

Como cada números G-natural dual está relacionado con los números enteros positivos mediante la función $\boldsymbol{U}$, entonces en la espiral que vamos a generar se dejan únicamente los puntos que representen números enteros positivos, que a su vez estén relacionados mediante $\boldsymbol{U}$ con los números G-primos duales, por ejemplo el punto que represente al número 8 se deja, pues $\boldsymbol{U}[(\mathbf{4},\mathbf{1})]=\mathbf{8}$ y $(\mathbf{4},\mathbf{1})$ es un número G-primo dual.

En consecuencia se obtienen las siguientes espirales que se definen como Espirales de Ulam para la distribución de los números G-primos duales.

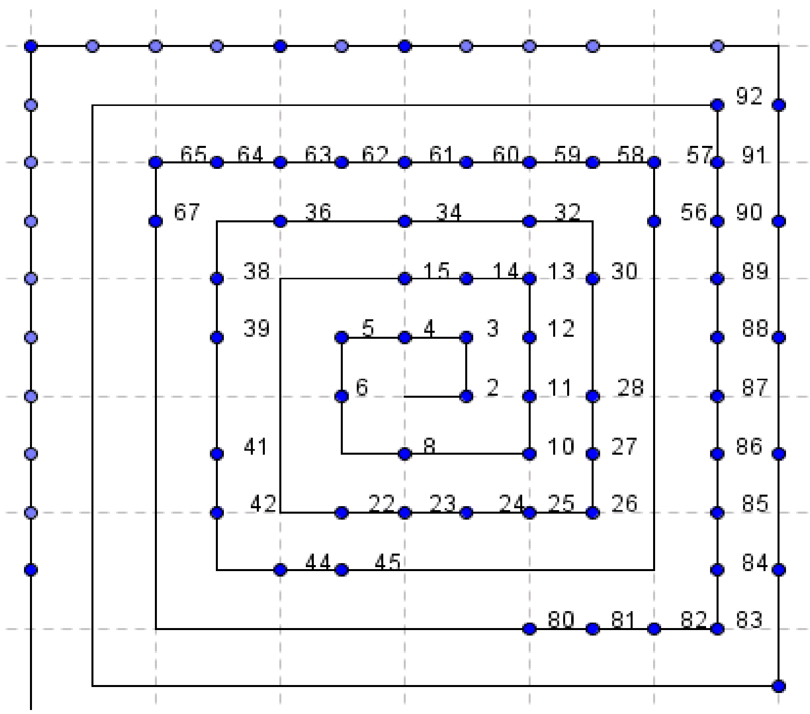


Figura 5. Espiral de Ulam para los números G-primos duales con primera componente menor de 20

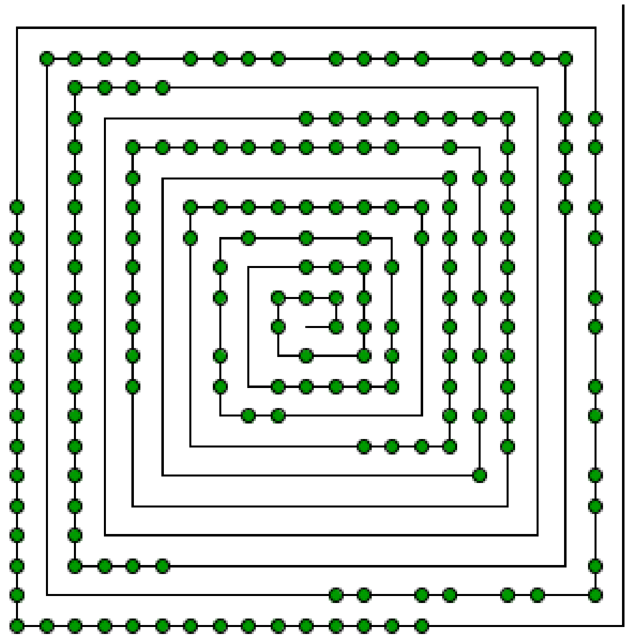


Figura 6. Espiral de Ulam para los números G-primos duales con primera componente menor de 30

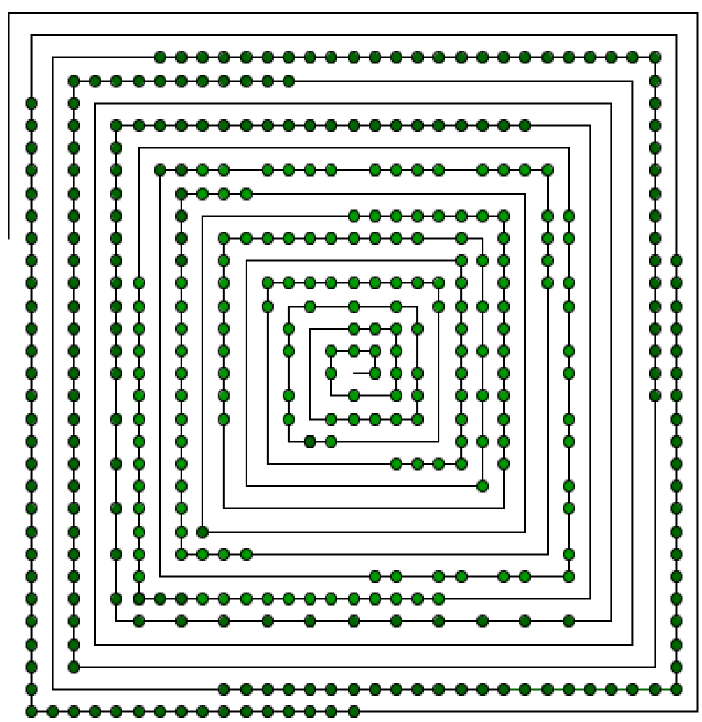


Figura 6. Espiral de Ulam para los primeros 1045 números G-naturales duales.

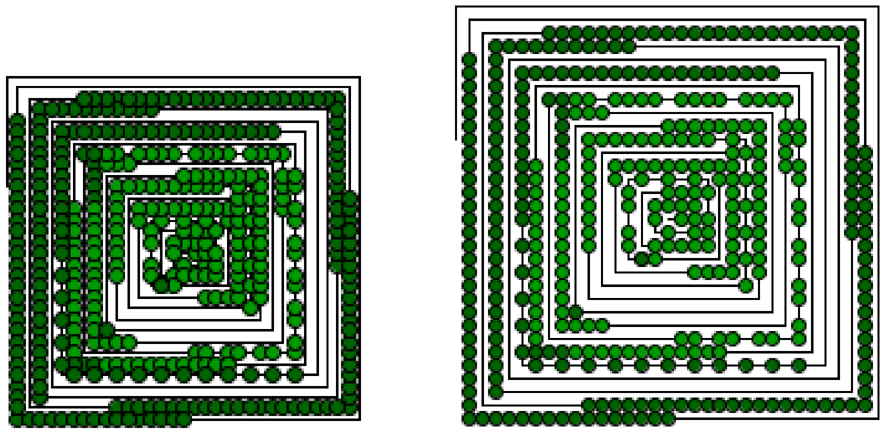


Figura 7. La misma figura 6. Pero con menos zoom.

Se observa que en las espirales anteriores tienden a verse triangulaciones en donde fluctúa la espiral, esto supone que la distribución de los números G-primos duales se encuentra relacionada con alguna forma triangular. Y como se conjeturo en el teorema de los números G-primos duales está relación se da por los números enteros triangulares.

Conclusiones

- El orden aditivo en D_g^+ no es total.
- El orden que se define en el conjunto cociente es un orden total.
- En el semianillo de los números naturales gaussianos duales se puede definir el algoritmo de la división con el cociente y el residuo únicos.
- Usando el algoritmo de Euclides es posible calcular la función indicatriz de Euler para los G-naturales duales y junto a la función de elementos comparables, se pueden obtener varios resultados que son esenciales en el presente trabajo.
- El teorema de los números G-primos duales es verdadero para los primeros 499999500000 números G-naturales duales.
- No fue posible hacer un estudio riguroso a la espiral de Ulam, debido a que el software donde se construyó imposibilitaba el dibujo de rectas sobre la espiral. Esto a su vez impedía realizar un estudio de la distribución de los G-primos duales, análogo a como se hace en los números enteros.
- No se cumple con los objetivos propuestos en el anteproyecto del trabajo, pero si los que se modifican y colocan en el trabajo.

Bibliografía

Apostol, T. (1984). *Introducción a la teoría anlítica de números .* Barcelona: Reverté.

Hebisch, U., & Weinert, H. J. (1992). *SEMIRINGS Algebraic Theory and Applications in Computer Science.* Stuttgart : World Scientific Publishing Co. Pte.Ltd.

Jiménez, H., & Luque, C. (2007). El anillo de los números Duales. En *Memorias XVII encuentro de Geometría y V de Aritmética* (págs. 159-194). Bogotá: Universidad Pedagogica Nacional.

Luque, C. (1993). *El cálculo: una versión sin el concepto de límite.* Bogotá: Universidad Pedagógica Nacional.CIUP.

Luque, C., Jiménez, H., & Ángel, J. (2009). *Representar estucturas algebraicas finitas y enumerables.* Bogotá: Javegraf.

Pérez, A., & Brausín, D. (2012). *Estudio de congruencias en números gaussianos duales.* Bogotá: Universidad Pedagogica Nacional.

Roman, S. (2008). *Lattices and Ordered Sets.* New York: Springer.

ANEXOS

A continuación se muestran algunas de las tablas usadas para la realización del presente estudio. En ellas, se observa la descomposición de cada dual (z) , junto con su respectivo $\boldsymbol{\pi(z)}$

z	$\varphi(z)$	z	$\varphi(z)$	z	$\varphi(z)$	z	$\varphi(z)$	z	$\varphi(z)$	z	$\varphi(z)$
(4,0)	4	(4,2)	4	(6,0)	11	(6,1)	11	(6,2)	11	(6,3)	11
(2,1)	2	(2,1)	2	(3,0)	3	(3,2)	3	(3,1)	3	(3,0)	3
(2,0)	2	(2,0)	2	(2,0)	2	(2,1)	2	(2,0)	2	(2,1)	2
(1,0)	1	(1,0)	1	(1,0)	1	(1,0)	1	(1,0)	1	(1,0)	1
	9		**9**		**17**		**17**		**17**		**17**
(6,4)	11	(6,5)	11	(8,0)	18	(8,2)	16	(8,4)	18	(8,6)	16
(3,2)	3	(3,1)	3	(4,0)	4	(4,1)	6	(4,0)	4	(4,1)	6
(2,0)	2	(2,1)	2	(4,2)	4	(4,3)	6	(4,2)	4	(4,3)	6
(1,0)	1	(1,0)	1	(2,1)	2	(2,1)	2	(2,1)	2	(2,1)	2
	17		**17**	(2,0)	2	(2,0)	2	(2,0)	2	(2,0)	2
				(1,0)	1	(1,0)	1	(1,0)	1	(1,0)	1
					31		33		31		33
(9,0)	27	(9,3)	27	(9,6)	27	(10,0)	34	(10,1)	34	(10,2)	34
(3,0)	3	(3,0)	3	(3,0)	3	(5,0)	10	(5,3)	10	(5,1)	10
(3,1)	3	(3,1)	3	(3,1)	3	(2,0)	2	(2,1)	2	(2,0)	2
(3,2)	3	(3,2)	3	(3,2)	3	(1,0)	1	(1,0)	1	(1,0)	1
(1,0)	1	(1,0)	1	(1,0)	1		47		47		47
	37		37		37						
(10,3)	34	(10,4)	34	(10,5)	34	(10,6)	34	(10,7)	34	(10,8)	34
(5,4)	10	(5,2)	10	(5,0)	10	(5,3)	10	(5,1)	10	(5,4)	10
(2,1)	2	(2,0)	2	(2,1)	2	(2,0)	2	(2,1)	2	(2,0)	2
(1,0)	1	(1,0)	1	(1,0)	1	(1,0)	1	(1,0)	1	(1,0)	1
	47		**47**		**47**		**47**		**47**		**47**
(10,9)	34	(12,0)	38	(12,1)	57	(12,2)	38	(12,3)	57	(12,4)	38
(5,2)	10	(6,0)	11	(4,3)	6	(6,1)	11	(4,1)	6	(6,2)	11
(2,1)	2	(6,3)	11	(3,1)	3	(6,4)	11	(3,0)	3	(6,5)	11
(1,0)	1	(4,0)	4	(1,0)	1	(4,2)	4	(1,0)	1	(4,4)	4
	47	(3,0)	3		67	(3,2)	3		67	(3,1)	3
		(2,0)	2			(2,0)	2			(2,0)	2
		(2,1)	2			(2,1)	2			(2,1)	2
		(1,0)	1			(1,0)	1			(1,0)	1
			72				72				72

z	$\varphi(z)$	z	$\varphi(z)$	z	$\varphi(z)$	z	$\varphi(z)$	z	$\varphi(z)$	z	$\varphi(z)$
(12,5)	57	(12,6)	38	(12,7)	57	(12,8)	38	(12,9)	57	(12,10)	38
(4,3)	6	(6,0)	11	(4,1)	6	(6,1)	11	(4,3)	6	(6,2)	11
(3,2)	3	(6,3)	11	(3,1)	3	(6,4)	11	(3,0)	3	(6,5)	11
(1,0)	1	(4,2)	4	(1,0)	1	(4,0)	4	(1,0)	1	(4,2)	4
	67	(3,0)	3		67	(3,2)	3		67	(3,1)	3
		(2,0)	2			(2,0)	2			(2,0)	2
		(2,1)	2			(2,1)	2			(2,1)	2
		(1,0)	1			(1,0)	1			(1,0)	1
			72				72				72
(12,11)	57	(14,0)	69	(14,1)	69	(14,2)	69	(14,3)	69	(14,4)	69
(4,1)	6	(7,0)	21	(7,4)	21	(7,1)	21	(7,5)	21	(7,2)	21
(3,2)	3	(2,0)	2	(2,1)	2	(2,0)	2	(2,1)	2	(2,0)	2
(1,0)	1	(1,0)	1	(1,0)	1	(1,0)	1	(1,0)	1	(1,0)	1
	67		**93**		**93**		**93**		**93**		**93**
(14,5)	69	(14,6)	69	(14,7)	69	(14,8)	69	(14,9)	69	(14,10)	69
(7,6)	21	(7,3)	21	(7,0)	21	(7,4)	21	(7,1)	21	(7,5)	21
(2,1)	2	(2,0)	2	(2,1)	2	(2,0)	2	(2,1)	2	(2,0)	2
(1,0)	1	(1,0)	1	(1,0)	1	(1,0)	1	(1,0)	1	(1,0)	1
	93		**93**		**93**		**93**		**93**		**93**
(14,11)	69	(14,12)	69	(14,13)	69	(15,0)	92	(15,1)	92	(15,2)	92
(7,2)	21	(7,6)	21	(7,3)	21	(5,0)	10	(5,2)	10	(5,4)	10
(2,1)	2	(2,0)	2	(2,1)	2	(3,0)	3	(3,2)	3	(3,1)	3
(1,0)	1	(1,0)	1	(1,0)	1	(1,0)	1	(1,0)	1	(1,0)	1
	93		**93**		**93**		**106**		**106**		**106**
(15,3)	92	(15,4)	92	(15,5)	92	(15,6)	92	(15,7)	92	(15,8)	92
(5,1)	10	(5,3)	10	(5,0)	10	(5,2)	10	(5,4)	10	(5,1)	10
(3,0)	3	(3,2)	3	(3,1)	3	(3,0)	3	(3,2)	3	(3,1)	3
(1,0)	1	(1,0)	1	(1,0)	1	(1,0)	1	(1,0)	1	(1,0)	1
	106		**106**		**106**		**106**		**106**		**106**
(15,9)	92	(15,10)	92	(15,11)	92	(15,12)	92	(15,13)	92	(15,14)	92
(5,3)	10	(5,0)	10	(5,2)	10	(5,4)	10	(5,1)	10	(5,3)	10
(3,0)	3	(3,2)	3	(3,1)	3	(3,0)	3	(3,2)	3	(3,1)	3
(1,0)	1	(1,0)	1	(1,0)	1	(1,0)	1	(1,0)	1	(1,0)	1
	106		**106**		**106**		**106**		**106**		**106**

z	$\boldsymbol{\varphi(z)}$	**z**	$\boldsymbol{\varphi(z)}$	**z**	$\boldsymbol{\varphi(z)}$	**z**	$\boldsymbol{\varphi(z)}$	**z**	$\boldsymbol{\varphi(z)}$	**z**	$\boldsymbol{\varphi(z)}$
(16,0)	68	(16,2)	74	(16,4)	68	(16,6)	74	(16,8)	68	(16,10)	74
(8,0)	18	(8,5)	28	(8,6)	18	(8,3)	28	(8,0)	18	(8,5)	28
(8,4)	18	(8,1)	28	(8,2)	18	(8,7)	28	(8,4)	18	(8,1)	28
(4,0)	4	(2,1)	2	(4,0)	4	(2,1)	2	(4,0)	4	(2,1)	2
(4,1)	6	(2,0)	2	(4,1)	6	(2,0)	2	(4,1)	6	(2,0)	2
(4,2)	4	(1,0)	1	(4,2)	4	(1,0)	1	(4,2)	4	(1,0)	1
(4,3)	6		135	(4,3)	6		135	(4,3)	6		135
(2,0)	2			(2,0)	2			(2,0)	2		
(2,1)	2			(2,1)	2			(2,1)	2		
(1,0)	1			(1,0)	1			(1,0)	1		
	129				129				129		

(16,12)	68	(16,14)	74	(18,0)	87	(18,1)	116	(18,2)	116	(18,3)	87
(8,2)	18	(8,7)	28	(9,0)	27	(9,5)	36	(9,1)	36	(9,6)	27
(8,6)	18	(8,3)	28	(6,4)	11	(2,1)	2	(2,0)	2	(6,3)	11
(4,0)	4	(2,1)	2	(6,2)	11	(1,0)	1	(1,0)	1	(6,5)	11
(4,1)	6	(2,0)	2	(6,0)	11		155		155	(6,1)	11
(4,2)	4	(1,0)	1	(3,2)	3					(3,2)	3
(4,3)	6		135	(3,1)	3					(3,1)	3
(2,0)	2			(3,0)	3					(3,0)	3
(2,1)	2			(2,0)	2					(2,1)	2
(1,0)	1			(1,0)	1					(1,0)	1
	129				159						159

(18,4)	116	(18,5)	116	(18,6)	87	(18,7)	116	(18,8)	116	(18,9)	87
(9,2)	36	(9,7)	36	(9,3)	27	(9,8)	36	(9,4)	36	(9,0)	27
(2,0)	2	(2,1)	2	(6,4)	11	(2,1)	2	(2,0)	2	(6,5)	11
(1,0)	1	(1,0)	1	(6,2)	11	(1,0)	1	(1,0)	1	(6,3)	11
	155		155	(6,0)	11		155		155	(6,1)	11
				(3,2)	3					(3,2)	3
				(3,1)	3					(3,1)	3
				(3,0)	3					(3,0)	3
				(2,0)	2					(2,1)	2
				(1,0)	1					(1,0)	1
	159				159						159

z	$\varphi(z)$	z	$\pi(z)$	z	$\varphi(z)$	z	$\varphi(z)$	z	$\varphi(z)$	z	$\varphi(z)$
(18,10)	116	(18,11)	116	(18,12)	87	(18,13)	116	(18,14)	116	(18,15)	87
(9,5)	36	(9,1)	36	(9,6)	27	(9,2)	36	(9,7)	36	(9,3)	27
(2,0)	2	(2,1)	2	(6,4)	11	(2,1)	2	(2,0)	2	(6,5)	11
(1,0)	1	(1,0)	1	(6,2)	11	(1,0)	1	(1,0)	1	(6,3)	11
	155		155	(6,0)	11		155		155	(6,1)	11
				(3,2)	3					(3,2)	3
				(3,1)	3					(3,1)	3
				(3,0)	3					(3,0)	3
				(2,0)	2					(2,1)	2
				(1,0)	1					(1,0)	1
					159						159

(18,16)	116	(18,17)	116	(24.0)	146	(24.1)	243	(24.2)	142	(24.3)	243
(9,8)	36	(9,4)	36	(3.0)	3	(3.2)	3	(3.1)	3	(3.0)	3
(2,0)	2	(2,1)	2	(8.0)	18	(8.3)	28	(8.6)	18	(8.1)	28
(1,0)	1	(1,0)	1	(4.2)	4	(1.0)	1	(4.3)	6	(1.0)	1
	155		155	(4.0)	4		275	(4.1)	6		275
				(6.0)	11			(6.5)	11		
				(6.3)	11			(6.2)	11		
				(2.0)	2			(2.0)	2		
				(2.1)	2			(2.1)	2		
				(12.0)	38			(12.1)	57		
				(12.6)	38			(12.7)	57		
				(1.0)	1			(1.0)	1		
					278				316		

(24.4)	148	(24.5)	243	(24.6)		(24.7)	243	(24.8)		(24.9)	243
(3.2)	3	(3.1)	3	(3.0)	3	(3.2)	3	(3.1)	3	(3.0)	3
(8.4)	18	(8.7)	28	(8.2)	18	(8.5)	28	(8.0)	18	(8.3)	28
(4.2)	4	(1.0)	1	(4.3)	6	(1.0)	1	(4.2)	4	(1.0)	1
(4.0)	4		275	(4.1)	6		275	(4.0)	4		275
(6.4)	11			(6.3)	11			(6.2)	11		
(6.1)	11			(6.0)	11			(6.5)	11		
(2.0)	2			(2.0)	2			(2.0)	2		
(2.1)	2			(2.1)	2			(2.1)	2		
(12.2)	38			(12.3)	57			(12.4)	38		
(12.8)	38			(12.9)	57			(12.10)	38		
(1.0)	1			(1.0)	1			(1.0)	1		
	280				174				132		

z	$\pi(z)$	z	$\pi(z)$	z	$\pi(z)$	z	$\pi(z)$	z	$\pi(z)$	z	$\pi(z)$
(24.10)		(24.11)	243	(24.12)		(24.13)	243	(24.14)		(24.15)	243
(3.2)	3	(3.1)	3	(3.0)	3	(3.2)	3	(3.1)	3	(3.0)	3
(8.6)	18	(8.1)	28	(8.4)	18	(8.7)	28	(8.2)	18	(8.5)	28
(4.3)	6	(1.0)	1	(4.2)	4	(1.0)	1	(4.3)	6	(1.0)	1
(4.1)	6		275	(4.0)	4		275	(4.1)	6		275
(6.1)	11			(6.0)	11			(6.5)	11		
(6.4)	11			(6.3)	11			(6.2)	11		
(2.0)	2			(2.0)	2			(2.0)	2		
(2.1)	2			(2.1)	2			(2.1)	2		
(12.5)	57			(12.6)	38			(12.7)	57		
(12.11)	57			(12.0)	38			(12.1)	57		
(1.0)	1			(1.0)	1			(1.0)	1		
	174				132				174		

(24.16)		(24.17)	243	(24.18)		(24.19)	243	(24.20)		(24.21)	243
(3.2)	3	(3.1)	3	(3.0)	3	(3.2)	3	(3.1)	3	(3.0)	3
(8.0)	18	(8.3)	28	(8.6)	18	(8.1)	28	(8.4)	18	(8.7)	28
(4.2)	4	(1.0)	1	(4.3)	6	(1.0)	1	(4.2)	4	(1.0)	1
(4.0)	4		275	(4.1)	6		275	(4.0)	4		275
(6.4)	11			(6.3)	11			(6.2)	11		
(6.1)	11			(6.0)	11			(6.5)	11		
(2.0)	2			(2.0)	2			(2.0)	2		
(2.1)	2			(2.1)	2			(2.1)	2		
(12.8)	38			(12.9)	57			(12.10)	38		
(12.2)	38			(12.3)	57			(12.4)	38		
(1.0)	1			(1.0)	1			(1.0)	1		
	132				174				132		

(24.22)		(24.23)	243	(28.0)		(28.1)		(28.2)		(28.3)	
(3.2)	3	(3.1)	3	4.0	4	4.3	6	4.2	4	4.1	6
(8.2)	18	(8.5)	28	7.0	21	7.2	21	7.4	21	7.6	21
(4.3)	6	(1.0)	1	2.0	2	(1.0)	1	2.0	2	(1.0)	1
(4.1)	6		275	2.1	2		28	2.1	2		28
(6.1)	11			14.0	69			14.1	69		
(6.4)	11			14.7	69			14.8	69		
(2.0)	2			(1.0)	1			(1.0)	1		
(2.1)	2				168				168		
(12.11)	57										
(12.5)	57										
(1.0)	1										
	174										

z	$\varphi(z)$	z	$\varphi(z)$	z	$\varphi(z)$	z	$\varphi(z)$	z	$\varphi(z)$	z	$\varphi(z)$
(28.4)		(28.5)		(28.6)		(28.7)		(28.8)		(28.9)	
4.0	4	4.3	6	4.2	4	4.1	6	4.0	4	4.3	6
7.1	21	7.3	21	7.5	21	7.0	21	7.2	21	7.4	21
2.0	2	(1.0)	1	2.0	2	(1.0)	1	2.0	2	(1.0)	1
2.1	2		28	2.1	2		28	2.1	2		28
14.2	69			14.3	69			14.4	69		
14.9	69			14.10	69			14.11	69		
(1.0)	1			(1.0)	1			(1.0)	1		
	168				168				168		
(28.10)		(28.11)		(28.12)		(28.13)		(28.14)		(28.15)	
4.2	4	4.1	6	4.0	4	4.3	6	4.2	4	4.1	6
7.6	21	7.1	21	7.3	21	7.5	21	7.0	21	7.2	21
2.0	2	(1.0)	1	2.0	2	(1.0)	1	2.0	2	(1.0)	1
2.1	2		28	2.1	2		28	2.1	2		28
14.5	69			14.6	69			14.7	69		
14.12	69			14.13	69			14.0	69		
(1.0)	1			(1.0)	1			(1.0)	1		
	168				168				168		
(28.16)		(28.17)		(28.18)		(28.19)		(28.20)		(28.21)	
4.0	4	4.3	6	4.2	4	4.1	6	4.0	4	4.3	6
7.4	21	7.6	21	7.1	21	7.3	21	7.5	21	7.0	21
2.0	2	(1.0)	1	2.0	2	(1.0)	1	2.0	2	(1.0)	1
2.1	2		28	2.1	2		28	2.1	2		28
14.8	69			14.9	69			14.10	69		
14.1	69			14.2	69			14.3	69		
(1.0)	1			(1.0)	1			(1.0)	1		
	168				168				168		
(28.22)		(28.23)		(28.24)		(28.25)		(28.26)		(28.27)	
4.2	4	4.1	6	4.0	4	4.3	6	4.2	4	4.1	6
7.2	21	7.4	21	7.6	21	7.1	21	7.3	21	7.5	21
2.0	2	(1.0)	1	2.0	2	(1.0)	1	2.0	2	(1.0)	1
2.1	2		28	2.1	2		28	2.1	2		28
14.11	69			14.12	69			14.13	69		
14.4	69			14.5	69			14.6	69		
(1.0)	1			(1.0)	1			(1.0)	1		
	168				168				168		