LAS ECUACIONES EN EL MUNDO DISCRETO: UN ESTUDIO SOBRE LAS ECUACIONES DIOFÁNTICAS

PABLO ANDRÉS BELTRÁN SOSA

UNIVERSIDAD PEDAGÓGICA NACIONAL

FACULTAD DE CIENCIA Y TECNOLOGÍA

DEPARTAMENTO DE MATEMÁTICAS

ESPECIALIZACIÓN EN EDUCACIÓN MATEMÁTICA

BOGOTÁ D.C.

2014

LAS ECUACIONES EN EL MUNDO DISCRETO: UN ESTUDIO SOBRE LAS ECUACIONES DIOFÁNTICAS

PABLO ANDRÉS BELTRÁN SOSA

Trabajo de grado presentado ante el Departamento de Matemáticas de la Universidad Pedagógica Nacional como requisito para optar por el título de Especialista en Educación Matemática.

Asesor:

YEISON ALEXANDER SÁNCHEZ RUBIO

UNIVERSIDAD PEDAGÓGICA NACIONAL

FACULTAD DE CIENCIA Y TECNOLOGÍA

DEPARTAMENTO DE MATEMÁTICAS

ESPECIALIZACIÓN EN EDUCACIÓN MATEMÁTICA

BOGOTÁ D.C.

2014

UNIVERSIDAD PEDAGOGICA NACIONAL

Educadora de educadores

FACULTAD DE CIENCIA Y TECNOLOGÍA
DEPARTAMENTO DE MATEMÁTICAS

ACTA DE EVALUACION DE TESIS DE GRADO

Escuchada la sustentación del Trabajo de Grado titulado ***"Las ecuaciones en el mundo discreto: Un estudio sobre las ecuaciones diofánticas"*** Presentado por el estudiante:

Pablo Andrés Beltrán Sosa - 2014182002

Como requisito parcial para optar al título de **Especialización en Educación Matemática**, analizado el proceso seguido por el estudiante en la elaboración del Trabajo y evaluada la calidad del escrito final, se le asigno la calificación de **Aprobado** con **50** puntos.

Observaciones:

En constancia se firma a los 03 días del mes de diciembre de 2014.

JURADOS

Director(a) del Trabajo: Profesor(a) _____
YELSON SANCHEZ

Jurado:

Profesor(a) _____
WILLIAM JIMÉNEZ

Dedicatoria

A Dios como creador supremo, quien me ha dado la fuerza y valentía para continuar con todos los proyectos que he realizado

A mi madre quien siempre ha estado Ahí, para mí, brindándome todo su amor y apoyo incondicional

A mis compañeros Edwin y Nicol quienes Siempre estuvieron al tanto en la elaboración de este trabajo de grado

Agradecimientos

A Dios por permitirme realizar este trabajo

A mis padres y hermanas por su apoyo incondicional

A mi asesor y director del trabajo de grado profesor Yeison Sánchez quien con su paciencia y sabiduría guio cada paso realizado en este trabajo de grado y es un ejemplo como profesional en educación

A los profesores de la especialización Mg. Leonardo Ángel, Mg. Edgar Guacaneme y Mg. William Jiménez, quienes contribuyeron de manera significativa en mi formación como especialista y en la construcción de este trabajo

A la profesora Lyda Mora quien aporto demasiado en mi formación como profesional y es un ejemplo a seguir como docente

A mis compañeros de la especialización quien con sus aportes en los seminarios dieron muchas ideas para la realización del presente trabajo

RESUMEN ANALÍTICO EN EDUCACIÓN

1. Información General	
Tipo de documento	Trabajo de Grado
Acceso al documento	Universidad Pedagógica Nacional. Biblioteca Central
Título del documento	Las ecuaciones en el mundo discreto: Un estudio sobre las ecuaciones diofánticas
Autor(es)	Beltrán Sosa, Pablo Andrés
Director	Sánchez Rubio, Yeison Alexander
Publicación	Bogotá, Universidad Pedagógica Nacional, 2014. 65p
Unidad Patrocinante	Universidad Pedagógica Nacional
Palabras Claves	*Ecuación Diofántica, Enteros Gaussianos, Métodos de solución ecuaciones diofánticas, Algoritmo de Euclides, Lema de Bezout*

2. Descripción
Se presenta el siguiente trabajo de grado en el marco de la Especialización en Educación Matemática, cuyo objetivo es analizar varios métodos de solución de algunas ecuaciones diofánticas: para ello se contempla un marco histórico de las ecuaciones diofánticas, un estudio de los métodos clásicos de solución a algunas ecuaciones diofánticas en el conjunto de los números enteros, y como parte del análisis se explora si en el conjunto de los números enteros gaussianos cuyas características (algebraicas) son similares a los de los enteros es posible adaptar los métodos estudiados para solucionar las ecuaciones diofánticas en este anillo.

3. Fuentes
Algunas de las fuentes utilizados son Angel, A. R. (1997). *Algebra Intermedia* (4a ed., Vol. 1). (O. P. Velazco, Trad.) Neucalpan de Juarez, Mexico: Pearson Educación. Boyer. (1992). *Historia de la matemática.* Madrid: Alianza editorial. Cardano, G. (1968). *Ars Magna or the rules of algebra.* (R. Witmer, Trad.) New York: Dover Publications, Inc. Chamizo Lorente, F. (2008). *Euler y la teoría de números.* México. Panizza, M., Sadovsky, P., & Sessa, C. (1999). La ecuación lineal con dos variables: entre la

unicidad y el infinito. *Enseñanza de las Ciencias*, 453-461.

Sarmiento Rondon, W. (2004). *Sobre las Ecuaciones Diofánticas.* Bucaramanga, Colombia: Universidad Industrial de Santander.

Van Der Waerden, B. L. (1985). *A History of Algebra.* Berlin, Alemania: Springer-Verlag.

4. Contenidos

El presente trabajo de grado se ha ordenado en cinco capítulos de la siguiente manera:

En el **capítulo uno,** denominado preliminares, se plantean los objetivos del trabajo de grado enmarcando la importancia y relevancia que tienen la elaboración de este documento.

El **capítulo dos** contiene datos históricos que exponen el desarrollo de las ecuaciones diofánticas en relación a los métodos de solución utilizados para resolverlas.

El **capítulo tres,** incluye un estudio acerca de varios de los métodos de solución a algunas ecuaciones diofánticas, que fueron seleccionados y organizados según los datos históricos del capítulo dos.

En el **capítulo cuatro** se muestra la estructura de los enteros gaussianos y sus propiedades más importantes, luego se plantean algunas ecuaciones diofánticas en dicho conjunto y posteriormente se analiza si los métodos aplicados en el conjunto de los enteros pueden ser aplicados en este conjunto numérico.

El **capítulo cinco** muestra las conclusiones relacionadas a los objetivos y los capítulos desarrollados.

Finalmente se presenta la bibliografía que fue conveniente al realizar el presente trabajo.

5. Metodología

La metodología en este trabajo de grado se enmarca tres etapas, la primera consultar los documentos de historia en las matemáticas para indagar como surgen y como son trabajadas las ecuaciones diofánticas y sus métodos de solución a lo largo de la historia. La segunda etapa consistió en analizar varios de los métodos encontrados para solucionar algunas ecuaciones, teniendo en cuenta aspectos como ¿Por qué funcionan? y ¿Bajo qué condiciones? Y la tercera etapa, consistió en determinar si dichos métodos pueden ser aplicados en el conjunto de los números enteros gaussianos para ecuaciones diofánticas, en este nuevo mundo, lo cual permitió generar conclusiones y reflexiones que nos conllevan al tratamiento de los objetos matemáticos desde una perspectiva tecnológica al profundizar, estudiar y examinar técnicas específicas del conocimiento matemático.

6. Conclusiones

- En la consulta histórica sobre ecuaciones diofánticas se detectan algunos métodos de solución que empleaban algunas civilizaciones y culturas para resolver las ecuaciones diofánticas definidas en este trabajo, pero estos métodos eran aplicados a ecuaciones de la forma $ax + by = c$ que estaban sujetas a sistemas de ecuaciones lineales. Desde lo anterior se puede concluir que aquellas civilizaciones buscaban soluciones únicas y solo fue hasta el estudio de Diofánto quien es él percusor de métodos de solución a estas ecuaciones sin estar sujeta a un sistema de ecuaciones lineales, dónde se empezaron a buscar soluciones infinitas, mostrando así que el problema de unicidad e infinidad se ha trabajado desde hace muchos años.
- El estudio de los métodos de solución de algunas ecuaciones diofánticas tanto en el anillo de los números enteros y en el de los enteros gaussianos, permite concluir que esto abre la posibilidad de que los maestros de matemáticas, tengamos más claridad entre las diferencias de conjuntos numéricos y las cualidades que los hace esenciales, además se ve como una herramienta potente para definir cualquier conjunto numérico.
- Una dificultad que se dio en este trabajo de grado, fue al momento de establecer los métodos de solución a las ecuaciones diofánticas seleccionadas en los enteros gaussianos, porque se trató de establecer de la misma manera que se hizo en los enteros, dejando de lado algunos aspectos importantes de este nuevo conjunto numérico, como las unidades y asociados, lo que luego permitió deducir que no todas las técnicas pueden ser llevadas de la misma manera a un conjunto con una estructura algebraica similar. Lo anterior permite reflexionar que esto se puede convertir en una herramienta poderosa para el docente, puesto que aquí se evidencia la diferencia entre la técnica y la tecnología, en la cual la tecnología será aquella que le permita al docente analizar cada concepto tiene en cuenta las características del universo de discurso del que se hable.

Elaborado por:	Pablo Andrés Beltrán Sosa
Revisado por:	Yeison Alexander Sánchez Rubio

Fecha de elaboración del Resumen:	16	10	2014

Contenido

Introducción

Este trabajo surge por el interés del autor en identificar si algunos métodos de solución a ecuaciones diofánticas en el conjunto de los números enteros, se pueden exportar a otro mundo discreto, entendido este como un conjunto numérico que cumpla las mismas propiedades del anillo de los enteros. En este trabajo las ecuaciones se toman como un elemento de estudio clave tanto en lo matemático como en lo histórico. Dentro del estudio de las ecuaciones, es importante reconocer el conjunto en el que se están planteando las ecuaciones y el conjunto de valores que se consideran pueden ser solución de la ecuación, ya que esto determinara de una manera u otra, las técnicas y métodos utilizados para encontrar o determinar el conjunto solución de las mismas. Es por ello que este trabajo de grado se enmarca en el conjunto de los números enteros y en conjuntos con una estructura algebraica de dominio de integridad que no sean campos, porque con ella trae un concepto importante a estudiar que es la divisibilidad, si se hubiese trabajado en conjuntos como los $\mathbb{Q}$, $\mathbb{R}$ o $\mathbb{C}$, la divisibilidad pierde sentido.

Basado en lo anterior se tendrá como hipótesis que los métodos de solución a las ecuaciones se cumplirán siempre y cuando en la estructura algebraica que se trabaje sea posible establecer algunas propiedades claves del conjunto de los números enteros. En el capítulo uno se establece los objetivos. En el capítulo dos se ubican algunos datos históricos que exponen el desarrollo de las ecuaciones diofánticas a partir del tratamiento de algunas civilizaciones y épocas, mostrando ideas de como solucionaban estas ecuaciones y qué métodos utilizaban para la solución de las mismas.

Desde lo anterior cabe señalar que acerca de ecuaciones Diofánticas se puede obtener información variada que brindan cualquier tipo de significados, algunos definen al objeto matemático de forma correcta y otros presentan información que da lugar a confusiones. Por ello en el capítulo dos se precisaran algunas definiciones y métodos de solución a ecuaciones diofánticas en el conjunto de los números enteros. De acuerdo con esto en el capítulo tres se realiza un estudio de algunos métodos encontrados al momento de solucionar ecuaciones diofánticas, estos métodos fueron seleccionados a partir de la historia de las matemáticas y algunos estudiados en el seminario de tecnología del programa académico Especialización en educación Matemática desarrollado en el periodo I del año 2014, el estudio que se hace es con el fin del por qué funcionan los métodos de solución y así poder comprender el uso que se le dio.

Basado en los dos capítulos anteriores se realiza un análisis en los enteros gaussianos, debido a que tiene una estructura similar al conjunto de los números enteros; ambos son dominios de integridad, en este análisis se establecen propiedades de divisibilidad, máximo común divisor, números primos, algoritmo de Euclides y otros que servirán para el desarrollo de los métodos encontrados en el capítulo 2 y 3, es por ello que en el

capítulo cuatro se presenta la elaboración de los nuevos métodos para llevarlos al nuevo mundo discreto y así verificar si estos métodos funcionan en el nuevo conjunto. I finalmente se encuentran las conclusiones del estudio y análisis de los capítulos 1, 2, 3 y 4.

1. Preliminares

1.1. Objetivos

General

Realizar un estudio sobre los métodos de solución de algunas ecuaciones diofánticas en dominios de Integridad.

Específicos

- Consultar distintas fuentes bibliográficas que permitan tener una visión histórica sobre las ecuaciones diofánticas.
- Estudiar los métodos de solución de algunas ecuaciones diofánticas, particularizando en las razones por las que estos funcionan.
- Consultar algunos conjuntos numéricos con una estructura algebraica similar o igual a la de los números enteros (i.e Enteros gaussianos, anillos de polinomios, enteros duales, naturales), y seleccionar uno de ellos.
- Observar si algunos de los métodos de solución de uno o más tipos de ecuaciones diofánticas, se puede utilizar en el conjunto numérico seleccionado para obtener la solución de ecuaciones planteadas en esta última estructura.
- Reconocer algunos elementos que aportan las ecuaciones diofánticas a nuestro papel docente.

2. Aspectos históricos de las ecuaciones diofánticas

En este capítulo se abordara la historia de las ecuaciones diofánticas, entendidas como ecuaciones con coeficientes enteros, cuyas soluciones se buscan en el conjunto de los enteros; sin embargo en la consulta de la misma se encontrarán ecuaciones cuyos coeficientes serán en el conjunto de los números racionales, pero luego se desarrollaran en el conjunto de los números enteros. Desde lo anterior se hará un recorrido por el planteamiento y solución de ecuaciones desde las culturas antiguas hasta el siglo XVI, ya que la información que se encuentra en la historia acerca de ecuaciones diofánticas es escasa.

En la indagación histórica realizada, se encontraron aportes de algunas culturas al planteamiento y solución de ecuaciones, destacando en algunas de ellas (las más antiguas) una representación con carácter netamente retórico ya que no poseían la notación simbólica actual a la que se está acostumbrado; igualmente, sus soluciones solo podían ser positivas o cero, dado que no tenían la noción de los números negativos que fueron posteriormente adaptados a la solución de ecuaciones, a través de la cultura Griega en el siglo VII y Árabe en el siglo IX (teniéndolos en cuenta como elementos o reglas de operación).

Algunas culturas antiguas como la babilónica, griega e india han encontrado en las matemáticas una base fundamental para su desarrollo y en las ecuaciones una herramienta para la solución de problemas de su entorno; en el siguiente problema planteado por los babilonios vemos un ejemplo de este último:

Supongamos, que tomamos $\frac{2}{3}$ *de* $\frac{2}{3}$ *de una cierta "cantidad" de cebada, se añaden 100 unidades de cebada y se restaura la "cantidad"*

A su vez hacen un trabajo con las ecuaciones para la solución de problemas netamente matemáticos que generaron la base de sus grandes conocimientos en esta ciencia. Ejemplo de ello lo podemos ver con los griegos en la obra de Euclides *Elementos,* un compilado de trece libros sobre problemas matemáticos y geométricos basados en la geometría plana, del espacio, razones y proporciones. Igualmente la obra del matemático Diofánto de Alejandría *Aritmética* compuesta por 12 capítulos (de los cuales solo se conocen los 6 primeros) propone y resuelve problemas sobre cantidades y combinaciones relacionadas con las medidas de lados, áreas, perímetros de triángulos y sumas de cuadrados que son resueltos de forma numérica; problemas como:

Todo cubo puede expresarse como suma de tres cubos. El producto de dos números, cada uno de los cuales es una suma de dos cuadrados, puede expresarse de dos maneras distintas como suma de dos cuadrados (Sarmiento, 2004)

Una de las culturas más antiguas en las que se encuentran registros de trabajos relacionados con ecuaciones diofánticas es la India, en los escritos *Shulbasutras*, principales fuentes del conocimiento matemático Indio durante los siglos VIII y I a.C. se logran visualizar de forma particular en el *baudhayana* algunos trabajos en torno a las soluciones geométricas de ecuaciones diofánticas de la forma $ax^2 = c$ y $ax^2 + bx = c$, (notación actual) se consideran diofánticas dado que se consideraban soluciones solo en el conjunto de los números enteros.

Sin duda alguna, dichos aportes han dejado un legado histórico que ha contribuido a la evolución, planteamiento y resolución de ecuaciones, en este sentido a continuación se dará una mirada con más detalle a los principales aportes hechos por algunas de estas culturas a la solución de ecuaciones diofánticas, en particular ecuaciones de las formas $ax + by = c$ llamadas ecuaciones diofánticas lineales y $a^2 + b^2 = c^2$ llamadas comúnmente ternas pitagóricas.

2.1 Babilonios

En los registros hallados de la cultura babilónica en las tablillas de arcilla, un gran número de ellas muestran como empleaban las matemáticas para solucionar los problemas, se encuentran algunos ejercicios que en el contexto actual se pueden solucionar con el uso de ecuaciones, un ejemplo tomado de una tablilla babilónica plantea la resolución de un sistema de ecuaciones en los siguientes términos:

$$\frac{1}{4}\,anchura + longitud = 7\ manos$$
$$longitud + anchura = 10\ manos$$

Para resolverlo los babilonios comienzan asignando el valor *5* a una *mano* y observaban que la solución podía ser:

$$Anchura = 20,\ longitud = 30$$

De la anterior situación se puede interpretar que los babilonios trabajaban sistemas de ecuaciones lineales de la forma $\begin{cases} ax + by = cz \\ dx + ey = fz \end{cases}$, para solucionarlo asignaban un valor a una de las variables, con el fin de llegar a un sistema de ecuaciones de dos variables, posteriormente el valor asignado tenía el propósito de no trabajar con fracciones, como se vio en el ejemplo anterior. Ahora ese valor que se le asigna se hace con el fin, de darle solución a la anchura y longitud en el conjunto de los números naturales, puesto que para ellos era de mejor utilidad trabajar las ecuaciones en dicho conjunto, no obstante los babilonios hallaban solo una solución a este sistema de ecuaciones, si se observa con detalle el ejemplo se pueden deducir más soluciones.

Ahora si se observa la solución a esta ecuación en el contexto actual, se puede utilizar el método de eliminación, que en la notación de hoy, sería:

$$\frac{y}{4} + x = 35$$
$$y + x = 50$$

Restando la segunda de la primera, se obtiene $\frac{3y}{4} = 15$, es decir, $y = 20$ e $x = 30$. Se dice que los babilónicos lograron resolver sistemas de ecuaciones con hasta diez incógnitas.

De lo anterior se puede deducir que un primer tratamiento de ecuaciones diofánticas se da con los babilonios, al trabajar sistemas de ecuaciones de las cuales las soluciones estaban dadas por números naturales, no obstante se aclara que no se encuentra evidencia del uso de ecuaciones de la forma $ax + by = c$, sin estar sujeta al sistema de ecuaciones.

Por otro lado, las ecuaciones diofánticas también aparecen en una de las tablillas en las que se encuentra evidencia del uso de ternas pitagóricas por los babilonios,

Figura 1: *Tablilla en arcilla babilonios*[1]

Se han dado muchas traducciones de esta tablilla, lo que permite dar diferentes interpretaciones de la misma, pero muchas de ellas poseen información suficiente, para afirmar que los babilonios conocían las ternas pitagóricas, es decir que son conocidas aproximadamente 1200 años antes de Pitágoras.

En una de las traducciones dadas a esta tablilla (*Tabla 1)*, se observan ocho columnas, de las cuales la columna 2, 3 y 5 tienen números y estos hacen ternas pitagóricas, se pueden detallar de la siguiente manera; si se elevan al cuadrado los números que se

[1] Tablilla qué pertenece a la colección Plimpton de la Universidad de Columbia (EE.UU), en Nueva York, la cual se encuentra catalogada con el número 322.

encuentran en la segunda y tercera columna y se realizar una resta generan un tercer número elevado al cuadrado ($z^2 - y^2 = x^2$ con $z > y$), se detallara un ejemplo, se seleccionan los números que se encuentran en las dos columnas de la 4 fila *12709* y *18541*, respectivamente.

$$18541^2 - 12709^2 = 343768681 - 161518681 = 182250000$$

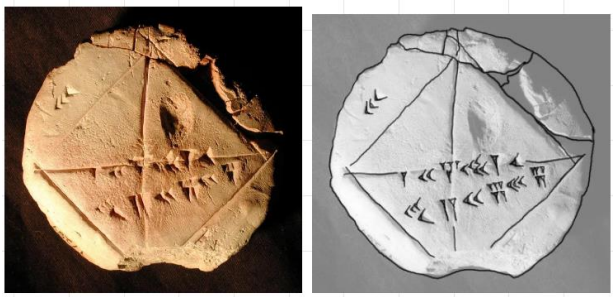
$$18541^2 - 12709^2 = 13500^2$$

Con lo anterior los babilonios utilizaban ya unos números cuadrados conocidos, para obtener otros usando operaciones entre ellos.

I, $\left(z/x\right)^2$	II, y	III, z	IV	x	p	q	α
[1, 59, 0,] 15 1.98340277	1, 59 119	2, 49 169	1	2, 0 120	12 12	5 5	44° 45' 37''
[1, 56, 56,] 58, 14, 50, 6, 15 (*) 1.949158552	56, 7 3367	**3, 12, 1** 1, 20, 25 11521 4825	2	57, 36 3456	1, 4 64	27 27	44° 15' 10''
[1, 55, 7,] 41, 15, 33, 45 1.918802127	1, 16, 41 4601	1, 50, 49 6649	3	1, 20, 0 4800	1, 15 75	32 32	43° 47' 14''
[1,] 5[3, 1]0. 29, 32, 2, 16 1.886247907	3, 31, 49 12709	5, 9, 1 18541	4	3, 45, 0 13500	2, 5 125	54 54	43° 16' 17''
[1,] 48, 54, 1, 40 1.815007716	1, 5 65	1, 37 97	5	1, 12 72	9 9	4 4	42° 04' 30''
[1,] 47, 6, 41, 40 1.785192901	5, 19 319	8, 1 481	6	6, 0 360	20 20	9 9	41° 32' 40''
[1,] 43, 11, 56, 28, 26, 40 1.719983676	38, 11 2291	59, 1 3541	7	45, 0 2700	54 54	25 25	40° 18' 55''
[1,] 41, 33, 59, 3, 45 (**) 1.692773438	13, 19 799	20, 49 1249	8	16, 0 960	32 32	15 15	39° 46' 18''
[1,] 38, 33, 36, 36 1.642669445	**9, 1** 8, 1 (***) 541 481	12, 49 769	9	10, 0 600	25 25	12 12	38° 47' 05''
1, 35, 10, 2, 28, 27, 24, 26, 40 1.586122566	1, 22, 41 4961	2, 16, 1 8161	10	1, 48, 0 6480	1, 21 81	40 40	37° 26' 14''
1, 33, 45 1.5625	45 45, 0 (****) 45 2700	**1, 15** 1, 15, 0 75 4500	11	1, 0 60 3600	1, 0 60	30 30	36° 52' 12''
1, 29, 21, 54, 2, 15 1.489416843	27, 59 1679	48, 49 2929	12	40, 0 2400	48 48	25 25	34° 58' 34''
[1,] 27, 0, 3, 45 (*****) 1.450017361	**7, 12, 1** 2, 41 (******) 25921 161	4, 49 289	13	4, 0 240	15 15	8 8	33° 51' 18''
1, 25, 48, 51, 35, 6, 40 1.43023882	29, 31 1771	53, 49 3229	14	45, 0 2700	50 50	27 27	33° 15' 43''
[1,] 23, 13, 46, 40 1.387160494	**56** 28 56 28	**53** 1, 46 53 106	15	1, 30 90 45	9 9	5 5	31° 53' 27''

Tabla 1: Traducción de la tablilla de arcilla

La columna I y II, hacen referencia a un lado y a la diagonal de diversos cuadrados, una ilustración de lo que se está empleando en esta tabla, lo da la *(figura 2)*. En las columnas VI y VII, aparecen los valore de *p* y *q* los cuales se interpretan como la parametrización diofántica, que se trataran más adelante y se hará una interpretación de la misma.



Tablilla cuneiforme YBC 7289 (1900 a.C.) representando un cuadrado de lado 30, con diagonal 42; 25, 35 cuyo cociente es 1; 24, 51, 10

Figura 2: *Interpretación de los números cuadrados.*

Todo lo anterior permite denotar que los babilonios dieron una interpretación al teorema de Pitágoras, pero ellos lo usaban para hallar longitudes a las diagonales de cuadrados, y al trabajar con dichas longitudes los llevaba a trabajar con números racionales como $\sqrt{2}$. Además de lo anterior en la historia se encuentra qué los babilonios ya conocían algunos números cuadrados, lo cual permitió que ellos hicieran procesos que los llevaban al uso de ternas pitagóricas, por esa razón en muchos textos se habla del trabajo que han tenido los babilonios, en cuanto a los números cuadrados.

2.2. Griegos

Los griegos por su parte en el siglo IV a.C. con el pitagórico Thymaridas de Paros propuso un método para resolver sistemas particulares de *n* ecuaciones lineales con *n* incógnitas afirmando que, si se conoce la suma de varias incógnitas, así como también las sumas parciales de una de ellas con cada una de las otras, y se suman todas estas sumas parciales, restando después la primera suma total y se divide la diferencia por el número de incógnitas disminuido en 2, se obtiene el valor de la primera; y de éste se deducen los demás"

Con la notación actual obtendríamos:

$$\begin{cases} x + x_1 + x_2 + \cdots + x_{n-1} = s \\ x + x_1 = k_1 \\ x + x_2 = k_2 \\ x + x_3 = k_3 \\ \vdots \\ x + x_{n-1} = k_{n-1} \end{cases}$$

Así

$$x = \frac{(k_1 + k_2 + k_3 + \cdots + k_{n-1}) - s}{n - 2}$$

En el siglo III donde la teoría de números una de las disciplinas de estudio favoritas de los Griegos, aparecieron las ecuaciones diofánticas a través de la obra del matemático

Griego Diofánto de Alejandría (Siglo III d.C) *Aritmética,* siendo allí donde tomaron su nombre de ecuaciones *Diofantinas* o *Diofánticas* como hoy las conocemos. Diofánto, un aritmético puro a diferencia de los matemáticos Griegos en su mayoría geómetras, plantea en su obra un tratado de 12 libros (de los cuales solo se conocen los 6 primeros), un compilado de problemas basados sobre la teoría de números, algunos disfrazados con un lenguaje aparentemente geométrico pero que en el fondo tratan sobre los números los cuales son enunciados de forma retórica, pero donde ya comenzaban a mezclarse algunos símbolos y abreviaturas que ayudaban al razonamiento de los problemas, dicho planteamiento a través de símbolos se denominó el "álgebra sincopada".

En estos libros se logran encontrar ecuaciones de diferentes grados y con varias incógnitas, pero en este trabajo se destacará ecuaciones de dos tipos en particular a las que Diofánto encuentra solución; la ecuaciones de la forma $ax - by = c$ sin estar sujeta a un sistema, la cual es utilizada por Diofanto para resolver problemas puramente matemáticos y es tratada en el libro I de *aritmética* y las ternas pitagóricas o ecuaciones de la forma $a^2 + b^2 = c^2$ que igualmente abarcan problemas sobre la descomposición de cuadrados y algunos problemas de aplicación en particular.

Al solucionar problemas puramente matemáticos con el uso de la ecuación $ax - by = c$, Diofánto propone una solución en términos de parametrización que será desarrollada en el siguiente capítulo, por otro lado también propone soluciones a sistemas de ecuaciones lineales en un lenguaje retórico donde el proceso que involucra de fondo y que no difiere mucho en relación a lo que hacemos hoy en día, es plantear las relaciones o ecuaciones entre cantidades en términos de una sola incógnita para resolver un sistema de ecuaciones simultáneas lineales utilizando el hecho de que se conoce la diferencia como operación, luego siempre es posible escribir una incógnita en términos de la otra como se verá en el siguiente ejemplo del libro I, (problema 1):

"Descomponer un número en dos partes cuya diferencia sea dada."

Suponga que sea 100 el número a descomponer y 40 la diferencia dada. Esto lleva a encontrar dos números tales que su suma sea 100 y su diferencia 40. Diofánto plantea su solución mediante un juego de palabras donde relaciona todas las cantidades, las opera y finalmente establece la solución; la solución en términos de Diofánto es:

Suponiendo que la parte menor es 1 aritmo[2]*, la mayor será 1 aritmo más 40 unidades, y, por tanto, la suma de ambas valdrá 2 aritmos más 40 unidades, la cual suma es 100. Restando los términos semejantes de los semejantes, es decir: 40 unidades de 100 y 40 unidades de 2 aritmos y 40 unidades, los 2 aritmos que quedan valdrán 60 unidades y cada aritmo 30, que será la parte menor, y la mayor 30 más 40, o sea: 70 unidades"*

[2] *Aritmo* es la forma como Diofanto llamó en el inicio del algebra sincopada a la incógnita.

Muy similar al método de Cardano, donde se logra ver como establece algunas relaciones entre el aritmo y los números y a partir de las operaciones llega a la solución buscada.

Por otra parte, en cuanto a las ternas pitagóricas de Diofánto hay que tener en cuenta lo siguiente: dados tres números *a, b* y *c* naturales no nulos, que satisfagan la ecuación $a^2 + b^2 = c^2$ se les llamará ternas pitagóricas, la cual a y b son magnitudes que pertenecen a los catetos y *c* a la hipotenusa de un triángulo pitagórico. Además de esto si el $mcd(a, b, c) = 1$ se llamará terna primitiva.

Diofánto, en el problema número 8 del libro II de *aritmética*, propone el siguiente ejemplo:

"Descomponer el cuadrado dado en dos cuadrados"

"Si queremos descomponer el número 16 en dos cuadrados y suponemos qué el primero es el cuadrado de un aritmo, el otro tendrá 16 unidades menos un cuadrado de aritmo, son un cuadrado. Formamos el cuadrado de un conjunto cualquiera de aritmos disminuidos en tantas unidades como tiene la raíz de 16 unidades, y sea el cuadrado de 2 aritmos menos 4 unidades"

$$16 = x^2 + (16 - x^2)$$
$$16 - x^2 = y^2$$
$$y^2 = (2x - 4)^2 = 4x^2 + 16 - 16x$$
$$16 - x^2 = 4x^2 + 16 - 16x$$
$$5x^2 = 16x$$
$$x = \frac{16}{5}$$
$$16 = \frac{256}{25} + \frac{144}{25}$$
$$16 = \left(\frac{16}{5}\right)^2 + \left(\frac{12}{5}\right)^2$$

Lo que pretendía Diofánto con esto era identificar a $16 - x^2$ con una expresión del tipo $\left(mx - \sqrt{16}\right)^2$. Para así obtener la terna pitagórica $\left(2pq, p^2 - q^2, p^2 + q^2\right)$, que se le atribuye a la parametrización de Diofánto de Alejandría, que también será desarrollada en el siguiente capítulo.

De esta manera se puede ver como Diofánto da solución a las ecuaciones de la forma $ax + by = c$ estableciendo relaciones entre valores conocidos y desconocidos de modo que la solución pueda ser planteada en términos de una variable, incluyendo de manera implícita la solución de un sistema de ecuaciones (mediante sustitución), pero sin tener

que recurrir a dicho proceso. Por otro lado para dar solución a las ternas pitagóricas Diofánto recurre a una sustitución no muy evidente $\left(mx-\sqrt{16}\right)^2$ desde una visión histórica ya que la información que brindan algunos documentos no es clara en torno al artificio utilizado por el matemático de Alejandría.

2.3. India

Durante el siglo VI el gran matemático y astrónomo Hindú Brahmagupta trabajó con ecuaciones lineales presentando una solución general a la ecuación lineal de primer grado, incluso también a la ecuación de segundo grado. En relación con la primera que es de nuestro interés propuso una afirmación que muestra la importancia que para este significo su método *kutakka* o en nuestro idioma el método pulverizador, "*Quien conozca el uso del método pulverizador así como las cifras, las cantidades positivas y negativas, la eliminación del término medio y las expresiones, llegará a ser un maestro entre los sabios." (Vera, 1970)*

El método consiste en hacer divisiones entre los coeficientes de las variables, e involucrar una nueva variable, hasta que el residuo sea nulo. Para resolver una ecuación de la forma $ax + by = c$, este método se asemeja al método de Diofánto. El método pulverizador también será desarrollado en el siguiente capítulo.

2.4. El desarrollo posterior a las civilizaciones antiguas

En el siglo VII los árabes recorrieron el suroeste del Mediterráneo, hecho que les permitió recopilar manuscritos y trabajos relacionados con el álgebra. Entre estos se encontraba la *Aritmética* o al menos una parte de ella. Las primeras traducciones y comentarios fueron publicados en árabe pero de estos no se conoce documento alguno, los únicos rastros están en las referencias de los bibliógrafos. Cuando los árabes plantearon sus ideas sobre álgebra aparentemente siguieron la tradición básica oriental basada en ideas geométricas, ya que no se logran observar notaciones algebraicas ni abstracciones generalizadas sobre números abstractos. Además ningún problema de la *Aritmética* ha sido encontrado en el álgebra de Al-khwarizmi o en los textos de álgebra oriental. Probablemente los árabes encontraron a Diofánto poco práctico para sus matemáticas utilizadas. Al-khwarizmi en su trabajo del algebra explica la forma de resolver una ecuación de segundo grado, para ello hacia uso de la geometría, estas ecuaciones de segundo grado se consideran en este trabajo como diofánticas puesto que el solo consideraba soluciones enteras y positivas, veamos un ejemplo:

Sea la ecuación $x^2 + 10x - 39 = 0$, Al-khwarizmi expresaba la ecuación de manera positiva ya que hacia representación geométrica de la misma, utilizando longitudes y áreas y estas no pueden ser negativas, por lo tanto la ecuación queda expresada $x^2 +$

$10x = 39$. El problema de resolver la ecuación, equivale a encontrar el lado del cuadrado amarillo de la *figura 3*. El primer término de la ecuación es x^2; es decir, el área del cuadrado amarillo. La suma de los cuatro rectángulos de color violeta es $4 \cdot 25x$, o bien $10x$, que es el segundo término de la ecuación. El área de los cuadrados verdes es $4 \cdot (2.5 \cdot 2.5) = 25$.

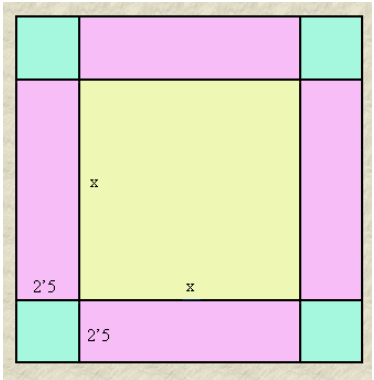


Figura 3: *Representación geométrica de Al-khwarizmi*

Ahora el área del cuadrado completo es $(x + 5)^2$ y este debe ser igual a la suma de las nueve partes que lo forman es decir:

$$(x + 5)^2 = x^2 + 10x + 25 = 39 + 25$$

Es decir $(x + 5)^2 = 39 + 25 = 64$, ahora extrayendo la raíz cuadrada de ambos miembros que tenemos se obtiene:

$$x + 5 = 8$$

Por lo tanto $x = 3$. Y de esta forma se solucionaba ecuaciones cuadráticas.

Luego del siglo VIII se presentó un estancamiento en el desarrollo de las ecuaciones diofánticas, en espacial durante la edad media, tiempo en el que los manuscritos de Diofánto permanecieron casi intactos por más de ocho siglos. La historia no da cuenta de cuando los libros faltantes de *Aritmética* fueron perdidos, pero la parte que actualmente se conoce (libros del I al VI) escapó al saqueo de Constantinopla por las Cruzadas en el año *1204* y posteriormente en el mismo siglo.

En el siglo X un musulmán conocido como Abul Kamil, continuó con los trabajos de Al-khwarizmi y fue hasta el XIII que el matemático Leonardo de pisa más conocido como Fibonacci aprovecho los aportes de Al-khwarizmi.

Luego en el periodo de la emigración de los sabios bizantinos, durante las conquistas turcas, las copias fueron enviadas a Italia entre los años *1461* y *1464*, cuestión que llevó

a la primera traducción al latín, hecha por W. Holzmann quién escribió bajo la versión griega de nombre X'ylander y publicada en el año *1575*.

Mientras tanto Bombelli, en *1572* publicó cuatro libros de álgebra con problemas entre ellos algunos de su autoría. Bachet, quién retomo las ideas de Bombelli y Holzmann hizo otra traducción en el año *1621* y publicó una segunda edición que publicó en *1670*, incluyendo algunas notas marginales de Fermat.

Ya en los años de 1600 a 1670 un matemático conocido cómo Pierre de Fermat acostumbraba a escribir las soluciones de problemas al margen de los libros. Fermat escribió en una de sus notas un ejemplar del texto griego de la aritmética de Diofánto, en el cual se puede citar lo que se conoce como el último teorema de Fermat:

"Es imposible encontrar la forma de convertir un cubo en la suma de dos cubos, una potencia cuarta en la suma de dos potencias cuartas, o en general cualquier potencia más alta que el cuadrado, en la suma de dos potencias de la misma clase. He descubierto para el hecho una demostración excelente. Pero este margen es demasiado pequeño para que (la demostración) quepa en él"(Bachet, 1621)

Dado lo anterior, muchos matemáticos se interesaron por demostrar dicho teorema, y lo que provocó esto fue la generación de nuevas ecuaciones diofánticas y métodos para resolverlas, un ejemplo para esto puede ser la ecuación Diofántica de la forma $x^2 + 3y^2 = z^3$, observemos el método de solución dado por Francois Viète:

Se toman dos números a y b primos entre sí, tal qué $a^3 > 9ab^2$, Viète genero la siguiente parametrización para resolver estas ecuaciones, $x = a^3 - 9ab^2, y = 3a^2b - 3b^3$ y $z = a^2 + 3b\hat{}2$. Ahora miremos el siguiente ejemplo, pero no con la condición establecida por viète con: $a = 3$ y $b = 2$ se verifica qué $a^3 = 27 < 9ab^2 = 108$, ahora se tiene que $x^2 + 3y^2 = z^3$ de donde:

$$(-81)^2 + 3(30)^2 = 21^3$$
$$6561 + 2700 = 9261$$

La anterior se considera ecuación Diofántica ya que sus coeficientes y su solución son expresadas en el conjunto de los números enteros, así también se puede indagar en ecuaciones como $x^2 - y^2 = z^3, x^3 + y^3 + z^3 = t^3$ entre otras, producto de la búsqueda en la demostración del último teorema de Fermat.

En los siglos XVIII y XIX se publicaron varias traducciones en diversos idiomas y basadas en las primeras ediciones mencionadas por Bachet y Holzmann, llegando a un trabajo final en *1890* de P. Tannery quien propuso una edición definitiva al texto griego "*La aritmética"*.

Sin duda muchos de los problemas que resolvió Diofánto se originaron en la teoría de números y su propósito fue buscar soluciones enteras para las ecuaciones que generaban tales problemas, estudio que posteriormente llevó al surgimiento de la rama de la teoría de números dedicada al trabajo con tales ecuaciones, conocido como *análisis Diofántico*. Dicho trabajo llevo a matemáticos como Fermat y Euler a desarrollar métodos enfocados a solucionar la ecuación $ax + by = c$, a continuación se muestra el método ingeniado por este último.

2.5. Euler

Euler por su parte, involucra un método simple que se repite varias veces, es fácil de aplicar, y para su desarrollo requiere el proceso de la división y las propiedades de los enteros bajo la suma y multiplicación. Este proceso es cómodo al ser más corto que el algoritmo de Euclides. Para ejemplificar se resolverá la siguiente ecuación diofántica

$$738x + 621y = 45$$

En primer lugar se observa si la ecuación tiene solución, para ello se busca el máximo común divisor entre a y b, en esta caso $a = 738$ y $b = 621$ y como $m.c.d.(728, 621) = 9$, la ecuación tiene solución ya que $9|45$

El método comienza despejando y,

$$y = \frac{45 - 738x}{621} = -x + \frac{-117x + 45}{621}$$

Como x, y deben ser enteros, se llama t a la fracción, por tanto:

$$t = \frac{-117x + 45}{621}, \qquad \text{con } t \in \mathbb{Z},$$

De aquí:

$$621t = -117x + 45$$

Ahora se realiza lo mismo con x, por tanto:

$$x = \frac{-621t + 45}{117} = -5t + \frac{-36t + 45}{117}$$

Y siendo

$$u = \frac{-36t + 45}{117}$$

Se tiene:

$$x = -5t + u$$

Ahora se despejando *t* se tiene:

$$t = \frac{-117u + 45}{36} = -3u + 1 + \frac{-9 + 9}{36} = -3u + 1 + v$$

Donde

$$v = \frac{-9u + 9}{36}, \qquad v \in \mathbb{Z}$$

Y por lo tanto

$$u = -4v + 1.$$

Una solución podría ser cuando $v = 0$, y por consiguiente $u = 1,\ t = -2$, de donde $x = 11,\ y = -13$ es una solución.

La solución general está dada por

$$u = -4v + 1$$
$$t = -3u + 1 + v = 13v - 2$$
$$x = -5t + u = -69v + 11$$
$$y = -x + t = 82v - 13$$
$$t, u, v, x\ e\ y\ \in \mathbb{Z}$$

Y de esta manera Euler resolvía ecuaciones diofánticas.

3. Algunos métodos de solución a ecuaciones Diofánticas

En este capítulo se hará un análisis de los diferentes métodos de solución que se encuentran al solucionar ecuaciones diofánticas de la forma $ax + by = c$ y $x^2 + y^2 = z^2$, algunos de estos fueron selectos por interés del autor y otros que fueron encontrados y se estudiaron desde la historia.

3.1. Ecuaciones diofánticas de la forma $ax + by = c$ sin estar sujetas a un sistema de ecuaciones lineales

3.1.1 Método de la falsa posición

Uno de los recursos que se puede utilizar para hallar soluciones a ecuaciones diofánticas de la forma $ax + by = c$ es utilizando el método conocido como falsa posición, desarrollado por los egipcios, aclarando que el método que se desarrollará en este ítem no es el mismo, se partirá de algo similar, pero este método fue propuesto en el seminario de matemáticas de la especialización 2014. Observe un ejemplo:

Sea la ecuación $3x + 7y = 27$ con la aclaración, de que solo se buscaran soluciones en el conjunto de los números enteros; ahora se realizará lo siguiente: Se asignaran dos valores cualquiera a las variables x e y por ejemplo $x = 4, y = 6$, con esto se obtiene:

$$3(4) + 7(6) = 12 + 42 = 54$$

Posteriormente se realiza una proporción entre los resultados obtenidos y los valores dados a las variables, de tal manera qué:

$$\frac{27}{54} = \frac{x}{4} = \frac{y}{6}$$

De dónde:

$$\frac{x}{4} = \frac{27}{54} \rightarrow x = 2 \text{ y } \frac{y}{6} = \frac{27}{54} \rightarrow y = 3.$$

Ahora este procedimiento permite hallar soluciones no necesariamente enteras si no racionales. La condición estricta que debe tener este método para hallar soluciones en el conjunto de los números enteros es la siguiente; si se tiene una ecuación diofántica de la forma $ax + by = c$ al momento de asignar los valores falsos $x = x_1$ e $y = y_1$ y reemplazarlos en la ecuación original su resultado debe ser un número que sea múltiplo o divisor del resultado original es decir, $ax_1 + by_1 = d$ dónde $d = ec$ y además $e = m.c.d.(x_1, y_1)$. Desde lo anterior se puede hallar solución entera a la ecuación diofántica dada, y no solo una se pueden hallar múltiples. Además de eso se podrá establecer una proporción entre los valores falsos y los valores verdaderos, no obstante

se tendría problemas con valores falsos como él 0 ya que en la proporción que se establece habrá una división por 0 y esto es algo no determinado.

Ahora de manera general se obtiene qué:

Sea la ecuación diofántica $ax + by = c$ se asignaran los valores falsos $x = x_1$ e $y = y_1$ con $x_1 \neq 0$ e $y_1 \neq 0$ de modo que ahora se obtiene la ecuación $ax_1 + by_1 = d$ con $d = cf$, de este modo se establece la siguiente proporción

$$\frac{c}{d} = \frac{x}{x_1} = \frac{y}{y_1}$$

Deduciendo qué:

$$\frac{x}{x_1} = \frac{c}{d} \rightarrow x = x_1 \frac{c}{d}$$

$$\frac{y}{y_1} = \frac{c}{d} \rightarrow y = y_1 \frac{c}{d}$$

Partiendo de lo anterior, se puede deducir el siguiente teorema:

Teorema: Sea la ecuación diofántica $ax + by = c$, sean $x = x_1$ e $y = y_1$ con $x_1, y_1 \in \mathbb{Z}$ valores falsos tal que $ax_1 + by_1 = d$, si se tiene que $d = cf$ y $f = m.c.d.(x_1, y_1)$ entonces los valores de x y y pertenecen al conjunto de los números enteros.

El siguiente paso es justificar el porqué de este método, primero se tiene que establecer que en este método hay que incurrir en el tanteo para poder hallar soluciones enteras ya que se desea buscar un d tal que $d = cf$ y ese $f = m.c.d(x_1, x_2)$; para la justificación de este método f toma un papel fundamental, ya que $f = mcd(x_1, y_1)$ teniendo esto se tiene lo siguiente, dadas las proporciones:

$$\frac{c}{d} = \frac{x}{x_1} = \frac{y}{y_1}$$

Como $d = cf$ se tiene:

$$\frac{c}{cf} = \frac{x}{x_1} = \frac{y}{y_1}$$

$$\frac{1}{f} = \frac{x}{x_1} = \frac{y}{y_1}$$

Luego se tiene qué

$$\frac{1}{f} = \frac{x}{x_1} \text{ y } \frac{1}{f} = \frac{y}{y_1}$$

$$x = \frac{x_1}{f} \text{ y } y = \frac{y_1}{f}$$

Y como $f = m.c.d.(x_1, y_1)$, entonces $f|x_1$ y $f|y_1$, de dónde se concluye qué

$$x = \frac{x_1}{f} = g \text{ y } y = \frac{y_1}{f} = h \text{ con } g, h \in \mathbb{Z}$$

Y de esta manera se trata de justificar el método, esto nos lleva al siguiente teorema:

Teorema: Sean $a, b, c \in \mathbb{Z}$. La ecuación diofántica $ax + by = c$ tiene solución entera si, y sólo si el máximo común divisor de a y b divide a c.

Demostración:

Supongamos que los números enteros x_0 e $y_0$son solución a la ecuación $ax + by = c$, con esto se tiene qué $ax_0 + by_0 = c$. Luego si $d = mcd(a, b)$, entonces

$$d = mcd(a, b) \rightarrow d|a \text{ y } d|b \rightarrow d|(ax_0 + by_0) \rightarrow d|c$$

3.1.2 El Algoritmo de Euclides en la solución de ecuaciones Diofánticas

Antes de observar los métodos para resolver ecuaciones de la forma $ax + by = c$ se analizará el algoritmo de Euclides, ya que este se utiliza en la mayoría de métodos:

A pesar de la concepción griega acerca de la matemática en dónde los números se entendían como magnitudes geométricas, el algoritmo de Euclides que se utilizó en la geometría como primera medida, se extendió a la teoría de números para hallar el máximo común divisor entre dos números a y b enteros que se denotara $m.c.d(a, b)$. Euclides en su libro VI en la proposición I.2 establece un método qué permite hallar la mayor medida común posible de dos segmentos (números), estableciendo lo siguiente:

Dados dos segmentos con magnitudes AB y CD, con $AB > CD$, restamos CD de AB tantas veces como sea posible. Si no hay residuo, entonces CD es la máxima medida común. Si se obtiene un residuo EA, éste es menor que CD y podemos repetir el proceso, es decir, restamos EA tantas veces como sea posible de CD, si al final no queda un residuo, EA es la medida común. En caso contrario obtenemos un nuevo residuo FC menor a EA, el proceso se repite hasta que en algún momento no se obtiene residuo. Entonces el último residuo obtenido es la mayor medida común.

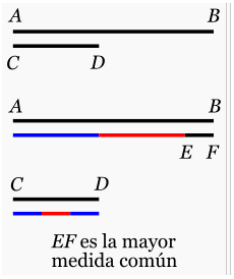


Figura 3: *Representación gráfica Algoritmo de Euclides*

Aunque el algoritmo y sus argumentos son geométricos, existe un algoritmo similar para ser aplicado de forma numérica.

Teorema[3] Sean $a, b \in \mathbb{Z}$ con $b > 0$ entonces existen dos enteros $q, r \in \mathbb{Z}^+$ únicos, tales que $a = bq + r$ con $0 \leq r < |b|$.

Ahora se darán unos ejemplos de este:

1. Sean los números 35 y 12, entonces por el algoritmo de la división se obtiene qué:

$$35 = 12 \cdot 2 + 11$$

2. Ahora sean los números -28 y 27, por lo algoritmo de la división se obtiene qué

$$-28 = 27(-2) + 26$$

Desde lo anterior; el algoritmo de Euclides y el algoritmo de la división, se establecerá en ciertos métodos para la solución a ecuaciones diofánticas, no obstante se harán ciertas variaciones a estos métodos que serán los siguientes:

1. Euclides en su algoritmo utiliza magnitudes mayores que 0, en estos métodos se utilizarán magnitudes que pertenezcan al conjunto de los números enteros.
2. En las magnitudes de Euclides, el establece que $AB > CD$, en el presente trabajo se tomaran dos números enteros tales que $a > b$ o $a < b$
3. Y por último en el algoritmo de la división se establece que $\exists q, r \in \mathbb{Z}^+ \ / \ a = bq + r$ con $0 \leq r < b$, en este trabajo $q, r \in \mathbb{Z}$

Ahora para hallar el $m.c.d.(a, b)$ se utiliza el algoritmo de la división repetitivamente hasta qué el residuo sea nulo (del mismo modo que Euclides obtenía la mayor medida común entre dos magnitudes) teniendo esto el último residuo mayor que cero es el $m.c.d.(a, b)$ es decir:

$$a = bq + r$$
$$b = rq_1 + r_1$$
$$r = r_1 q_2 + r_2$$

[3] La demostración de este teorema se puede encontrar en libros de teoría de números

$$\vdots$$

$$r_{n-1} = r_n q_{n+1} + r_{n+1}$$
$$r_n = r_{n+1} q_{n+2} + 0$$

Realizando este procedimiento se tendría que $m.c.d.(a,b) = r_{n+1}$ y con esto se tendría el algoritmo de Euclides de forma numérica. Observe un ejemplo:

Sean 252 y 198

$$252 = 198 \cdot 1 + 54$$

$$198 = 54 \cdot 3 + 36$$

$$54 = 36 \cdot 1 + 18$$

$$36 = 18 \cdot 2 + 0$$

Luego el $m.c.d(252, 198) = 18$

Ahora teniendo en cuenta esto, con el algoritmo de Euclides se puede hallar el $m.c.d.(a,b)$, y este se expresar como una combinación lineal, es decir $sean\ a, b \in \mathbb{Z}$ y $m.c.d.(a,b) = c$ se tiene qué $c = ax + by$, este se tiene por el lema de Bezout qué establece lo siguiente:

Teorema: Si $a, b \in \mathbb{Z}$, con $m.c.d(a,b) = c$,entonces existen enteros x y y tales que

$$c = ax + by$$

El anterior teorema garantiza la existencia de un número que se puede expresar como combinación lineal, y este es el menor entero positivo, pero no deduce cual es, quien permite hallar ese número es el Algoritmo de Euclides. Observe el siguiente ejemplo:

Sean 252 y 198, utilizando el algoritmo de Euclides se tiene qué el $m.c.d.(252{,}198) = 18$, y por el lema de Bezout se establece la siguiente ecuación:

$$252x + 198y = 18$$

Ahora deducida la anterior ecuación se le llamara ecuación diofántica lineal, y el método que se empleará en esta sección es el siguiente.

Primero se intuirá que tiene solución, teniendo en cuenta esto se realizara el algoritmo de la división hasta hallar el máximo común divisor, cada vez que se realice el algoritmo de la división se despejara el residuo. Observe el ejemplo

Sea la ecuación $252x + 198y = 18$, con esto se tiene qué

$$252 = 198 \cdot 1 + 54 \qquad \rightarrow \qquad 1) \quad 54 = 252 - 198 \cdot 1$$

$$198 = 54 \cdot 3 + 36 \quad \rightarrow \quad 2) \quad 36 = 198 - 54 \cdot 3$$

$$54 = 36 \cdot 1 + 18 \quad \rightarrow \quad 3) \quad 18 = 54 - 36 \cdot 1$$

Teniendo esto se empieza a sustituir valores, se sustituye 2) en 3) lo cual queda:

$$18 = 54 - (198 - 54 \cdot 3)$$

Por lo tanto:

$$4) \quad 18 = 54(4) - 198$$

Luego se sustituye 1) en 4):

$$18 = (252 - 198 \cdot 1)4 - 198$$

Llegando así a:

$$18 = 254(4) + 198(-5)$$

Y así se obtienen una solución particular a la ecuación, la cual es $x = 4$ y $y = -5$ es así como se halla una solución a la ecuación Diofántica establecida como combinación lineal del $m.c.d(253,198)$

Ahora observe el siguiente ejemplo:

$$22x + 31y = 128$$

Aplicando el algoritmo de Euclides para hallar el máximo común divisor se obtiene qué $m.c.d(22,31) = 1$ y por el lema de Bezout se tiene qué:

$$22x + 31y = 1$$

Y realizando el procedimiento qué se utilizó para resolver la ecuación $252x + 198y = 18$, se obtienen las soluciones $x = -7$ y $y = 5$, pero como la ecuación a solucionar es $22x + 31y = 128$, y no $22x + 31y = 1$, se multiplican las soluciones encontradas por 128 y se llega a dos soluciones que serán $x = -896$ y $y = 648$.

Después de lo anterior, surge una pregunta, ¿cómo encontrar más soluciones, sin tener que realizar el método reiteradamente?, una solución a esta pregunta es la siguiente:

Sea la ecuación $ax + by = c$ con $x = x_0$ y $y = y_0$ dos soluciones particulares, otra solución que se le puede dar a la solución es $x = x_0 + b$ y $y = y_0 + (-a)$, observe que esta es otra solución:

$$a(x_0 + b) + b\big(y_0 + (-a)\big) = ax_0 + ab + by_0 - ab = ax_0 + by_0$$

Por lo anterior se tiene que $ax_0 + by_0 = c$, por lo anterior se tiene qué $x = x_0 + b$ y $y = y_0 + (-a)$ son soluciones a la ecuación lineal diofántica $ax + by = c$.

Evidentemente se pueden hallar las soluciones generales a partir de la solución general, esto es; Sea $ax + by = c$ con $x = x_0$ y $y = y_0$ dos soluciones particulares, otra solución que se le puede dar a la solución es $x = x_0 + b$ y $y = y_0 + (-a)$, se tiene que las soluciones generales a la ecuación serán de la forma:

$$x = x_0 + kb \text{ y } y = y_0 + (-ka) \text{ con } k \in \mathbb{Z}$$

3.1.3 Método de Diofánto

Diofánto por su parte, trabajo en la solución de ecuaciones $ax + c = by$ sin estar sujeta a un sistema, (Van Der Waerden, 1985) en su libro plasma el método en el cual Diofánto utiliza el algoritmo de Euclides, para hallar soluciones a estas ecuaciones que lo veremos esbozado a continuación:

Sea la ecuación $29x + 4 = 8y$, para solucionarla primero debemos determinar el $mcd(29,8)$ ya que este debe dividir a 4 es importante que el máximo común divisor de a y b divida a 4, si no es así se debe buscar una ecuación equivalente a la dada que tenga como $mcd(a, b) = 1$, verificado a esto se procederá a utilizar el algoritmo de Euclides establecido para teoría de números, de tal manera qué:

$8 = 29(0) + 8$, de esta manera se expresará de la siguiente forma $x = 0y + z$

Luego se realiza la división del divisor entre el resto de tal forma qué

$29 = 8(3) + 5$, expresándola de forma $y = 3z + t$

Continuamos con $8 = 5(1) + 3$, expresándola como $z = 1t + u$

Ahora $5 = 3(1) + 2$, expresándola como $t = 1u + v$

Luego $3 = 2(1) + 1$, expresándola como $u = 1v + w$

Desde lo anterior Diofánto establece que las divisiones se realizan hasta que el residuo sea 1, luego de eso hay que observar cuantas divisiones se efectuaron en nuestro caso fueron 5, esto es importante para establecer un c' que será negativo cuando el número de divisiones sea impar y será positivo cuando el número de divisiones sea par, agregado a esto esté viene dado de la forma $c' = -c$ en este caso es negativo porque el número de operaciones efectuadas es impar, de esta manera nuestro $c' = -4$, luego de esto se establece lo siguiente $v + c' = gw$ de los cuales c' ya se conoce y g es el residuo de la penúltima división, de este modo se obtiene qué:

$$v - 4 = 2w$$

Cuando se llega a estese le asigna un valor cualquiera a w y se obtiene el v, luego de obtener el v y como ya se conoce el w nos devolvemos a las expresiones que habíamos dejado con las ecuaciones, llegando así a obtener los valores de x e y. Para nuestro caso

asignamos un valor de $w = 2$ y con este obtuvimos como soluciones a $x = 24$ y $y = 87$ quienes son soluciones a la ecuación diofántica planteada. Ahora con este método se pueden obtener infinitas soluciones en los números enteros.

Ahora de manera general.

Sea la ecuación $ax + c = by$ ahora el $mcd(a, b) = d$ tal que $d \,/\, c$, ahora efectuaremos las divisiones

$$b = ka + s \text{ De dónde } x = ky + z$$

$$a = k_1 s + s_1 \text{De dónde } y = k_1 z + t$$

$$s = k_2 s_1 + s_2 \text{ De dónde } z = k_2 t + t_1$$

$$\vdots$$

$$s_n = k_{n+2} s_{n+1} + 1 \text{ De dónde } t_{n-1} = k_{n+2} t_n + t_{n+1}$$

Luego de eso se obtiene

$$t_n + c' = k_{n-1} t_{n+1}$$

Se le asigna un valor cualquiera a $t_{n+1} = e$ de tal manera qué $t_n = k_{n-1} e - c'$ y luego se empieza a reemplazar en las expresiones obtenidas al realizar las divisiones. Ahora observe por qué funciona y de dónde se establecen las parametrizaciones:

Sea la ecuación $ax + c = by$ ahora el $mcd(a, b) = d$ tal que $d \,/\, c$, en la forma generales se realizó el algoritmo de Euclides, ahora se analizará cada algoritmo de la división, se tenía qué $b = ka + s$, reemplazando en la ecuación original se tiene qué:

$$ax + c = (ka + s)y$$

De dónde $ax + c = kay + sy \rightarrow a[x - ky] + c = sy$, ahora se realizara la siguiente sustitución, sea $z = x - ky$, de lo cual se obtiene la siguiente ecuación:

$$az + c = sy$$

De la sustitución realizada se obtiene qué $\boldsymbol{x = ky + z}$, ahora se continúa con la ecuación $az + c = sy$, se tiene qué $a = k_1 s + s_1$reemplazando en la nueva ecuación se tiene qué:

$$(k_1 s + s_1)z + c = sy$$

Ahora $k_1 sz + s_1 z + c = sy \rightarrow s_1 z + c = s(y - k_1 z)$, ahora sea $t = y - k_1 z$, de la cual se obtiene una nueva ecuación qué es:

$$s_1 z + c = st$$

Ahora por la segunda sustitución, se puede establecer la segunda parametrización que será $y = k_1 z + t$, ahora si se continúa el proceso y se llega hasta el máximo común divisor se obtiene qué:

La penúltima ecuación obtenida seria:

$$s_n t_n + c = s_{n+1} t_{n-1}$$

Ahora sea $s_{n+1} = k_{n+2} s_{n+1} + 1$, sustituyendo en la ecuación original se obtendría:

$$(k_{n+2} s_{n+1} + 1) t_n + c = s_{n+1} t_{n-1}$$

De lo cual:

$$t_n + c = s_{n+1}(t_{n-1} - k_{n+2} t_n)$$

Sea $t_{n+1} = t_{n-1} - k_{n+2} t_n$, llegando así a la ecuación

$$t_n + c = s_{n+1} t_{n+1}$$

Y de esta manera se justifica el método.

3.1.4 Método de pulverización

Este método es muy similar al método de Diofánto, se pulverizará la siguiente ecuación:

$$31x + 5 = 9y \qquad (1)$$

El método consiste en hacer divisiones entre los coeficientes de las variables, e involucrar una nueva variable, hasta que el residuo sea nulo. La primera división será entre 29 y 8, de lo cual se tiene:

$$31 = 9\,(3) + 4,$$

Y con el cociente 3 se deduce una nueva ecuación:

$$y = 3x + u \qquad (2)$$

Se sustituye este valor de y en la ecuación (1):

$$31x + 5 = 9(3x + u) \rightarrow 31x + 5 = 27x + 8u \rightarrow 4x + 5 = 9u\,(3)$$

Ahora se encontrará el cociente entre 9 y 4:

$$9 = 4\,(2) + 1$$

Y con el cociente 1, se forma una nueva ecuación:

$$x = 2u + v$$

La cual se sustituye en (3):

$$4\,(2u + v) + 5 = 9u \rightarrow 8u + 4v + 5 = 9u \rightarrow 4v + 5 = u \quad (4)$$

El proceso de los cocientes termina aquí, puesto que si se busca el cociente entre 4 y 1, no se obtiene residuo, es decir: $4 = 1\,(4) + 0$; lo que significa que se logro pulverizar la ecuación.

Por tanto todo el proceso depende del valor que se le asigne a v, y para encontrar el valor de las variables x, y, es necesario devolverse en el proceso, es decir:

$$\text{Si } v = 4 \rightarrow \text{en (4): } 4\,(4) + 5 = u \rightarrow u = 21$$
$$\text{Si } u = 21 \rightarrow \text{en (3): } 4x + 5 = 9\,(21) \rightarrow x = 46$$
$$\text{Si } x = 46, u = 21 \rightarrow \text{en (2): } y = 3\,(46) + 21 \rightarrow y = 159$$

De dónde se obtiene $x = 46$ e $y = 159$

Este método es muy similar al método utilizado por Diofánto solo varia en que al momento de realizar la parametrización en cada algoritmo de Euclides, ellos sustituyen de una vez, Diofánto por el contrario sustituye a partir del último parámetro. Ahora esta similitud se pudo dar por dos razones; la primera es dada por los registros históricos, la cual conlleva a que los indios tomaron como base el trabajo realizado por Diofánto debido a que él realizo su trabajo alrededor del siglo III d.c. y los persas invadieron Alejandría hacia el siglo V d.c. llevándose consigo muchos textos que estaban en la biblioteca de Alejandría, entre esos textos pudieron estar los textos de Diofánto que sirvieron como textos de estudio a la India, la segunda se puedo dar que tanto en la India como Diofánto hayan trabajado sobre este método contemporáneamente.

3.2. Ecuaciones Diofánticas de la forma $x^2 + y^2 = z^2$

3.1 Método de Diofánto

Diofánto en su libro II de *Aritmética* propone en el ejercicio 8 descomponer un cuadrado en dos cuadrados, con un razonamiento semejante al siguiente:

Suponga que se quiere descomponer el número 25 en dos cuadrados, siendo x^2 el primer número, con esto el segundo número será $x^2 - 25$, este también debe ser cuadrado, que lo notaremos $y^2 = 25 - x^2$, seguido a esto Diofanto identifica a y^2 con la siguiente expresión $\left(mx - \sqrt{25}\right)^2$ con *m* un número racional mayor que uno, es decir que obtiene:

$$y^2 = 25 - x^2 = \left(mx - \sqrt{25}\right)^2$$

$$\rightarrow 25 - x^2 = (mx - 5)^2$$

De esa igualdad se obtiene

$$25 - x^2 = m^2x^2 - 10mx + 25 \rightarrow 10mx = m^2x^2 + x^2 \rightarrow 10mx = x^2(m^2 + 1)$$

Como $x > 0$ se tiene que:

$$\frac{10m}{m^2+1} = x \rightarrow y^2 = 25 - \left(\frac{10m}{m^2+1}\right)^2 \rightarrow y^2 = 25 - \frac{100m^2}{(m^2+1)^2} \rightarrow y^2 = \frac{25(m^2-1)^2}{(m^2+1)^2}$$

Cómo $y > 1$ y $m > 1$ se obtiene

$$y = \frac{5(m^2-1)}{m^2+1}$$

Y así se puede llegar a qué el número 25 se expresa como:

$$25 = x^2 + y^2 \rightarrow 25 = \left(\frac{10m}{m^2+1}\right)^2 + \left(\frac{5(m^2-1)}{m^2+1}\right)^2$$

Pero si se observa hay dificultades ya que muchas de las ternas pitagóricas serán números racionales, para ello Diofánto parametrizó estos valores de la siguiente manera, si se quiere solucionar una terna pitagórica $x^2 + y^2 = z^2$, se sigue el procedimiento anterior de forma general llegando así a los valores de x e y que serán:

$$x = \frac{2mz}{m^2+1}$$

$$y = \frac{z(m^2-1)}{m^2+1}$$

De tal forma que:

$$z^2 = \left(\frac{2mz}{m^2+1}\right)^2 + \left(\frac{z(m^2-1)}{m^2+1}\right)^2$$

Si m es entero, entonces solo basta con multiplicar por $\frac{(m^2+1)^2}{z^2}$ a los dos lados de la igualdad, lo cual genera:

$$(m^2+1)^2 = (2m)^2 + (m^2-1)^2$$

De esta forma, ya se tendría la terna pitagórica $(2m, m^2-1, m^2+1)$ para m un entero positivo, vea un ejemplo: Sea $m = 8$, con lo cual se obtiene $2m = 16$, ahora $m^2 - 1 =$

63 y $m^2 + 1 = 65$,, de tal manera que $65^2 = 63^2 + 16^2$, de donde $4225 = 3969 + 256$ y efectivamente funciona este método.

Ahora si m es racional es decir se expresa de la forma $m = \frac{p}{q}, q \neq 0$, se tendría que:

$$(m^2+1)^2 = (2m)^2 + (m^2-1)^2 \rightarrow \left(\left(\frac{p}{q}\right)^2 + 1\right)^2 = \left(2\frac{p}{q}\right)^2 + \left(\left(\frac{p}{q}\right)^2 - 1\right)^2$$

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

Luego se multiplica a los dos lados de la igualdad por q^4, quedando así:

$$(p^2+q^2)^2 = (2pq)^2 + (p^2-q^2)^2$$

Y de este modo se tiene la terna pitagórica $(2pq, p^2-q^2, p^2+q^2)$ para p y q enteros positivos tales qué $p > q$

Ahora se justificará el porqué del número m, que expresa Diofánto para la solución de ternas pitagóricas. Se partirá de lo siguiente:

Sea la terna pitagórica $a^2 + b^2 = c^2$, qué también se puede escribir de la forma:

$$\frac{a^2}{c^2} + \frac{b^2}{c^2} = 1$$

Qué es equivalente a:

$$\left(\frac{a}{c}\right)^2 + \left(\frac{b}{c}\right)^2 = 1$$

Ahora si se toma $x = \frac{a}{c}$ y $y = \frac{b}{c}$, se puede deducir:

$$x^2 + y^2 = 1$$

Lo que se considera como una circunferencia unitaria con centro en el origen, ahora se considera una recta l tal que uno de sus puntos pase por las coordenadas $(1,0)$ y tenga otro punto que pase por la circunferencia unitaria, agregado a esto se considera qué tenga pendiente m con m un número racional

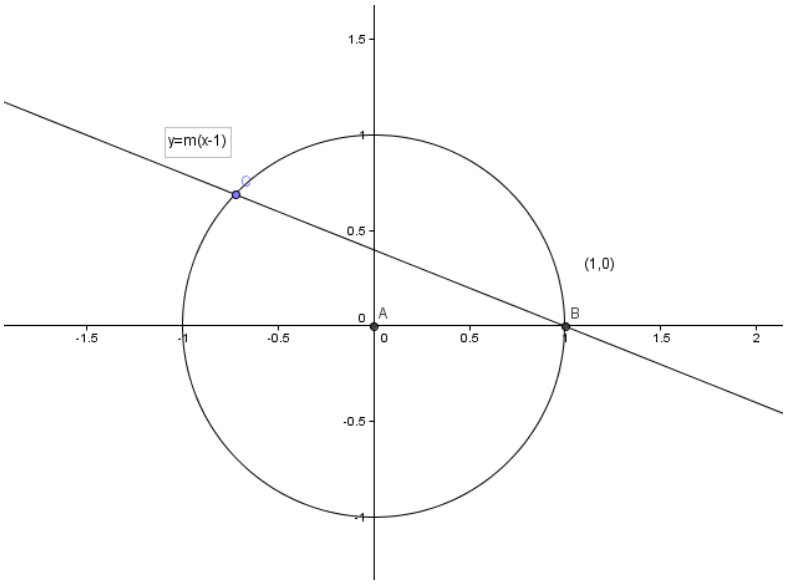


Figura 4: *Circulo unitario y recta* $y = m(x - 1)$

A partir de lo anterior se tiene lo siguiente, $\boldsymbol{x^2 + y^2 = 1}$ y $\boldsymbol{y = m(x - 1)}$ y con esto se obtiene:

$$x^2 + m^2(x - 1)^2 = 1$$

$$x^2 + m^2x^2 - 2m^2x + m^2 = 1$$

$$(m^2 + 1)x^2 - 2m^2x + m^2 - 1 = 0$$

Realizando la división de polinomios correspondiente obtenemos que tiene dos soluciones una es $(x - 1)$ y la otra $(m^2 + 1)x + (-m^2 + 1)$, luego de esto se obtiene que la coordenada en x para el punto C es:

$$x = \frac{m^2 - 1}{m^2 + 1}$$

Sustituyendo esta coordenada en la ecuación $y = m(x - 1)$, se obtiene qué:

$$y = m\left(\frac{m^2 - 1}{m^2 + 1} - 1\right)$$

Llegando así la coordenada:

$$\left(\frac{m^2 - 1}{m^2 + 1}, \frac{-2m}{m^2 + 1}\right)$$

Que satisfacen lo siguiente:

$$\left(\frac{m^2 - 1}{m^2 + 1}\right)^2 + \left(\frac{-2m^2}{m^2 + 1}\right) = 1$$

Ahora al multiplicar la ecuación por $(m^2+1)^2$ se obtiene:

$$(m^2-1)^2+(2m)^2=(m^2+1)^2$$

La cual ya fue analizada en el método anterior para llegar a la parametrización

$$(2pq, p^2-q^2, p^2+q^2)$$

Lo anterior muestra que Diofánto utilizo elementos geométricos para resolver problemas algebraicos, de los cual se deduce que m en la pendiente de una recta que pasa por la circunferencia unitaria utilizada por Diofánto para parametrizar el método visto en este apartado.

3.2.2 Método de Fibonacci

Con la sucesión de Fibonacci, se pueden generar ternas pitagóricas, a partir del siguiente método.

Considere cuatro números de Fibonacci consecutivos cualesquiera, a partir de dichos números sigua las siguientes indicaciones, basadas en un triángulo rectangulo:

- El producto de los dos números que se encuentran en los extremos, generan un cateto.
- El doble del producto de los dos números del medio genera el otro cateto.
- La suma de los cuadrados de los números intermedios, genera la hipotenusa.

El método general seria, considere los números $f_n, f_{n+1}, f_{n+2}, f_{n+3}$ de la sucesión de Fibonacci, de tal manera que $a=f_nf_{n+3}$, $b=2f_{n+1}f_{n+2}$ y $c=(f_{n+1})^2+(f_{n+2})^2$. De esta manera la terna pitagórica (a,b,c) con los números de la sucesión de Fibonacci seria

$(f_nf_{n+3}, 2f_{n+1}f_{n+2}, (f_{n+1})^2+(f_{n+2})^2)$ Veaun ejemplo:

La sucesión de Fibonacci está dada por 1,1,2,3,5,8,13,21,34, ... , ahora los números a seleccionar serán: $f_n=2, f_{n+1}=3, f_{n+2}=5$ y $f_{n+3}=8$, luego la terna pitagórica seria:

$$a=2\cdot 8=16, \qquad b=2\cdot 3\cdot 5=30 \text{ y } c=3^2+5^2=34$$

$$a^2+b^2=16^2+30^2=1156$$

$$a^2+b^2=1156=34^2=c^2$$

Ahora se analizará por qué funciona este método, observe la justificación:

Se tiene qué $a=f_nf_{n+3}, b=2f_{n+1}f_{n+2}$ y $c=(f_{n+1})^2+(f_{n+2})^2$, por ende:

$$a^2 + b^2 = (f_n f_{n+3})^2 + (2f_{n+1}f_{n+2})^2$$

Pero se tiene qué $f_n = f_{n+2} - f_{n+1}$ y $f_{n+3} = f_{n+1} + f_{n+2}$ por la sucesión de Fibonacci, de tal modo qué:

$$a^2 + b^2 = ([f_{n+2} - f_{n+1}][f_{n+1} + f_{n+2}])^2 + (2f_{n+1}f_{n+2})^2$$

$$a^2 + b^2 = ([f_{n+2}]^2 - [f_{n+1}]^2)^2 + (2f_{n+1}f_{n+2})^2$$

$$a^2 + b^2 = ([f_{n+2}]^2 - [f_{n+1}]^2)^2 + 4(f_{n+1})^2(f_{n+2})^2$$

$$a^2 + b^2 = (f_{n+2})^4 - 2(f_{n+2})^2(f_{n+1})^2 + (f_{n+1})^4 + 4(f_{n+1})^2(f_{n+2})^2$$

$$a^2 + b^2 = (f_{n+2})^4 + 2(f_{n+2})^2(f_{n+1})^2 + (f_{n+1})^4$$

De tal forma qué:

$$a^2 + b^2 = ((f_{n+2})^2 + (f_{n+1})^2)^2$$

Y como se tiene qué $c = (f_{n+1})^2 + (f_{n+2})^2$ sustituyendo se llega a:

$$a^2 + b^2 = c^2$$

Y de esta forma queda justificado el método de Fibonacci para resolver ecuaciones Diofánticas e la forma $a^2 + b^2 = c^2$.

Ahora bien los métodos estudiados en este capítulo para resolver ecuaciones diofánticas de la forma $\boldsymbol{ax + by = c}$ y $\boldsymbol{a^2 + b^2 = c^2}$, no son los únicos existen otros que no fueron analizados en este capítulo, debido a que estos fueron de mayor interés para el autor ya que ayudara a deducir algunos conceptos en el otro mundo discreto.

4. Exportando los métodos de solución a otro mundo discreto

En este capítulo se estudiaran los métodos de solución, vistos en el capítulo anterior pero en otro mundo discreto, para ello se estudiarán los enteros gaussianos notados como $\mathbb{Z}[i]$, ya que es un dominio de integridad y en el cual ya hay varios estudios realizados.

4.1 Enteros Gaussianos

Las ecuaciones lineales diofánticas en los números enteros requieren de varios conceptos matemáticos de los números reales para la solución al momento de utilizar los métodos; métodos relacionados con la divisibilidad y sus propiedades, algoritmo de la división, algoritmo de Euclides, lema de Bezout, que se obtienen a partir del estudio de la divisibilidad. Desde lo anterior un primer análisis en este nuevo conjunto numérico es la divisibilidad en los enteros gaussianos, para ello se precisaran algunas definiciones:

Los números enteros gaussianos se definirán de la siguiente manera, *Sea $\mathbb{Z}$ el conjunto de los números enteros. Se definen los enteros gaussianos por:*

$$\mathbb{Z}[i] = \{a + bi \in \mathbb{C} \mid a, b \in \mathbb{Z}\} \subseteq \mathbb{C}$$

Para definir la estructura de los números enteros tenemos que trabajar con operaciones, para ello se definirá la adición y el producto en $\mathbb{Z}[i]$.

Adición

Sean $t, z \in \mathbb{Z}(i)$, tal que $t = (a + bi)$ y $z = (c + di)$, su suma será:

$$t + z = (a + bi) + (c + di) = ((a + c) + (b + d)i)$$

Producto

Sean $t, z \in \mathbb{Z}(i)$, tal que $t = (a + bi)$ y $z = (c + di)$, su producto será:

$$tz = (a + bi) \cdot (c + di) = ((ac - bd) + (ad + cb)i)$$

Teniendo lo anterior se observan las propiedades[4] qué cumplen los $\mathbb{Z}[i]$ con la suma, que son las siguientes:

- Asociativa

[4] No se harán demostraciones, pues estas se pueden encontrar en trabajos relacionados con variable compleja como (Jiménez , 2013).

$$(a+bi)+\big((c+di)+(e+fi)\big)=\big((a+bi)+(c+di)\big)+(e+fi)$$

- Conmutativa

$$(a+bi)+(c+di)=(c+di)+(a+bi)$$

- Elemento neutro de la adición

$$(a+bi)+(0+0i)=(0+0i)+(a+bi)=(a+bi)$$

- Inverso aditivo

$$(a+bi)+((-a)+(-b)i)=(a-a)+(b-b)i=0+0i$$

- Cancelativa

$$Si\ \ (a+bi)+(c+di)=(a+bi)+(e+fi)\rightarrow(c+di)=(e+fi)$$

Ahora observemos las propiedades de los $\mathbb{Z}[i]$ con el producto:

- Asociativa

$$(a+bi)\cdot\big((c+di)\cdot(e+fi)\big)=\big((a+bi)\cdot(c+di)\big)\cdot(e+fi)$$

- Conmutativa

$$(a+bi)\cdot(c+di)=(c+di)\cdot(a+bi)$$

- Elemento neutro de la multiplicación

$$(a+bi)\cdot(1+0i)=(1+0i)\cdot(a+bi)=(a+bi)$$

- Cancelativa

$$Si\ \ (a+bi)(c+di)=(a+bi)(e+fi)\rightarrow(c+di)=(e+fi)$$

Ahora observemos que se cumple la propiedad distributiva de la multiplicación con respecto a la suma:

$$(a+bi)\cdot\big((c+di)+(e+fi)\big)=(a+bi)\cdot(c+di)+(a+bi)\cdot(e+fi)$$

Dado lo anterior se puede establecer qué $(\mathbb{Z}[i],+,\cdot)$ es un anillo conmutativo y con unidad, al igual que el conjunto de los números enteros, pero como también cumple la propiedad cancelativa el $(\mathbb{Z}[i],+,\cdot)$ es un dominio de integridad, debido a esto se darán las definiciones y propiedades que serán de gran ayuda al momento de solucionar ecuaciones diofánticas en $\mathbb{Z}[i]$.

Norma

Ahora se definirá la norma en $\mathbb{Z}[i]$, qué será útil más adelante; para ello se precisará de la siguiente manera:

Sea $(a+bi) \in \mathbb{Z}[i]$, se definirá la norma de $(a+bi)$ como:

$$\| (a+bi) \| = a^2 + b^2$$

Lo anterior será de gran ayuda para definir unidades, primos y el algoritmo de la división en $\mathbb{Z}[i]$. Algo importante de aclarar es que muchos $\mathbb{Z}[i]$ tienen la misma norma, observe el siguiente ejemplo:

Sea $(3+4i)$ su norma es 25, ahora miremos el número $(0+5i)$, su norma es 25.

Orden en $\mathbb{Z}[i]$

Debido a que los $\mathbb{C}$ no son ordenados los $\mathbb{Z}[i]$ tampoco, pero se les puede dar un orden parcial, un primer intento es ordenarlos según su norma, es decir:

Sea $(a+bi), (c+di) \in \mathbb{Z}[i]$ se dice que $(a+bi) < (c+di)$ si $\|(a+bi)\| < \|(c+di)\|$

Si se adopta la anterior definición, se tendría un problema y este es que muchos $\mathbb{Z}[i]$ tienen la misma norma es decir serian iguales como ejemplo se tendría que $(3+4i)$ y $(0+5i)$ son iguales, por ende este criterio de orden no sería conveniente.

Por otro lado se le podría dar un orden lexicográfico, es decir:

Sea $(a+bi), (c+di) \in \mathbb{Z}[i]$ si:

1. $b < a \rightarrow (c+di) < (a+bi)$
2. $a = c \ \wedge \ d < b \ \rightarrow \ (c+di) < (a+bi)$
3. $a < b \rightarrow (a+bi) < (c+di)$
4. $a = c \ \wedge \ b < d \ \rightarrow \ (a+bi) < (c+di)$

Pero el orden lexicográfico también tiene un problema, veamos un ejemplo sea $(1+i)$ y $(1-i)$, por el orden lexicográfico tenemos qué $(1-i) < (1+i)$ ahora si multiplicamos por $(1+i)$ a los dos lados de la igualdad se debería seguir cumpliendo la desigualdad, pero observemos que esto no sucede:

$$(1+i)(1-i) < (1+i)(1+i)$$

Y esto es

$$(2+0i) > (0+2i)$$

Pero si se multiplica por $(1-i)$ en ambos lados de la igualdad, si se sigue manteniendo la desigualdad. Desde lo anterior el orden lexicográfico no sería una buena definición de orden. Por lo anterior se puede deducir que el anillo de los $\mathbb{Z}[i]$ no son ordenados.

4.2. Divisibilidad en $\mathbb{Z}[i]$

Dado lo anterior se definirá divisibilidad en los $\mathbb{Z}[i]$*:*

Definición: Sea $w \in \mathbb{Z}[i]$, $z \in \mathbb{Z}[i]$, se dice que w divide a z si y sólo si existe un $r \in \mathbb{Z}[i]$, tal qué $z = wr$. Observe los siguientes ejemplos:

1. $3|6i$ por qué $6i = 3(2i)$
2. $(2-i)|(1+2i)$ por qué $(2-i)(i) = (1+2i)$

De la anterior definición surge la pregunta ¿Qué criterios habrá para saber cuándo un número gaussiano divide a otro? dar respuesta a esta pregunta conlleva a un sistema de ecuaciones, por ejemplo, en el caso anterior cuando se quiere saber si $(2-i)$ divide a $(1+2i)$ se plantea:

$$(1+2i) = (2-i)\cdot(a+bi) = \big((2a+b)+(-a+2b)i\big)$$

De donde:

$$1 = 2a + b$$
$$2 = -a + 2b$$

Qué es un sistema de ecuaciones lineales diofánticas ya que queremos que las soluciones sean enteras, para este caso se tiene que resolviendo el sistemas tenemos que $b = 1$ y $a = 0$.

Ahora se dará un ejemplo en el que no cumple: $(3+i)$ no divide a $(6+i)$, por qué si lo dividiera se tendría que:

$$(6+i) = (3+i)(a+bi) = \big((3a-b)+(3b+a)i\big)$$

De donde:

$$6 = 3a - b$$
$$1 = 3b + a$$

Como es un sistema de ecuaciones lineales diofánticas este no tiene solución debido a que los valores de a y b no son números enteros.

Ahora para que un $\mathbb{Z}[i]$ divida a otro, el sistema de ecuaciones lineales que se deduce debe tener solución única o no tener y este se debe a la propiedad cancelativa, es decir que finalmente quien puede decir fácilmente si el sistema podría o no tener solución es el determínate del sistema quien coincide con la norma del número que divide.

Esto quiere decir que la norma se relaciona estrechamente con la divisibilidad, esto se refleja mejor en la siguiente propiedad:

Propiedad 1. [Norma y divisibilidad]: Sean $z, w \in \mathbb{Z}[i]$ entonces se cumple qué:

$$si\ z|w\ en\ \mathbb{Z}[i] \rightarrow \| z \| \mid \| w \|\ en\ \mathbb{Z}$$

Observemos que el reciproco no es cierto:

Sea $(7-i)$ y $(2+i)$ ahora se mirará si $(2+i) \mid (7-i)$, al momento de obtener las normas de los enteros gaussianos se llega a:

$$\|(7-i)\| = 50$$

$$\|2+i\| = 5$$

Ahora se tiene qué $\|(2+i)\| \mid \|(7-i)\|$ pero no se cumple qué $(2+i) \mid (7-i)$ ya qué:

$$(7-i) = (2+i)(a+bi)$$

Es decir qué:

$$(7-i) = ((2a-b) + (2b+a)i)$$

Con este se obtiene un sistema de ecuaciones

$$\begin{cases} 2a-b = 7 \\ a+2b = -1 \end{cases}$$

Al solucionar el sistema de ecuaciones se obtiene que el valor numérico para a y b son números racionales, lo qué no satisface la definición de entero gaussiano.

Otras Propiedades de divisibilidad en $\mathbb{Z}[i]$

En este apartado se hará un estudio de las propiedades de divisibilidad en los $\mathbb{Z}[\boldsymbol{i}]$, para ello se hará un paralelo con las propiedades de los $\mathbb{Z}$, para determinar similitudes.

Lo primero que se debe hacer es identificar las unidades, recordemos que una unidad en $\mathbb{Z}$ son aquellas que se al multiplicarse por sí mismas resulta ser 1 y dividen a todo el conjunto de los números esteros, en este caso 1 y -1. Ahora se definirán las unidades en lo $\mathbb{Z}[i]$.

Sea $w \in \mathbb{Z}[\boldsymbol{i}]$, w será unidad si y solo si $\exists z \in \mathbb{Z}[\boldsymbol{i}], tal$ qué $w \cdot z = 1$.

Por la propiedad 1, si $wz = 1$ entonces $\|w\| \mid \|1\|$ luego la norma de $||w|| = 1$ de lo anterior fácilmente se puede deducir que los candidatos a unidades en los $\mathbb{Z}[\boldsymbol{i}]$ son**:**

$$(1), (-1), (i) \text{ y } (-i)$$

Y podemos comprobar que $(1)(1) = 1$, $(-1)(-1) = 1$, $(i)(-i) = 1$, luego efectivamente estas cuatros son unidades, y estas son únicos debido a que su norma debe ser 1, $a^2 + b^2 = 1$.

Ahora recordemos algunas de las propiedades de la divisibilidad en los enteros, $\forall a, b \in \mathbb{Z}$ se tiene que:

1. $a|a$

2. Si $a|b$ y $b|c$ entonces $a|c$
3. $1|a$
4. $a|0$
5. Si $0|a$ entonces $a = 0$ (No hay divisores de cero)
6. Si $a|1$ entonces $a = 1$ ó $a = -1$
7. Si $a|b$ y $b|a$ entonces $a = -b$ ó $a = b$
8. $a|(-a)$
9. Si $a|b$ entonces $|a| \leq |b|$
10. Si $a|b$ entonces $a|bc$
11. Si $a|b$ y $a|c$ entonces $a|(b + c)$
12. Si $b \neq 0$, entonces $\exists!\, q, r \in \mathbb{Z}$, tal que $a = bq + r$ con $0 \leq r < |b|$

Antes de empezar a mirar si se cumplen o no estas propiedades en los Gaussianos, para facilitar la escritura de aquí en adelante notaremos el gaussiano $(a + bi)$ como la pareja ordenada (a, b).

Propiedad 2: $(a, b) \mid (a, b)$

Demostración:

Para qué (a, b) divida a (a, b) por la definición de divisibilidad se tiene que:

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

Para que esto sea cierto $(x, y) = (1,0)$, por tal razón $(a, b) \mid (a, b)$

Propiedad 3: $Si\ (a, b) \mid (c, d) \wedge (c, d) \mid (e, f) \rightarrow (a, b) \mid (e, f)$

Demostración:

Si $(a, b) \mid (c, d)$ y $(c, d) \mid (e, f)$ por la definición de divisibilidad en los enteros gaussianos se tiene qué:

$$(c, d) = (a, b)\ (g, h)\ \wedge\ (e, f) = (c, d)(s, r)$$

Es decir qué:

$$(e, f) = (c, d)(s, r) = [(a, b)(g, h)](s, r)$$

Por la propiedad asociativa se tiene qué:

$$[(a, b)(g, h)](s, r) = (a, b)[(g, h)(s, r)]$$

Por tal razón se cumple qué,

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

Propiedad 4: $(1,0) \mid (a, b)$

La demostración de esta propiedad es inmediata por la definición de divisibilidad y elemento neutro en los gaussianos.

Propiedad 5: $(a,b) \mid (0,0)$

Demostración:

Por la definición de divisibilidad se tiene que si $(a,b) \mid (0,0)$, entonces

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

Para que esto suceda $(x,y) = (0,0)$, por lo tanto $(a,b) \mid (0,0)$

Propiedad 6: Si $(0,0) \mid (a,b) \rightarrow (a,b) = (0,0)$

Demostración:

Si $(0,0) \mid (a,b)$ se tiene qué:

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

Pero todo número gaussiano multiplicado por $(0,0)$ es $(0,0)$ se tiene que $(a,b) = (0,0)$.

Propiedad 7: Si $(a,b) \mid (1,0)$ entonces (a,b) es unidad.

La demostración de esta propiedad es consecuencia directa de la definición de divisibilidad y la definición de unidades.

Asociados en $\mathbb{Z}[i]$: En los enteros, se tiene que dos números p y q son asociados si, p | q y $q \mid p$. De la misma forma se definirán los asociados en los $\mathbb{Z}[i]$, es decir sea $(p,q),(p',q') \in \mathbb{Z}[i]$,$(p,q)$y (p',q') son asociados si y solo si $(p,q) \mid (p',q')$ y $(p',q') \mid (p,q)$

Teniendo en cuenta lo anterior (p,q) tiene exactamente cuatro asociados qué son:

1. (p,q)
2. $(-p,q)$
3. $(p,-q)$
4. $(-p,-q)$

Propiedad 8: Si $(a,b) \mid (c,d) \wedge (c,d) \mid (a,b) \rightarrow$ (a,b) y (c,d) son asociados,

Demostración:

Si $(a,b) \mid (c,d) \wedge (c,d) \mid (a,b)$ se tiene que:

$$(c,d) = (a,b)(e,f) \wedge (a,b) = (c,d)(g,h)$$

Es decir qué

$$(c,d) = [(c,d)(g,h)](e,f)$$

Por la propiedad asociativa de los $\mathbb{Z}[i]$ se obtiene

$$(c,d) = (c,d)[(g,h)(e,f)]$$

Por la propiedad cancelativa de la multiplicación se llega a:

$$1 = (g, h)(e, f)$$

Es decir que (g, h) y (e, f) deben ser unidades, con esto se llega a qué si $(a, b) \mid (c, d) \wedge (c, d) \mid (a, b)$ entonces

1. $(a, b) = (c, d)$
2. $(a, b) = (c, -d)$
3. $(a, b) = (-c, d)$
4. $(a, b) = (-c. -d)$

Propiedad 9: $(a, b) \mid (a, -b)$, $(a, b) \mid (-a, b) \wedge (a, b) \mid (-a, -b)$

La demostración de esta propiedad sale como consecuencia directa de la propiedad 2 y definición de las unidades.

Propiedad 10: Si $(a, b) \mid (c, d) \rightarrow \|(a, b)\| < \|(c, d)\|$

Demostración

Por la propiedad 1 se tiene que si $(a, b) \mid (c, d)$ entonces

$$\|(a, b)\| \mid \|(c, d)\|$$

Como las normas son números reales sea a $\|(a, b)\| = t$ y $\|(c, d)\| = s$ con $t, s \in \mathbb{R}$, reemplazando se tiene que:

$$t \mid s$$

Por la una propiedad de divisibilidad en los enteros se tiene que si $t \mid s \rightarrow |t| < |s|$, como t y s son normas entonces son positivas se tiene que

$$t < s$$

Reemplazando se llega a:

$$\|(a, b)\| < \|(c, d)\|$$

Y con esto queda demostrado.

Propiedad 11: Sea $(a, b) \in \mathbb{Z}[i]$ entonces $\exists!\,(c, d)$, tal qué $c \in \mathbb{Z}^+$ y $d \in \mathbb{Z}^+ \cup \{0\}$, y (c, d) es asociado de (a, b)

Propiedad 12: Si $(a, b) \mid (c, d) \rightarrow (a, b) \mid ((c, d)(e, f))$

Demostración.

Como $(a, b) \mid (c, d)$, por la definición de divisibilidad en los $\mathbb{Z}[i]$, se tiene qué,

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

Luego,

$$(c,d)(e,f) = [(a,b)(r,s)](e,f)$$

Por la asociativa se tiene:

$$[(a,b)(r,s)](e,f) = (a,b)[(r,s)(e,f)]$$

Por tal razón se llega a qué,

$$(a,b)|\big((c,d)(e,f)\big)$$

Propiedad 13: Si $(a,b) \mid (c,d) \ \wedge (a,b) \mid (e,f) \rightarrow (a,b) \mid [(c,d)+(e,f)]$

Demostración:

Por la definición de divisibilidad se tiene qué:

$$(c,d) = (a,b)(g,h) \ \wedge (e,f) = (a,b)(j,k)$$

Sumando se obtiene qué

$$(c,d)+(e,f) = (a,b)(g,h) + (a,b)(j,k)$$

De lo cual

$$(a,b)(g,h) + (a,b)(j,k) = (a,b)[(g,h)+(j,k)]$$

Por lo cual se llega a qué:

$$(a,b) \mid [(c,d)+(e,f)]$$

Propiedad 14 [Algoritmo de la división en $\mathbb{Z}[i]$]: Sean $z, w \in \mathbb{Z}[i]$, con z no nulo, entonces existen $q, r \in \mathbb{Z}[i]$, tales qué $w = zq + r$, con $0 \leq \|r\| < \|z\|$.

Demostración:

Primer caso: Sea $w = (a,b)\ y\ z = (c,0)$ con $a,b,c \in \mathbb{Z}$. Luego existen $q_1, q_2, r_1, r_2 \in \mathbb{Z}$, tales qué:

$$a = cq_1 + r_1 \ \ y \ \ b = cq_2 + r_2 \ con\ |r_i| < \frac{|c|}{2}$$

Reescribiendo se tiene qué:

$$(a,b) = (c,0)(q_1,q_2) + (r_1,r_2)$$

$$\|r_1 + r_2\| = r_1^2 + r_2^2 \leq \frac{c^2}{2} < c^2$$

De este modo tenemos existen $q = (q_1,q_2),\ r = (r_1,r_2)$ tal que $w = zq + r$ con $0 \leq \|r\| < \|z\|$.

Segundo Caso: Sea $w = (a,b)\ y\ z = (c,d)$, por el caso anterior se sabe que existen q, r_1 ta les qué:

$$w\bar{z} = (a,b)(c,-d) = (c^2+d^2)q + r_1 \; con \; \|r_1\| \; < \; \|c^2+d^2\|$$

Con $r_1 = (a,b)(c,-d) - (c^2+d^2)q$, a su vez esto es:

$$r_1 = (a,b)(c,-d) - (c^2+d^2)q = [(a,b) - (c,d)q](c,-d)$$

Ahora se define a r como:

$$r = (a,b) - (c,d)q$$

De esto se obtiene qué:

$$r_1 = r(c,-d)$$

Desde lo anterior se deduce qué:

$$\|r\|(c^2+d^2) = \|r(c,-d)\| = \|r_1\| \leq \|c^2+d^2\|$$

Simplificando se obtiene:

$$0 \leq \|r\| < \|z\|$$

Cumpliéndose qué:

$$w = zq + r$$

Observe los siguientes ejemplos:

1. Dividir $(13{,}21)$ entre $(4{,}0)$

   Es decir que $(13{,}21) = (4{,}0)(q,t) + (r,s)$ con $\|(r,s)\| < \|(4{,}0)\|$, como

   $$15 = 4(4) - 1 \; \wedge 21 = 4(5) + 1$$

   Con lo anterior se tiene que

   $$(13{,}21) = (4{,}0)(4{,}5) + (-1+i)$$

2. Dividir $(7{,}2)$ entre $(3{,}1)$

   Se tiene que $\|(3{,}1)\| = 10$ y $(7{,}2)(3,-1) = (23,-1)$ ahora como

   $$23 = 10(2) + 3 \; \wedge \; -1 = 10(0) - 1$$

   De tal manera se llega a qué $(q,t) = (2{,}0)$ y $(r_1,s_1) = (3,-1)$ ahora sea:

   $$(r,s) = (7{,}2) - (2{,}0)(3{,}1) = (1{,}0)$$

   Y es así como se obtiene qué:

$$(7,2) = (3,1)(2,0) + (1,0)$$

Primos en $\mathbb{Z}[i]$

La definición de primo en $\mathbb{Z}[i]$, se hará de la misma forma en la que se define primo en los números enteros, y esta es:

Un número $(p,q) \in \mathbb{Z}[i]$, se dice qué es primo si y solo si, (p,q) es divisible únicamente por las unidades y por los asociados, es decir que un número primo tiene a lo sumo ocho divisores. Ya con esta definición surge la pregunta ¿Y cuáles son los primos en $\mathbb{Z}[i]$? , pero antes de dar solución a esta pregunta se retomara la definición de divisibilidad, pero se hará de otra manera ya conocemos que si $(c,d)|(a,b)$ se tiene que cuando $(a,b) = (c,d)(x,y)$ es decir qué $(a,b) = (cx - dy, cy + dx)$, esto lleva al siguiente sistema de ecuaciones:

$$cx - dy = a$$
$$dx + cy = b$$

Qué solucionándolo mediante una matriz ampliada, esto es:

$$\begin{vmatrix} c & -d \\ d & c \end{vmatrix}$$

Lo cual sería:

$$\begin{vmatrix} c & -d \\ d & c \end{vmatrix} = c^2 + d^2$$

Y llegando a sus soluciones llegamos a:

$$x = \frac{\begin{vmatrix} a & -d \\ b & c \end{vmatrix}}{\begin{vmatrix} c & -d \\ d & c \end{vmatrix}} = \frac{ac + bd}{c^2 + d^2}$$

Lo que conlleva a que tiene solución en los enteros si $c^2 + d^2 | ac + bd$, ahora la otra solución será:

$$y = \frac{\begin{vmatrix} c & a \\ d & b \end{vmatrix}}{\begin{vmatrix} c & -d \\ d & c \end{vmatrix}} = \frac{bc - ad}{c^2 + d^2}$$

Lo que conlleva a que tiene solución en los enteros si $c^2 + d^2 | bc - ad$,

Ahora desde lo anterior se estudiarán los irreducibles o primos en los enteros gaussianos, surge la idea de cuando un número es primo en los $\mathbb{Z}[i]$, una primera pregunta es ¿Los primos en $\mathbb{Z}$ serán primos en $\mathbb{Z}[i]$?, para ello se realizará lo siguiente:

Sea $z \in \mathbb{Z}[i]$ con $z = (p,o)$, p primo en los $\mathbb{Z}$, ahora $\|(p,o)\| = p^2$, ahora sea un $w \in \mathbb{Z}[i]$, $w \mid z$ si $\|w\| \mid p^2$, como $w = (a,b)$, se tiene qué $\|w\| \mid \|z\|$ esto es:

$$(a^2 + b^2) \mid p^2$$

Luego para qué lo anterior suceda se debe cumplir alguno de los siguientes casos:

1. $a^2 + b^2 = 1$
2. $a^2 + b^2 = p^2$
3. $a^2 + b^2 = p$

En el 1. Se tiene qué si $a^2 + b^2 = 1$ es porqué w tiene que ser unidad, pero ya sabemos que z es divisible por las unidades, ahora se analizará el 2. $a^2 + b^2 = p^2$, por el sistema de ecuaciones se tiene qué:

$$p^2|ap$$
$$p^2|-bp$$

Ahora para que esto suceda $a = \pm ph$ y $b = \pm pk$, de tal manera qué:

$$p^2 = a^2 + b^2 = (h^2 + k^2)p^2$$

Es decir qué $h^2 + k^2 = 1$, y para qué esto suceda tiene que pasar qué:

$$h = 1 \quad k = 0$$
$$h = -1 \quad k = 0$$
$$h = 0 \quad k = 1$$
$$h = 0 \quad k = -1$$

Con esto se llega a qué w es asociado, lo cual también se sabe que z debe ser divisible por sus asociados

Por último se analiza el criterio 3. $a^2 + b^2 = p$, por el sistema de ecuaciones lineales se tiene qué:

$$p|ap$$
$$p|-bp$$

Es decir qué $(p, 0) = (a, b)(a, -b) = (a^2 + b^2, ab - ab)$, con esto esta segunda nos ayuda a descartar algunos primos en los $\mathbb{Z}$ que no son primos en los $\mathbb{Z}[i]$, veamos algunos ejemplos:

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

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

$$(13,0) = (3,2)(3,-2)$$

Es decir qué, $2, 5\ y\ 13$ no son primos en los $\mathbb{Z}[i]$.

Lo anterior conlleva al siguiente teorema:

Teorema: Sea $(p, 0) \in \mathbb{Z}[i]$, $(p, 0)$ es primo si la ecuación diofántica $a^2 + b^2 = p$ no tiene solución en los$\mathbb{Z}$

Máximo Común Divisor en $\mathbb{Z}[i]$

Un problema que surge al momento de definir el máximo común divisor en el anillo de los $\mathbb{Z}[i]$, es el orden, puesto que no se puede establecer cuál es el más grande, desde lo anterior surgen dos preguntas ¿Existe el $m.c.d.$? y si existe es ¿único?, si se la existencia, surge el problema de la unicidad ya qué cada número del conjunto de los $\mathbb{Z}[i]$, , tiene cuatro asociados. Desde lo anterior se propone la siguiente definición para el máximo común divisor que se notara como MCD:

Sea $(a,b),(c,d) \in \mathbb{Z}[i]$, $(e,f) = MCD((a,b),(c,d))$ si y solo si:

1. $(e,f) \mid (a,b) \ \wedge \ (e,f) \mid (c,d)$
2. $\forall (g,h) \in \mathbb{Z}[i]$ si $(g,h) \mid (a,b) \ \wedge \ (g,h) \mid (c,d) \rightarrow (e,f) \mid (g,h)$
3. (e,f) será el determinado por la propiedad 11

Garantizando la existencia y la unidad ahora la pregunta es ¿Cómo hallarlo?, para ello se establecerá el algoritmo de la Euclides en los $\mathbb{Z}[i]$

Algoritmo de Euclides en $\mathbb{Z}[i]$

De igual forma qué se definió el algoritmo de Euclides en el conjunto$\mathbb{Z}$, se definirá en los $\mathbb{Z}[i]$ el cual consiste en: Se utiliza el algoritmo de la división en $\mathbb{Z}[i]$ repetitivamente hasta qué el residuo sea nulo, teniendo esto el último residuo mayor que cero es el máximo común divisor, es decir:

$$(a,b) = (c,d)(q,t) + (r,s)$$
$$(c,d) = (r,s)(q_1,t_1) + (r_1,s_1)$$
$$(r,s) = (r_1,s_1)(q_2,t_2) + (r_2,s_2)$$

$$\vdots$$

$$(r_{n-1},s_{n-1}) = (r_n,s_n)(q_{n+1},t_{n+1}) + (r_{n+1},s_{n+1})$$
$$(r_n,s_n) = (r_{n+1},s_{n+1})(q_{n+2},t_{n+2}) + (0,0)$$

Realizando este procedimiento se tendría que el $MCD\big((a,b),(c,d)\big) = (r_{n+1},s_{n+1})$ y de esta manera se obtiene el algoritmo de Euclides de forma numérica en los $\mathbb{Z}[i]$. Veamos un ejemplo:

Sean $(2,5)\ y\ (3,-1)$

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

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

$$(1,2) = (1,0)(1,2) + (0,0)$$

Luego el $MCD((2,5),(3,-1)) = (1,0)$

Ahora teniendo en cuenta lo anterior, con el algoritmo de Euclides en $\mathbb{Z}[i]$ se puede hallar el $MCD((a,b),(c,d))$, y este nos lleva al *Lema de Bezout en lo*s $\mathbb{Z}[i]$, el cual nos dice que el máximo común divisor en los $\mathbb{Z}[i]$ se puede expresar como una combinación lineal, es decir $sean\ z,t \in \mathbb{Z}[i]$ y $MCD(z,t) = w$ se tiene qué $w = zx + ty$, es decir

Teorema Lema de Bezout en $\mathbb{Z}[i]$**:** Si $z,t \in \mathbb{Z}[i]$ con $MCD(z,t) = w$,entonces $\exists x,y \in \mathbb{Z}[i]$ tales que

$$w = zx + ty$$

Con el ejemplo del caso anterior se tiene qué como $MCD((2,5),(3,-1)) = (1,0)$, entonces

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

A continuación se definía por ultimo primos relativos.

Primos Relativos en $\mathbb{Z}[\boldsymbol{i}]$

Sean $(a,b),(c,d) \in \mathbb{Z}[i]$, (a,b) y (c,d) son primos relativos si y solo si $M.C.D.[(a,b),(c,d)] = (r,s)$ con (r,s) una unidad.

Ya definido el máximo común divisor y primos relativos, surge la pregunta ¿Cómo hallar el $M.C.D.$?, para ello se utilizará el algoritmo de Euclides.

4.3 Métodos de solución para ecuaciones de la forma $(\boldsymbol{a},\boldsymbol{b})\boldsymbol{X} + (\boldsymbol{c},\boldsymbol{d})\boldsymbol{Y} = (\boldsymbol{e},\boldsymbol{f})$

En este apartado se analizaran los métodos de solución utilizados en los enteros y se tratará de llevarlos al conjunto de los enteros gaussianos, a partir de lo anterior se da el primer método.

4.3.1 Método del Algoritmo de Euclides y Lema de Bezout para resolver ecuaciones diofánticas en $\mathbb{Z}[\boldsymbol{i}]$.

En este apartado se resolverán ecuaciones diofánticas utilizando el algoritmo de Euclides y el Lema de Bezout en los $\mathbb{Z}[i]$ para resolver ecuaciones diofánticas.

Sea la ecuación diofántica

$$(2,5)x + (3,-1)y = (-7,24)$$

Iniciamos aplicando el algoritmo de Euclides a los términos que acompañan a las variables:

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

ii. $(3,-1) = (1,2)(0,-1) + (1,0)$
iii. $(1,2) = (1,0)(1,2) + (0,0)$

Como el máximo común divisor $(1,0)$, por el Lema de Bezout se establece qué:

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

Teniendo en cuenta esto, se realiza de nuevo el algoritmo de Euclides para los términos que acompañan a las variables, pero como ya lo habíamos realizado, ahora se despejaran los residuos de **ii** y **i** respectivamente:

a) $(1,2) = (2,5) - (3,-1)(0,1))$
b) $(1,0) = (3,-1) - (1,2)(0,-1)$

Ahora se reemplaza (a) en (b), y se tiene qué:

$$(1,0) = (3,-1) - [(2,5) - (3,-1)(0,1)](0,-1)$$

De lo cual se obtiene:

$$(1,0) = (3,-1) - [(2,5)(0,-1) - (3,-1)(1,0)]$$

Luego

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

Llegando a

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

Por lo tanto

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

Ahora para hallar la solución a la ecuación diofántica solo basta multiplicar $(-7,24)$ a la ecuación, es decir:

$$(-7,24)(1,0) = (3,-1)[(2,0)(-7,24)] + (2,5)[(0,1)(-7,24)]$$

Esto da

$$(-7,24) = (3,-1)[(-14,48)] + (2,5)[(-24,-7)]$$

Es decir que la solución a la ecuación diofántica es:

$$y = (-14,48) \wedge x = (-24,-7)$$

4.3.2 Método de Diofánto.

Sea la ecuación diofántica

$$(4,3)X + (-3,-2) = (8,4)Y$$

Ahora se inicia con el algoritmo de Euclides y se parametriza al estilo de Diofánto,

1. $(8,4) = (4,3)(1,0) + (4,1)$, la parametrización de Diofánto es $X = (1,0)Y + Z$
2. $(4,3) = (4,1)(1,0) + (0,2)$, entonces $Y = (1,0)Z + U$
3. $(4,1) = (0,2)(0,-2) + (0,1)$, de lo cual $Z = (0,-2)U + V$

Siguiendo con lo que estableció Diofánto se tiene que llegar a una ecuación de la forma

$$U + (e+f)' = GV$$

Dónde $(e+f)'$ es la constante que suma y depende del número de divisiones efectuadas, si el número es par la constante sumará, pero si es impar la constante restará. Dado lo anterior y según el ejemplo establecido la constante en este caso restara. G será el residuo anterior al máximo común divisor, es decir que en este ejemplo es $(0,2)$. Ahora mirando el algoritmo de Euclides se observa qué el máximo común divisor es $(0,1)$, pero según la definición dada en la sección **4.2** El máximo común divisor en este caso debe ser $(1,0)$, por esta razón la ecuación anterior quedara de la siguiente manera:

$$1) \qquad (0,1)U - (-3,-2) = (0,2)V$$

Si el máximo común divisor hubiese sido $(1,0)$, la ecuación hubiese quedado:

$$U - (-3,-2) = (0,2)V$$

Ahora para resolver la ecuación $1)$ primero se debe multiplicar por $(0,-1)$ para que así la variable U quede multiplicada por la unidad $(1,0)$, qué es igual a 1, multiplicando toda la ecuación lleva a :

$$U - (-2,3) = (2,0)V$$

Teniendo esto se continua al estilo Diofánto, se le asigna un valor cualquiera a V en este caso se le asignara $V = (1,2)$, de tal manera que

$$U = (0,7)$$

Como se tienen dos valores $V = (1,2)$ y $U = (0,7)$, se empieza a reemplazar en las parametrizaciones establecidas llegando a:

1. $V = (1,2)$

2. $U = (0,7)$
3. $Z = (15,2)$
4. $Y = (15,9)$
5. $X = (30,11)$

Teniendo este resultado se llega a que dos posibles soluciones son $X = (30,11)$ y $Y = (15,9)$, si se reemplaza en la ecuación original se tiene:

$$(4,3)(30,11) + (-3,-2) = (8,4)(15,9)$$

$$(87,134) + (-3,-2) = (84,132)$$

$$(84,132) = (84,132)$$

Ahora si se le asigna otro valor a V se pueden obtener otras soluciones distintas a las planteadas.

Observe otro ejemplo, sea la ecuación

$$(3,2)X + (-13,18) = (4,3)Y$$

Se solucionará con el método de Diofánto,

1. $(4,3) = (3,2)(1,0) + (1,1)$ La parametrización queda $X = (1,0)Y + Z$
2. $(3,2) = (1,1)(2,0) + (1,0)$, De la cual se establece $Y = (2,0)Z + U$

De lo anterior se llega a la ecuación:

$$Z + (-13,18) = (1,1)U$$

Sea $U = (2,2)$ se tiene qué:

$$Z = (13,-14)$$

Ahora reemplazando en las parametrizaciones se tiene que:

- $U = (2,2)$
- $Z = (13,-14)$
- $Y = (28,-26)$
- $X = (41,-40)$

Con lo anterior se tendrían las soluciones $X = (41,-40)$ y $Y = (28,-26)$ reemplazando en la ecuación original se tiene:

$$(3,2)(41,-40) + (-13,18) = (4,3)(28,-26)$$

$$(203,-38) + (-13,18) = (190,-20)$$

$$(190, -20) = (190, -20)$$

Con lo anterior se deduce que el método de Diofánto funciona en los $\mathbb{Z}[i]$. La justificación de este método es similar a la utilizada en el capítulo 3.

4.4 Métodos de solución Para ecuaciones de la forma $(\boldsymbol{a}, \boldsymbol{b})^{\mathbf{2}} + (\boldsymbol{c}, \boldsymbol{d})^{\mathbf{2}} = (\boldsymbol{e}, \boldsymbol{f})^{\mathbf{2}}$

Una primera pregunta que surge es ¿Cuáles y cómo serán las ternas pitagóricas en los $\mathbb{Z}[i]$? La primera idea que puede surgir es la siguiente:

Sea $a, b, c \in \mathbb{Z}$ con $a^2 + b^2 = c^2$ serán ternas pitagóricas en $\mathbb{Z}[i]$ aquellas que:

$$(a, 0)^2 + (b, 0)^2 = (c, 0)^2$$

Ahora para determinar si es cierto se obtiene qué

$$(a, 0)(a, 0) + (b, 0)(b, 0) = (a^2 - 0{,}0 + 0) + (b^2 - 0{,}0 + 0)$$

De lo cual se llega a:

$$(a^2, 0) + (b^2, 0) = (a^2 + b^2, 0)$$

Como $a^2 + b^2 = c^2$ se concluye qué:

$$(a^2 + b^2, 0) = (c^2, 0)$$

Y con esto se comprueba qué $(a, 0)^2 + (b, 0)^2 = (c, 0)^2$
Otras postuladas hacer triadas pitagóricas son las siguientes, sean $a, b, c \in \mathbb{Z}$ con $a^2 + b^2 = c^2$ serán ternas pitagóricas en $\mathbb{Z}[i]$ aquellas que:

$$(0, a)^2 + (0, b)^2 = (0, c)^2$$

Observe un ejemplo

Sea la triada pitagórica $3^2 + 4^2 = 5^2$

$$(0{,}3)^2 + (0{,}4)^2 = (0{,}3)(0{,}3) + (0{,}4)(0{,}4) = (-9{,}0) + (-16{,}0) = (-25{,}0)$$

Evidentemente no cumple con las características, por ende se descarta como triada pitagórica. Ahora se observaran las siguientes:

Sea $a, b, c \in \mathbb{Z}$ con $a^2 + b^2 = c^2$, serán triadas pitagóricas en los $\mathbb{Z}[i]$ aquellas que:

$$(a, a)^2 + (b, b)^2 = (c, c)^2$$

Se probará que es cierto:

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

$$(0,2a^2) + (0,2b^2) = (0,2a^2 + 2b^2) = (0,2(a^2 + b^2))$$

Como $a^2 + b^2 = c^2$, se llega a:

$$(a,a)^2 + (b,b)^2 = (0,2c^2)$$

Ahora como $(c,c)^2 = (c^2 - c^2, c^2 + c^2) = (0,2c^2)$, por lo cual se concluye qué:

$$(a,a)^2 + (b,b)^2 = (c,c)^2$$

Ya definidas las triadas pitagóricas en $\mathbb{Z}[i]$, se analizaran si los métodos en los enteros funcionan en este mundo discreto.

4.4.1 Parametrización de Diofánto

Diofánto estableció una parametrización para hallar ternas pitagóricas en los enteros estas son:

$(2pq, p^2 - q^2, p^2 + q^2)$ Para p y q enteros positivos tales qué $p > q$, esta parametrización fue estudiada en el capítulo anterior, se analizará si se puede establecer en las ternas pitagóricas gaussianas. Sea

$$(2pq,0)^2 + (p^2 - q^2,0)^2 = (4p^2q^2,0) + (p^4 - 2p^2q^2 + q^4,0)$$

$$(2pq,0)^2 + (p^2 - q^2,0)^2 = (p^4 + 2p^2q^2 + q^4,0)$$

Ahora como $(p^2 + q^2,0)^2 = (p^4 + 2p^2q^2 + q^4,0)$ de tal manera se puede concluir qué:

$$(2pq,0)^2 + (p^2 - q^2,0)^2 = (p^2 + q^2,0)^2$$

Por lo cual se puede concluir que la parametrización de Diofánto para ternas pitagóricas es válida en las ternas pitagóricas gaussianas de la forma $(a,0)^2 + (b,0)^2 = (c,0)^2$. Observe un ejemplo:

Se $p = 4$ y $q = 3$, se tiene por lo anterior qué:

$$(2(4)(3),0)^2 + ((4)^2 - (3)^2,0)^2 = (24,0)^2 + (7,0)^2 = (576,0) + (49,0) = (625,0)$$

Ahora como $(625,0) = (25,0)^2 = ((4)^2 + (3)^2,0)^2$, se tiene que se cumple la parametrización, observe ahora para las ternas pitagóricas de la forma $(a,a)^2 + (b,b)^2 = (c,c)^2$, sea la ecuación:

$$(2pq,2pq)^2 + (p^2 - q^2, p^2 - q^2)^2 = (0,4p^2q^2 + 4p^2q^2) + (0,2p^4 - 4p^2q^2 + 2q^4)$$

$$(2pq,2pq)^2 + (p^2 - q^2, p^2 - q^2)^2 = (0,2p^4 + 4p^2q^2 + 2q^2)$$

Ahora como $(p^2+q^2, p^2+q^2)^2 = (0{,}2p^4 + 4p^2q^2 + 2q^2)$, de tal manera que se puede concluir que:

$$(2pq, 2pq)^2 + (p^2-q^2, p^2-q^2)^2 = (p^2+q^2, p^2+q^2)^2$$

Observe un ejemplo

Sea $p = 5$ y $q = 4$, ahora se tiene qué:

$$(2[4][5],2[4][5])^2 + ([5]^2-[4]^2, [5]^2-[4]^2)^2 = (0{,}3200) + (0{,}162) = (0{,}3362)$$

Por otro lado se tiene qué $([5]^2+[4]^2, [5]^2+[4]^2)^2 = (0{,}3362)$, de lo cual se concluye qué:

$$(2[4][5],2[4][5])^2 + ([5]^2-[4]^2, [5]^2-[4]^2)^2 = ([5]^2+[4]^2, [5]^2+[4]^2)^2$$

4.4.2 Método de Fibonacci en $\mathbb{Z}[i]$

En el capítulo 3 de este trabajo, se podían deducir algunas ternas pitagóricas a partir de la sucesión de Fibonacci, recordando qué $a = f_n f_{n+3}$, $b = 2f_{n+1}f_{n+2}$ y $c = (f_{n+1})^2 + (f_{n+2})^2$, ahora se observará si se cumple en los $\mathbb{Z}[i]$, sean los números $f_1 = 2, f_2 = 3, f_3 = 5$ y $f_4 = 8$, observe en las primeras ternas pitagóricas gaussianas qué:

$$([2][8], 0)^2 + (2[3][5], 0)^2 = (256{,}0) + (900{,}0) = (1156{,}0)$$

Ahora observe qué $([3]^2+[5]^2, 0)^2 = (1156{,}0)$, de lo cual se deduce qué

$$([2][8], 0)^2 + (2[3][5], 0)^2 = ([3]^2+[5]^2, 0)^2$$

Si se realizan más ejemplos se puede llegar a conjeturar qué:

$$(f_n f_{n+3}, 0)^2 + (2f_{n+1}f_{n+2}, 0)^2 = ([f_{n+1}]^2 + [f_{n+2}]^2, 0)^2$$

Con f_n, f_{n+1}, f_{n+2} y f_{n+3} pertenecientes a la sucesión de Fibonacci. Observe la Justificación

Sea $a = f_n f_{n+3}$, $b = 2f_{n+1}f_{n+2}$ y $c = (f_{n+1})^2 + (f_{n+2})^2$, de lo cual se tiene que:

$$\begin{aligned}(a, 0)^2 + (b, 0)^2 &= (f_n f_{n+3}, 0)^2 + (2f_{n+1}f_{n+2}, 0)^2 \\ &= ([f_n f_{n+3}]^2, 0) + (4[f_{n+1}f_{n+2}]^2, 0)\end{aligned}$$

Ahora:

$$(a, 0)^2 + (b, 0)^2 = ([f_n f_{n+3}]^2 + 4[f_{n+1}f_{n+2}]^2, 0)$$

Como $[f_n f_{n+3}]^2 + 4[f_{n+1}f_{n+2}]^2$ es un número real, la demostración es igual a la justificación explicada en el capítulo 3, luego se concluye qué:

$$(a,0)^2+(b,0)^2=([f_{n+1}]^2+[f_{n+2}]^2,0)^2$$

Qué es lo mismo qué:

$$(a,0)^2+(b,0)^2=(c,0)^2$$

Ya justificado el anterior se observa si se cumple en las segundas ternas pitagóricas, sea la terna pitagórica gaussiana de la forma

$$(a,a)^2+(b,b)^2=(c,c)^2$$

Con $a=f_nf_{n+3}$, $b=2f_{n+1}f_{n+2}$ y $c=(f_{n+1})^2+(f_{n+2})^2$, siendo f_n, f_{n+1}, f_{n+2} y f_{n+3} pertenecientes a la sucesión de Fibonacci, se tendría qué:

$$(f_nf_{n+3},f_nf_{n+3})^2+(2f_{n+1}f_{n+2},2f_{n+1}f_{n+2})^2=([f_{n+1}]^2+[f_{n+2}]^2,[f_{n+1}]^2+[f_{n+2}]^2)^2$$

Observe un ejemplo, sea $f_1=2, f_2=3, f_3=5$ y $f_4=8$ se tendría qué:

$$([2][8],[2][8])^2+(2[3][5],2[3][5])^2=(0{,}512)+(0{,}1800)=(0{,}2312)$$

Ahora $([3]^2+[5]^2,[3]^2+[5]^2)^2=(0{,}2312)$, de lo cual se deduce qué:

$$([2][8],[2][8])^2+(2[3][5],2[3][5])^2=([3]^2+[5]^2,[3]^2+[5]^2)^2$$

Justificación:

$$(f_nf_{n+3},f_nf_{n+3})^2+(2f_{n+1}f_{n+2},2f_{n+1}f_{n+2})^2=(0{,}2[f_nf_{n+3}]^2)+(0{,}8[f_{n+1}f_{n+2}]^2)$$

Ahora como se tiene qué $f_n=f_{n+2}-f_{n+1}$ y $f_{n+3}=f_{n+1}+f_{n+2}$ por la sucesión de Fibonacci, de tal modo qué:

$$(a,a)^2+(b,b)^2=(0,2\{[f_{n+2}-f_{n+1}][f_{n+1}+f_{n+2}]\}^2)+(0{,}8[f_{n+1}f_{n+2}]^2)$$

$$(a,a)^2+(b,b)^2=(0{,}2\{[f_{n+2}]^2-[f_{n+1}]^2\}^2)+(0{,}8[f_{n+1}f_{n+2}]^2)$$

$$(a,a)^2+(b,b)^2=(0{,}2\{[f_{n+2}]^2-[f_{n+1}]^2\}^2)+(0{,}8[f_{n+1}]^2[f_{n+2}]^2)$$

$$(a,a)^2+(b,b)^2=(0{,}2\{[f_{n+2}]^2-[f_{n+1}]^2\}^2+8[f_{n+1}]^2[f_{n+2}]^2)$$

$$(a,a)^2+(b,b)^2=(0{,}2\{[f_{n+2}]^4-2[f_{n+2}]^2[f_{n+1}]^2+[f_{n+1}]^4\}+2\{4[f_{n+1}]^2[f_{n+2}]^2\})$$

$$(a,a)^2+(b,b)^2=(0{,}2\{[f_{n+2}]^4-2[f_{n+2}]^2[f_{n+1}]^2+[f_{n+1}]^4+4[f_{n+1}]^2[f_{n+2}]^2\})$$

$$(a,a)^2+(b,b)^2=(0{,}2\{[f_{n+2}]^4+2[f_{n+2}]^2[f_{n+1}]^2+[f_{n+1}]^4\})$$

Llegando así

$$(a,a)^2+(b,b)^2=(0{,}2\{[f_{n+2}]^2+[f_{n+1}]^2+\}^2)$$

Ahora como $(c,c)^2=(0{,}2\{[f_{n+2}]^2+[f_{n+1}]^2+\}^2)$ se tiene qué:

$$(a,a)^2 + (b,b)^2 = (c,c)^2$$

De esta forma se justifica que el método de la sucesión de Fibonacci también funciona en las ternas pitagóricas gaussianas.

5. Conclusiones y Reflexiones

1. En la consulta histórica sobre ecuaciones diofánticas se detectan algunos métodos de solución que empleaban algunas civilizaciones y culturas para resolver las ecuaciones diofánticas definidas en este trabajo, pero estos métodos eran aplicados a ecuaciones de la forma $ax + by = c$ que estaban sujetas a sistemas de ecuaciones lineales. Desde lo anterior se puede concluir que aquellas civilizaciones buscaban soluciones únicas y solo fue hasta el estudio de Diofánto quien es él percusor de métodos de solución a estas ecuaciones sin estar sujeta a un sistema de ecuaciones lineales, dónde se empezaron a buscar soluciones infinitas, mostrando así que el problema de unicidad e infinidad se ha trabajado desde hace muchos años.
2. En el estudio histórico se encuentra evidencia del trabajo que realizo Diofánto y otros matemáticos para resolver las ecuaciones de la forma $ax + by = c$ sin estar sujetas a sistemas de ecuaciones lineales. Diofánto trabajó estas ecuaciones para resolver problemas netamente matemáticos, pero no se encuentra evidencia alguna si estas ecuaciones responden a soluciones de problemas relacionados con un contexto no necesariamente matemático.
3. En el estudio de la historia se evidencia que el trabajo de Fermat en especial el denominado "*El último teorema de Fermat*", quien dijo que no haría la demostración debido al espacio insuficiente de la hoja, condujo a muchos matemáticos a tratar de solucionar este teorema, pero al momento de darles soluciones produjo otros tipos de ecuaciones diofánticas de grado mayor o igual a 2.
4. Al momento de analizar los métodos de solución a las ecuaciones diofánticas en el conjunto de los enteros, se puede observar que muchos de ellos funcionan debido a la divisibilidad y sus propiedades, esto se debe al tipo de estructura algebraica que tienen los enteros y además abre la posibilidad de realizar estudios acerca de los métodos, en otros conjuntos que tengan una estructura algebraica similar, por ejemplo los duales, polinomios, etc.
5. La estructura de los enteros gaussianos $\mathbb{Z}[i]$, tiene la misma estructura que los números$\mathbb{Z}$, salvo el orden; lo que permitió abordar conceptos interesantes como la divisibilidad y sus propiedades, números primos, $m.c.d.$, entre otros, que fueron fundamentales en el desarrollo de este trabajo, lo que permite deducir qué que sería interesante abordar una teoría de números en los $\mathbb{Z}[i]$.
6. Los métodos estudiados para resolver ecuaciones diofánticas en los enteros, también sirven para resolver ecuaciones diofánticas en los enteros gaussianos, esto se debe al que los dos conjuntos tiene la misma estructura, de esto surge una pregunta como ¿Los métodos estudiados en este trabajo, también funcionan en el anillo de los polinomios, en los números duales o en cualquier estructura similar a la de los números enteros?

7. El estudio de los métodos de solución de algunas ecuaciones diofánticas tanto en el anillo de los números enteros y en el de los enteros gaussianos, permite concluir que esto abre la posibilidad de que los maestros de matemáticas, tengamos más claridad entre las diferencias de conjuntos numéricos y las cualidades que los hace esenciales, además se ve como una herramienta potente para definir cualquier conjunto numérico.
8. Una dificultad que se dio en este trabajo de grado, fue al momento de establecer los métodos de solución a las ecuaciones diofánticas seleccionadas en los enteros gaussianos, porque se trató de establecer de la misma manera que se hizo en los enteros, dejando de lado algunos aspectos importantes de este nuevo conjunto numérico, como las unidades y asociados, lo que luego permitió deducir que no todas las técnicas pueden ser llevadas de la misma manera a un conjunto con una estructura algebraica similar. Lo anterior permite reflexionar que esto se puede convertir en una herramienta poderosa para el docente, puesto que aquí se evidencia la diferencia entre la técnica y la tecnología, en la cual la tecnología será aquella que le permita al docente analizar cada concepto tiene en cuenta las características del universo de discurso del que se hable.

6. Bibliografía

Angel, A. R. (1997). *Algebra Intermedia* (4a ed., Vol. 1). (O. P. Velazco, Trad.) Neucalpan de Juarez, Mexico: Pearson Educación.

Boyer. (1992). *Historia de la matemática.* Madrid: Alianza editorial.

Cardano, G. (1968). *Ars Magna or the rules of algebra.* (R. Witmer, Trad.) New York: Dover Publications, Inc.

Chamizo Lorente, F. (2008). *Euler y la teoría de números.* México.

Espinosa, G. M. (2005). Mexico DF.

Gay, A. (s.f.). *La ciencia, a técinca y la tecnologia .* Tecnorededucativa.

Jiménez , D. (2013). *Aritmética* (Tercera ed.). Valparaiso, Chile: Universidad Valparaiso.

Lehmann, C. (1989). *Geometría Analítica .* Mexico D. F.: Limusa S.A.

Losada Liste, R. (2008). En busca del Arca Perdida. *Revista Sigma* , 85-99.

Panizza, M., Sadovsky, P., & Sessa, C. (1999). La ecuación lineal con dos variables: entre la unicidad y el infinito. *Enseñanza de las Ciencias*, 453-461.

Parra Machío, R. (2009). *Ecuaciones Diofánticas.*

Perez Delgado , J. (1988). *El que hacer matemático. Un recorrido por la historia.* Sevilla, España: Orbis Barcelona.

Sarmiento Rondon, W. (2004). *Sobre las Ecuaciones Diofánticas.* Bucaramanga, Colombia: Universidad Industrial de Santander.

Suma, R. (2005). Fracciones Continuas, números metalicos y sucesiones generalizadas de Fibonacci. *Suma*, 53-63.

UPN, D. (2011). *Criterios para la realizacón y evaluación de trabajo de grado.* Bogotá.

Van Der Waerden, B. L. (1985). *A History of Algebra.* Berlin, Alemania: Springer-Verlag.

Vasco, C. E. (1986). *Ecuaciones de Primero y Segundo Grado.* Bogotá: Notas de Matemáticas.