UN RECORRIDO POR LAS ECUACIONES DIOFÁNTICAS, EL ESTUDIO DENTRO DEL ANILLO DE LOS POLINOMIOS CON COEFICIENTES ENTEROS

BRANDON ALEXANDER SUAREZ REYES

UNIVERSIDAD PEDAGÓGICA NACIONAL
FACULTAD DE CIENCIA Y TECNOLOGÍA
DEPARTAMENTO DE MATEMÁTICA
LICENCIATURA EN MATEMÁTICAS
BOGOTÁ D.C.
2018

UN RECORRIDO POR LAS ECUACIONES DIOFÁNTICAS, EL ESTUDIO DENTRO DEL ANILLO DE LOS POLINOMIOS CON COEFICIENTES ENTEROS

BRANDON ALEXANDER SUAREZ REYES
Código: 2013240066
C.C.: 1013641037

Trabajo presentado al Departamento de Matemáticas de la Universidad Pedagógica Nacional como requisito para optar al título de Licenciado en Matemáticas

Asesor: JORGE PÁEZ
Co-director: PABLO BELTRÁN

Firma asesor

UNIVERSIDAD PEDAGÓGICA NACIONAL
FACULTAD DE CIENCIA Y TECNOLOGÍA
DEPARTAMENTO DE MATEMÁTICA
LICENCIATURA EN MATEMÁTICAS
BOGOTÁ D.C.
2018

Agradecimientos

A la Universidad Pedagógica Nacional por darme la oportunidad de formarme como licenciado en matemáticas.

A Alejandro y Hermencia, mis padres, por su constante apoyo y motivación para lograr sacar adelante este trabajo y brindarme los mejores consejos para la vida.

A los profesores Pablo Beltrán, Jorge Páez y Alberto Donado por su acompañamiento en el desarrollo de este trabajo, sus críticas constructivas e ideas que fueron de vital importancia la elaboración de este documento.

A Kelly, quien me dio el primer empujón anímico para emprender este trabajo y fue un apoyo incondicional durante el desarrollo del mismo.

1. Información General	
Tipo de documento	Trabajo de grado
Acceso al documento	Universidad Pedagógica Nacional. Biblioteca Central
Titulo del documento	Un recorrido por las ecuaciones diofánticas, el estudio dentro del anillo de los polinomios con coeficientes enteros
Autor(es)	Suárez Reyes Brandon Alexander
Director	Páez Ortegón Jorge
Publicación	Bogotá. Universidad Pedagógica Nacional, 2018. 59 p.
Unidad Patrocinante	Universidad Pedagógica Nacional
Palabras Claves	ECUACIONES DIOFÁNTICAS; ANILLO DE POLINOMIOS; TERNAS PITAGÓRICAS.

2. Descripción

En el siguiente trabajo de grado se presenta un estudio que surge como interés del autor, el cual tiene como objetivo estudiar si distintos métodos de solución a ecuaciones diofánticas en los enteros son aplicables en el anillo de polinomios con coeficientes enteros. Con miras a cumplir el objetivo se inicia dando una mirada a hechos históricos de los polinomios y personajes que estuvieron involucrados con estos, posteriormente se revisaron algunos métodos de solución a ecuaciones diofánticas en los enteros. A continuación, se inicia el estudio del anillo en el que se pretende trabajar, observando en especial divisibilidad y propiedades de esta, para luego analizar si los métodos que funcionan en los enteros se pueden aplicar en el anillo en cuestión.

3. Fuentes

Aznar, E. (2007-2012). Biografías, matemáticos: *Enrique R. Aznar*. España. recuperado de https://www.ugr.es/~eaznar/matematicos

Beltrán, P. (2014) *Las ecuaciones en el mundo discreto: un estudio sobre las ecuaciones diofánticas*. Tesis especialización en educación matemática. Universidad Pedagógica Nacional. Bogotá, Colombia.

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

Casalderrey, M. (2000). *Cardano y Tartaglia. Las matemáticas en el renacimiento italiano.* Nivola.

Castellanos, J. (s.f.*) Estructuras Algebraicas*. Recuperado de: http://www.mat.ucm.es/~arrondo/estruturas1

Falk, M. Acevedo, M. (1997). *Recorriendo el álgebra: de la solución de ecuaciones al álgebra abstracta*. Universidad Nacional de Colombia.

Fraleigh, J. (1988) *Álgebra abstracta, primer curso*. ADDISON-WESLEY IBEROAMERICANA S.A. Wilmington, E.E.U.U.

Lentin, A. Rivaud, J. (1973) *Álgebra moderna*. Aguilar S.A. de ediciones. Madrid, España.

Palacios, E. M. (s.f.*) Anillos de Polinomios*. Recuperado de: http://www.ugr.es~bullejos/AlgI/polinomios.pdf

Pettofrezzo, A. Byrkit, D. (1972) *Introducción a la teoría de números*. Prentice-Hall inter-nacional. Nueva Jersey, E.E.U.U.

4. Contenidos

El siguiente trabajo se estructuró en cinco capítulos, en el primero se presentan los objetivos que se consideraron para la elaboración del mismo, en el segundo se muestran algunos personajes trascendentes en la historia de los polinomios y un suceso de relevancia en el desarrollo de este objeto matemático.

En el tercer capítulo se realiza una recopilación de algunos métodos de solución de ecuaciones diofánticas en los números enteros. El cuarto capítulo muestra que las propiedades de anillo se cumplen en dichos polinomios, se revisan propiedades y criterios de divisibilidad y se prueban los métodos de solución elegidos.

El quinto y último capítulo está destinado a presentar las conclusiones que produjo el trabajo, teniendo en cuenta aspectos propiamente de la matemática, del desarrollo matemático del autor y aportes a la labor docente. Finalmente se presenta la bibliografía utilizada durante la elaboración del trabajo.

5. Metodología

La metodología de este trabajo de grado se divide en cuatro etapas, la primera buscar hechos históricos relacionados con polinomios, la segunda estudiar algunos métodos de solución a ecuaciones diofánticas en el anillo de los enteros, fijando la atención en condiciones necesarias y detallando los procedimientos que se deben seguir. La tercera etapa se centra en explorar el anillo de los polinomios con coeficientes enteros, mostrar que propiedades se cumplen allí, profundizando un poco en aspectos relativos a divisibilidad. La cuarta y última se centró en probar si lo métodos estudiados en la etapa dos se podían exportar al anillo explorado en la etapa tres, de esta manera lograr concluir respecto a cada una de las etapas desarrolladas.

6. Conclusiones

- Aunque tanto Z como Z[X] son dominios enteros, se logró mostrar que en lo relativo a orden se comportan de manera diferente. En Z con el orden usual se obtiene una relación que efectivamente es de orden, mientras que en Z[X] la relación establecida no resulta serlo.
- El método de falsa posición logró exportarse, realizándolo tal cual se hace en los enteros. Al igual que los métodos para solucionar ternas pitagóricas.
- El método de Diofanto aunque con aspectos pendientes, logró exportarse realizando algunos cambios.
- El método de pulverización que hace uso del algoritmo de Euclides, no se logró exportar exitosamente por esta misma razón, no es seguro en dos dominios enteros se puedan realizar procedimientos iguales.

- Este trabajo me aportó a la capacidad de investigar en matemáticas, lo que debe ser un permanente en el profesor durante toda su vida.
- Las ecuaciones diofánticas aportan al profesor de matemáticas solidez en sus conocimientos, hay muchos conceptos que se deben utilizar al querer solucionar una ecuación de este tipo.
- Durante este trabajo hubo momentos difíciles, en los que no se veía cómo poder concluirlo dado que no se lograban solucionar las ecuaciones planteadas. Pero la persistencia, constancia y uso de diferentes estrategias matemáticas llevo a elaborar un trabajo que genera orgullo en el autor. En la vida de un docente de matemáticas esto es muy importante, porque, aunque haya días duros, en los que pareciera que no se logran los objetivos, tarde o temprano el camino se iluminará y así generará aún más satisfacción de la esperada.
- Es importante que el profesor de matemáticas siga trabajando en matemáticas, esto da un desarrollo lógico a su manera de abordar un problema y así puede transmitir a sus estudiantes diferentes conocimientos y estrategias que les pueden ser útiles. Adicionalmente saber más matemática ayuda a que los saberes se transmitan de mejor manera, porque nadie puede enseñar lo que no sabe y entre más se tenga conocimiento de una temática mejor será el proceso de enseñanza.
- Queda en estudio la relación que debe darse entre los coeficientes de los polinomios en una ecuación diofántica, para establecer si se puede aplicar el método de Diofanto.
- El desarrollo de este trabajo deja como interrogante si dicha exportación funciona en anillos similares, como el de los Zp o el de los números duales, este podría ser un tema de estudio futuro.

Elaborado por:	Suárez Reyes Brandon Alexander
Revisado por:	Páez Ortegón Jorge

Fecha de elaboración del Resumen:	27	05	2018

Índice general

1. Preliminares 2

1.1. Objetivos 2

1.1.1. General 2

1.1.2. Específicos 2

2. Aspectos históricos de los polinomios 3

3. Algunos métodos de solución a ecuaciones diofánticas 7

3.1. Ecuaciones diofánticas de la forma $ax + by = c$ 7

3.1.1. Falsa posición 7

3.1.2. Método de Diofanto 8

3.1.3. Pulverización 11

3.2 Ecuaciones diofánticas de la forma $a^2 + b^2 = c^2$ 14

3.2.1. Método de Fibonacci 14

3.2.2. Método de Diofanto 16

4. Exportando métodos de solución 18

4.1. El Anillo de los polinomios con coeficientes enteros $\mathbb{Z}[X]$ 18

4.2. Divisibilidad en $\mathbb{Z}[X]$ 22

4.3. Métodos de solución para ecuaciones $p(x)X + g(x) = k(x)Y$ en $\mathbb{Z}[X]$ 34

4.3.1. Falsa posición 34

4.3.2. Método de Diofanto 35

4.3.3. Algoritmo de la división en la solución de ecuaciones diofánticas 39

4.4. Métodos de solución para ecuaciones $(h(x))^2 + (g(x))^2 = (k(x))^2$ en $\mathbb{Z}[X]$ 42
4.4.1. Método de Fibonacci 42
4.4.2. Método de Diofanto 46
5. Conclusiones, reflexiones y proyecciones 49
6. Bibliografía 51

Introducción

Este trabajo surge del interés del autor en abordar la solución de ecuaciones diofánticas en el anillo de los polinomios, esto luego de participar en un espacio académico dirigido por el actual co-director del trabajo de grado, quien desarrolló un estudio de ecuaciones diofánticas en los enteros gaussianos y presentó como una opción el análisis de dichas ecuaciones en otro tipo de anillos. Luego de presentar el anteproyecto ante la Licenciatura en Matemáticas el tema se acotó, por sugerencia del lector se debía especificar que tipo de coeficientes tendrían los polinomios, fue así como se decidió elegir los coeficientes enteros.

Teniendo en cuenta lo anterior se estructuró el siguiente trabajo en cinco capítulos, en el primero se presentan los objetivos que se consideraron para la elaboración de este trabajo, en el segundo se muestran algunos personajes trascendentes en la historia de los polinomios y su desarrollo.

En el tercer capítulo se realiza una recopilación de algunos métodos de solución de ecuaciones diofánticas en los números enteros, esto para tener claridad en la forma de aplicarlos, ya que estos serán los que se pongan a prueba en el anillo elegido. El cuarto capítulo muestra que las propiedades de anillo se cumplen en dichos polinomios, se revisan propiedades y criterios de divisibilidad y se prueban los métodos de solución elegidos.

El quinto y último capítulo está destinado a presentar las conclusiones que produjo el trabajo, teniendo en cuenta aspectos propiamente de la matemática, del desarrollo matemático del autor y aportes a la labor docente.

1. Preliminares

1.1. Objetivos

1.1.1. General

Realizar un estudio sobre métodos de solución de ecuaciones diofánticas en el anillo de los polinomios con coeficientes enteros.

1.1.2. Específicos

- Consultar distintas fuentes bibliográficas que permitan tener una visión histórica sobre polinomios.
- Estudiar métodos de solución de ecuaciones diofánticas en los enteros.
- Estudiar el anillo de los polinomios, en particular cuando los coeficientes son números enteros.
- Observar si algunos de los métodos de solución de uno o más tipos de ecuaciones diofánticas dados en los enteros se puede exportar al anillo de los polinomios, esto con el fin de obtener la solución a ecuaciones diofánticas planteadas en dicho anillo.
- Reconocer algunos elementos que aportan las ecuaciones diofánticas y el anillo de los polinomios al rol docente, específicamente en matemáticas.

2. Aspectos históricos de los polinomios

Son muchos los matemáticos que han estado involucrados con polinomios, en particular con hallar las raíces de dichos objetos matemáticos, es por ello que se centrará la atención en un hecho histórico referente a ello. Pero antes se revisará un poco la vida de quienes estuvieron involucrados, para este caso Cardano, Tartaglia, Ferrari y Ruffini.

Gerolamo Cardano (1501-1576)

Hijo ilegítimo de Fazio Cardano, un abogado italiano con bastos conocimientos matemáticos, tanto así que da Vinci lo consultaba cuando tenía dudas en aspectos geométricos. Gerolamo inició como asistente de su padre, el cual esperaba que este estudiase derecho pero yendo en su contra se inclinó por la medicina, consiguiendo graduarse en 1525.

Luego de malgastar la herencia que le dejó su padre se dedicó al juego (naipes, dados, etc.)dado que era más lo que ganaba que lo que perdía, tiempo después quiso ejercer la medicina pero fracasó por su mala reputación y entró en la pobreza. en 1539 se acercó a Tartaglia, quien se había dado a conocer luego de ganar un reto matemático solucionando ecuaciones de tercer grado. Cardano se ganó la confianza de Tartaglia, al punto que este último le reveló su método para solucionar dichas ecuaciones, con la condición de no hablar de esto hasta que él lo publicará. Pero años después Cardano publicaría su obra Ars Marga, donde explicaba los métodos de solución que Tartaglia desarrolló. Cardano era astrólogo, por esto paso un corto tiempo en prisión, para terminar sus días ejerciendo como médico. Produjo un libro autobiográfico y y con conceptos de probabilidad, eso dada su experiencia en el juego, el libro se llamo *De propria vita* y allí predecía su muerte para el 20 de septiembre de 1576, al parecer ese día se suicidó para que su predicción fuera correcta.

Niccolo Fontana (Tartaglia)(1499-1557)

Niccolo sufrió un ataque por parte de un soldado francés, el cual le causó tartamudez

y de allí provino su apodo. Estudió de manera empírica griego, latín y matemática, siendo esta última con la que se ganó la vida dando clases.

Se hizo famoso al ganar un desafío (que se abordará más adelante) a Ferro, con el cual llamó la atención de los matemáticos más importantes del momento, pero Cardano publicó sus métodos en un acto deshonesto y dado que él tenía más prestigió en la comunidad no le hicieron mucho caso a Tartaglia.

Más tarde Tartaglia tuvo la oportunidad de debatir con Ferrari, luego de haberlo derrotado en el desafio se mostraba muy confiado para el debate, pero Ferrari mostró mayor dominio en el tema y lo derrotó. De ahí en adelante Tartaglia tuvo una vida difícil y murió en la condición en que nació, la pobreza.

Lodovico Ferrari(1522-1565)

Muy joven se hizo secretario de Cardano, quien notó que no solo era bueno escribiendo y leyendo sino que también aprendía matemática con facilidad. Fue así que Ferrari empezó a incursionar en el mundo de la matemática, cuando Cardano se mudó de ciudad fue Ferrari quien con solo 20 años lo reemplazo en el trabajo que desempañaba como profesor.

Trabajo de la mano de Cardano para escribir sobre la soluciones de ecuaciones cúbicas y cuárticas, aunque no desarrollaron métodos propios aprovecharon los trabajos de Ferro, de los que no hay evidencia, y el que Tartaglia le confesó a Cardano esperando que no lo revelara. Luego de publicar el libro y ante el comprensible enojo de Tartaglia, Ferrari se enfrentó en debate publico a este, al cual derrotó.

Regreso a su ciudad natal joven, millonario y con mucho prestigio a vivir con su hermana, la cual fue sindicada por Cardano de haberlo envenenado con arsénico, esto porque no lloró en su funeral y luego de heredar contrajo matrimonio.

Paolo Ruffini(1765-1822)

Desde muy joven Paolo mostró interés por la matemática, tanto así que cuando pudo ingresar a la universidad fue una de las opciones que eligió, también estudio medicina,

filosofía y literatura. Luigi Fantini fue su profesor de geometría y Paolo Cassiani el de cálculo, este último incursionó en la política y su reemplazo en la cátedra que impartía fue el aún estudiante Ruffini. Tiempo después Fantini perdió la visión, razón por la cual Ruffini también se hizo cargo de la que fuera su cátedra,

Ruffini se hizo muy conocido al postular que las ecuaciones quínticas no se podían solucionar por radicales, trabajo que llegó a ser abordado por Bezout, Euler e incluso Lagrange, pero ninguno tuvo éxito en encontrar soluciones o probar que no era posible. La demostración utilizaba teoría de grupos de alta complejidad, llegó a superar a Lagrange en el dominio de este tema, pero fue un adelantado para su tiempo y no le prestaron mucha atención, a excepción de Cauchy que reconoció la importancia de los aportes de Ruffini y generalizó mcuhas de sus ideas en los trabajos que desarrollo sobre el grupo de las permutaciones.

Se destacó por la invención de un algoritmo para hallar raíces de polinomios, algoritmo que aún se utiliza y es conocido como la regla de Ruffini.

Luego de dar un vistazo a la vida de estos personajes, se revisará el momento de la historia al que se hacia referencia.

Desde los babilonios se conocían métodos para solucionar ecuaciones cuadráticas, el desarrollo de estas temáticas lleva a Italia en el siglo XVI donde se empezarían a solucionar ecuaciones cúbicas, el primer protagonista fue Ferro y posteriormente Tartaglia quien descubrió métodos para otro tipo de cúbicas. Estos dos se desafiaron públicamente, desafió en el cual cada uno debía plantear 30 problemas, y en un plazo estipulado se deberían entregar resueltos. Al culminar el plazo Tartaglia entregó los 30 ejercicios resueltos, mientras que Ferro no pudo solucionar ninguno.

Para ese momento Cardano se interesó en lo que pudiera saber Tartaglia, por ello fue hasta donde este y se ganó su confianza, luego de un tiempo Tartaglia le enseño sus estudios bajo la promesa de no hablar de ellos con nadie hasta que él los publicara. Cardano en un acto de total deslealtad publicó su libro más conocido Ars Magna, en el cual estaban explicados los métodos en los que trabajó Tartaglia, el cual no se quedó ca-

llado y reportó este hecho pero su reclamo fue indiferente dado que Cardano era mucho más conocido. Quien salió a atender su reclamo fue Ferrari, mano derecha de Cardano, quien aceptó tener un debate público en el cual se abordarán temas de álgebra. En dicho discurso Ferrari dio una paliza a Tartaglia, quien prefirió darse por vencido y retirarse, dado que Ferrari tenía muchos más fundamentos matemáticos que él. Tartaglia murió en la pobreza, mientras que Cardano gracias a sus obras termino sus días de una forma económicamente más cómoda, al igual que Ferrari.

3. Algunos métodos de solución a ecuaciones diofánticas

En este capítulo se estudiarán algunos métodos para la solución de ecuaciones diofánticas de la forma $ax + by = c$ y $a^2 + b^2 = c^2$, dichos métodos se seleccionaron con base en el trabajo de Beltrán (2014). Los métodos se ejemplificarán en los números enteros.

3.1. Ecuaciones diofánticas de la forma $ax + by = c$

A continuación se presentarán tres métodos de solución para este tipo de ecuaciones, se analizarán las condiciones que deben cumplirse y se mostrarán ejemplos de como aplicar cada método.

3.1.1. Falsa posición

Se parte de una ecuación de la forma $ax + by = c$ donde $a, b, c \in \mathbb{Z}$ y son valores conocidos, mientras que x e $y \in \mathbb{Z}$ pero son las incógnitas. El primer paso es suponer soluciones $x = x_0$ e $y = y_0$ de esta manera se obtiene la ecuación $ax_0 + by_0 = d$, bajo la condición de que d sea múltiplo de c, es decir $d = cf$ y adicional que f sea el máximo común divisor de x_0 e y_0. Luego de ello se plantea la siguiente proporción:

$$\frac{c}{d} = \frac{x}{x_0} = \frac{y}{y_0}$$

De dicha proporción se puede deducir que $x_0 \neq 0$ e $y_0 \neq 0$, despejando a x e y se obtiene:

$$\frac{c}{d} = \frac{x}{x_0} \rightarrow x = \frac{cx_0}{d} \rightarrow x = \frac{cx_0}{cf} \rightarrow x = \frac{x_0}{f}$$
$$\frac{c}{d} = \frac{y}{y_0} \rightarrow y = \frac{cy_0}{d} \rightarrow y = \frac{cy_0}{cf} \rightarrow y = \frac{y_0}{f}$$

Al momento de despejar se evidencia el porqué $d = cf$, ya que esto permite cancelar c y como $f = MCD(x_0, y_0)$ entonces $f|x_0$ y $f|y_0$. Si no se cumplieran estas condiciones la solución podría ser racional puesto que no se garantizaría que el denominador efectivamente divida al numerador.

Ejemplo: sea la ecuación $2x + 6y = 14$ se asignan valores cualesquiera a las incógnitas, por ejemplo $x = 2$ e $y = 4$ y se reemplaza en la parte izquierda de la igualdad, obteniendo:

$$2(2) + 6(4) = 4 + 24 = 28$$

Posteriormente se realiza una proporción entre los resultados que se obtuvieron y los valores que se dieron a las incógnitas, de la siguiente manera:

$$\frac{14}{28} = \frac{x}{2} = \frac{y}{4}$$

De allí se obtiene que:

$$\frac{14}{28} = \frac{x}{2} \rightarrow x = 1$$
$$\frac{14}{28} = \frac{y}{4} \rightarrow y = 2$$

Reemplazando los valores obtenidos para las incógnitas se tiene:

$$2(1) + 6(2) = 14$$

3.1.2. Método de Diofanto

Se parte de una ecuación de la forma $ax + c = by$, se debe cumplir que el máximo común divisor entre a y b divida a c, teniendo esto se aplica el algoritmo de Euclides, de la siguiente manera:

$$b = a \cdot q_1 + r_1 \text{ donde } 0 \leq r_1 < a$$

de esta manera se plantea la siguiente ecuación:

$$x = y \cdot q_1 + z$$

Continuando con el algoritmo se tiene:

$$a = r_1 \cdot q_2 + r_2 \text{ donde } 0 \leq r_2 < r_1$$
$$r_1 = r_2 \cdot q_3 + r_3 \text{ donde } 0 \leq r_3 < r_2$$

De esta manera se plantean correspondientemente las ecuaciones:

$$y = z \cdot q_2 + t$$
$$z = t \cdot q_3 + k$$

Diofanto planteó que se debe dejar de dividir cuando el residuo sea 1, suponiendo que luego de n divisiones se obtiene tal residuo, se llega a la siguiente expresión:

$$r_n = r_{n+1} \cdot q_{n+2} + 1 \rightarrow u = v \cdot q_{n+2} + w$$

Luego de este procedimiento se plantea la siguiente expresión:

$$v + c' = g \cdot w$$

Donde g es el penúltimo residuo, es decir, $g = r_{n+1}$. Para determinar el valor de c' se deben contar la cantidad de divisiones que se realizaron, de ser un número par $c' = c$, de los contrario $c' = -c$. Se asigna un valor cualquiera a w, con esto se obtiene v y haciendo sustituciones se obtienen los valores de x e y.

Veamos un ejemplo en $\mathbb{Z}$: solucionar la ecuación $18x + 6 = 5y$
Lo primero que se hace es mirar que el $MCD(18, 5) = 1$ divide a 6, dado que se cumple se procede a realizar el algoritmo de Euclides. Obteniendo:

$$5 = 18 \cdot 0 + 5$$

De allí se plantea

$$x = 0 \cdot y + z \tag{1}$$

Continuando con el algoritmo de Euclides:

$$18 = 5 \cdot 3 + 3$$
$$5 = 3 \cdot 1 + 2$$
$$3 = 2 \cdot 1 + 1$$

De cada uno de los pasos anteriores se plantean:

$$y = 3 \cdot z + t \tag{2}$$

$$z = t + v \tag{3}$$

$$t = v + w \tag{4}$$

Dado que se realizaron un número par de divisiones se tiene que $c' = c$, observando el penúltimo residuo se aprecia que $g = 2$, con estos valores y asignando $w = 2$ obtenemos el valor de v:

$$v + 6 = 2 \cdot 2$$
$$v = -2$$

Con este valor y reemplazando en (4) se obtiene:

$$t = -2 + 2$$
$$t = 0$$

Ahora reemplazando en (3):

$$z = 0 - 2$$
$$z = -2$$

Con este valor en (2) se obtiene:

$$y = 3 \cdot (-2) + 0$$
$$y = -6$$

Para conocer a x solo falta reemplazar en (1), de allí se obtiene:

$$x = 0 \cdot (-6) + (-2)$$
$$x = -2$$

De esta manera se obtiene una pareja de valores que son solución para la ecuación, a continuación se verificará que efectivamente satisfacen la ecuación:

$$18(-2) + 6 = 5(-6)$$
$$-36 + 6 = -30$$
$$-30 = -30$$

3.1.3. Pulverización

Este método es muy similar al de Diofanto, también se parte de una ecuación de la forma $ax + c = by$ y se utiliza el algoritmo de Euclides, se inicia con:

$$a = b \cdot q_1 + r_1 \text{ donde } 0 \leq r_1 < b$$

De allí se plantea:

$$y = q_1 \cdot x + u$$

Luego se reemplaza el valor de y en la ecuación que se quiere solucionar:

$$ax + c = b(q_1 \cdot x + u)$$
$$ax + c = bq_1x + bu$$

De allí se despeja bu:

$$(a - bq_1)x + c = bu \tag{5}$$

Ahora se retoma el algoritmo de Euclides:

$$b = r_1 \cdot q_2 + r_2 \text{ donde } 0 \leq r_2 < r_1$$

Dado este resultado se plantea:

$$x = q_2 \cdot u + t$$

Se reemplaza el valor de x en (5):

$$(a - bq_1)(q_2u + t) + c = bu \tag{6}$$

Se vuelve al algoritmo de Euclides:

$$r_1 = r_2 \cdot q_3 + r_3 \text{ donde } 0 \leq r_3 < r_2$$

Se plantea

$$u = q_1 \cdot t + v$$

Luego se reemplaza este valor en (6). Se sigue así hasta llegar al penúltimo residuo del algoritmo de Euclides, se supondrá que esto sucede luego de n divisiones, allí se obtendría:

$$r_{n-2} = r_{n-1} \cdot q_n + r_n \text{ donde } 0 \leq r_n < r_{n-1}$$

De allí se plantearía una ecuación donde resulta una nueva incógnita, a esta se le asignará un valor cualquiera y se empezarán a hacer reemplazos con el fin de obtener los valores x e y. A continuación se planteará como ejemplo la misma ecuación que se solucionó con el método de Diofanto, esto para evidenciar el parecido entre los dos métodos y sus diferencias.

Solucionar la ecuación $18x + 6 = 5y$

Primero se aplica el algoritmo de Euclides de la siguiente manera:

$$18 = 5 \cdot 3 + 3$$

De allí se plantea:

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

Ahora se reemplaza el valor de y en la ecuación, obteniendo:

$$18x + 6 = 5(3x + u)$$
$$18x + 6 = 15x + 5u$$

$$3x + 6 = 5u \tag{8}$$

Continuando con el algoritmo de Euclides se tiene:

$$5 = 3 \cdot 1 + 2 \text{ de allí } x = u + t$$

Se reemplaza en (8) este valor que se obtiene para x:

$$3(u + t) + 6 = 5u$$
$$3u + 3t + 6 = 5u$$

$$3t + 6 = 2u \tag{9}$$

Retomando el algoritmo de Euclides se tiene:

$$3 = 2 \cdot 1 + 1 \text{ de allí } u = t + v$$

Reemplazando este valor de u en (9) se obtiene que:

$$3t + 6 = 2(t + v)$$
$$3t + 6 = 2t + 2v$$

$$t + 6 = 2v \tag{10}$$

Dado que el residuo que se obtuvo en el algoritmo de Euclides es 1 se deja de aplicar, ahora se da un valor a v y se empiezan a reemplazar valores para obtener la solución. Para este caso se asigna $v = 2$, y reemplazando en (10) se obtiene:

$$t + 6 = 2(2)$$
$$t = -2$$

Ahora se sustituye este valor de t en (9):

$$3(-2) + 6 = 2u$$
$$u = 0$$

Reemplazando este valor de u en (8) se obtiene:

$$3x + 6 = 5(0)$$
$$x = -2$$

Ya se obtuvo el valor de x, reemplazando este y el de u en (7) se obtendrá y:

$$y = 3(-2) + 0$$
$$y = -6$$

Con este proceso se dedujo que $x = -2$ e $y = -6$, los mismo resultados obtenidos en el método de Diofanto, pero se pueden generar soluciones distintas dando diferentes valores a v.

3.2. Ecuaciones diofánticas de la forma $a^2 + b^2 = c^2$

En esta sección se abordarán dos métodos para obtener las conocidas ternas pitagóricas, teniendo en cuenta que los números de dichas ternas corresponden a las medidas de los catetos e hipotenusa de un triángulo rectángulo, en este caso los catetos son a y b y la hipotenusa c.

3.2.1. Método de Fibonacci

La sucesión de Fibonacci está dada por:

$$f_1 = 1 \qquad f_2 = 1 \qquad f_3 = 2 \qquad ... \qquad f_n = f_{n-1} + f_{n-2}$$

A partir de dicha sucesión se pueden conseguir ternas pitagóricas, para ello se deben elegir cuatro números consecutivos y luego seguir los siguientes pasos:

- Realizar el producto de los dos números ubicados en los extremos, con esto se obtiene la medida del un cateto
- Realizar el doble producto de los números que están en el medio, de esta manera se obtiene la medida del otro cateto

- Sumar los cuadrados de los números del medio, esto para obtener la medida de la hipotenusa

Para llevar a cabo los pasos anteriores se eligen los números f_n, f_{n+1}, f_{n+2} y f_{n+3} de la sucesión de Fibonacci, y aplicando los pasos se obtine:

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

Ahora se procederá a probar que efectivamente con estos pasos se obtiene una terna pitagórica.
Lo primero que se realizará es observar qué es $a^2 + b^2$:

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

Reemplazando $f_n = f_{n+2} - f_{n+1}$ y $f_{n+3} = f_{n+1} + f_{n+2}$ se obtiene:

$$\begin{gathered}
a^2 + b^2 = [(f_{n+2} - f_{n+1}) \cdot (f_{n+1} + f_{n+2})]^2 + [2(f_{n+1} \cdot f_{n+2})]^2 \\
a^2 + b^2 = [(f_{n+2})^2 - (f_{n+1})^2]^2 + [2(f_{n+1} \cdot f_{n+2})]^2 \\
a^2 + b^2 = [(f_{n+2})^2 - (f_{n+1})^2]^2 + 4(f_{n+1})^2 \cdot (f_{n+2})^2 \\
a^2 + b^2 = (f_{n+2})^4 - 2(f_{n+2})^2(f_{n+1})^2 + (f_{n+1})^4 + 4(f_{n+1})^2 \cdot (f_{n+2})^2 \\
a^2 + b^2 = (f_{n+2})^4 + 2(f_{n+2})^2(f_{n+1})^2 + (f_{n+1})^4 \\
a^2 + b^2 = [(f_{n+2})^2 + (f_{n+1})^2]^2
\end{gathered}$$

Reemplazando el valor de c se obtiene que $a^2 + b^2 = c^2$, lo que se quería probar.
A continuación se presentará un ejemplo, sean los números consecutivos 3, 5, 8 y 13, siguiente los pasos anteriores se tiene:

$$a = 3 \cdot 13 = 39 \qquad b = 2(5 \cdot 8) = 80 \qquad c = 5^2 + 8^2 = 89$$

Ahora se eleva al cuadrado cada término:

$$a^2 = 1521 \qquad b^2 = 6400 \qquad c^2 = 7921$$

Basta realizar la suma para verificar que $39^2 + 80^2 = 89^2$.

3.2.2. Método de Diofanto

Diofanto propone como ejercicio descomponer un cuadrado en otros dos, para ello realiza un procedimientos deductivo obteniendo:

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

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

De esta manera se obtiene:

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

Ahora se multiplicará $\frac{(m^2+1)^2}{z^2}$ en los dos lados de la ecuación, lo que genera:

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

Si m es entero solo basta reemplazarlo por cualquier número para verificar que funciona, para este caso se tomará $m = 4$, se obtiene:

$$(4^2+1)^2 = (2\cdot 4)^2 + (4^2-1)^2$$

$$17^2 = 8^2 + 15^2$$

$$289 = 64 + 225$$

Es evidente que el método funciona. Ahora si m fuera un racional se tiene que $m = \frac{p}{q}$ con $q \neq 0$, reemplazando este valor de m se llega a:

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

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

Multiplicando en ambos lados por q^4 se obtiene:

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

Este método funciona para enteros positivos tales que $p > q$, de no ser así el valor $p^2 - q^2$ sería negativo y dado que es la medida de uno de los catetos siempre debe ser positivo. Para verificar la funcionalidad de dicho método se reemplazarán p y q, sean estos $p = 4$ y $q = 3$ se tiene:

$$(4^2 + 3^2)^2 = (2 \cdot 4 \cdot 3)^2 + (4^2 - 3^2)^2$$

$$(16 + 9)^2 = (2 \cdot 12)^2 + (16 - 9)^2$$

$$25^2 = 24^2 + 7^2$$

$$625 = 576 + 49$$

Con este ejemplo queda verificado que el método funciona.

4. Exportando métodos de solución

Antes de analizar los métodos de solución se realizará un estudio sobre el anillo en que se trabajará.

4.1. El Anillo de los polinomios con coeficientes enteros $\mathbb{Z}[X]$

Para empezar se definirá que es un polinomio, para ello partimos de $(\mathbb{Z}, +, \cdot)$ el anillo de los números enteros, $\mathbb{Z}[X]$ es el conjunto de los polinomios en una indeterminada X con coeficientes en $\mathbb{Z}$. Para las siguientes definiciones se hace uso de Fraleigh (1988) y Lentin y Rivaud (1973), un polinomio $p(x)$ es una suma formal finita:

$$\sum_{i=o}^{n} a_i x^i = a_0 + a_1 x + a_2 x^2 + ... + a_n x^n \text{ donde } a_i \in \mathbb{Z}$$

De ahora en adelante se utilizará la siguiente notación cuando sea conveniente:

$$\sum_{i=o}^{n} a_i x^i = a_0 + a_1 x + a_2 x^2 + ... + a_n x^n = (a_0, a_1, a_2, ..., a_n)$$

Ejemplos de ello son: $4x^3 + 2x + 1 = (1, 2, 0, 4)$ y $x^2 = (0, 0, 1)$.
Dichos a_i son los coeficientes del polinomio, si para algún $i > 0$ el coeficiente $a_i \neq 0$ el mayor de dichos valores de i es el grado del polinomio, si no se cumple para para ningún $i > 0$ entonces el polinomio es de grado cero, exceptuando el polinomio nulo $0(x) = 0$ que se presentará más adelante. Por ejemplo para $p(x) = x^5 + 3x^2 + 2x$ se tiene que el grado es 5, para $q(x) = x^3 + 1$ el grado es 3. Dada la notación que se manejará el grado se puede determinar según la longitud de la *n-ada*, si se tiene una terna el grado será dos, una cuaterna implicará un grado 3 y así sucesivamente. Cuando se haga referencia a grado se notará de la siguiente manera:

$$gr(p) = m \qquad \text{donde } p \in \mathbb{Z}[X],\ m \in \mathbb{N} \text{ y } m \text{ es el grado de } p.$$

A continuación se definirán las operaciones suma y multiplicación dentro del conjunto $\mathbb{Z}[X]$:

- Suma:

  Sean $p(x) = (a_0, a_1, a_2, ..., a_n)$ y $q(x) = (b_0, b_1, b_2, ..., b_m)$ la suma se define de la siguiente manera:

$$p(x) + q(x) = (c_0, c_1, c_2, ..., c_n)$$

  donde se supone que $m > n$ y $b_i = 0$ para todo $n < i \leq m$, de esta manera $c_i = a_i + b_i$.

  Teorema: Sean $p(x) = \sum_{i=o}^{n} a_i x^i$ y $q(x) = \sum_{i=o}^{m} b_i x^i \in \mathbb{Z}[X]$ con $gr(p) = n$ y $gr(q) = m$ entonces $gr(p + q) \leq max(n, m)$.

  Demostración. La demostración se dividirá en dos casos, el primero es que los dos polinomios sean del mismo grado, esto es $n = m$, cuando se realice la suma el coeficiente $a_n + b_m$ será el de mayor grado, pero dado que a_n y $b_m \in \mathbb{Z}$ se puede dar que $a_n + b_m = 0$ dado que hay inversos aditivos, en dicho caso este término del polinomio se anularía, por lo cual su grado sería a lo más $n - 1$. De no anularse el término el grado de dicha suma sería n, con lo cual se obtiene que $gr(p + q) \leq n$. El segundo caso es que sin perdida de generalidad $n > m$, en esta situación el coeficiente de mayor grado luego se efectuar la suma sería a_n, por lo cual se puede garantizar que $gr(p + q) = n$. Del anterior razonamiento se puede concluir que $gr(p + q) \leq max(n, m)$ □

- Multiplicación:

  Sean $p(x) = (a_0, a_1, a_2, ..., a_n)$ y $q(x) = (b_0, b_1, b_2, ..., b_m)$ la multiplicación se define de la siguiente manera:

$$p(x) \cdot q(x) = (d_0, d_1, ..., d_i, ..., d_{n+m})$$

  Donde:

$$d_i = \sum_{k=0}^{i} a_k b_{i-k}$$

Teorema: Sean $p(x) = \sum_{i=o}^{n} a_i x^i$ y $q(x) = \sum_{i=o}^{m} b_i x^i \in \mathbb{Z}[X]$ con $gr(p) = n$ y $gr(q) = m$ entonces $gr(p \cdot q) = m + n$.

Demostración. Dada la definición de multiplicación se puede concluir que el coeficiente del término de mayor grado es $a_n b_m$, donde a_n y $b_m \in \mathbb{Z}$, dado que $\mathbb{Z}$ no tiene divisores de cero ya que este es un dominio entero se puede garantizar que $a_n b_m \neq 0$. Con lo anterior se garantiza que el término $a_n b_m x^{n+m}$ no se hace nulo, por ende $gr(p \cdot q) = m + n$. □

Teorema: el conjunto $\mathbb{A}[X]$ de todos los polinomios en una indeterminada X con coeficientes en un anillo $\mathbb{A}$, es un anillo bajo la suma y multiplicación polinomial. Si $\mathbb{A}$ es conmutativo entonces $\mathbb{A}[X]$ lo es, y si $\mathbb{A}$ tiene unitario 1, entonces 1 también es unitario en $\mathbb{A}[X]$.(Fraleigh, 1988, p. 269)
Dado que $\mathbb{Z}$ es un anillo conmutativo con unitario y este es 1, el anterior teorema garantiza que $\mathbb{Z}[X]$ es un anillo conmutativo que también tiene como unitario a 1. De esta manera se puede concluir que $\mathbb{Z}[X]$ cumple las siguientes propiedades para la suma:

- Asociativa

$$p(x) + (q(x) + r(x)) = (p(x) + q(x)) + r(x)$$

- Elemento neutro

$$\text{Existe } 0(x) = (0) \text{ tal que } p(x) + 0(x) = 0(x) + p(x) = p(x)$$
$$\text{Se definirá de acuerdo a Palacios (s.f) que } gr(0) = -\infty$$

- Inverso

$$\text{Para todo } p(x) \text{ existe } -p(x) \text{ tal que } p(x) + (-p(x)) = 0(x) = (0)$$

- Conmutativa

$$p(x) + q(x) = q(x) + p(x)$$

Para la multiplicación se cumplen las siguientes propiedades:

- Asociativa

$$p(x) \cdot (q(x) \cdot r(x)) = (p(x) \cdot q(x)) \cdot r(x)$$

- Conmutativa

$$p(x) \cdot q(x) = q(x) \cdot p(x)$$

- Elemento neutro de la multiplicación

$$\text{Existe } e(x) = (1) \text{ tal que } p(x) \cdot e(x) = e(x) \cdot p(x) = p(x)$$

Adicional a esto se cumple la propiedad distributiva, la cual relaciona las dos operaciones definidas, suma y multiplicación, de la siguiente manera:

$$p(x) \cdot (q(x) + r(x)) = p(x) \cdot q(x) + p(x) \cdot r(x)$$

Con lo anterior se tiene que $\mathbb{Z}[X]$ tiene estructura de anillo al igual que $\mathbb{Z}$, pero adicionalmente $\mathbb{Z}$ es un dominio entero así que se procederá a demostrar que $\mathbb{Z}[X]$ también lo es, para ello se recurre a un teorema encontrado en Castellanos (s.f. p.14).
Teorema: Si $\mathbb{A}$ es un dominio entero entonces $\mathbb{A}[X]$ también lo es, y las unidades de $\mathbb{A}[X]$ son las mismas que las de $\mathbb{A}$.

Demostración. Sean $p(x) = (a_0, a_1, a_2, ..., a_n)$ y $q(x) = (b_0, b_1, b_2, ..., b_m) \in \mathbb{A}[X]$, se centrará la atención en observar que sucede si $p(x) \cdot q(x) = (0)$.
Se supone que $p(x) \cdot q(x) = (0)$ entonces $gr(p \cdot q) = -\infty$, de allí $m + n = -\infty$, por ende $m = -\infty$ ó $n = -\infty$ con esto se concluye que $p(x) = (0)$ ó $q(x) = (0)$, lo que implica que $\mathbb{A}[X]$ es un dominio entero.
Para determinar las unidades se supone que $p(x) \cdot q(x) = 1$, de allí $m + n = 0$ pero $m, n \in \mathbb{N}$ por tal razón $m = n = 0$, con esto $p(x) = a$ y $q(x) = b$ donde $a, b \in \mathbb{A}$ y son unidades de este. □

Del anterior teorema se concluye que $\mathbb{Z}[X]$ es un dominio entero, es decir no tiene divisores de cero y por ende se puede afirmar que se cumple la propiedad cancelativa, esto es:

$$\text{Si } p(x) \cdot q(x) = p(x) \cdot r(x) \text{ entonces } q(x) = r(x)$$

Adicional el teorema proporciona las unidades de $\mathbb{Z}[X]$, estos son los polinomios:

$$u_1(x) = (1) \qquad \text{y} \qquad u_2(x) = (-1)$$

Luego de explorar la estructura de $\mathbb{Z}[X]$ se buscará comparar sus elementos, para el caso de $\mathbb{Z}$ esto es posible y resulta una relación de orden, ahora se definirá una relación en $\mathbb{Z}[X]$ con el fin de poder comparar dichos elementos.

$$\text{Sean } p(x), q(x) \in \mathbb{Z}[X] \text{ se dice que } p(x) \prec q(x) \text{ si y solo si } gr(p) \leq gr(q)$$

Bajo esta relación hay muchos polinomios que no se pueden comparar, un ejemplo de ello son $p(x) = (1, 0, 0, 1)$ y $q(x) = (5, 16, 5, 5)$ aunque tienen coeficientes diferentes no se pueden relacionar.

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

A partir de lo trabajado anteriormente se definirá divisibilidad en $\mathbb{Z}[X]$:

> *Definición*: sean $p(x)$, $s(x) \in \mathbb{Z}[X]$, se dice que $s(x)$ divide a $p(x)$ $(s(x)|p(x))$ si y solo si existe un único $q(x) \in \mathbb{Z}[X]$ tal que $p(x) = s(x) \cdot q(x)$.

Un ejemplo de esto es: $(1, 1)|(-1, 0, 1)$ ya que $(-1, 0, 1) = (1, 1) \cdot (-1, 1)$

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

A continuación se realizará un estudio de propiedades de divisibilidad en $\mathbb{Z}[X]$, para ello se partirá de las propiedades que se cumplen en $\mathbb{Z}$. Para todo a, b ,$c \in \mathbb{Z}$ se cumple que:

1. $a|a$

2. Si $a|b$ y $b|c$ entonces $a|c$

3. $1|a$

4. $a|0$

5. Si $a|0$ entonces $a = 0$ (No hay divisores de 0)

6. Si $a|1$ entonces $a = 1$ o $a = -1$

7. Si $a|b$ y $b|a$ entonces $a = -b$ o $a = b$

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 $0 \leq r < |b|$

Propiedad 1: $p(x)|p(x)$

Demostración. Esta propiedad es consecuencia inmediata de la existencia de unitario en $\mathbb{Z}[X]$, puesto que $p(x) \cdot e(x) = p(x)$, esto satisface la definición de divisibilidad obteniendo así que $p(x)|p(x)$. □

Propiedad 2: Si $p(x)|q(x)$ y $q(x)|r(x)$ entonces $p(x)|r(x)$

Demostración. utilizando la definición de divisibilidad se tiene dado que
$p(x) \cdot k(x) = q(x)$ y $q(x) \cdot m(x) = r(x)$, reemplazando $q(x)$ se obtiene:

$$[p(x) \cdot k(x)] \cdot m(x) = r(x)$$

Utilizando la propiedad asociativa de la multiplicación se tiene que:

$$p(x) \cdot [k(x) \cdot m(x)] = r(x)$$

Dada la existencia de $k(x) \cdot m(x)$ y aplicando la definición de divisibilidad en $\mathbb{Z}[X]$ se concluye que $p(x)|r(x)$. □

Propiedad 3: $e(x)|p(x)$

La demostración de esta propiedad es inmediata, esto por la definición de divisibilidad en $\mathbb{Z}[X]$ y que (1) es el unitario en $\mathbb{Z}[X]$.

Propiedad 4: $p(x)|0(x)$

Demostración. Sea $p(x) \in \mathbb{Z}[X]$, para que $p(x)$ divida a $0(x)$ debe cumplirse que:

$$p(x) \cdot q(x) = 0(x)$$

Dado que $\mathbb{Z}[X]$ es un dominio entero la única opción para $q(x)$ es ser igual a $0(x)$. Utilizando la existencia de $0(x)$ y la definición de divisibilidad en $\mathbb{Z}[X]$ queda demostrado que $p(x)|0(x)$. □

Propiedad 5: Si $0(x)|p(x)$ entonces $p(x) = (0)$

Demostración. Dado que $\mathbb{Z}[X]$ es un dominio entero esta propiedad es inmediata. □

Propiedad 6: Si $p(x)|e(x)$ entonces $p(x)$ es unidad.

Demostración. la demostración es consecuencia de la definición de divisibilidad en $\mathbb{Z}[X]$, y se tiene que las unidades son (1) y (-1). □

Asociados en $\mathbb{Z}[X]$: primero se recordará que en $\mathbb{Z}$ se definen como asociados dos números p y q tales que $p|q$ y $q|p$, al definir de la misma manera asociados en $\mathbb{Z}[X]$ se tiene que dos polinomios $p(x)$ y $q(x)$ son asociados si y solo si $p(x)|q(x)$ y $q(x)|p(x)$. Sea $p(x) = (a_0, a_1, ..., a_n)$ y teniendo en cuenta la definición de asociado, $p(x)$ tendrá exactamente dos asociados, ellos son:

1. $p(x) = (a_0, a_1, ..., a_n)$
2. $-p(x) = (-a_0, -a_1, ..., -a_n)$.

Propiedad 7: Si $p(x)|q(x)$ y $q(x)|p(x)$ entonces $p(x) = q(x)$ o $p(x) = -q(x)$

Demostración. Se tienen dadas:

$$q(x) = p(x) \cdot m(x) \tag{11}$$

$$p(x) = q(x) \cdot k(x) \tag{12}$$

reemplazando $p(x)$ en (11) se obtiene que:

$$q(x) = [q(x) \cdot k(x)] \cdot m(x)$$

Utilizando la propiedad asociativa se obtiene:

$$q(x) = q(x) \cdot [k(x) \cdot m(x)]$$

Dada la estructura de $\mathbb{Z}[X]$ se tiene propiedad cancelativa, aplicándola se obtiene:

$$(1) = k(x) \cdot m(x)$$

Es decir que $k(x)$ y $m(x)$ deben ser unidades, en particular $k(x)$, dado que las unidades son (1) y (-1) se puede concluir que:

$$k(x) = (1) \qquad \text{o} \qquad k(x) = (-1)$$

Al reemplazar $k(x)$ en (12) se concluye que $p(x) = q(x)$ o $p(x) = -q(x)$. □

Propiedad 8: $p(x)| - p(x)$

Demostración. utilizando la definición de divisibilidad en $\mathbb{Z}[X]$ para que $p(x)| - p(x)$ se debe cumplir que $p(x) \cdot q(x) = -p(x)$, basta hacer $q(x) = (-1)$ para obtener dicha igualdad. Dada la existencia de (-1) queda demostrado que $p(x)| - p(x)$. □

Propiedad 9: Si $p(x)|q(x)$ entonces $p(x) \prec q(x)$, es decir $gr(p) \leq gr(q)$

Demostración. Se tiene que $p(x)|q(x)$, esto es:

$$p(x) \cdot s(x) = q(x)$$

Sean $gr(p) = m$, $gr(s) = l$ y $gr(q) = n$, dos polinomios que sean iguales deben tener el mismo grado, esto es:

$$gr(p \cdot s) = gr(q)$$

Aplicando la propiedad del grado para la multiplicación (pag. 18) se tiene:

$$m + l = n$$

Dado que m,l,$n \in \mathbb{N}$ y utilizando la definición de menor que, se deduce que $m \leq n$, con lo que se demuestra que $p(x) \prec q(x)$. □

Propiedad 10: Si $p(x)|q(x)$ entonces $p(x)|q(x) \cdot s(x)$

Demostración. Se tiene que $p(x)|q(x)$, esto es:

$$p(x) \cdot t(x) = q(x)$$

Por la propiedad cancelativa de la multiplicación en $\mathbb{Z}[X]$ se puede multiplicar en ambos lados de la igualdad por el mismo valor:

$$[p(x) \cdot t(x)] \cdot s(x) = q(x) \cdot s(x)$$

Aplicando la propiedad asociativa de la multiplicación se obtiene que:

$$p(x) \cdot [t(x) \cdot s(x)] = q(x) \cdot s(x)$$

Por la definición de divisibilidad en $\mathbb{Z}[X]$ se demuestra que $p(x)|q(x) \cdot s(x)$. □

Propiedad 11: Si $p(x)|q(x)$ y $p(x)|s(x)$ entonces $p(x)|[q(x) + s(x)]$

Demostración. Por la definición de divisibilidad en $\mathbb{Z}[X]$ se tiene que:

$$p(x) \cdot t(x) = q(x) \qquad\qquad p(x) \cdot k(x) = s(x)$$

Sumando se obtiene:

$$p(x) \cdot t(x) + p(x) \cdot k(x) = q(x) + s(x)$$

Aplicando la propiedad distributiva se obtiene que:

$$p(x) \cdot [t(x) + k(x)] = q(x) + s(x)$$

Utilizando la definición de divisibilidad en $\mathbb{Z}[X]$ se demuestra que $p(x)|[q(x)+s(x)]$. □

Propiedad 12(Algoritmo de la división en $\mathbb{Z}[X]$)

Para el caso de $\mathbb{Z}[X]$ este algoritmo tiene restricciones, no se cumple para todo par de polinomios, dado que en ocasiones aparecen coeficientes racionales. Luego de los análisis realizados en el desarrollo del trabajo de grado se obtuvo el siguiente resultado:

Sean $p(x) = (a_0, a_1, ..., a_n)$ y $k(x) = (b_0, b_1, ..., b_m) \in \mathbb{Z}[X]$, $p(x) \neq (0)$. Si

- $b_m | b_i \ \forall i \in I, I = \{0, 1, 2, ..., m\}$

- $b_m | a_j \ \forall j \in J, J = \{m, m+1, ..., n\}$

Entonces existen únicos $q(x)$ y $r(x)$ en $\mathbb{Z}[X]$, tales que $p(x) = q(x) \cdot k(x) + r(x)$ con $gr(r) < gr(p)$.

Demostración. Se tomarán dos casos, el primero que $gr(p) < gr(k)$, basta tomar a $q(x) = (0)$ y $r(x) = p(x)$ y de esta manera se tiene que $p(x) = (0) \cdot k(x) + p(x)$, donde $gr(p) < gr(k)$.
El segundo caso es que $gr(p) \geq gr(k)$, se recurrirá a la forma usual en que se dividen polinomios, planteando la siguiente división:

$$\begin{array}{l|l} a_n x^n + a_{n-1} x^{n-1} + ... + a_1 x + a_0 & b_m x^m + b_{m-1} x^{m-1} + ... + b_1 x + b_0 \\ & \\ & \end{array}$$

Se tiene que $b_m | a_n$ de allí que $a_n = b_m \cdot c_t$, de esta manera se obtiene el primer término de $q(x)$, el cual con certeza es entero. Ahora se supone que $c_t \cdot b_{m-1} = d$, $d \in \mathbb{Z}$, así sucesivamente se procede obteniendo:

$$\begin{array}{l|l} a_n x^n + a_{n-1} x^{n-1} + ... + a_1 x + a_0 & b_m x^m + b_{m-1} x^{m-1} + ... + b_1 x + b_0 \\ \underline{-a_n x^n - d x^{n-1} - ...} & \\ & \end{array}$$

Realizando las operaciones correspondientes se llega a:

$$\begin{array}{l|l} a_n x^n + a_{n-1}x^{n-1} + ... + a_1 x + a_0 & b_m x^m + b_{m-1}x^{m-1} + ... + b_1 x + b_0 \\ \cancel{-a_n x^n} - dx^{n-1} - ... & \\ \hline (a_{n-1} - d)x^{n-1} + ... & c_t x^{n-m} \end{array}$$

Ahora bien, se tiene que $b_m | a_{n-1}$ y por la forma en que se consiguió d también $b_m | d$, como todos son enteros se recurre a propiedades de divisibilidad en $\mathbb{Z}$, en particular la propiedad 11, de allí que $b_m | (a_{n-1} - d)$ por ende se supone que $a_{n-1} - d = b_m \cdot c_{t-1}$. Aplicando esto a la división que se estaba realizando, se obtiene:

$$\begin{array}{l|l} a_n x^n + a_{n-1}x^{n-1} + ... + a_1 x + a_0 & b_m x^m + b_{m-1}x^{m-1} + ... + b_1 x + b_0 \\ \cancel{-a_n x^n} - dx^{n-1} - ... & \\ \hline \cancel{(a_{n-1} - d)x^{n-1}} + ... & c_t x^{n-m} + c_{t-1}x^{n-m-1} \\ -\cancel{(a_{n-1} - d)x^{n-1}} - ... & \end{array}$$

Para los demás coeficientes se realiza un proceso análogo, teniendo en cuenta que dicho procedimiento culminará en el coeficiente de $p(x)$ cuyo grado sea igual a m. Obteniendo:

$$\begin{array}{l|l} a_n x^n + a_{n-1}x^{n-1} + ... + a_1 x + a_0 & b_m x^m + b_{m-1}x^{m-1} + ... + b_1 x + b_0 \\ \cancel{-a_n x^n} - dx^{n-1} - ... & \\ \hline \cancel{(a_{n-1} - d)x^{n-1}} + ... & c_t x^{n-m} + c_{t-1}x^{n-m-1} + ... + c_0 \\ -\cancel{(a_{n-1} - d)x^{n-1}} - ... & \\ \vdots & \\ r(x) & \end{array}$$

Donde $q(x) = c_t x^{n-m} + c_{t-1}x^{n-m-1} + ... + c_0$, dado que para todo subíndice de c se tiene que $c \in \mathbb{Z}$ entonces $q(x) \in \mathbb{Z}[X]$, por la forma en que se procede se puede afirmar que

$r(x) \in \mathbb{Z}[X]$ y con certeza será de grado menor al de $k(x)$, esto porque $b_m | a_m$ lo cual implica que dicho término de $p(x)$ se puede anular. Así se obtiene que existen $q(x)$ y $r(x)$ pertenecientes a $\mathbb{Z}[X]$ tales que $p(x) = q(x) \cdot k(x) + r(x)$ y $gr(r) < gr(k)$.
Ahora se verificará la unicidad, para ello se supone que:

$$p(x) = q_1(x) \cdot k(x) + r_1(x) \qquad \text{y} \qquad p(x) = q_2(x) \cdot k(x) + r_2(x)$$

Igualando las expresiones se obtiene:

$$q_1(x) \cdot k(x) + r_1(x) = q_2(x) \cdot k(x) + r_2(x)$$

Transponiendo términos y aplicando propiedad distributiva se obtiene:

$$[q_1(x) - q_2(x)] \cdot k(x) = r_2(x) - r_1(x)$$

De allí se obtiene que $k(x) | (r_2(x) - r_1(x))$, pero $gr(r_1) < gr(k)$ y $gr(r_2) < gr(k)$, dadas estas condiciones la única posibilidad es que $r_2(x) - r_1(x) = (0)$, es decir $r_1(x) = r_2(x)$, y reemplazando esto se obtiene:

$$[q_1(x) - q_2(x)] \cdot k(x) = (0)$$

dado que $k(x) \neq (0)$ se debe cumplir que $q_1(x) - q_2(x) = (0)$, de allí que $q_1(x) = q_2(x)$.
Con lo que se demuestra la unicidad de $q(x)$ y $r(x)$. □

A continuación se plantearán tres ejemplos, uno en el que no se cumplen las condiciones del teorema anterior y efectivamente no se puede realizar el algoritmo de la división, y otro dos donde sí se cumplen y el algoritmo funciona:
Ejemplo 1:
Sean $p(x) = (3, 5, 8, 4)$ y $k(x) = (2, 3)$, hallar $q(x)$ y $r(x)$.
Lo primero es identificar el polinomio de mayor grado, para este caso $gr(p) > gr(k)$ entonces $p(x) = q(x) \cdot k(x) + r(x)$, realizando la división se obtiene:

$$(3, 5, 8, 4) = \left(\frac{13}{27}, \frac{16}{9}, \frac{4}{3}\right) \cdot (2, 3) + \left(\frac{55}{27}\right)$$

Como se puede ver, para este caso tanto $q(x)$ como $r(x)$ no pertenecen a $\mathbb{Z}[X]$.

Ejemplo 2:

Sean $p(x) = (4, 2)$ y $k(x) = (2, 8, 6)$, hallar $q(x)$ y $r(x)$.

De nuevo se busca el polinomio de mayor grado, para este caso $gr(k) > gr(p)$ entonces $k(x) = q(x) \cdot p(x) + r(x)$, realizando la división se obtiene:

$$(2, 8, 6) = (-2, 3) \cdot (4, 2) + (10)$$

Se obtienen $q(x)$ y $r(x)$ pertenecientes a $\mathbb{Z}[X]$.

Ejemplo 3:

Sean $p(x) = (5, 7, 12, 12, 9, 15)$ y $k(x) = (6, 24, 3)$, hallar $q(x)$ y $r(x)$.

En este caso $gr(p) > gr(k)$ entonces $p(x) = q(x) \cdot k(x) + r(x)$, realizando la división se obtiene:

$$(5, 7, 12, 12, 9, 15) = (-2242, 290, -37, 5) \cdot (6, 24, 3) + (13457, 52075)$$

Para este caso se plantearon polinomios de mayor grado, y aunque los coeficientes de $q(x)$ y $r(x)$ son "grandes", estos pertenecen a $\mathbb{Z}[X]$.

Criterios de irreducibilidad

A continuación se dará un vistazo a criterios de divisibilidad (irreducbilidad) en $\mathbb{Z}[X]$, presentes en Fraleigh (1988) y Lentin y Rivaud (1973):

- Criterio 1

  Sean $p(x) = (a_0, a_1, ..., a_n)$ y $q(x) = (b_0, b_1) \in \mathbb{Z}[X]$ con $a_n, b_1 \neq 0$. Si $q(x)|p(x)$ entonces $b_1|a_n$ y $b_0|a_0$.

  Demostración. Por la definición de divisibilidad en $\mathbb{Z}[X]$ se tiene:

  $$p(x) = k(x) \cdot q(x)$$

  Sea $k(x) = (c_0, c_1, ..., c_m)$, reemplazando se obtiene:

  $$(a_0, a_1, ..., a_n) = (c_0, c_1, ..., c_m) \cdot (b_0, b_1)$$

Aplicando la definición de multiplicación de $\mathbb{Z}[X]$:

$$(a_0, a_1, ..., a_n) = (c_0 \cdot b_0, ..., c_m \cdot b_1) \cdot (b_0, b_1)$$

Para que dicha igualdad se cumpla deben ser iguales componente a componente, de allí que:

$$a_0 = c_0 \cdot b_0 \qquad \text{y} \qquad a_n = c_m \cdot b_1$$

Aplicando la definición de divisibilidad en $\mathbb{Z}$ se demuestra que $b_1|a_n$ y $b_0|a_0$. $\square$

Las demostraciones de los criterios que se presentarán a continuación se pueden encontrar en libros de álgebra abstracta, por ello no se presentarán en este documento.

- Criterio 2 (Teorema del factor)
  Sea $p(x) \in \mathbb{Z}[X]$, se dice que $x - \alpha$ con $\alpha \in \mathbb{Z}$ es un factor de de $p(x)$ si y solo si $p(\alpha) = 0$.

- Criterio 3 (Teorema del residuo)
  Sea $p(x) \in \mathbb{Z}[X]$, el valor de $p(\alpha)$ con $\alpha \in \mathbb{Z}$ es igual al residuo de dividir $p(x)$ entre $x - \alpha$.

- Criterio 4
  Sea $p(x) \in \mathbb{Z}[X]$ de grado dos o tres. Entonces $p(x)$ es reducible en $\mathbb{Z}[X]$ si solo si existe un $\alpha \in \mathbb{Z}$ tal que $p(\alpha) = 0$.

Definición: un polinomio $p(x) = (a_0, a_1, ..., a_n) \in \mathbb{Z}[X]$ se llama primitivo si y solo si:

$$MCD(a_0, a_1, ..., a_n) = 1.$$

- Criterio 5 (Lema de Gauss)

  Si $p(x) \in \mathbb{Z}[X]$ un polinomio primitivo se puede factorizar como $p(x) = k(x) \cdot r(x)$ con $k(x), r(x) \in \mathbb{Q}[X]$, entonces $p(x)$ puede expresarse como $p(x) = q(x) \cdot h(x)$ donde $q(x), h(x) \in \mathbb{Z}[X]$.

  Definición: un polinomio $p(x) = (a_0, a_1, ..., a_n) \in \mathbb{Z}[\mathbb{X}]$ se dice mónico si $a_n = 1$.

- Criterio 6

  Si $p(x)$ es un polinomio mónico con $a_0 \neq 0$ y si existe $\alpha \in \mathbb{Z}$ tal que $p(\alpha) = 0$, entonces $\alpha | a_0$.

- Criterio 7 (criterio de Eisenstein)

  Sea $p(x) = (a_0, a_1, ..., a_n) \in \mathbb{Z}[X]$, sea $p \in \mathbb{Z}$ un número primo tal que $p \nmid a_n$, $p | a_i$ para todo $i = 0, 1, 2, ..., n-1$ y $p^2 \nmid a_0$ entonces $p(x)$ es irreducible en $\mathbb{Z}[X]$.

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

Para abordar lo que serían los primos en $\mathbb{Z}[X]$, se retomará la definición de primo en $\mathbb{Z}$, un polinomio es primo o irreducible si y solo si únicamente lo dividen las unidades y los asociados, bajo esta definición un polinomio primo tendrá exactamente cuatro divisores. Sea $p(x)$ un polinomio primo, los divisores de este son:

1) $p(x)$
2) $-p(x)$
3) (1)
4) (-1)

Para determinar si un polinomio es primo se utilizarán los criterios de irreducibilidad presentados anteriormente y los casos de factorización ya conocidos.

Máximo común divisor en $\mathbb{Z}[X]$

Dado que en $\mathbb{Z}$ el $M.C.D.$ se define como el mayor divisor que tengan en común n números enteros, para este caso se definirá de manera similar.

Definición: un polinomio $d(x) \in \mathbb{Z}[X]$, divisor común de mayor grado de $p_1(x), p_2(x), ..., p_n(x)$

se llama máximo común divisor ($M.C.D.$) de dichos n polinomios.

Para obtener el M.C.D. en $\mathbb{Z}$ se utiliza en algoritmo de Euclides, se verá en el siguiente ejemplo como se consigue.
Para hallar el M.C.D. de 48 y 80 se realiza el algoritmo de Euclides de manera usual, así:

$$80 = (1)48 + 32$$
$$48 = (1)32 + 16$$
$$32 = (2)16 + 0$$

El penúltimo residuo de las divisiones es el máximo común divisor, 16 en este caso.
Para el caso de $\mathbb{Z}[X]$ el algoritmo de Euclides no se puede garantizar entre dos polinomios, se deberían cumplir las condiciones de la propiedad 12 tantas veces como divisiones se deban realizar. A lo largo de este trabajo no se lograron encontrar dos polinomios que cumplan dichas condiciones, en los casos que se podían realizar dos o más divisiones el último residuo conseguido era no nulo, es decir no se llegaba al cero, por ende el algoritmo de Euclides en el caso de $\mathbb{Z}[X]$ se culmina al obtener un residuo de grado cero.
A continuación se mostrará mediante un ejemplo que, el algoritmo de Euclides no funciona como medio para conseguir el M.C.D. entre dos polinomios.
Hallar el M.C.D. entre $p(x) = (2, 3, 1)$ y $k(x) = (3, 10, 9, 2)$. Para empezar se revisan las condiciones de la propiedad 12, dado que no se cumplen, el algoritmo de la división no se puede realizar y por ende el de Euclides tampoco. Pero los dos polinomios se pueden factorizar, obteniendo:

$$(2, 3, 1) = (1, 1)(2, 1)$$
$$(3, 10, 9, 2) = (1, 1)(3, 1)(1, 2)$$

Luego de esto se hace evidente que el $M.C.D.[(2, 3, 1), (3, 10, 9, 2)] = (1, 1)$.

4.3. Métodos de solución para ecuaciones $p(x)X + g(x) = k(x)Y$ en $\mathbb{Z}[X]$

A continuación se tratará de realizar la exportación de métodos de solución de ecuaciones diofánticas, se presentarán tres métodos al igual que en el capítulo 3, a diferencia que pulverización no está dado que el algoritmo de Euclides no funciona en $\mathbb{Z}[X]$ como lo hace en $\mathbb{Z}$.

4.3.1. Falsa posición

Sea la ecuación $(3,0,1)X + (1,1)Y = (9,8,4,1)$ se deben suponer valores X_0 e Y_0 tales que el resultado sea múltiplo de $(9,8,4,1)$, es por ello que se supondrá:

$$X_0 = (4,2)$$
$$Y_0 = (6,4)$$

Reemplazando estos valores se obtiene:

$$(3,0,1)(4,2) + (1,1)(6,4) = (12,6,4,2) + (6,10,4) = (18,16,8,2)$$

Se puede observar que con estos valores el resultado es múltiplo de $(9,8,4,1)$, solo basta multiplicarlo por (2). Luego de verificar esto se procede a realizar el trabajo con razones:

$$\frac{(9,8,4,1)}{(18,16,8,2)} = \frac{X}{(4,2)}$$
$$\frac{(9,8,4,1)}{(18,16,8,2)} = \frac{Y}{(6,4)}$$

De allí se obtienen:

$$X = (2,1)$$
$$Y = (3,2)$$

Ahora se comprobará si efectivamente los valores hallados son solución para la ecuación diofántica:

$$(3,0,1)(2,1) + (1,1)(3,2) = (6,3,2,1) + (3,5,2) = (9,8,4,1)$$

Cabe destacar que lo complejo en este método es encontrar polinomios tales que al hacer la igualdad entre razones los coeficientes no se vayan a los racionales.

4.3.2. Método de Diofanto

Se centrará el trabajo en ecuaciones donde $gr(p) = gr(k) + 1$, el método presentará algunas variaciones al aplicado en enteros, para ello se presentarán ejemplos y luego se concluirán condiciones.

Ejemplo 1:

Sea la ecuación:

$$(2, 6, 2)X + (-4, 12, 6) = (4, 2)Y$$

Lo primero que se hará es buscar el $M.C.D.$ entre $p(x)$ y $k(x)$, para ello se factorizan ambos polinomios, obteniendo así:

$$p(x) = (2, 6, 2) = (2)(1, 3, 1)$$
$$k(x) = (4, 2) = (2)((2, 1)$$

Por ende $M.C.D.[p(x), k(x)] = (2)$, se debe cumplir que dicho máximo común divisor divida a $g(x)$, se verificará esto:

$$g(x) \div (2) = (-4, 12, 6) \div (2) = (-2, 6, 3)$$

Ahora se plantea la ecuación diofántica cambiando a $g(x)$ por el $M.C.D.[p(x), k(x)]$, es decir:

$$(2, 6, 2)X + (2) = (4, 2)Y$$

Se inicia el algoritmo de Euclides:

$$(4, 2) = [0] \cdot (2, 6, 2) + (4, 2) \text{ de allí se obtiene } X = (0)Y + Z$$
$$(2, 6, 2) = [1, 1] \cdot (4, 2) + (-2) \text{ de allí se obtiene } Y = (1, 1)Z + W$$

Ahora se plantea $Z + g^*(x) = G \cdot W$, donde G es el penúltimo residuo, $g^*(x) = g(x)$ dado que se realizó un número par de divisiones y $W = (0, 1)$, obteniendo:

$$Z = (4, 2) \cdot (0, 1) - (2)$$
$$Z = (0, 4, 2) - (2)$$
$$Z = (-2, 4, 2)$$

Teniendo Z es posible reemplazarlo para obtener Y:

$$Y = (1,1)(-2,4,2) + (0,1)$$
$$Y = (-2,2,6,2) + (0,1)$$
$$Y = (-2,3,6,2)$$

Se realiza el procedimiento para obtener X:

$$X = (0)(-2,3,6,2) + (-2,4,2)$$
$$X = (0) + (-2,4,2)$$
$$X = (-2,4,2)$$

Teniendo los valores X e Y se comprobará que son solución para la ecuación planteada:

$$¿(2,6,2)(-2,4,2) + (-4,12,6) = (4,2)(-2,3,6,2)?$$
$$¿(-4,-4,24,20,4) + (-4,12,6) = (-8,8,30,20,4)?$$
$$(-8,8,30,20,4) = (-8,8,30,20,4)$$

Ejemplo 2:

Sea la ecuación:

$$(2,6,2)X + (-4,0,12,6) = (4,2)Y$$

Realizando un procedimiento análogo al del ejemplo anterior se obtiene que:

$$M.C.D.[p(x), k(x)] = (2)$$

es evidente que este divide a $g(x)$, por ende se plantea la nueva ecuación:

$$(2,6,2)X + (2) = (4,2)Y$$

Realizando el algoritmo de Euclides se obtiene:

$$(4,2) = [0] \cdot (2,6,2) + (4,2) \text{ de allí se obtiene } X = (0)Y + Z$$
$$(2,6,2) = [1,1] \cdot (4,2) + (-2) \text{ de allí se obtiene } Y = (1,1)Z + W$$

Ahora $g^*(x) = g(x)$, $G = (4, 2)$ y $W = (0, 0, 1)$, de allí:

$$Z = (4, 2) \cdot (0, 0, 1) - (2)$$
$$Z = (0, 0, 4, 2) - (2)$$
$$Z = (-2, 0, 4, 2)$$

Reemplazando Z y W para obtener Y se llega a:

$$Y = (1, 1)(-2, 0, 4, 2) + (0, 0, 1)$$
$$Y = (-2, -2, 5, 6, 2)$$

Como $X = 0Y + Z$, se tiene que $X = Z = (-2, 0, 4, 2)$, ahora se reemplazarán los valores X e Y para verificar que son soluciones de la ecuación:

$$¿(2, 6, 2)(-2, 0, 4, 2) + (-4, 0, 12, 6) = (4, 2)(-2, -2, 5, 6, 2)?$$
$$(-8, -12, 16, 34, 20, 4) = (-8, -12, 16, 34, 20, 4)$$

Luego de estos primeros dos ejemplos se llega a estas primeras condiciones:

- $M.C.D[p(x), k(x)] = d(x)$ tal que $gr(d) = 0$
- $d(x)|g(x)$
- $gr(w) = gr(g) - 1$

De esta última condición y con base en los ejemplos abordados, se puede conjeturar que si $g(x) = 6x^{n+1} + 12x^n - 4$ el valor asignado a W debe ser x^n.

Ejemplo 3:
Sea la ecuación:

$$(12, 9, 0, 6)X + (153, 600, 150) = (3, 0, 3)Y$$

Realizando un procedimiento análogo al de los ejemplos anteriores se obtiene que:

$$M.C.D.[p(x), k(x)] = (3)$$

es evidente que este divide a $g(x)$, por ende se plantea la nueva ecuación:

$$(12, 9, 0, 6)X + (3) = (3, 0, 3)Y$$

Realizando el algoritmo de Euclides se obtiene:

$$(3, 0, 3) = [0] \cdot (12, 9, 0, 6) + (3, 0, 3) \text{ de allí se obtiene } X = (0)Y + V$$
$$(12, 9, 0, 6) = [0, 2] \cdot (3, 0, 3) + (12, 3) \text{ de allí se obtiene } Y = (0, 2)V + Z$$
$$(3, 0, 3) = [-4, 1] \cdot (12, 3) + (51) \text{ de allí se obtiene } V = (-4, 1)Z + W$$

Ahora $g^*(x) = -g(x)$, $G = (12, 3)$ y $W = (0, 1)$, de allí:

$$Z = (12, 3) \cdot (0, 1) + (3)$$
$$Z = (3, 12, 3)$$

Reemplazando Z y W para obtener Y se llega a:

$$V = (-12, -44, 0, 3) = X$$
$$Y = (3, -12, -85, 0, 6)$$

Ahora se reemplazarán los valores X e Y para verificar que son soluciones de la ecuación:

$$¿(12, 9, 0, 6)(-12, -44, 0, 3) + (153, 600, 150) = (3, 0, 3)(3, -12, -85, 0, 6)?$$
$$(9, -36, -246, -36, -237, 0, 18) = (9, -36, -246, -36, -237, 0, 18)$$

Ahora el interés está en hallar la relación que debe haber entre $g(x)$, $p(x)$ y $k(x)$, luego de abordar diversos ejemplo no se logró ver que relación se debe cumplir, esta tarea quedará como objeto de estudio por parte del autor del trabajo de grado y del lector que lo quiera intentar.

En los enteros se plantea la existencia de infinitas soluciones a partir de una conocida, para ese caso sean la ecuación $ax + by = c$ y x_0, y_0 una solución para dicha ecuación, las soluciones infinitas serían:

$$x = x_0 + n \cdot \frac{b}{d}$$
$$y = y_0 - n \cdot \frac{a}{d}$$

Con $n \in \mathbb{Z}$ y $d = MCD(a, b)$.

Para el caso de $\mathbb{Z}[X]$ las soluciones infinitas se obtienen de la siguiente manera:

$$X = X_0 + n \cdot k(x)$$

$$Y = Y_0 + n \cdot p(x)$$

Con $n \in \mathbb{Z}$.

Retomando el ejemplo 1, se tenían $X_0 = (-2, 4, 2)$ y $Y_0 = (-2, 3, 6, 2)$, se obtendrá otra solución aplicando lo anterior:

$$X = (-2, 4, 2) + 5 \cdot (4, 2) = (-2, 4, 2) + (20, 10) = (18, 14, 2)$$

$$Y = (-2, 3, 6, 2) + 5 \cdot (2, 6, 2) = (-2, 3, 6, 2) + (10, 30, 10) = (8, 33, 16, 2)$$

Ahora se verificará si efectivamente son soluciones para la ecuación:

$$(2, 6, 2)X + (-4, 12, 6) = (4, 2)Y$$

Reemplazando se obtiene:

$$¿(2, 6, 2)(18, 14, 2) + (-4, 12, 6) = (4, 2)(8, 33, 16, 2)?$$
$$¿(36, 136, 124, 40, 4) + (-4, 12, 6) = (32, 148, 130, 40, 4)?$$
$$(32, 148, 130, 40, 4) = (32, 148, 130, 40, 4)$$

Con esto se verifica que se pueden conseguir infinitas soluciones partiendo de una conocida.

4.3.3. Algoritmo de la división en la solución de ecuaciones diofánticas

Sea la ecuación:

$$p(x)X + k(x)Y = g(x)$$

Si $p(x) = q(x) \cdot k(x) + r(x)$ y $r(x)|g(x)$ entonces la ecuación tiene solución.

Demostración. Se parte de la primera hipótesis, es decir $p(x) = q(x) \cdot k(x) + r(x)$, se procede a despejar $r(x)$, obteniendo:

$$p(x) - q(x) \cdot k(x) = r(x)$$

Utilizando la segunda hipótesis se puede decir que $g(x) = r(x) \cdot u(x)$, entonces se multiplica en ambos lados de la igualdad por $u(x)$:

$$u(x) \cdot [p(x) - q(x) \cdot k(x)] = u(x) \cdot r(x)$$
$$u(x) \cdot p(x) - u(x) \cdot q(x) \cdot k(x) = g(x)$$

Basta factorizar un -1 en $q(x)$ y aplicar la propiedad conmutativa del producto para obtener:

$$p(x) \cdot u(x) + k(x) \cdot [-q(x)] \cdot u(x) = g(x)$$

De esta manera se encontraron $X = u(x)$ e $Y = [-q(x)] \cdot u(x)$ que son solución para la ecuación planteada. □

Ejemplo 1:
hallar valores X e Y que satisfagan la siguiente ecuación:

$$(4, 4, 8)X + (2, 4)Y = (12, 8)$$

Se procede a realizar el algoritmo de la división, notando que se satisfacen las condiciones para este:

$$(4, 4, 8) = (0, 2)(2, 4) + (4)$$

Ahora se verifica que $r(x) = (4)$ divida a $g(x)$:

$$(12, 8) = (4)(3, 2)$$

Se despeja (4) y se multiplica por $(3, 2)$ en cada lado de la igualdad:

$$(4, 4, 8) - (0, 2)(2, 4) = (4)$$
$$(3, 2)[(4, 4, 8) - (0, 2)(2, 4)] = (3, 2)(4)$$

Se realizan algunos de los productos y se factoriza -1 en $(0, 2)$:

$$(4, 4, 8)[(3, 2)] + (2, 4)[(0, -2)(3, 2)] = (12, 8)$$
$$(4, 4, 8)[(3, 2)] + (2, 4)[(0, -6, -4)] = (12, 8)$$

De esta manera se hallaron $X = (3, 2)$ e $Y = (0, -6, -4)$, se verificará que efectivamente satisfacen la ecuación:

$$¿(4, 4, 8)[(3, 2)] + (2, 4)[(0, -6, -4)] = (12, 8)?$$
$$¿(12, 20, 32, 16) + (0, -12, -32, -16) = (12, 8)?$$
$$(12, 8) = (12, 8)$$

Ejemplo 2:
hallar valores X e Y que satisfagan la siguiente ecuación:

$$(18, 9, 12, 9)X + (3, 6, 3)Y = (24, 36, 12)$$

Se inicia con el algoritmo de la división:

$$(18, 9, 12, 9) = (-2, 3)(3, 6, 3) + (24, 12)$$

Se verifica que $(24, 12)$ divida a $(24, 36, 12)$:

$$(24, 36, 12) = (24, 12)(1, 1)$$

Ahora se realiza el despeje y la multiplicación:

$$(18, 9, 12, 9) + (2, -3)(3, 6, 3) = (24, 12)$$
$$(1, 1)[(18, 9, 12, 9) + (2, -3)(3, 6, 3)] = (1, 1)(24, 12)$$
$$(18, 9, 12, 9)[(1, 1)] + (3, 6, 3)[(2, -3)(1, 1)] = (24, 36, 12)$$
$$(18, 9, 12, 9)[(1, 1)] + (3, 6, 3)[(2, -1, -3)] = (24, 36, 12)$$

De esta manera se obtuvieron $X = (1, 1)$ e $Y = (2, -1, -3)$ como soluciones para la ecuación, a continuación se verificara que lo son:

$$¿(18, 9, 12, 9)(1, 1) + (3, 6, 3)(2, -1, -3) = (24, 36, 12)?$$
$$¿(18, 27, 21, 21, 9) + (6, 9, -9, -21, -9) = (24, 36, 12)?$$
$$(24, 36, 12) = (24, 36, 12)$$

4.4. Métodos de solución para ecuaciones de la forma $(h(x))^2 + (g(x))^2 = (k(x))^2$ en $\mathbb{Z}[X]$

4.4.1. Método de Fibonacci

Lo primero que se debe hacer es establecer la sucesión de polinomios con la cual se va a trabajar, a continuación se presentarán tres ejemplos de sucesión, dos en los cuales funcionan los pasos mostrados en la sección 3.2.1. y uno en el que no.

Ejemplo 1
Sean $p_1(x) = x^m$, $p_2(x) = x^m$ y $p_n(x) = p_{n-1} + p_{n-2}$. Es evidente que la sucesión de polinomios será: $x^m, x^m, 2x^m, 3x^m, 5x^m, 8x^m, ...$, es decir, lo que se establece es:

$$p_n(x) = f_n x^m$$

Dadas las propiedades de los exponentes la demostración se reduce a la elaborada para la sucesión de Fibonacci en $\mathbb{Z}$, por esta razón solamente se presentará un ejemplo.
Sean los cuatro términos consecutivos $5x^m, 8x^m, 13x^m$ y $21x^m$, se procede a encontrar al terna:

$$h(x) = 5x^m \cdot 21x^m = 105x^{2m}$$
$$g(x) = 2(8x^m \cdot 13x^m) = 208x^{2m}$$
$$k(x) = (8x^m)^2 + (13x^m)^2 = 233x^{2m}$$

Se procede a elevar al cuadrado cada término:

$$(h(x))^2 = 11025x^{4m}$$
$$(g(x))^2 = 43264x^{4m}$$
$$(k(x))^2 = 54289x^{4m}$$

Con realizar la suma se puede evidenciar que se cumple que $(h(x))^2 + (g(x))^2 = (k(x))^2$.
Ejemplo 2
Sean $p_1(x) = 0$, $p_2(x) = 1$ y $p_n(x) = x \cdot p_{n-1} + p_{n-2}$. Los términos que siguen de la

sucesión serían: $p_3(x) = x, p_4(x) = x^2+1, p_5(x) = x^3+2x, p_6(x) = x^4+3x^2+1, ...$ Como se evidencia cada término es mayor en 1 grado al anterior, y es usando los grados que se mostrará que el método de Fibonacci no funciona en esta sucesión. Se seleccionarán cuatro términos consecutivos y se tomarán en cuenta sus grados:

$$gr(p_n) = n-2 \qquad gr(p_{n+1}) = n-1 \qquad gr(p_{n+2}) = n \qquad gr(p_{n+3}) = n+1$$

Se procederá a buscar la terna, para este caso el grado de los componentes de dicha terna:

$$gr(h) = gr(p_n \cdot p_{n+3}) = gr(p_n) + gr(p_{n+3}) = n-2+n+1 = 2n-1$$
$$gr(g) = gr(p_{n+1} \cdot p_{n+2}) = gr(p_{n+1}) + gr(p_{n+2}) = n-1+n = 2n-1$$

Para el grado de $k(x)$ la atención se debe fijar en cada uno de los polinomios de la sucesión que lo componen, es decir:

$$gr((p_{n+1})^2) = 2gr(p_{n+1}) = 2(n-1) = 2n-2$$
$$gr((p_{n+2})^2) = 2gr(p_{n+2}) = 2(n) = 2n$$

Dado que para obtener $k(x)$ estos dos últimos polinomios se deben sumar y, en ninguno hay coeficientes negativos, se puede asegurar que:

$$gr(k) = 2n$$

Ahora se centrará la atención en el grado de cada término de la terna elevado al cuadrado:

$$gr(h^2) = 2(2n-1) = 4n-2$$
$$gr(g^2) = 2(2n-1) = 4n-2$$
$$gr(k^2) = 2(2n) = 4n$$

Se procede a determinar el grado de la suma entre $(h(x))^2$ y $(g(x))^2$:

$$gr(h^2+g^2) = 4n-2$$

Dado que $gr(h^2+g^2) \neq gr(k^2)$ se puede concluir que $(h(x))^2+(g(x))^2 \neq (k(x))^2$.

Ejemplo 3

Sean $p_1(x)=1$, $p_2(x)=x$ y $p_n(x)=p_{n-1}+p_{n-2}$. Los siguientes términos de la sucesión serían: $p_3(x)=x+1, p_4(x)=2x+1, p_5(x)=3x+2, p_6(x)=5x+3, p_7(x)=8x+5$.... Con esto se puede concluir que:

$$p_n(x)=f_{n-1}x+f_{n-2} \qquad \forall n>2$$

Se seleccionaran cuatro términos consecutivos, siendo estos:

$$p_n(x)=f_{n-1}x+f_{n-2},\ p_{n+1}(x)=f_nx+f_{n-1},\ p_{n+2}(x)=f_{n+1}x+f_n \text{ y}$$
$$p_{n+3}(x)=f_{n+2}x+f_{n+1}$$

se procede a buscar la terna correspondiente:

$$h(x)=p_n(x)\cdot p_{n+3}(x)=(f_{n-1}x+f_{n-2})(f_{n+2}x+f_{n+1})$$
$$g(x)=2(p_{n+1}(x)\cdot p_{n+2}(x))=2(f_nx+f_{n-1})(f_{n+1}x+f_n)$$
$$k(x)=(p_{n+1}(x))^2+(p_{n+2}(x))^2=(f_nx+f_{n-1})^2+(f_{n+1}x+f_n)^2$$

Solucionando las operaciones indicadas se obtiene:

$$h(x)=(f_{n-1}f_{n+2})x^2+(f_{n-1}f_{n+1}+f_{n-2}f_{n+2})x+(f_{n+1}f_{n-2})$$
$$g(x)=2[(f_nf_{n+1})x^2+(f_n^2+f_{n-1}f_{n+1})x+(f_{n-1}f_n)]$$
$$k(x)=(f_n^2+f_{n+1}^2)x^2+2(f_nf_{n-1}+f_{n+1}f_n)x+(f_{n-1}^2+f_n^2)$$

Ahora se eleva al cuadrado cada término:

$$(h(x))^2=(f_{n-1}^2f_{n+2}^2)x^4+2(f_{n-1}f_{n+2}^2+f_{n+1}f_{n-1}^2)x^3+...$$
$$(g(x))^2=(4f_n^2f_{n+1}^2)x^4+8(f_nf_{n+1}^2f_{n-1}+f_n^3f_{n+1})x^3+...$$
$$(k(x))^2=(f_n^4+2f_n^2f_{n+1}^2+f_{n+1}^4)x^4+4(f_nf_{n+1}^2f_{n-1}+f_n^3f_{n-1}+f_nf_{n+1}^3+f_n^3f_{n+1})x^3+...$$

Se mostrará la igualdad entre los coeficientes de x^4 y se dejará al lector comprobar que se cumple para los demás coeficientes. Primero se sumarán los coeficientes en $(h(x))^2$ y $(g(x))^2$:

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

Ahora se factorizará el coeficiente en $(k(x))^2$:

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

Luego de ver los pasos de la sección 3.2.1. y dado que en este caso se cumplen las condiciones, se puede afirmar que:

$$(f_{n-1}f_{n+2})^2 + (2f_n f_{n+1})^2 = (f_n^2 + f_{n+1}^2)^2$$

A continuación se verificará que el proceso funciona mediante dos ejemplos.

Ejemplo 1:

Para este caso se utilizarán $p_4(x)$, $p_5(x)$, $p_6(x)$ y $p_7(x)$, se procede a buscar la terna:

$$h(x) = (2x+1)(8x+5) = 16x^2 + 18x + 5$$
$$g(x) = 2(3x+2)(5x+3) = 30x^2 + 38x + 12$$
$$k(x) = (3x+2)^2 + (5x+3)^2 = 34x^2 + 42x + 13$$

Ahora se eleva al cuadrado cada término de la terna:

$$(h(x))^2 = 256x^4 + 576x^3 + 484x^2 + 180x + 25$$
$$(g(x))^2 = 900x^4 + 2280x^3 + 2164x^2 + 912x + 144$$
$$(k(x))^2 = 1156x^4 + 2856x^3 + 2648x^2 + 1092x + 169$$

Al realizar la suma de $(h(x))^2$ y $(g(x))^2$ se puede concluir que efectivamente:

$$(16x^2 + 18x + 5)^2 + (30x^2 + 38x + 12)^2 = (34x^2 + 42x + 13)^2$$

Ejemplo 2:

Se utilizarán $p_8(x)$, $p_9(x)$, $p_{10}(x)$ y $p_{11}(x)$, estas son:

$$p_8(x) = 13x + 8$$
$$p_9(x) = 21x + 13$$
$$p_{10}(x) = 34x + 21$$
$$p_{11}(x) = 55x + 34$$

Se procede a buscar la terna:

$$h(x) = (13x + 8)(55x + 34) = 715x^2 + 882x + 272$$
$$g(x) = 2(21x + 13)(34x + 21) = 1428x^2 + 1766x + 546$$
$$k(x) = (21x + 13)^2 + (34x + 21)^2 = 1597x^2 + 1974x + 610$$

Ahora se eleva al cuadrado cada término de la terna:

$$(h(x))^2 = 511225x^4 + 1261260x^3 + 1166884x^2 + 479808x + 73984$$
$$(g(x))^2 = 2039184x^4 + 5043696x^3 + 4678132x^2 + 1928472x + 298116$$
$$(k(x))^2 = 2550409x^4 + 6304956x^3 + 5845016x^2 + 2408280x + 372100$$

Al realizar la suma de $(h(x))^2$ y $(g(x))^2$ se puede concluir que efectivamente:

$$(715x^2 + 882x + 272)^2 + (1428x^2 + 1766x + 546)^2 = (1597x^2 + 1974x + 610)^2$$

Sin perdida de generalidad se puede asumir en $p_2(x)$ un grado cualquiera para x, de esta manera se obtendrán polinomios de mayor grado, que de igual manera serán ternas pitagóricas.

4.4.2. Método de Diofanto

Se abordará la igualdad lograda por Diofanto asumiendo a m entero, es decir:

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

Se reemplazará a m por un polinomio $p(x) = a_n x^n + ... + a_1 x + a_0$ y se observará que sucede, primero con $(m^2 + 1)^2$:

$$((a_n x^n + a_{n-1} x^{n-1} + ... + a_1 x + a_0)^2 + 1)^2$$

$$= ((a_n^2 x^{2n} + 2a_n a_{n-1} x^{2n-1} + ... + 2a_1 a_0 x + a_0^2) + 1)^2$$

$$= (a_n^2 x^{2n} + 2a_n a_{n-1} x^{2n-1} + ... + 2a_1 a_0 x + a_0^2 + 1)^2$$

$$= a_n^4 x^{4n} + 4a_n^2 a_n a_{n-1} x^{4n-1} + ... + 4(a_0^2 + 1)a_1 a_0 x + (a_0^2 + 1)^2$$

$$= a_n^4 x^{4n} + 4a_n^2 a_n a_{n-1} x^{4n-1} + ... + 4(a_0^2 + 1)a_1 a_0 x + a_0^4 + 2a_0^2 + 1$$

Ahora con $(2m)^2 + (m^2 - 1)^2$

$$(2(a_n x^n + ... + a_1 x + a_0))^2 + ((a_n x^n + a_{n-1} x^{n-1} + ... + a_1 x + a_0)^2 - 1)^2$$

$$= (2a_n x^n + 2a_{n-1} x^{n-1} + ... + 2a_0)^2 + ((a_n^2 x^{2n} + 2a_n a_{n-1} x^{2n-1} + ... + 2a_1 a_0 x + a_0^2) - 1)^2$$

$$= 4a_n^2 x^{2n} + 8a_n a_{n-1} x^{2n-1} + ... + 4a_0^2 + (a_n^2 x^{2n} + 2a_n a_{n-1} x^{2n-1} + ... + 2a_1 a_0 x + a_0^2 - 1)^2$$

$$= 4a_n^2 x^{2n} + 8a_n a_{n-1} x^{2n-1} + ... + 4a_0^2 + a_n^4 x^{4n} + 4a_n^2 a_n a_{n-1} x^{4n-1} + ... + 4(a_0^2 - 1)a_1 a_0 x + a_0^4 - 2a_0^2 + 1$$

Cabe notar que al resolver $(a_n^2 x^{2n} + 2a_n a_{n-1} x^{2n-1} + ... + 2a_1 a_0 x + a_0^2 - 1)^2$ resultan términos negativos como:

$$-4a_n a_{n-1} x^{2n-1} - ... - 4a_1 a_0 x - 2a_0^2$$

Reduciendo términos semejantes se obtiene:

$$= a_n^4 x^{4n} + 4a_n^2 a_n a_{n-1} x^{4n-1} + ... + 4a_n^2 x^{2n} + 4a_n a_{n-1} x^{2n-1} + ... + 4(a_0^2 + 1)a_1 a_0 x + a_0^4 + 2a_0^2 + 1$$

Como se puede observar al realizar las operaciones en cada lado obtenemos el mismo resultado, por ende se puede asegurar que:

$$(p(x)^2 + 1)^2 = (2p(x))^2 + (p(x)^2 - 1)^2 \qquad \forall p(x) \in \mathbb{Z}[X]$$

Ahora se verificará el resultado utilizando $p(x) = 3x^2 + 3$ y $p_1(x) = 5x^3 - 2x + 4$.
Ejemplo 1, $p(x) = 3x^2 + 3$:

$$((3x^2 + 3)^2 + 1)^2 = (2(3x^2 + 3))^2 + ((3x^2 + 3)^2 - 1)^2$$

$$(9x^4 + 18x + 9 + 1)^2 = (6x^2 + 6)^2 + (9x^4 + 18x + 9 - 1)^2$$

$$(9x^4 + 18x + 10)^2 = 36x^4 + 72x^2 + 36 + (9x^4 + 18x + 8)^2$$

$$81x^8 + 324x^6 + 504x^4 + 360x^2 + 100 = 36x^4 + 72x^2 + 36 + 81x^8 + 324x^6 + 468x^4 + 288x^2 + 64$$

$$81x^8 + 324x^6 + 504x^4 + 360x^2 + 100 = 81x^8 + 324x^6 + 504x^4 + 360x^2 + 100$$

Ejemplo 2, $p(x) = 5x^3 - 2x + 4$ se retomará la notación por *n-adas* dado que la notación habitual es un poco extensa en este caso:

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

$$((16,-16,4,40,-20,0,25) + (1))^2 = (8,-4,10)^2 + ((16,-16,4,40,-20,0,25) - (1))^2$$

$$(17,-16,4,40,-20,0,25)^2 = (64,-64,16,160,-80,0,100) + (15,-16,4,40,-20,0,25)^2$$

$$(289,-584,392,1232,-1944,960,2290,-2400,600,2000,-1000,0,625)$$

$$= (289,-584,392,1232,-1944,960,2290,-2400,600,2000,-1000,0,625)$$

5. Conclusiones, reflexiones y proyecciones

Conclusiones

- Aunque tanto $\mathbb{Z}$ como $\mathbb{Z}[X]$ son dominios enteros, se logró mostrar que en lo relativo a orden se comportan de manera diferente. En $\mathbb{Z}$ con el orden usual se obtiene una relación que efectivamente es de orden, mientras que en $\mathbb{Z}[X]$ la relación establecida no resulta serlo.

- El método de falsa posición logró exportarse, realizándolo tal cual se hace en los enteros. Al igual que los métodos para solucionar ternas pitagóricas.

- El método de Diofanto aunque con aspectos pendientes, logró exportarse realizando algunos cambios.

- El método de pulverización que hace uso del algoritmo de Euclides, no se logró exportar exitosamente por esta misma razón, no es seguro en dos dominios enteros se puedan realizar procedimientos iguales.

- Este trabajo me aportó a la capacidad de investigar en matemáticas, lo que debe ser un permanente en el profesor durante toda su vida.

- Las ecuaciones diofánticas aportan al profesor de matemáticas solidez en sus conocimientos, hay muchos conceptos que se deben utilizar al querer solucionar una ecuación de este tipo.

Reflexiones

- Durante este trabajo hubo momentos difíciles, en los que no se veía cómo poder concluirlo dado que no se lograban solucionar las ecuaciones planteadas. Pero la persistencia, constancia y uso de diferentes estrategias matemáticas llevo a elaborar un trabajo que genera orgullo en el autor. En la vida de un docente de matemáticas esto es muy importante, porque, aunque haya días duros, en los que

pareciera que no se logran los objetivos, tarde o temprano el camino se iluminará y así generará aún más satisfacción de la esperada.

- Es importante que el profesor de matemáticas siga trabajando en matemáticas, esto da un desarrollo lógico a su manera de abordar un problema y así puede transmitir a sus estudiantes diferentes conocimientos y estrategias que les pueden ser útiles. Adicionalmente saber más matemática ayuda a que los saberes se transmitan de mejor manera, porque nadie puede enseñar lo que no sabe y entre más se tenga conocimiento de una temática mejor será el proceso de enseñanza.

Proyecciones

- Queda en estudio la relación que debe darse entre los coeficientes de los polinomios en una ecuación diofántica, para establecer si se puede aplicar el método de Diofanto.

- El desarrollo de este trabajo deja como interrogante si dicha exportación funciona en anillos similares, como el de los z_p o el de los números duales, este podría ser un tema de estudio futuro.

6. Bibliografía

Aznar, E. (2007-2012). Biografías, matemáticos: *Enrique R. Aznar*. España. recuperado de https://www.ugr.es/∼eaznar/matematicos

Beltrán, P. (2014) *Las ecuaciones en el mundo discreto: un estudio sobre las ecuaciones diofánticas*. Tesis especialización en educación matemática. Universidad Pedagógica Nacional. Bogotá, Colombia.

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

Casalderrey, M. (2000). *Cardano y Tartaglia. Las matemáticas en el renacimiento italiano.* Nivola.

Castellanos, J. (s.f). *Estructuras algebraicas*. Universidad Complutense de Madrid. Recuperado de http://www.mat.ucm.es/∼arrondo/estructuras1

Falk, M. Acevedo, M. (1997). *Recorriendo el álgebra: de la solución de ecuaciones al álgebra abstracta.* Universidad Nacional de Colombia.

Fraleigh, J. (1988) *Álgebra abstracta, primer curso*. ADDISON-WESLEY IBEROAMERICANA S.A. Wilmington, E.E.U.U.

Lentin, A. Rivaud, J. (1973) *Álgebra moderna*. Aguilar S.A. de ediciones. Madrid, España.

Palacios, E. M. (s.f.) *Anillos de Polinomios*. Recuperado de http://www.ugr.es/∼bullejos/AlgI/polinomios.pdf

Pettofrezzo, A. Byrkit, D. (1972) *Introducción a la teoría de números*. Prentice-Hall internacional. Nueva Jersey, E.E.U.U.