SUCESIONES RECURRENTES EN DOS VARIABLES COMO MÉTODO PARA ENCONTRAR UNIDADES EN EXTENSIONES CUADRÁTICAS DE Z "P_t"

Nicolás Mahecha Fraile

C.C.1033746898

COD.2013140029

Trabajo de grado asociado al estudio de un asunto de interés profesional del autor, como requisito parcial para optar al título de Licenciado en Matemáticas.

Director
William Alfredo Jiménez

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

1. Información General	
Tipo de documento	Trabajo de Grado.
Acceso al documento	Universidad Pedagógica Nacional. Biblioteca Central.
Título del documento	Sucesiones recurrentes en dos variables como método para encontrar unidades en extensiones cuadráticas de $\boldsymbol{Z}$ "$\boldsymbol{P_t}$"
Autor(es)	Mahecha Fraile, Nicolás
Director	Jiménez Gómez, William Alfredo
Publicación	Bogotá. Universidad Pedagógica Nacional, 2018. Pág. 90
Unidad Patrocinante	Universidad Pedagógica Nacional.
Palabras Claves	Extensión cuadrática, primo, unidad, sucesiones recurrentes, cuasinorma.

2. Descripción

Este trabajo está dirigido a interesados en indagar sobre teoría de números, sucesiones recurrentes en extensiones cuadráticas, el trabajo se basa en la indagación y exploración de algunas extensiones cuadráticas de los enteros en donde se caracterizan elementos denominados primos, compuesto, unidades y asociados a través de la relación de divisibilidad, al igual que se caracterizan en los números enteros y en este modelo obtener definiciones y características de estos elementos más amplias, para en otras estructuras como en el conjunto de los números enteros o naturales.

A partir de dichas definiciones en el documento se describe un método para hallar las unidades en estas extensiones ya que resultan ser numerables, además, de criterios para reconocer cuándo un número puede ser definido como unidad, primo, compuesto o asociado, dado que en la indagación se utilizó como herramienta de exploración a través, de patrones encontrados en tablas y dichas tablas fueron generadas por un software, para los interesados en profundizar, en los anexos del documento se encuentra el código con el fin de lograr un mayor comprensión de los lectores.

3. Fuentes

Fraleigh, J. (1988). Algebra abstracta. Wilmington, Delaware, E.U.A.: ADDISON-

WESLEY IBEROAMERICANA.
Luque, C., Torres, J., & Mora, L. (2006). Estructuras análogas a los números reales. Bogotá, Colombia: Nomos S.A.
Muñoz, J. (2002). Introducción a la teoría de conjuntos. Bogotá, Colombia: Panamericana, Formas e Impresos S:A:.
Rubiano, G., Gordillo, J., & Luis, J. (2004). Teoría de números [para principiantes]. Bogotá, Colombia: Universidad Nacional de Colombia.
Jiménez, H. (2006). ESTUDIO ALGEBRAICO DE LOS NÚMEROS DUALES (Tesis para obtener título de pregrado). Universidad Pedagógica Nacional de Colombia. Bogotá, Colombia.
Takeuchi, Y. (1976). Sucesiones. México: Editorial Limusa.
Zuckerman, H., & Nieven, I. (1976). Introducción a la teoría de números. México: Limusa.
MEN, M. D. (2006). Estándares básicos de competencias en Lenguaje , Matemáticas, Ciencias y Ciudadanas. Bogotá. Recuperado de: http://www. mineducacion. gov. co/1621/articles- 340021_recurso.

4. Contenidos

El documento contiene conceptos matemáticos propios de la teoría de números, algebra lineal, sucesiones, estructuras algebraicas y teoría de conjuntos, los cuales se van mencionando de una forma secuencial a medida que sean necesarios con el fin de desarrollar el objetivo general que está en el documento.

El documento esta organizado en nueve apartados, este comienza con los objetivos generales y específicos, luego un marco referencial el cual contiene los conceptos matemáticos preliminares que se pueden encontrar en la literatura y que son necesarios para el desarrollo del trabajo, luego, se definen los conjuntos $\boldsymbol{P_t}$ los cuales son las extensiones cuadráticas de los enteros en donde se desarrolla el problema planteado y se hace una descripción de las estructura algebraica de estos, de aquí, se establece una relación de divisibilidad para definir los elementos llamados primos, compuestos, unidades y asociados los cuales después de ser caracterizados se encuentra un método para encontrarlos usando sucesiones recurrentes en dos variables y haciendo uso de matrices y sus propiedades para realizar algunas demostraciones o facilitar la escritura de las sucesiones, al finalizar en el anexo contiene el código del programa utilizado para hacer exploraciones en estas extensiones cuadráticas.

5. Metodología

El interés de este estudio nace en el seminario del álgebra de la UPN en donde a través de la exploración se intenta resolver problemas que se relacionen con la línea del algebra, lo primero fue definir un conjunto que tuviera una estructura tal que permitiera estudiar la relación de divisibilidad, luego se empiezan a buscar elementos similares a los que se describen en los enteros en la teoría de números, al tratar de caracterízalos y encontrarlos se desarrolla un software que permite a través de la visualización de sus

resultados encontrar patrones numéricos, que partir de conjeturas, demostraciones y a medida que avanza la exploración van surgiendo preguntas, para desarrollar una teoría de corolarios y teoremas; En mucho casos al encontrar una conjetura y tratar de demostrarla se hace evidente que es necesario demostrar otros teoremas previos quedando así una serie de teoremas y corolarios ordenados de una forma secuencial y en dicho orden se documentaron en este trabajo con el fin de responder una de las preguntas que surgieron en el seminario y es en la que se enmarca el problema planteado.
6. Conclusiones
En el documento se detalla cómo surgen la mayoría de teoremas y corolarios a partir de la exploración y además, como teorías y conceptos matemáticos que son abordados en el plan de estudio de la licenciatura en matemáticas del DMA-UPN en distintas disciplinas que también pueden relacionarse directamente con el fin de solucionar un problema, en este caso el problema es describir un método para encontrar unidades en una extensiones cuadráticas particulares de los números enteros, el cual se logró caracterizando sucesiones recurrentes con dos variables.Para consolidar teóricamente este método fue necesario implementar teoría de matrices, sucesiones, teoría de números teoría de anillo y teoría de conjuntos. De la misma manera se logró a partir del proceso inductivo ampliar las nociones de números primos, compuestos, asociados y unidades ya que las definiciones postuladas de estos elementos no pierden sentido al aplicarlas en los naturales, enteros y otras extensiones cuadráticas de los enteros, y además brindando herramientas teóricas y de exploración (código desarrollado por el autor encontrado en anexos del trabajo) para continuar futuras indagaciones en otras estructuras tipo anillo.

Elaborado por:	Nicolás Mahecha Fraile
Revisado por:	William Alfredo Jiménez Gómez

Fecha de elaboración del Resumen:	24	04	2018

AGRADECIMIENTOS

En esta parte del documentos quiero agradecer a María Teresa Sanabria , Diana Patricia Fraile y Roberto Mahecha que son mi abuela materna y padres respetivamente, ya que gracias al apoyo incondicional de ellos he podido cumplir mis metas propuestas y sé que siempre podré contar con ellos, también quiero agradecer al profesor William Jiménez de la Universidad Pedagógica Nacional de Colombia ya que sin su asesoramiento no podría haber culminado este trabajo además de ser un ejemplo como docente y matemático, al profesor Yeison Sánchez ya que fue una gran influencia en mi formación como docente y logró transmitirme la filosofía de que para hacer matemáticas no se necesita más que querer hacerlo, y no puedo terminar esta sección sin nombrar a Fabio Norberto Rincón, Nicole Mateus, Santiago Barbosa y Santiago Murcia, amigos y compañeros de la carrera que lograron ocupar un espacio en esta sección..

Contenido

Ilustraciones

Tablas

1 INTRODUCCIÓN

En la Universidad Pedagógica Nacional de Colombia específicamente en la Licenciatura en Matemáticas se ha trabajado en un espacio no curricular denominado seminario del algebra, asisten estudiantes manera voluntaria y algunos profesores que dirigen el grupo para abordar y estudiar temas o problemas relacionados con la línea del algebra, en el transcurso del año 2014 y 2015 se trabajó la divisibilidad en diferentes conjuntos numéricos. Los conjuntos estudiados fueron extensiones cuadráticas de los números denominados “súper-conjuntos” en el seminario del algebra, estos tienen estructura tipo anillo conmutativo como los números de Minkowsky, los gaussianos y los duales, estudiando allí la relación de divisibilidad y caracterizando elementos como los primos, compuestos, asociados y unidades.

El propósito inicial del seminario era demostrar el teorema fundamental de la aritmética en conjuntos numéricos no usuales es decir diferentes al conjunto de los números enteros o naturales, y para ello se empezó por definir dos operaciones, revisar que propiedades cumplen estos conjuntos con dichas operaciones, seguido de esto, caracterizar las unidades, primos, asociados y compuestos, esto se hizo con ayuda de un programa diseñado por el autor cuyo código será descrito como anexo de este documento, con el programa se agilizaron cuentas aritméticas como sumas y multiplicaciones entre estos elementos, ya que por la cantidad de elementos de estos en estos súper-conjuntos reduce en gran medida el tiempo para explorar y así hacer conjeturas y respectivas demostraciones.

2 JUSTIFICACIÓN

Este trabajo es una muestra a la manera de “hacer matemáticas” en el “seminario del álgebra” de la Licenciatura en Matematicas del DMA-UPN en el periodo del 2015-I y 2015-II, también, como la exploración y la programación, son herramientas útiles para llegar a la conjeturarían y posteriormente la demostración, además, del interés por definir objetos ya existentes en otras estructuras pero que dichas definiciones también sean válidas en todas las estructuras, es decir, que si se define de cierta manera un número primo en una nueva estructura esta definición también sea válida en otra, por ejemplo para los números enteros o naturales, esto implica que se amplía la noción de dicho objeto matemático que para en caso son los números primos, compuestos, asociados y unidades.

El trabajo también muestra la importancia de ciertos espacios académicos de la Licenciatura en Matemáticas ya que reúne conceptos matemáticos abordados en teoría de números, álgebra lineal, sucesiones y series, teoría de conjuntos, teoría de grupos y anillos y aritmética, además, que para desarrollar este trabajo de indagación, investigación y documentación es necesario hacer uso de procesos como la comunicación, formulación de problemas, razonamiento y la modelación que son cuatro de los cinco procesos generales según Los Estándares en Competencias Matemáticas brindados(MEN, 2006) por el ministerio de educación y que cómo docente en formación es fundamental conocer medios para desarrollarlos en los futuros estudiantes que tendré a cargo.

Finalmente otro aspecto importante de este trabajo es mostrar como un problema que se genera a partir de un ambiente de investigación es un medio para relacionar directamente conceptos de diversas teorías y de nuevo ampliando la noción de estos conceptos y las relaciones entre ellos, cómo en este trabajo particular que relaciona directamente las matrices, las sucesiones, la relación de divisibilidad, clases de equivalencia, orden y elementos de una estructura algebraica

.

3 PLANTEAMIENTO DEL PROBLEMA

Durante el estudio de las extensiones cuadráticas de los enteros "$\boldsymbol{P_t}$" definidas más adelante, se logró encontrar que sus elementos pueden ser catalogados como unidades, primos, compuestos o asociados ya que se comportan de manera similar a los mismos elementos de los enteros, pero, aunque se comportan de la misma manera hay algunas diferencias estas animaron al estudio en estas extensiones en particular, por ejemplo, que aquí la cantidad de unidades no es finita es decir que hay infinitos elementos con inverso multiplicativo pero no todos los elementos tienen inverso multiplicativo, dado esto se empezó a complicar la tarea de definir cuáles se pueden llamar primos, compuestos, unidades o asociados por lo cual se empieza a buscar un método el cual permita diferenciarlos y además encontrar las unidades.

Como el problema consiste en caracterizar sucesiones de dos variables definidas por recurrencia donde los elementos de dicha sucesión resulten ser las unidades de $\boldsymbol{P_t}$, para cada súper-conjunto la sucesión caracterizada debe servir como herramienta para deducir todas las unidades de este, para llegar a resolver esta pregunta es necesario tocar ciertos temas de las extensiones cuadráticas las cuales serán abordadas en el documento, estos temas son:

-La estructura algebraica de las extensiones cuadráticas $\boldsymbol{P_t}$

-Definiciones de los números primos, compuestos, asociados y unidades en $\boldsymbol{P_t}$

-Orden lexicográfico en $\boldsymbol{P_t}$

Como se relacionan las sucesiones de dos variables definidas por recurrencia con las matrices $2x2$ y a su vez con las unidades de $\boldsymbol{P_t}$,Estos temas serán abordados ya que son necesarios para demostrar la solución al problema y así finalmente mostrar cuales son y cómo generar las sucesiones de dos variables definidas por recurrencia que generan todas las unidades de $\boldsymbol{P_t}$.

4 OBJETIVOS

Ya teniendo conocimiento del problema que se pretende abordar, se plantearan los objetivos para tener más claridad de lo que se pretende responder en este documento.

4.1 Objetivo general

-Encontrar un método utilizando para caracterizar sucesiones de dos variables definidas por recurrencia para encontrar las unidades en conjuntos $\boldsymbol{P_t}$ donde t es de la forma $n^2 + \frac{n}{2p}$ donde n, p son números naturales.

4.2 Objetivos específicos

-Definir los súper-conjuntos $\boldsymbol{P_t}$ y dos operaciones en estos conjuntos y explicar su estructura algebraica.

-Consolidar la definición de número primo, compuesto, asociado y unidad en los números enteros, naturales y algunas extensiones cuadráticas de los enteros**.**

-Desarrollar y utilizar un software como herramienta para la conjuración de algunos teoremas que se plantearan en el documento, y que este genere las sucesiones que solucionan el objetivo general, además, de las unidades de los súper-conjuntos $\boldsymbol{P_t}$**.**

5 MARCO DE REFERECIA

En esta unidad se explicitaran algunos conceptos matemáticos y se enunciarán teoremas que serán utilizados en el cuerpo del trabajo, estos se enunciaran en un orden similar en el que se necesitarán, dado la anterior lo primero será hablar de las extensiones cuadráticas, ya que con ellas se definen los súper-conjuntos que son la base de todo el trabajo.

5.1 Extensiones cuadráticas

En un conjunto R con dos operaciones definidas que serán llamadas suma (+) y multiplicación (*), si existe un $c \in R$ tal que la ecuación cuadrática $x^2 = c$ no tiene solución se puede generar una extensión cuadrática de R o también a través de alguna condición impuesta por el autor como es el caso de los números duales los cuales se mencionarán más adelante, llamemos esta extensión el conjunto S donde los elementos de S son de la forma $a + bk$ donde $a, b \in R$ y $k^2 = c$, esto implica que la ecuación $x^2 = c$ si tiene solución en S y su solución es 0+1k $(Fraleight, 1988)$, hay un ejemplo muy conocido que el conjunto de los números complejos, este es una extensión cuadrática de los números reales.

5.1.1 El campo de los números complejos

Este primer ejemplo nos muestra una extensión cuadrática expuesta por (Luque, Mora y Torres, 2006), en "el conjunto de los números reales" como todos sabemos por algunos teoremas se cumple que para todo número real a si $a \neq 0$ entonces $a^2 > 0$, lo que implica que ningún número cuadrado es negativo y por tanto ningún número negativo tiene raíz cuadrada, en particular -1 así que se define un nuevo elemento denotado i donde $i = \sqrt{-1}$.

Estos números serían de la forma:

$$z = a + bi\ con\ i^2 = -1$$

Además, aclaran que incluir este nuevo elemento puede acarrear problemas si no se establecen reglas claras para su manejo, como por ejemplo:

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

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

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

$$1 = -1$$

Se incluyó este ejemplo para mostrar que no necesariamente las propiedades del conjunto de partida con sus operaciones se heredan en la extensión cuadrática, y por ello es necesario comenzar revisado que propiedades se mantienen y cuales difieren, centrándose en las propiedades que sean de utilidad para resolver el problema de estudio.

A continuación el mismo libro muestra otro ejemplo de una extensión cuadrática la cual el más parecida estructuralmente a las extensiones que se abordará en el trabajo ya que es un anillo conmutativo.

5.1.2 El anillo ordenado de los números duales

Estos números son conocidos como los *números duales* o *números de Study*, este conjunto numérico interesa más por tener estructura de anillo conmutativo, es en estas estructuras donde estudiar la relación de divisibilidad permite caracterizar elementos que en estructuras como campos no tiene mucho sentido, así que se definirán que propiedades estructurales deben tener estos conjuntos para considerarse anillos conmutativos, de nuevo (Luque et al., 2006) comenta que en los números reales para todo a y b números reales se cumple que:

$$si\ ab = 0, \qquad entonces\ a = 0\ o\ b = 0$$

En el caso particular en que $a = b$, este resultado implica que:

$$si\ a^2 = 0, \qquad entonces\ a = 0$$

Para lo cual no existe un real diferente de 0 cuyo cuadrado sea 0, por lo cual se plantea la ecuación $x^2 = 0$ con x diferente de 0 y dado que esto no es posible en los reales, así generando una extensión cuadrática de los números reales donde sus elementos son de la forma:

$$z = a + bn \; con \; n^2 = 0, y \; n \neq 0$$

Ya abordando el concepto de extensión cuadrática, es necesario conocer la mínima estructura algebraica necesaria para generar una extensión cuadrática, esta estructura es un anillo.

5.2 ANILLOS

Después de tener un conjunto numérico se continúa definiendo dos operaciones que se puedan ensamblar y que cumplan una serie de propiedades para hablar allí de una estructura multiplicativa, las propiedades necesarias se enuncian a continuación.

5.2.1 Propiedades de un conjunto numérico con una operación

Lo principal es definir algunos tipos de estructuras algebraicas por medio de las propiedades que cumple un conjunto numérico con una operación binaria, dado un conjunto G una operación binaria es una función cuyo dominio es AxB y su codominio es un conjunto C.

Dado un conjunto con una operación $(S,*)$, se dice que la operación está bien definida si y solo si cumple la propiedad clausurativa o es cerrada es decir

Definición. S es cerrado para la operacion $*$ si y solo si $a * b \in S$ para todas las $a, b \in S$. (Fraleigh, 1988).

Ahora teniendo un conjunto numérico G con una operación bien definida se puede hablar de las siguientes propiedades:

Definición. Una operación binaria $*$ bajo el conjunto S es ***conmutativa*** si y solo si $(a * b) = (b * a)$ para toda $a, b \in G$, (Fraleigh, 1988).

Definición. La operación * es ***asociativa*** si y solo si $a * b \ * c = a * (b * c)$ para toda $a, b, c \in G$, (Fraleigh, 1988).

También es necesario hablar por ahora de dos elementos importantes que pueden aparecer en conjuntos cuando se define una operación, los cuales son el elemento identidad y el elemento inverso, pero estos se caracterizaran en la definición de grupo como se hace en $(Fraleigh, 1988)$.

Definición. Un ***grupo*** $G, *$ es un conjunto G, junto con una operación binaria $*$ en G, tal que satisface los siguientes axiomas:

- La operación binaria $*$ es asociativa
- Existe un elemento e en G tal que $e * x = x * e = x$ para todas las $x \in G$ (Este elemento e es un elemento identidad para $*$ en G).
- Para cada a en G existe un elemento a' en Gcon la propiedad de que
$$a' * a = a * a' = e$$
(El elemento a' es un ***inverso*** de a respecto a $*$).

Ya como se definió grupo y conmutatividad se definirá grupo abeliano como está en $(Fraleigh, 1988)$.

Un grupo $G, *$ es ***abeliano*** si su operación binaria $*$ es conmutativa.

5.2.2 Monoides y monoides conmutativos

Hasta el momento se tienen definidas dos estructuras algebraicas las cuales son los grupos y los grupos abelianos, además, en necesario definir otra estructura algebraica llamada monoide

Definición. Un ***monoide*** (G,$*$), es un conjunto G, junto con una operación binaria en G, tal que satisface el siguiente axioma

- La operación binaria $*$ es asociativa
- Existe un elemento e en G tal que $e * x = x * e = x$ para todas las $x \in G$

Si un grupoide también cumple la propiedad conmutativa es un ***monoide conmutativo***

Cabe resaltar que aunque en las definiciones de las estructuras algebraicas ya mencionadas no mencionan la propiedad clausurativa en su definición, estas si la cumplen, así lo resalta $(Fraleigh, 1998)$.

Se pueden hacer uniones entre estas estructuras por medio de ciertas propiedades que pueden cumplir dos operaciones binarias bien definidas en un mismo conjunto por ejemplo la propiedad distributiva, dado un conjunto G con dos operaciones $+$ y $*$ las que llamarán suma y multiplicación respectivamente y de nuevo se definirá la propiedad distributiva a través de la definición de anillo $(Fraleigh, 1998)$, y con esto es posible definir anillo unitario y anillo unitario conmutativo.

Definición. Un ***anillo*** $(\boldsymbol{R}, +,*)$ es un conjunto $\boldsymbol{R}$ junto con dos operaciones binarias $+$ y $*$, definidas en $\boldsymbol{R}$ tal que satisfacen los siguientes axiomas:

- $(\boldsymbol{R}, +)$ es un grupo abeliano.
- $\boldsymbol{R},*$ es asociativo.
- Para todas $a, b, c \in \boldsymbol{R}$, se cumple la ***ley distributiva a izquierda*** $\boldsymbol{a} * (\boldsymbol{b} + \boldsymbol{c}) = (\boldsymbol{a} * \boldsymbol{b}) + (\boldsymbol{a} * \boldsymbol{c})$ y la ***ley distributiva a derecha*** $(\boldsymbol{a} + \boldsymbol{b}) * \boldsymbol{c} = (\boldsymbol{a} * \boldsymbol{c}) + (\boldsymbol{b} * \boldsymbol{c})$

Definición. Un anillo $(\boldsymbol{R}, +,*)$, es un ***anillo unitario*** si y solo si $(\boldsymbol{R},*)$ tiene elemento identidad.

Definición. Un anillo unitario $(\boldsymbol{R}, +,*)$**,** es un ***anillo unitario conmutativo*** si y solo si $(\boldsymbol{R},*)$ cumple la propiedad conmutativa.

Ya terminando esta sección se puede decir que los anillos son una estructura con dos operaciones, donde la segunda operación tiene estructura multiplicativa ya que distribuye con la primera operación que resulta ser un grupo abeliano, y dado que la segunda operación no cumple la propiedad invertiva, permite estudiar la relación de divisibilidad y con esta relación caracterizar ciertos elementos.

5.3 DIVISIBILIDAD.

La divisibilidad en los conjuntos numéricos con estructura de anillo es la relación que permite hablar de números primos, compuestos, asociados y unidades, estos números serán unos de los objetos ya caracterizados por medio de clases de equivalencia.

Se trabajará la relación divisibilidad de una manera análoga como la definen en Zuckerman y Nieven (1976), en el libro definen la divisibilidad en los enteros como:

Definición. Un entero b es divisible por un entero a, no cero, si existe un número c entero tal que $b = ac$, esto se escribe $a|b$ y se lee a divide a b y a es un ***divisor*** de b.

Se modificará esta definición de divisibilidad ampliándola precisamente para cualquier anillo con estructura multiplicativa, entonces, la definición que se trabajará para la divisibilidad será:

Definición. Dado un anillo $\boldsymbol{G}$, se dice que un número $b \in \boldsymbol{G}$ es divisible por un número $a \in \boldsymbol{G}$, diferente de cero, si existe un número $c \in \boldsymbol{G}$ tal que $b = ac,$ donde $a, b, c \in \boldsymbol{G}$, este se escribe $a|b$ y se lee a divide a b

Tomando el "cero" como el elemento idéntico en $\boldsymbol{G}$ con la operación suma.

Esta definición es más general y en sí funciona también para $\boldsymbol{Z},$ ahora como en $\boldsymbol{Z}$ trabajando con esta definición se generan elementos llamados unidades, primos, compuestos y asociados, esto da pauta para preguntarse si estos elementos se pueden encontrar en otros anillos, y además, si estos se pueden caracterizar.

5.3.1 Unidades, primos, compuestos y asociados

Como se mencionó anteriormente, al tratar con la divisibilidad da pie para empezar a trabajar en números como los son las unidades, los primos, los compuestos y los asociados, tomando en cuenta que se trabajará con anillos unitarios se empezará definiendo unidad como se definen en (Fraleigh, 1988) y en seguida número primo y compuesto.

Definición. Sea $\boldsymbol{R}$ un anillo con unitario, un elemento u en $\boldsymbol{R}$ es una ***unidad*** de $\boldsymbol{R}$ si tiene un inverso multiplicativo en $\boldsymbol{R}$.

Definición. Se dice que un entero $p > 1$ es un ***número primo***, o simplemente que es un ***primo***, en caso de que no exista un divisor d de p que satisfaga $1 < d < p$. Si un entero $a > 1$ no es un primo, entonces se dice que es un número ***compuesto***.

Definición. Un elemento a en $\boldsymbol{R}$ es un ***asociado*** de un elemento b en $\boldsymbol{R}$ si existe una unidad u en $\boldsymbol{R}$ tal que $a = bu$.

Al igual que con la definición de divisibilidad más adelante se modificarán estas definiciones para que sean más acorde a los súper-conjuntos trabajados, como se mencionó anteriormente si se pueden caracterizar estos elementos en los súper-conjuntos, pero por ejemplo la cantidad de unidades resulta ser infinita, así que ahora es necesaria una herramienta que permita encontrar cuales son las unidades sin recurrir a un software, para ello las sucesiones definidas por recurrencia serán un método para encontrar dichas unidades.

5.4 SUCESIONES

Esta sección menciona definiciones y teoremas que se abordan en el estudio de sucesiones en el trabajo y serán de utilidad para encontrar las unidades de los súper-conjuntos.

Un conjunto ordenado de números se llama ***una sucesión***. En la sucesión:

$$A = \{a_1, a_2, \dots, a_n, \dots\}$$

El numero a_n que ocupa el n-esimo puesto se llama ***el n-esimo elemento*** o ***el n-esimo término*** de la sucesión. La sucesión se denota abreviadamente.

$$A = \{a_n\}$$

Así, una sucesión es una función cuyo dominio es el conjunto $\boldsymbol{N}$ de todos los números naturales; al número $\boldsymbol{n} \in \boldsymbol{N}$ le corresponde el n-esimo o enésimo elemento de la sucesión (Takeuchi, 1976).

Aparte de la definición de sucesión se necesitarán otras propiedades que cumplen las sucesiones como la convergencia, divergencia, límite de una sucesión, si esta es acotada superior o inferior mente y más aún en las sucesiones definidas por recurrencia, estas propiedades se definirán como están en el libro sucesiones y series de (Takeuchi, 1976).

Definición. Se dice que un sucesión es ***creciente*** si

$$a_1 \leq a_2 \leq a_3 \leq \cdots \leq a_n \leq a_{n+1} \leq \cdots$$

Y decreciente si

$$a_1 \geq a_2 \geq a_3 \geq \cdots \geq a_n \geq a_{n+1} \geq \cdots$$

O sea que es creciente si

$$n > k \; inplica \; a_n \leq a_k$$

Y es decreciente si

$$n < k \; inplica \; a_n \leq a_k$$

Definición. Una sucesión $\{a_n\}$ es ***acotada superiormente*** si existe una constante M' tal que:

$$a_n \leq M' para \; toda \; n$$

Definición. Una sucesión $\{a_n\}$ es ***acotada inferiormente*** si existe una constante M_0 tal que:

$$a_n \geq M_0 \; para \; toda \; n$$

Ya teniendo en cuenta estos conceptos que se utilizarán en el documento se dará comienzo hablando de los súper-conjuntos $\boldsymbol{P_t}$, los cuales, son los objetos en los que se plantea el objetivo de este trabajo.

6 ESTRUCTURA ALGEBRAICA DE P_t

En esta unidad se definirán la familia de conjuntos llamados $\boldsymbol{P_t}$ en los cuales se planteo el problema de este trabajo, también, se explicará el tipo de estructura algebraica que comparten estos conjuntos al definirles dos operaciones, “suma” y “multiplicación”.

6.1 Súper-conjuntos P_t

Los súper-conjuntos $\boldsymbol{P_t}$ son extensiones cuadráticas de los números enteros, que como se mencionó en el titulo 6, cada ecuación $x^2 = t$ sin solución donde t es un entero positivo, genera una extensión cuadrática llamada aquí $\boldsymbol{P_t}$.

6.2 Definición de un conjunto P_t

Los elementos de $\boldsymbol{P_t}$ son de la forma $a + bk$ donde $k^2 = t\ , k \notin \boldsymbol{Z} \wedge t > 1$, y $a, b \in \boldsymbol{Z}$ quedando así:

$$\boldsymbol{P_t} = \{a + bk \mid k^2 = t \wedge t, a, b \in \boldsymbol{Z}, k \notin \boldsymbol{Z} \wedge t > 1\}$$

El conjunto $\boldsymbol{P_t}$ se dota de dos operaciones llamadas suma $(+)$ y multiplicación $(*)$ definidas de la siguiente manera:

Definición.

$$a + bk \ + \ c + dk \ = \ a + c \ + \ b + d \ k$$

Definición.

$$a + bk \ * \ c + dk \ = \ ac + bdk^2 \ + \ ad + bc \ k$$

Dadas estas dos operaciones en $\boldsymbol{P_t}$ seguiremos con demostrar las propiedades que estas cumplen.

6.3 Propiedades de la suma en P_t

En esta sección se demostrarán propiedades que $(\boldsymbol{P_t}, +)$ cumple para ser un grupo abeliano (la asociatividad, conmutatividad, existencia del módulo e inversos aditivos), tenga muy en cuenta que en las demostraciones de esta sección los pasos que no tienen justificación es porque son las propiedades de anillo en $(\boldsymbol{Z}, +, *)$.

-$(P_k, +)$ es asociativa.

Sean $x, y, z \in P_t$ donde $x = a + bk,\ y = c + dk$ y $z = e + fk$ se tiene que:

$$
\begin{aligned}
& z + \ \ y + z \\
& = \ a + bk \ + \ \ c + dk \ + \ e + fk \\
& = \ a + bk \ + \ \ c + e \ + (d + f \ \ k) \\
& = \ a + \ c + e \ \ + \ b + \ d + f \ \ k \\
& = \ \ a + c \ + e \ + \ \ b + d \ + f \ \ k \\
& = \ \ a + c \ + \ b + d \ k \ + \ e + f \ k \\
& = \ \ a + bk \ + \ c + dk \ \ + \ c + f \ \ k \\
& = \ x + y \ \ + z
\end{aligned}
$$

■

-$(P_k, +)$ es conmutativa

Demostración:

Dados $x, z \in P_t$, donde $x = \ a + bk \ \ y\, z = \ c + dk$, se tiene que

$$
\begin{aligned}
x + z &= \ a + bk \ + \ c + dk \\
&= \ a + c \ + \ b + d \ k \\
&= \ c + a \ + \ d + b \ k \\
&= \ c + dk \ + \ a + bk \\
&= z * x
\end{aligned}
$$

■

-$(\boldsymbol{P_k}, +)$ es modulativa, donde el elemento neutro es $e = 0 + 0k$.

Demostración:

Suponga que $\exists e \in P_t \forall x \in P_t$ donde $x = \ a + bk \ \ y\ e = (c + dk)$ tal que $x + e = x$, entonces

$$x + e = x$$
$$a + bk \ + \ c + dk \ = \ a + bk$$
$$a + c \ + \ b + d \ k = \ a + bk$$
$$es\ decir\ que$$
$$a + c = a$$
$$b + d = b$$
$$c = 0\ y\ d = 0\ por\ que\ en\ \boldsymbol{Z}\ existe\ modulo$$

Entonces si $\exists e \in P_k \forall x \in P_k$ donde $e = (0 + 0k)$ tal que $x + e = x$ y dado que $P_k, +$ es conmutativa entonces, $x + e = e + x = x$, así que $(P_t, +)$ es modulativa.

■

-$(P_k, +)$ tiene elemento inverso.

Demostración:

Suponga que $\forall x \in P_t \exists (-x) \in P_k$ donde $x = \ a + bk \ \ y\ -x = (c + dk)$ tal que $x + (-x) = e$, entonces

$$x + (-x) = e$$
$$a + bk \ + \ c + dk \ = \ 0 + 0k$$
$$a + c \ + \ b + d \ k = \ 0 + 0k$$
$$es\ decir\ que$$
$$a + c = 0$$
$$b + d = 0$$

$c = -a\ y\ d = -b$ por que en $\boldsymbol{Z}$ existen inversos

Entonces, si se cumple que $\forall x \in P_t\ \exists (-x) \in P_t$ donde $-x = ((-a) + (-b)k)$ tal que $x + (-x) = e$ y dado que $P_t, +$ es asociativa entonces, $x + \ -x \ = \ -x \ + x = e$, así que $(P_t, +)$ es modulativa.

■

Dado que $(\boldsymbol{P_t},+)$ es un grupo se cumple que es cancelativa a derecha y a izquierda $(Fraleigh, 1988)$, es decir que si $a+b=a+c$ inpica que $b=c$ y si $b+a=c+a$ implica que $b=c$.

6.4 Propiedades de la multiplicación en P_k

Ahora se demostrarán que $(\boldsymbol{P_t},*)$ cumple las propiedades necesarias para ser un grupo conmutativo con modulo.

-$(P_k,*)$ es asociativa.

Demostración:

Sean $x,y,z \in \boldsymbol{P_t}$ donde $x=a+bk$, $y=c+dk$ y $z=e+fk$ con a,b,c,d enteros se tiene que:

$$x * \ \ y * z$$
$$= \ a+bk \ * \ \ c+dk \ * \ e+fk$$
$$= \ a+bk \ * \ \ ce+dfk^2 \ + \ cf+de \ k$$
$$= \ \ ace+adfk^2 \ + \ bcf+bde \ k^2 \ + \ (bce+bdfk^2)+(acf+ade \ \ k$$
$$= \ \ ace+adfk^2 \ + \ bcfk^2+bdek^2 \ \ + \ (bcek+bdfk^2k)+(acfk+adek$$
$$= \ \ ace+bdek^2 \ + \ adfk^2+bcfk^2 \ \ + \ acfk+bdfk^2k \ + \ adek+bcek \ \ )$$
$$= \ \ ace+bdek^2 \ + \ adf+bcf \ k^2 \ \ + \ acf+bdfk^2 \ + \ ade+bce \ \ k)$$
$$= \ ac+bdk^2 \ + \ ad+bc \ k \ * \ e+fk$$
$$= \ a+bk \ * \ c+dk \ \ * \ e+fk$$
$$= \ x*y \ \ *z$$

■

-$(P_t,*)$ es conmutativa

Demostración:

Dados $x,z \in P_t, donde\ x = \ a+bk \ \ y\ z= \ c+dk$ con a,b,c,d enteros, se tiene que:

$$x*z= \ a+bk \ * \ c+dk$$
$$= \ ac+bdk^2 \ + \ ad+bc \ k$$

$$= \; ca + dbk^2 \;+\; da + cd \; k$$
$$= \; c + dk \;\; * (a + bk)$$
$$= z * x$$

■

-$(P_k,*)$ es modulativa, donde el elemento neutro es $e = 1 + 0k$.

Demostración:

Suponga que $\exists e \in P_t \forall x \in P_t$ donde $x = \; a + bk \;\; y\; e = (c + dk)$ con a, b, c, d enteros tal que $x + e = x$, entonces,

$$x + e = x$$
$$a + bk \;\; * \;\; c + dk \;\; = \;\; a + bk$$
$$ac + bdk^2 \;\; + \;\; ad + bc \;\; k = \;\; a + bk$$
$$es\ decir\ que$$
$$ac + bdk^2 = a$$
$$bad + bc = b$$

$c = 1\; y\; d = 0$ resolviendo el sistema de ecuaciones en $\boldsymbol{Z}$.

Entonces si $\exists e \in P_t \forall x \in P_k$ donde $e = (1 + 0k)$ tal que $x * e = x$ y dado que $P_t,*$ es conmutativa entonces, $x * e = e * x = x$, así que $P_t,*)$ es modulativa.

■

Ahora $(P_t,*)$ no tiene elemento inverso multiplicativo $\forall x \in P_t$y a continuación se mostrará por qué no:

Suponga que $\forall x \in P_t\; \exists (x^{-1}) \in P_t$ donde $x = \; a + bk \;\; y\; x^{-1} = (c + dk)$ tal que $x * x^{-1} e$, entonces

$$x * x^{-1} = e$$
$$a + bk \;\; * \;\; c + dk \;\; = \;\; 1 + 0k$$
$$ac + bdk^2 \;\; + \;\; ad + bc \;\; k = \;\; 1 + 0k$$

es decir que

$$ac + bdk^2 = 0$$
$$ad + bc = 0$$

resolviendo el sistema de ecuaciones en $\boldsymbol{Z}$ queda:

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

Entonces esta es la forma de c y d y para que x^{-1} exista, $\forall x \in P_t$ se debe cumplir que $c, d \in \boldsymbol{Z}$, pero si $x = (1 + 2k)$ cuando $k^2 = t = 2$ tenemos que $c = -\frac{1}{7}$ y $d = -\frac{2}{7}$, por lo cual $c, d \notin \boldsymbol{Z}$, y es por esto que $(P_k,*)$ no cumple la propiedad invertiva.

■

-($\boldsymbol{P_t}, +,*$) distributiva con la multiplicación respecto a la suma.

Sean $x, y, z \in P_t$ donde $x = a + bk,\ y = c + dk$ y $z = e + fk$ con a, b, c, d enteros se tiene que:

$$\begin{aligned}
& a + bk \ * \ \ c + dk \ + \ e + fk \\
&= \ a + bk \ * \ \ c + e \ + (d + f \ \ k) \\
&= \ a \ c + e \ + bk^2 \ d + f \ \ + \ a \ d + f \ + b \ c + e \ \ k \\
&= \ \ ac + ae \ + \ bk^2d + bk^2f \ \ + \ \ ad + af \ + \ bc + be \ \ k \\
&= \ \ ac + ae \ + \ bk^2d + bk^2f \ \ + \ \ ad + af \ k + \ bc + be \ k \\
&= \ \ ac + bk^2d \ + \ ad + bc \ k \ + (\ ae + bk^2f \ + \ af + be \ k) \\
&= \ \ ac + bdk^2 \ + \ ad + bc \ k \ + (\ ae + bfk^2 \ + \ af + be \ k) \\
&= \ \ a + bk \ * \ c + dk \ \ + (\ a + bk \ * \ e + fk \ )
\end{aligned}$$

■

Dadas ya las demostraciones anteriores ($\boldsymbol{P_t}, +,*$) tiene estructura tipo anillo conmutativo con unitario, esto da pie para empezar a trabajar la divisibilidad en estos súper-conjuntos, para dar más claridad a cómo se opera en estos conjuntos se plantean los siguientes ejemplos, piense súper-conjunto P_5 y los elementos $6 + 5k$ y $2 + 1k$, la suma de ellos dos sería $6 + 5k \ + \ 2 + 1k \ = \ 6 + 2 \ + \ 5 + 1 \ k = 8 + 6k$, y la multiplicación de ellos dos sería $6 + 5k \ * \ 2 + 1k \ = \ 6 * 2 + 5 * 1 * k^2 \ + \ 5 * 2 + 6 * 1 \ k$ como $k^2 = t = 5$ queda $6 + 5k \ * \ 2 + 1k \ = \ 6 * 2 + 5 * 1 * t \ + \ 5 * 2 + 6 * 1 \ = \ 12 + 5 * 5 \ + \ 10 + 6 \ k = 37 + 16k$.

7 TEORÍA DE NÚMEROS EN $\boldsymbol{P_t}$ (RELACION DE DIVISIBILIDAD)

Como se mostró en el titulo anterior los súper-conjuntos $\boldsymbol{P_t}$ tienen estructura tipo anillo conmutativa con unidad, se dice que $(P_t,*)$ tiene estructura multiplicativa donde se puede hablar de una relación de divisibilidad y esto permite cuestionarse ¿ elementos pueden considerarse primos, asociados, unidades y compuestos?, en este capítulo se definirán estos elementos utilizando la relación ya mencionada y utilizando definiciones tales que funcionen también en los enteros o naturales, podría decirse que una visión más amplia del concepto de nùmero primo, asociado, unidad y compuesto.

Esta unidad es importante pues es el punto donde surge el problema planteado de este documento, pero antes de hablar de esto se explicará cómo representar los elementos de $\boldsymbol{P_t}$ como parejas ordenadas con el fin de facilitar la escritura y dar una lectura más compacta al lector.

7.1 Representación de los elementos de P_t como parejas ordenadas

Cada elemento de $\boldsymbol{P_t}$ se puede representar como una pareja ordenada, en la tesis de ((Tafur, 2006), 2006) muestra cómo se definen las operaciones de los números Duales en plano cartesiano $\boldsymbol{R^2}$ **,** de la misma manera se definen tomando a $\boldsymbol{P_t}$ en $\boldsymbol{R^2}$, en donde si $x \in \boldsymbol{P_t}$ y $x = a + bk$ entonces x será representado por la pareja $(a, b) \in \boldsymbol{R^2}$, definiendo así la suma y la multiplicación:

Definición. Dadas las parejas ordenadas a, b , c, d $\in R^2$ se define la operación suma como a, b $+$ c, d $= (a + c, b + d)$

Definición. Dadas las parejas ordenadas a, b , c, d $\in \boldsymbol{R^2}$ se define la operación multiplicación como a, b $*$ c, d $= (ac + bdk^2, ad + bc)$

El isomorfismo anterior no se demostrará ya que en la tesis "**ESTUDIO ALGEBRAICO DE LOS NÚMEROS DUALES"** (Jiménez, 2006, pg.12)

Con estas dos operaciones definidas se puede establecer un isomorfismo entre los $\boldsymbol{P_t}$ y $\boldsymbol{R^2}$**,** y por ello de aquí en adelante donde sea conveniente se trabajará con la escritura de parejas ordenadas, y además, trabajar con un isomorfo en $\boldsymbol{R^2}$ permite establecer un orden total de los elementos de $\boldsymbol{P_t}$ (orden lexicográfico), no sobra aclarar que este orden no es compatible con las operaciones ya definidas, es decir, aquí no es posible definir un conjunto de positivos.

7.2 Divisibilidad en P_t

Como se mostró los súper-conjuntos $\boldsymbol{P_t}$ tienen estructura de tipo anillo conmutativo con unidad y esto permitirá hablar de la relación de divisibilidad definiéndola de manera similar que en el conjunto $\boldsymbol{Z}$:

Definición. Sean los números $a, b \in \boldsymbol{P_t}$**,** se dice que a divide a b si y solo si existe un número $c \in \boldsymbol{P_t}$ tal que $ac = b$, se escribe $a|b$ y se lee a es un divisor de b o a divide a b.

Para demostrar posteriores teoremas y definir algunos conceptos es necesario introducir un conjunto llamado aquí ***conjunto de divisores*** *de x.*

Definición. Dado un elemento $a \in \boldsymbol{P}_t$ se llama ***conjunto de divisores de a*** al conjunto cuyos elementos dividen a a en $\boldsymbol{P_t}$ y se escribe $D(a)$, en lenguaje conjuntista se define como:

$$D\ a\ = \{x \in \boldsymbol{P}_t : x|a\}$$

Teorema 1. Sean los números $a, b, c \in P_k$, si $a|b$ y $b|c$, entonces $a|c$

Demostración:

Dados $a, b, c \in \boldsymbol{P_t}$**,** donde $a|b$ y $b|c$, por definición de división se tiene que existen $d, f \in \boldsymbol{P_k}$ tal que $a * d = b$ y $b * f = c$, sea $g \in \boldsymbol{P_t}$ donde $g = d * f$,

$c = b * f = \ a * d\ * f = a *\ d * f\ = a * g$ así que existe un $g \in \boldsymbol{P_t}$ tal que $a * g = c$, entonces, $a|c$.

Al trabajar con la relación de divisibilidad en los números enteros se hablan de unidades, primos, compuestos y asociados, así que en este trabajo al tener un conjunto tipo anillo y una definición de divisibilidad, en este momento de la indagación surge la siguiente pregunta: ¿en $\boldsymbol{P_t}$ también se pueden caracterizar elementos que se comporten de forma similar que en los $\boldsymbol{Z}$?

Para continuar esta parte del trabajo se quiere buscar que números pueden ser unidades, para ello se observa cómo se comportan las unidades en $\boldsymbol{Z}$ $(1$ y $-1)$, los cuales cumplen dos propiedades en $\boldsymbol{Z}$ que se tendrán en cuenta para buscar los candidatos a ser unidades en $\boldsymbol{P_t}$, estas propiedades son:

a. -1 divide a 1, es decir las unidades dividen al neutro multiplicativo
b. Las unidades dividen a cualquier número de $\boldsymbol{Z}$.

7.2.1 Unidades en P_t

Teniendo en cuanta las dos propiedades anteriores se buscan elementos en $\boldsymbol{P_t}$ que también cumplan estas propiedades ya que serán los primeros elementos a caracterizar como unidades, se tiene que el módulo en $\boldsymbol{P_t}$ divide a todo los demás elementos por la definición de divisibilidad y si un elemento divide al módulo este dividirá a los demás elementos del conjunto por el teorema 1, cumpliendo así la segunda propiedad, así que si se encuentran números que cumplan la primera propiedad, entonces, cumplirá las dos y es así como se halla un método para encontrar dichos elementos.

En $\boldsymbol{P_t}$ el modulo es $(1,0)$, así que si se encuentran números que tengan inverso multiplicativos, por definición estos dividirán a (1,0), para esto se diseñó un software dotado con un algoritmo para la división en estos conjuntos, el software por su código muestra las unidades como parejas ordenadas y además la muestra en orden lexicográfico, por lo tanto se dará la definición de este orden, además, que este orden será utilizado varias veces en teoremas y conjeturas posteriores dentro de este documento.

Definición. Dadas las parejas $a,b\ ,\ c,d\ \in \boldsymbol{R}^2$, $(a,b) \succcurlyeq (c,d)$ si y sólo si $(a \geq b) \vee (\ a = b\ \wedge\ c \geq d\ )$, y este se llama orden lexicográfico.

Al buscar los divisores del módulo en $\boldsymbol{P_2}$ el programa nombrado" divisores unidades y sucesiones de P_t " brindó los siguientes resultados:

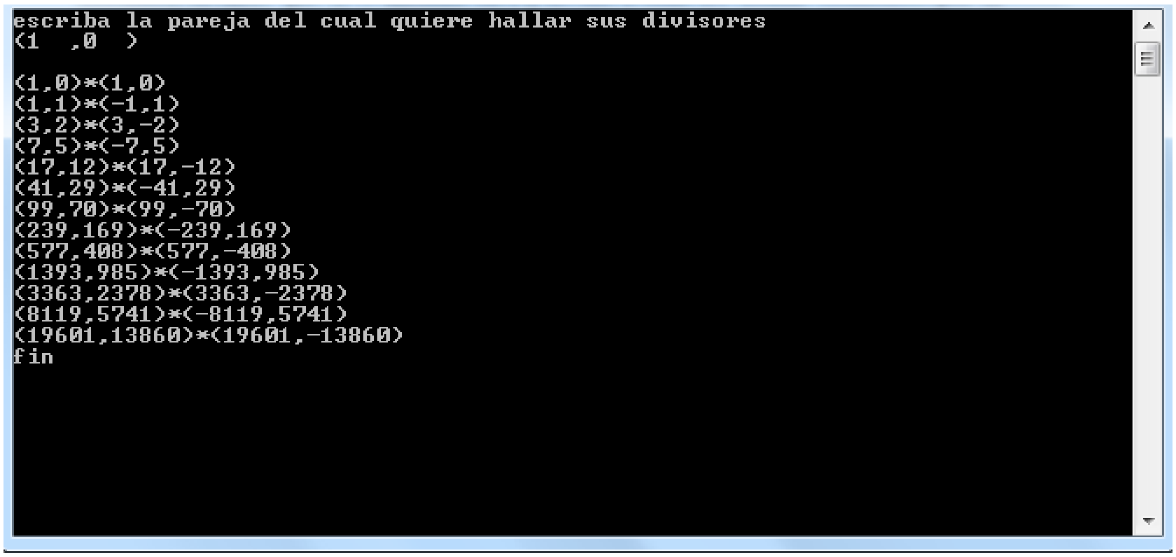


Ilustración 1.Resultados del programa al buscar los divisores de (1,0)

En la ilustración 1 se muestran los resultados encontrados por el programa, como se observa a partir de la tercera línea, en cada línea hay un par de parejas ordenadas y el producto de cada par de estas es (1,0), de estos resultados se puede concluir que si la pareja $a,b\ |e$ entonces $(a,-b)$ o $(-a,b)$ es su inverso multiplicativo, ahora revisemos esto:

Caso 1

$$a,b\ *\ a,-b$$
$$=\ a^2 - k^2b^2, ab - ab$$
$$= (a^2 - k^2b^2, 0)$$

En este casos debe cumplir que $a^2 - k^2b^2 = 1$

Caso 2

$$a, b \;\; * \;\; -a, b$$
$$= \;\; k^2b^2 - a^2, ab - ab$$
$$= (k^2b^2 - a^2, 0)$$

En este caso se debe cumplir que $k^2b^2 - a^2 = 1$

Ahora usando una propiedad del valor absoluto tenemos que $\; x - y \; = |y - x|$, aplicándolo acá surge el siguiente lema y el siguiente lema y el siguiente teorema.

Lema 1. $\; -1{,}0 \; |(1{,}0)$

$\; 1{,}0 \;\; = \;\; -1 * -1 + 0 * 0k^2, -1 * 0 + 1 * 0 \;\; = \;\; -1{,}0 \;\; * \;\; -1{,}0$, es decir que para $\; -1{,}0 \;\; existe\, el \;\; -1{,}0$ tal que $\; -1{,}0 \;\; * \;\; -1{,}0 \;\; = \;\; 1{,}0$ entonces $\; -1{,}0 \; |(1{,}0)$

Teorema 2. Sea $x, e \in P_t$ donde $x = (a, b)$ y $e = (1{,}0)$, si a $|a^2 - k^2b^2| = 1$, entonces, $x|e$.

Demostración. Sea $x, e \in \boldsymbol{P}_t$ donde $x = (a, b)$ y $e = (1{,}0)$, si a $|a^2 - k^2b^2| = 1$ entonces $x|e$.

Sea $\; x \in \boldsymbol{P_t}$ donde $x = (a, b)$ y $\; |a^2 - k^2b^2| = 1$, existe un $\; y \in \boldsymbol{P}_t$ donde

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

$$a, b \;\; * \;\; a, -b$$
$$= (a^2 - k^2b^2, ab - ab)$$
$$= (a^2 - k^2b^2, 0)$$

Caso 1. Si $\; a^2 - k^2b^2 = 1$

Entonces

$$a, b \;\; * \;\; a, -b \;\; = (1{,}0)$$

Así que $\; a, b \;\; |e$

Caso 2. Si $a^2 - k^2b^2 = -1$

Entonces

$$a, b \;\; * \;\; a, -b \;\; = (-1{,}0)$$

Y es decir que $\; a, b \; | \; -1{,}0$, también se tiene que $\; -1{,}0 \; |e$, por el lema 1 y teorema 2 concluimos que $\; a, b \;\; |e$

■

Teorema 3. Sea $x, e \in \boldsymbol{P_t}$ donde $x = (a, b)$ y $e = (1,0)$, si $x|e$, entonces, $|a^2 - k^2b^2| = 1$.

Demostración. Si a, b $|e$ significa que tiene inverso multiplicativo y como se mostró anteriormente su inverso multiplicativo es de la forma $(\frac{a}{a^2-k^2b^2}, \frac{-b}{a^2-k^2b^2})$ y esto garantiza que $\frac{a}{a^2-k^2b^2}, \frac{-b}{a^2-k^2b^2} \in \boldsymbol{Z}$**,** además, por la definición de $\boldsymbol{P_t}$ también $k^2 \in \boldsymbol{Z}$ **y** por la cerradura de la suma y el producto en $\boldsymbol{Z}$ se garantizaran los siguientes pasos:

$$\left(\frac{a}{a^2-k^2b^2}\right)^2, \left(\frac{-b}{a^2-k^2b^2}\right)^2 \in \boldsymbol{Z}$$

$$\left(\frac{a}{a^2-k^2b^2}\right)^2, \left(\frac{-b}{a^2-k^2b^2}\right)^2 * k^2 \in \boldsymbol{Z}$$

$$\frac{a^2}{(a^2-k^2b^2)^2}, \frac{k^2b^2}{(a^2-k^2b^2)^2} \in \boldsymbol{Z}$$

$$\frac{a^2}{(a^2-k^2b^2)^2}, \frac{-k^2b^2}{(a^2-k^2b^2)^2} \in \boldsymbol{Z}$$

$$\frac{a^2}{(a^2-k^2b^2)^2} + \frac{-k^2b^2}{(a^2-k^2b^2)^2} \in \boldsymbol{Z}$$

$$\frac{a^2-k^2b^2}{(a^2-k^2b^2)^2} \in \boldsymbol{Z}$$

$$\frac{1}{a^2-k^2b^2} \in \boldsymbol{Z}$$

Así que $a^2 - k^2b^2 = \pm 1$ concluyendo que $a^2 - k^2b^2 \ = 1$

■

Recordando que $k^2 = t$ y que t es un entero positivo se puede reescribirla expresión como $a^2 - tb^2 = \pm 1$, estas ecuaciones se llaman ecuaciones de Pell Fermat (Rubiano, Gordillo, & Luis, 2004) las cuales son de la forma $x^2 - Dy^2 = \pm 1$, en otras palabras las parejas (x, y) que son soluciones enteras a una ecuación de Pell Fermat resultan ser las unidades de $\boldsymbol{P_t}$ (en este caso $D = t$), en el trabajo no se pretende profundizar o indagar con estudios asociados a esta ecuación pero no sobra mostrar que existe una relación entre las unidades de estos conjuntos y las ecuaciones de Pell Fermat.

Hasta el momento con ayuda del software se han encontrado que existen elementos en $\boldsymbol{P_t}$ que tienen inverso multiplicativo diferentes del $(1,0)$ y $(-1,0)$, se ha mostrado que los elementos que tienen inverso multiplicativo dividen a unidad y tal comportamiento es igual a las unidades en $\boldsymbol{Z}$ dando como resultado:

Definición. Dado e neutro multiplicativo de $\boldsymbol{P_t}$ y un número $x \in \boldsymbol{P_t}$ si existe un $y \in \boldsymbol{P_t}$ tal que $xy = e$ entonces x es ***unidad***.

Corolario 1. Sea $x, e \in \boldsymbol{P_t}$ donde $x = \ a, b\ $ y $e = (1,0)$, si $x|e$ entonces x es unidad.

Corolario 2. Sea $x \in \boldsymbol{P_t}$ donde $x = \ a, b\ $, $|a^2 - k^2b^2| = 1$ si y solo si x es unidad

Teorema 4. Sea $x_1, x_2, x_3, x_4, e \in \boldsymbol{P_t}$ donde $x_1 = \ a, b\ , x_2 = \ -a, b\ , x_3 = \ a, -b\ , x_4 = (-a, -b)$ $y\ e = (1,0)\ si\ x_1|e$ entonces $x_2|e, x_3|e\ y\ x_4|e$

Demostración. Sea $x_1, x_2, x_3, x_4, e \in \boldsymbol{P_t}$ donde $x_1 = \ a, b\ , x_2 = \ -a, b\ , x_3 = \ a, -b\ , x_4 = (-a, -b)$, $e = (1,0)$ y $x_1|(1,0)$

■

Por propiedades de los enteros se tiene que $-a\ ^2 = a^2$ y $-b^2\ = b^2$

Como $\ a, b\ |e$ entonces se tiene que $\ a^2 - tb^2\ = 1$

$$a^2 - tb^2\ = 1$$

$$|\ -a\ ^2 - t\ -b\ ^2| = 1$$

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

Entonces $(-a, -b)|e$

Ahora

$$a^2 - tb^2\ = 1$$

$$|\ -a\ ^2 - tb^2| = 1$$

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

Entonces $(-a, b)|e$

Ahora

$$a^2 - tb^2\ = 1$$

$$|a^2 - t\ -b\ ^2| = 1$$

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

Entonces $(a,-b)|e$

■

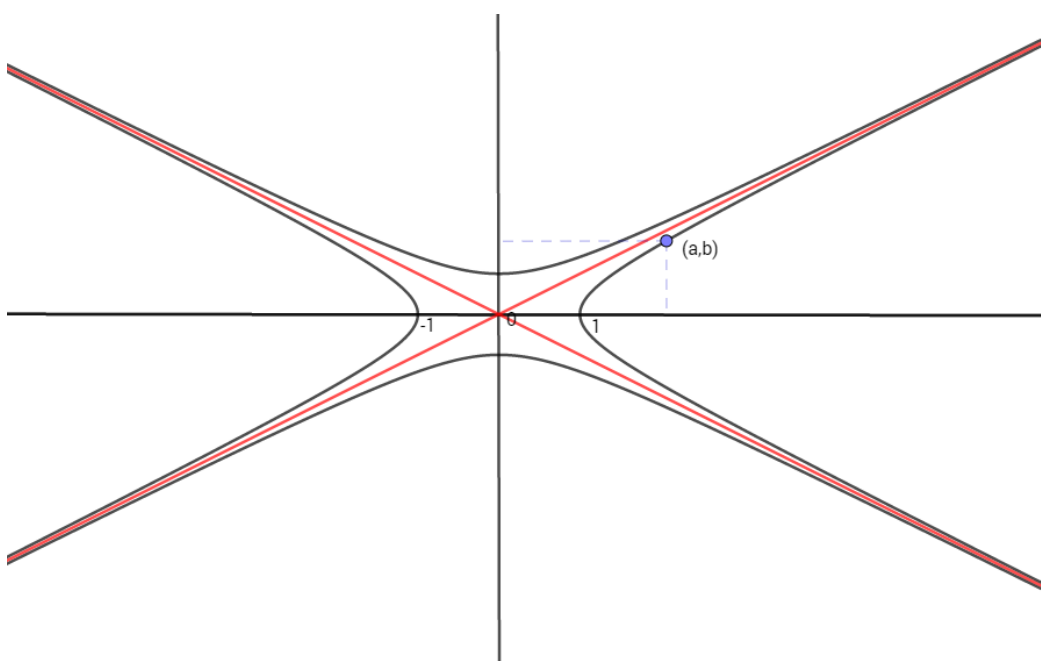
Corolario 3. Sea $x_1, x_2, x_3, x_4 \in \boldsymbol{P_t}$ donde $x_1 = (a,b)$, $x_2 = (-a,b)$, $x_3 = (a,-b)$, $x_4 = (-a,-b)$ y x_1 es unidad, entonces, x_2, x_3 y x_4 también son unidades.

Ya se tienen definidas las unidades, una manera de comprobar si un elemento de $\boldsymbol{P_t}$ es unidad usando el corolario 2, y gracias al corolario 3 al encontrar una unidad inmediatamente se obtienen 3 unidades nuevas.

De nuevo viendo la ilustración 1, el software muestra que existen varias unidades, pero no dice con certeza si hay más por las limitaciones de la memoria RAM, entonces ¿Cuántas unidades hay en un conjunto $\boldsymbol{P_t}$?, y dicha pregunta será respondida haciendo uso de las sucesiones de las cuales se hablará más adelante.

La ecuación $a^2 - k^2b^2 = 1$ también brindo un método para dividir el conjunto en clases de equivalencias a través de una relación de equivalencia que llamaré ***cuasinorma***, estas clases de equivalencia serán una herramienta muy útil para definir los elementos que nos faltan (primos, asociados y compuestos), ahora, para demostraciones posteriores hablaremos de algunas propiedades que cumplen estas unidades.

Si tomamos la ecuación de Pell Fermat $a^2 - tb^2 = 1$ y se grafica en el plano cartesiano donde $x = a$ y $y = b$ da como resultado dos hipérbolas donde sus asíntotas son las



rectas $y = \frac{1}{t}$ y $y' = \frac{1}{t}$ como se muestra a continuación.

Ilustración 2. Gráfica de la Ecuación de Pell Fermat de las unidades en el plano cartesiano

Se puede concluir a partir de la ilustración 2 que la componente a siempre será mayor que la componente b en una unidad $u = (a, b)$ con componentes positivas, el único caso en que no se cumple esto cuando la unidad es $(1,1)$, pero esta unidad solo es unidad en P_2, la justificación es la siguiente vamos a suponer que existe una unidad de la forma $u = (a, a)$ esto significa que $a^2 - ta^2 = 1$, $a^2(1-t) = 1$, $a^2|1-t| = 1$, como a es entero se tiene que $a^2 = |a^2|$, $a^2 = \frac{1}{|1-t|}$ como a es entero esto solo puede ocurrir cuando $t = 2$, así que la primera unidad de P_2 es $(1,1)$, y además, si $t > 2$ no existe una unidad con componentes iguales y tomado la ilustración 2 como justificación se puede decir que todas las unidades de $\boldsymbol{P_t}$ cumplen que su primera componente es mayor que la segunda, esta propiedad la usaremos para futuras demostraciones al igual que otras que serán demostradas en esta sección.

Corolario 4. La primera unidad de componentes positivas en P_2 es $(1,1)$ usando el orden lexicografico.

Corolario 5. En P_2 se cumplen que en toda unidad con componentes positivas la primera componente es mayor que la segunda (con el orden usual en $\boldsymbol{Z}$) a excepción de la primera unidad (primera unidad de componentes positivas usando el orden lexicográfico).

Corolario 6. En P_t con $t > 2$ se cumple que en toda unidad con componentes positivas la primera componente es mayor que la segunda (con el orden usual en $\boldsymbol{Z}$) .

En los tres corolarios anteriores se proponen teniendo en cuenta que t es un número entero no cuadrado ya que son nuestros conjuntos en estudio.

Teorema 5 Dadas dos unidades u_a y u_b con componentes positivas si se tiene que $u_a < (u_a * u_b)$ y $u_b < (u_a * u_b)$ con el orden lexicográfico.

Demostración: Sea $u_a = (a, b)$ y $u_b = (c, d)$ cada una con componentes positivas se tiene que $u_a * u_b = (ac + tbd, ad + cb)$, portanto $ac + tbd > a$ y $ac + tbd > c$ concluyendo que $u_a < (u_a * u_b)$ y $u_b < (u_a * u_b)$ por la definición de orden lexicográfico.

Para continuar con otras propiedades de las unidades es necesario introducir un nuevo concepto llamado ***cuasinorma***, ya que dichas propiedades serán retomadas cuando se comience a hablar de las sucesiones.

7.2.2 Cuasinorma en P_t

Al trabajar con las unidades de $\boldsymbol{P_t}$ se demostró que si para un elemento $x = (a, b)$ se tiene que $|a^2 - k^2b^2| = 1$ entonces x es unidad, a partir de esto se propone la siguiente definición.

Definición. Dado $x \in \boldsymbol{P_t}$ con $x = (a, b)$, la ***cuasinorma*** de x es igual a p donde $p = |a^2 - k^2b^2|$ y se escribe $||x|| = p$ o $||(a, b)|| = p$.

Teorema 6. Para todo $x \in \boldsymbol{P_t}$ existe un número entero p tal que $|\ x| \ = p$.

Demostración: Sea $x \in \boldsymbol{P_t}$ con $x = (a, b)$ se tiene que como $a, b, k^2 \in \boldsymbol{Z}$, entonces, $a^2, b^2 \in \boldsymbol{Z}$ y en consecuencia $|a^2 - k^2b^2| \in \boldsymbol{Z}$ por ser $\boldsymbol{Z}, +, *$ un anillo, si $p = |a^2 - k^2b^2|$ entonces existe $p \in \boldsymbol{Z}$ tal que $x \ = p$.

■

Ahora, con la cuasinorma de un elemento de $\boldsymbol{P_t}$ se define la siguiente relación.

Definición. Dados $x, y \in \boldsymbol{P_t}$ se dice que x está relacionado con y si y solo si $|\ x\ | = ||y||$.

Esta relación resulta ser de equivalencia ya que es transitiva, simétrica y reflexiva como se mostrara a continuación:

Si está x relacionado con y y y esta relacionado con z entonces x está relacionado con z

Si x relacionado con y y y esta relacionado con z significa que $||x|| = ||y||$ y $y \ = ||z||$ como la relación de igualdad es transitiva se tiene que $||x|| = ||z||$ y por la definición de la relación x está relacionado con y quedado así demostrada la transitividad.

Si está x relacionado con y significa que $||x|| = ||y||$ y como la igualdad es simétrica se tiene que $||y|| = ||x||$ y por la definición de la relación y está relacionado con x quedado así demostrada la simetría.

Sea $d = ||x||$ tenemos que $d = d$ entonces $||x|| = ||x||$ esto significa que x está relacionado con x quedado así demostrada la reflexividad.

Con esto queda demostrado que la relación es de equivalencia, ya que una relación de equivalencia debe cumplir estar tres propiedades según el libro "*Introducción a la teoría de conjuntos*" $(Muñoz, 2002)$.

■

Esta relación de equivalencia se utilizara para caracterizar elementos de $\boldsymbol{P_t}$**,** por ahora se postulara el siguiente teorema.

Teorema 7. Para todo $x, y \in P_t$ se tiene que $||x|| * ||y|| = ||x * y||$

Demostración: Sean $x, y \in \boldsymbol{P_t}$ donde $x = \ a, b\ , y = \ c, d\ ,\ \ x\ \ = p$ y $\ y\ \ = q$, se tiene que

$$
\begin{aligned}
\boldsymbol{x} \ * \ y \ &= |(a, b| \ * \ c, d \\
&= a^2 - k^2b^2 \ * \ c^2 - k^2d^2 \\
&= \ a^2 - k^2b^2 \ * \ c^2 - k^2d^2 \\
&= a^2c^2 - a^2k^2d^2 - k^2b^2c^2 + k^4b^2d^2 \\
&= |a^2c^2 - \mathrm{k}^2a^2d^2 - k^2b^2c^2 + k^4b^2d^2| \\
&= |a^2c^2 + k^4b^2d^2 - \mathrm{k}^2a^2d^2 - k^2b^2c^2| \\
&= |a^2c^2 + k^4b^2d^2 - \mathrm{k}^2a^2d^2 - k^2b^2c^2 + (2k^2acbb - k^2 2acbd)| \\
&= |a^2c^2 + 2k^2acbb + k^4b^2d^2 - \mathrm{k}^2a^2d^2 - k^2 2acbd - k^2b^2c^2| \\
&= |a^2c^2 + 2ack^2bd + k^4b^2d^2 - \mathrm{k}^2a^2d^2 - k^2 2acbd - k^2b^2c^2| \\
&= |a^2c^2 + 2ack^2bd + k^4b^2d^2) - k^2(a^2d^2 + 2adbc + b^2c^2| \\
&= \ (ac + k^2bd\ ^2 - k^2(ad + bc)^2| \\
&= |\ ac + k^2bd, ad + bc\ | \\
&= \ |\ a, b \ * \ c, d\ | \\
&= |\ x * y\ |
\end{aligned}
$$

■

Teorema 8. Dado $x \in \boldsymbol{P_t}$ *con* $x = (a, b)$ *si* $\|\boldsymbol{x}\| = 0$, entonces, $x = (0,0)$

Demostración: Suponga que existe un $x = (a, b) \in \boldsymbol{P_t}$ tal que $||x|| = 0$ y x no es $(0,0)$, Por definición de cuasinorma, esto significa que $|a^2 - k^2b^2| = 0$

$$a^2 - k^2b^2 = 0$$

$$a^2 = k^2b^2$$

$$a = kb$$

Pero se sabe k no es un entero y si $a = kb$ entoces a no sería entero, y si a no es entero no es cierto que $(a, b) \in \boldsymbol{P_t}$ contradiciendo la hipótesis, por tanto $x = (0,0)$.

■

En el libro de algebra abstracta de (Fraleigh, 1988)se define cuándo un conjunto tiene divisores de 0, este dice así, dado a un anillo R se dice que R tiene divisores de cero "0" si y solamente si existen un a y un b diferentes de 0 tal que $ab = 0$ $(Fraleigh, 1988)$, además, si un anillo es no tiene divisores de 0 es un dominio de integridad, y un dominio de integridad es un anillo cancelativo $(Fraleigh, 1988)$.

Teorema 9. $\boldsymbol{P_t}$ Es cancelativo.

Demostración: Supongamos que $\boldsymbol{P_t}$ tiene divisores de 0 (en este caso $0 = (0,0)$) o sea que existen $a, b \in \boldsymbol{P_t}$ tales $a \neq (0,0)$ y $b \neq (0,0)$ y $a * b = 0$ como $\|0\| = 0$ por el teorema 7 se tiene que $\|a * b\| = 0$ y que $\|a\| * \|b\| = 0$ por el teorema 6, eso significa que $\|a\| = 0$ o $\|b\| = 0$ ya que los enteros no tienen divisores de 0, ahora si $\|a\| = 0$ o $\|b\| = 0$ entonces $a = (0,0)$ o $b = (0,0)$ por el teorema 8 y esto contradice la hipótesis por tanto se concluye lo siguiente:

a. $\boldsymbol{P_t}$ no tiene divisores de 0.
b. $\boldsymbol{P_t}$ es un dominio entero dado que no tiene divisores de 0 $(Fraleigh, 1988)$.
c. $\boldsymbol{P_t}$ es un anillo cancelativo dado que es un dominio entero $(Fraleigh, 1988)$.

Ya con estos teoremas que muestran propiedades de la cuasinorma es posible volver a retomar un instante el temas de las unidades o mostrar otras propiedades que cumplen.

Teorema 10. Sean (a,b) y (c,d) unidades con componentes positivas, existe una unidad (x,y) tal que $(a,b)(x,y)=(c,d)$ y no es posible que las componentes de (x,y) sean negativas simultáneamente.

Demostración: Sean (a,b) y (c,d) unidades se tiene que (a,b) divide a (c,d) por que $(a,b)|e$ y $e|(c,d)$, es decir, que existe un (x,y) tal que $(a,b)(x,y)=(c,d)$,y además, por el teorema 7 se tiene que $|(a,b)|*|(x,y)|=|(c,d)|$, como (a,b) y (c,d) son unidades, por el corolario 2 se tiene que $|(a,b)|=1=|(c,d)|$, es decir que $1*|(x,y)|=1$, y la única manera para que esto ocurra es que $|(x,y)|=1$ concluyendo que existe (x,y) y además que esta es unidad también.

Ahora, supongamos que x y y son negativas simultáneamente esto implicaría que $(a,b)*(x,y)=(c,d)$, $(ax+tby,ay+bx)=(c,d)$, como x y y son negativos en los enteros se tiene que $ax+tby$ es negativo y $ax+tby=c$ pero c es positivo y negativo a la vez llegando así a una contradicción, concluyendo que existe la unidad (x,y) tal que $(a,b)*(x,y)=(c,d)$ y no es posible que las componentes de (x,y) sean negativas simultáneamente.

■

Teorema 11. Dada una unidad (a,b) *si* $a^2-tb^2=1$ su inverso multiplicativo es $(a,-b)$ y si $a^2-tb^2=-1$ su inverso es $(-a,b)$.

(Tenga presente que $\boldsymbol{|a^2+k^2b^2|=|a^2+tb^2|}$ ***Ya que*** $\boldsymbol{t=k^2}$)

Demostración:

Dada una unidad (a,b), si $a^2-tb^2=1$ se tiene que $(a,b)(a,-b)=(a^2-tb,ab-ba)=(1,0)$

Ahora si $a^2-tb^2=-1$ se tiene que $(a,b)(-a,b)=(tb-a^2,ba-ab)=((-1)(a^2-tb^2),ba-ab)=((-1)(-1),0)=(1,0)$

■

El siguiente teorema es de suma importancia ya que será usado más adelante cuando se tome el tema de las sucesiones.

Teorema 12. Si (a,b) es la primera unidad con componentes positivas, entonces, $(a^2+tb^2,2ab)=(a,b)^2$, es la segunda unidad usando el orden lexicográfico.

Demostración: se tiene que (a,b) es la primera unidad de componentes positivas y se quiere concluir que $(a^2+tb^2,2ab)$ es la segunda unidad, para concluir esto supondremos que existe una unidad (c,d) tal que $\ a,b\ \ <\ \ c,d\ \ <(a^2+tb^2,2ab)$ y $(c,d)\neq(a^2+tb^2,2ab)$ para llegar a una contradicción.

Como (a,b) y (c,d) son unidades se tiene que existe un (x,y) que es unidad donde sus componentes no son negativas simultáneamente por el teorema 10 tal que $\ a,b\ \ \ x,y\ \ =(c,d)$, y esto nos abre tres casos, el caso uno es que x y y tengan componentes positivas simultáneamente el caso dos que x sea negativa y el caso tres que y sea negativa.

Caso 1

Se tiene que las componentes de $\ x,y\ $ son positivas simultáneamente entonces $\ a,b\ \ \ x,y\ \ =(c,d)$ por el teorema 5 $\ x,y\ \ <(c,d)$ y teniendo en cuenta que (c,d) es la segunda unidad y (a,b) es la primera $\ x,y\ \ =(a,b)$ por tanto $\ a,b\ \ \ a,b\ \ =(c,d)$, $a^2+tb^2,2ab)=(c,d)$ contradiciendo la hipótesis que $(c,d)\neq(a^2+tb^2,2ab)$ asi que el primer caso no se puede dar.

Caso 2.

Se tiene la unidad de la forma $\ -x,y\ $ tal que $\ a,b\ \ -x,y\ \ =(c,d)$ donde $x>0$ y $y>0$, partiendo de esto se dirá que:

Parte (a)

Si $x^2-ty^2=1$

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

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

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

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

Y según el teorema 10 esto no puede ocurrir ya que (a,b) al igual que (c,d) tienen componentes positivas, entonces, entonces $(-x,-y)$ no puede tener componentes negativas simultáneamente llegando así a una contradicción.

Parte (b).

Si $x^2 - ty^2 = -1$ donde $x > 0$ y $y > 0$

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

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

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

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

Y por el teorema 5 se tiene que $a,b \quad > (c,d)$ y como (a,b) es la primera unidad significa que $a,b \quad < (c,d)$ al mismo tiempo llegando así a una contradicción.

Caso 3.

Se tiene la unidad de la forma $x,-y$ tal que $a,b \quad x,-y \quad = \quad c,d$ donde $x > 0$ y $y > 0$, partiendo de esto se dirá que:

Parte (a)

Si $x^2 - ty^2 = 1$

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

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

Siendo este el mismo caso 2 parte (b) llegando a la misma contradicción.

Parte (b)

Si $x^2 - ty^2 = -1$ donde $x > 0$ y $y > 0$

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

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

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

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

Siendo este el mismo caso 2 parte (a) llegando a la misma contradicción, y así finalmente se concluye que esta unidad (c,d) no puede existir y que la segunda unidad de componentes positivas es $(a^2 + tb^2, 2ab)$ donde (a,b) es la primera unidad de componentes positivas.

■

Como vimos una unidad (a,b) cumple que $|a^2 - tb^2| = 1$esta condiciones fue una herramienta fuerte para hacer demostraciones y la seguirá siendo para unas futuras demostraciones, por tanto, se introducirá una sección que hablara de ella y se verán los usos que se le dará en el trabajo.

Teorema 13. Dadas las unidades u_1 y u_n donde estas son la primera y la enésima unidad de las unidades de componentes positivas con el orden lexicográfico, se tiene que $u_n = (u_1)^n$

Demostración: se tiene que $u_2 = (u_1)^2$ por el teorema 12, ahora suponga que $u_n = (u_1)^n$, para concluir que $u_{n+1} = (u_1)^{n+1}$, supongamos que $u_{n+1} = (c,d)$ y que $u_n < (c,d) \leq (u_1)^{n+1}$, como u_n y (c,d) son unidades se tiene que u_n tiene inverso multiplicativo y es u_n^{-1}, entonces, $u_n * u_n^{-1} * (c,d) = (c,d)$, sea $(x,y) = u_n^{-1} * (c,d)$ como ambas son unidades se tiene que el producto de sus cuasinormas es 1 por lo tanto (x,y) es unidad y por definición debe tener inverso multiplicativo, hasta el momento reemplazando tendríamos que $u_n * (x,y) = (c,d)$, ahora, como u_n y (c,d) tiene componentes positivas no es posible que (x,y) tenga componentes negativas simultáneamente, por tanto esta unidad (x,y) debe tener ambas componentes positivas o solo una negativa abriendo así tres casos.

Caso 1.

Se tiene la unidad de la forma $(-x,y)$ donde $x > 0$ y $y > 0$ tal que $u_n(-x,y) = (c,d)$ partiendo de esto se dirá que:

Parte (a)

Si $x^2 - ty^2 = 1$

$$u_n(-x,y) = (c,d)$$

$$u_n(-x,y)(-x,-y) = (c,d)(-x,-y)$$

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

$$u_n = (c,d)(-x,-y)$$

Y según el teorema 10 esto no puede ocurrir ya que u_n al igual que (c,d) tienen componentes positivas, entonces, este (x,y) no puede tener componentes negativas simultáneamente llegando así a una contradicción.

Parte (b).

Si $x^2 - ty^2 = -1$

$$u_n \;\; -x, y \;\; = (c, d)$$

$$u_n \;\; -x, y \;\; x, y \;\; = (c, d) \;\; x, y$$

$$u_n(1,0) = (c, d)(x, y)$$

$$u_n = (c, d)(x, y)$$

Y por el teorema 5 se tiene que $u_n > (c, d)$ y como $u_n < (c, d)$ por hipótesis se llega a una contradicción.

Caso 2.

Se tiene la unidad de la forma $\;\; x, -y \;\;$ tal que $u_n \;\; x, -y \;\; = (c, d)$ partiendo de esto se dirá que:

Parte (a)

Si $x^2 - ty^2 = 1$

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

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

Siendo este el mismo caso 2 parte (b) llegando a la misma contradicción.

Parte (b)

Si $x^2 - ty^2 = -1$

$$u_n \;\; x, -y \;\; = (c, d)$$

$$u_n \;\; x, -y \;\; -x, -y \;\; = (c, d) \;\; -x, y -$$

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

$$u_n = (c, d)(-x, -y)$$

Siendo este el mismo caso 2 parte (a) llegando a la misma contradicción.

Caso 3. En que las componentes de (x, y) son positivas.

En esta caso $x,y \ = (a_1, b_1)$ concluyendo que $u_n * \ x,y \ = (c,d)$, como $u_n = \ u_1{}^{n}$, $u_1{}^{n} * (a_1, b_1) = (c,d)$, $u_1{}^{n} * u_1 = (c,d)$, $u_1{}^{n+1} = (c,d)$ ya que si $x,y \ > (u_1)$ se tendría que $u_n * \ x,y \ > u_1$, $u_n * \ x,y \ > \ u_1{}^{n+1}$, $c,d \ > \ u_1{}^{n+1}$ siendo esto una contradicción con la hipótesis, por lo tanto este $x,y \ = u_1$ y concluyendo que $c,d \ = \ u_1{}^{n} * u_1 = \ u_1{}^{n+1} = u_{n+1}$.

Corolario 7. Toda unidad de componentes positivas se puede escribir como una potencia de la primera unidad de componentes positivas en $\boldsymbol{P_t}$.

En este momento se definirán unos subconjuntos de $\boldsymbol{P_t}$ a partir de la definición de cuasinorma ya que estos nos servirán para definir asociados, primos y compuestos en $\boldsymbol{P_t}$

Definición. Dado un $y \in \boldsymbol{P_t}$ con $y = (a,b)$ la ***clasenorma*** de y es un conjunto donde están todos los elementos de $\boldsymbol{p_t}$ que tienen la misma cuasinorma que y este conjunto se escribe $[y]$, definido en leguaje conjuntista sería:

$$y \ = \{x: ||x|| = ||y||\}$$

Corolario 8. Todas las unidades pertenecen la clase $[(1,0)]$

7.2.3 Asociados en $\boldsymbol{P_t}$

En esta sección se definirán cuáles son los asociados de un numero en $\boldsymbol{P_t}$**,** teniendo en cuenta el comportamiento de los asociaos en $\boldsymbol{Z}$ como se hizo con las unidades, en $\boldsymbol{Z}$ los asociados se obtienen al multiplicar un número por las unidades, es decir, el -2 es el asociado del 2 porque es el producto entre la unidad -1 y el número 2.

Definición. Dados $x, y, z \in \boldsymbol{P_t}$ donde x es unidad y $z = x * y$, entonces z es un ***asociado*** de y.

Corolario 9. Dados $x \in \boldsymbol{P_t}$ x es asociado de x.

Nuevamente haciendo uso del software mencionado anteriormente se buscaron los asociados de un número cualquiera no unidad de $\boldsymbol{P_t}$, y como resultado mostro que existen varios asociados con los números ensayados, por ejemplo el $(2,2)$ en P_2:

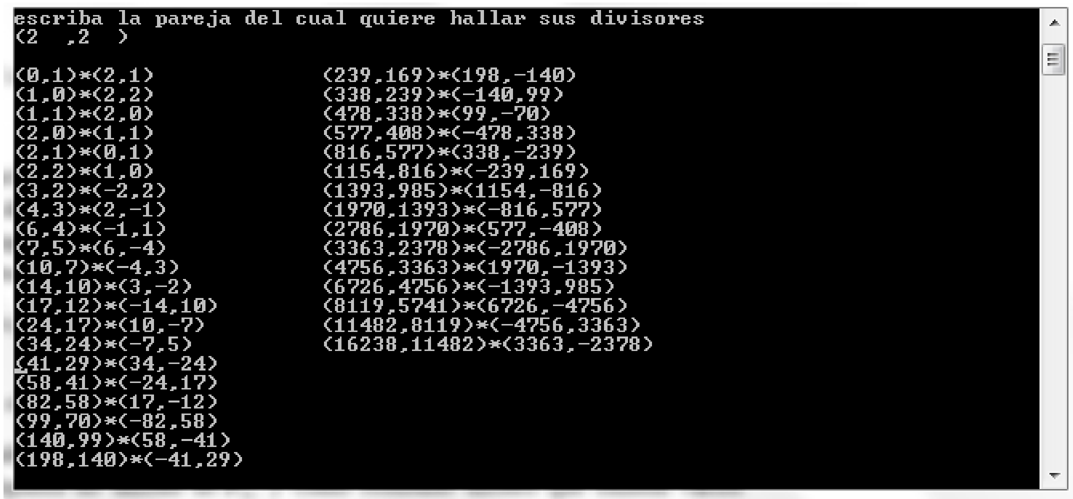


Ilustración 3.Asociados de $(2,2)$ *en* P_2

Teorema 10. Dado $x \in \boldsymbol{P_t}$ existe un asociado de x por cada unidad en $\boldsymbol{P_t}$

Demostración. Sean $x, y, z, a, a' \in \boldsymbol{P_t}$ donde y, z son unidades, $a = x * y$, $a' = x * z$, $y \neq z$, suponga que $a = a'$

$$a = a'$$

$$x * y = x * z$$

$$y = z$$

Contradiciendo que $y \neq z$ así que por cada unidad existe un asociado de x.

■

Teorema 11. Dados $x, y \in P_t$ si x es asociado de y entonces $x \in [y]$.

Demostración. Si x es asociado de y entonces existe una unidad z tal que $y * z = x$, por el corolario 2 se tiene que $z = 1$, por el teorema 5 se tiene que existe un $p \in \boldsymbol{Z}^+$ tal que $y = p$ y por el teorema 6 podemos decir que $x = y * z = y * z = p * 1 = p$, es decir que $x = y$, y por definición de clasenorma se tiene que $x \in [y]$**.**

■

Teorema 12. Dado $x \in \boldsymbol{P_t}$ con $x = a, b$, entonces, $-a, b$, $a, -b$, $-a, -b \in [x]$**.**

Demostración. Se tiene que $x \quad = |a^2 - k^2b^2|$, y además, por propiedades de ***Z*** que

$-a \;\; ^2 = a^2$ y $(-b)^2 = b^2$ entonces

$$-a, b \quad = |(-a)^2 - k^2b^2| = \; a^2 - k^2b^2 \; = | \; x \; |$$

así que $-a, b \;\; \in \;\; x$

$$a, -b \quad = |a^2 - k^2(-b)^2| = \; a^2 - k^2b^2 \; = | \; x \; |$$

así que $a, -b \;\; \in \;\; x$

$$-a, b - \quad = |(-a)^2 - k^2(-b)^2| = \; a^2 - k^2b^2 \; = | \; x \; |$$

así que $(-a, -b) \in [x]$

■

Inmediatamente demostrado este teorema se espera el reciproco, este reciproco no fue posible demostrarlo con la teoría obtenida hasta el momento, y aunque no parece, es necesario implementar mucha más teoría para demostrarlo por lo mismo este teorema tendrá un papel especial en este documento lo llamaremos la “***conjetura del tamaño de la clase norma***” ya que al demostrarlo se puede asegurar que el tamaño de todas las clasenormas es el mismo, a continuación se mostrará el enunciado y la primera idea de demostración mostrando cuál fue el obstáculo para culminar la demostración y a su vez haciendo una invitación al lector a intentar demostrarlo de esta forma, ya que aunque no pudo ser demostrada por el autor utilizando la teoría mencionada hasta el momento, no afirma que no sea posible.

Conjetura del tamaño de la clasenorma. Dados $x, y \in \boldsymbol{P_t} \;\; x \in [y]$ entonces x es asociado de y.

Demostración sugerida: Para demostrar este teorema basta con encontrar una unidad u tal que $x * u = y$, y para ello es necesario partir la demostración en tres partes las cuáles serán las siguientes:

a) Suponer que existe un elemento $u = (p, q)$ y deducir como es la forma de p y q.
b) Demostrar que si existe ese elemento u entonces $\quad u \quad = 1$ para decir que esta es unidad

c) Demostrar que $p, q \in \boldsymbol{Z}$ para asi afirmar que existe tal u en $\boldsymbol{P_t}$

Parte a:

Supongamos que existe un $u = (p, q) \in \boldsymbol{P_t}$ tal que $x * u = y$, sea $x = (a, b)$ y $y = (c, d)$

$$x * u = y$$

$$a, b \ * \ p, q \ = \ c, d$$

$$ap + k^2 bq = c$$

$$bp + aq = d$$

Resolviendo el sistema de ecuaciones nos queda:

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

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

Parte b:

Se tiene que $x \in [y]$, por definición de clasenorma $\mid x \mid = \mid y \mid$ es decir que $|a^2 - k^2 b^2| = |c^2 - k^2 d^2|$ el cual se tendrá en cuenta más adelante

Sea u de la forma:

$$u = | \ \frac{ac - k^2 bd}{a^2 - k^2 b^2}, \frac{ad - bc}{a^2 - k^2 b^2} \ |$$

$$u \ = | \ \frac{ac - k^2 bd}{a^2 - k^2 b^2} \ ^2 - k^2 \ \frac{ad - bc}{a^2 - k^2 b^2} \ ^2 \ |$$

$$u \ = | \frac{ac - k^2 bd \ ^2}{a^2 - k^2 b^2 \ ^2} - k^2 \frac{ad - bc \ ^2}{a^2 - k^2 b^2 \ ^2} |$$

$$u \ = \frac{ac - k^2 bd \ ^2 - k^2 \ ad - bc \ ^2}{a^2 - k^2 b^2 \ ^2}$$

$$u \ = | \frac{a^2 c^2 - 2k^2 acbd + k^4 b^2 d^2 \ - k^2 \ a^2 d^2 - 2abbc + b^2 c^2}{a^2 - k^2 b^2 \ ^2} |$$

$$u \ = | \frac{a^2 c^2 - 2k^2 acbd + k^4 b^2 d^2 \ - \ k^2 a^2 d^2 - k^2 2abbc + k^2 b^2 c^2}{a^2 - k^2 b^2 \ ^2} |$$

$$u \quad = \left| \frac{a^2c^2 + k^4b^2d^2 \; - \; k^2a^2d^2 + k^2b^2c^2 \; + \; 2k^2acbd - 2k^2acbd}{a^2 - k^2b^2 \;\; ^2} \right|$$

$$u \quad = \left| \frac{a^2c^2 + k^4b^2d^2 \; - \; k^2a^2d^2 + k^2b^2c^2}{a^2 - k^2b^2 \;\; ^2} \right|$$

$$u \quad = \left| \frac{a^2c^2 + k^4b^2d^2 - k^2a^2d^2 - k^2b^2c^2}{a^2 - k^2b^2 \;\; ^2} \right|$$

$$u \quad = \left| \frac{a^2c^2 - k^2a^2d^2 + k^4b^2d^2 - k^2b^2c^2}{a^2 - k^2b^2 \;\; ^2} \right|$$

$$u \quad = \left| \frac{a^2 \;\; c^2 - k^2d^2 \;\; - k^2b^2 \;\; c^2 - k^2d^2}{a^2 - k^2b^2 \;\; ^2} \right|$$

$$u \quad = \left| \frac{(a^2 - k^2b^2)(c^2 - k^2d^2)}{a^2 - k^2b^2 \;\; ^2} \right|$$

Y como $|a^2 - k^2b^2| = |c^2 - k^2d^2|$

$$u \quad = \left| \frac{\pm \;\; a^2 - k^2b^2 \;\; ^2}{a^2 - k^2b^2 \;\; ^2} \right|$$

$$u \quad = | \pm 1|$$

$$u \quad = 1$$

Y por el corolario 2, u es unidad.

Parte c:

Ahora, sólo falta demostrar que $p, q \in \boldsymbol{Z}$ esta es la parte que no ha sido posible demostrar y se resume a demostrar que si dados $a, b, c, d \in Z$ donde $a^2 + tb^2 \;\; = |c^2 + td^2|$ y $p = \frac{ac - k^2bd}{a^2 - k^2b^2}, q = \frac{ad - bc}{a^2 - k^2b^2}$ entonces $p, q \in Z$, esta es la parte a la que el lector es invitado a intentar demostrar, sin embargo, este teorema no será necesario para el desarrollo del trabajo pero resultó interesante y por es mencionado.

Hasta aquí se menciona la teoría necesaria de las unidades en $\boldsymbol{P_t}$ para solucionar el problema planteado y se abordará ahora que son los números primos y compuestos en los súper-conjuntos $\boldsymbol{P_t}$. }

7.2.4 Primos y compuestos en P_t

Según la definición de número primo en los enteros, los primos son aquellos números cuyos divisores son las unidades y sus asociados, dado que en $\boldsymbol{P_t}$ la cantidad de divisores de un número en $\boldsymbol{P_t}$ es “grande” en comparación con $\boldsymbol{Z}$ como lo mostró el programa, se usarán las clasenormas y un conjunto llamado el conjunto de divisores.

Definición. Se llamara conjunto de divisores de x al conjunto conformado por todos los números que dividen a x y este e escribe D_x, en lenguaje conjuntista se define:

$$D_x = \{y \in \boldsymbol{P_t} : y|x \}$$

Siguiendo la definición en los **Z**, con el corolario 2 y teorema 8 se define así un número primo.

Definición. Se dice que $x \in \boldsymbol{P_t}$ es ***primo*** si y solo si $| \; x \; | \neq 1$ y para todo $y \in D_x \quad y \quad = 1 \; o \quad y \quad = | \; x \; |$

Esta definición asegura que si a un elemento lo divide una unidad o un asociado exclusivamente resulta res primo al igual que los primos en $\boldsymbol{Z}$, por ejemplo pensemos es el numero $(2,2)$ en $\boldsymbol{P_3}$ se tiene que $\quad (2,2) \quad = 8$, además, $(1,1) \, * \, (2,0) = (2,2)$ es decir que $\; 1,1 \;, (2,0) \; \in \; D_{(2,2)}$ y pues $\quad (1,1) \quad = 2, \quad (2,0) \quad = 4$ es decir que ninguno de estas dos números son unidades o asociados de $(2,2)$, por ende, $(2,2)$ no debería ser primo, sino más bien un compuesto, por ello la definición anterior.

Ahora suponga de un $x \in \boldsymbol{P_t}$ donde existe un $y \in D_x$ y $| \; y \; | \neq | \; x \; | \neq 1$, x es un candidato para considerarse compuesto, esperando que al igual que en $\boldsymbol{Z}$ este también sea producto de al menos dos primos de $\boldsymbol{P_t}$.

Definición. Se dice que $x \in \boldsymbol{P_t}$ es ***compuesto*** si y solo existe un $y \in D_x$ tal que $| \; y \; | \neq | \; x \; | \neq 1$

En esta unidad se definieron las unidades los asociados y utilizando la clasenorma se definieron los primos y compuestos en $\boldsymbol{P_t}$, además, si tenemos un elemento de $\boldsymbol{P_t}$ usando la cuasinorma podemos establecer si dos números son asociados, el conjunto de divisores podemos decir que tipo de número es (primo o compuesto), además se agrando un poco más los conocido de su estructura ya que ahora sabemos que es un dominio entero y las implicaciones que lleva ser dominio entero ya mencionadas algunas anteriormente.

Como ya se mencionó, la cardinalidad del conjunto de unidades es igual a la de los asociados, ahora si tenemos un número primo todos los números que pertenezcan a su clasenorma será también un número primo y funciona igual para los compuestos, así que si tenemos un número primo al multiplicarlo con una unidad obtendremos otro primo. Con esto podemos hablar del planteamiento del problema.

7.3 Planteamiento del problema

Ya con la teoría obtenida hasta el momento se puede pensar en abordar el problema planteado, la primera pregunta es ¿cuántas unidades hay?, ¿cuantos asociados de un número? y ¿hay un método para hallar las unidades usando sucesiones recurrentes en dos variables?, hasta el momento solo podemos decir es si un número es primo compuesto o unidad, Al continuar explorando estos se observó que las unidades se pueden obtener a partir de un patrón que define unas sucesiones recurrentes en dos variables y que son una herramienta clave para resolver el problema de esta trabajo y así con ellas responder si ¿ hay un método para hallar unidades y saber cuántas unidades hay?.

8 MÉTODO DE ABORDAR EL PROBLEMA

Para desarrollar el problema se comienza observando el comportamiento de las unidades con componentes positivas de $\boldsymbol{P_t}$ ordenadas con el orden lexicográfico, ya que al estar ordenadas de esta manera es posible observar patrones en ellas y a su vez, establecer conjeturas y desarrollar teoremas ya más enfatizados a la solución del problema para este trabajo.

8.1 Comportamiento de las unidades en P_t

Una de las preguntas que se pretende responder es ¿cuántas unidades hay en $\boldsymbol{P_t}$**?**, para ello nuevamente se hace uso del programa con el fin de deducir un método diferente para hallar las unidades y el total de ellas, y así no depender el software.

	$t=2$	$t=3$	$t=5$	$t=6$	$t=7$	$t=8$	$t=10$
u_0	(1,0)	(1,0)	(1,0)	(1,0)	(1,0)	(1,0)	(1,0)
u_1	(1,1)	(2,1)	(2,1)	(5,2)	(8,3)	(3,1)	(3,1)
u_2	(3,2)	(7,4)	(9,4)	(49,20)	(127,48)	(17,6)	(19,6)
u_3	(7,5)	(26,15)	(38,17)	(485,198)	(2024,765)	(99,35)	(117,37)
u_4	(17,12)	(97,56)	(161,72)	(14801,1960)	(32257,12192)	(577,204)	(724,228)

Tabla 1. Primeras 5 unidades para algunos valores de t

Se explicaran algunas cosas de la tabla 1 que servirán también más adelantes, lo primero es que el trabajo se centrará en hallar las unidades con componentes positivas, ya que recordando, si tenemos una unidad en consecuencia tenemos otras tres por el corolario 3, por ello en la tabla se colocaron solo unidades de componentes positivas, segundo, siempre se describirá como u_0 al módulo de la multiplicación.

Note que en la tabla 1 no importa el valor de t siempre se cumple que $u_0 < u_1 < u_2 < u_3 < u_4$ con el orden lexicográfico y por el código del programa se puede asegurar que no existe una unidad menor a u_4 de componentes positivas que no esté en la tabla, así que utilizar el orden lexicográfico resulta conveniente y útil para estudiar la carnalidad del conjunto de unidades este conjunto lo denotaremos U_t

Definición. $U_t = \{x \in \boldsymbol{P_t}: x\ es\ unidad\}$

Sea u_i un elemento de U_t las componentes de u_i se denotaran $a_i\ y\ b_i$, es decir, $u_i = (a_i, b_i)$, viendo la tabla 1 cuando $t = 5, a_3 = 38$ y $b_3 = 17$ para $u_3$definir cada componente de una unidad resulta ser de utilidad ya que explorando la tabla se indujo que estas unidades se pueden describir de una manera recurrente, es decir, una unidad se puede deducir utilizando las componentes de la unidad anterior, por ejemplo cuando $t = 2$ fíjese en u_1, u_2 y u_3 de aquí se tiene que $b_1 = 1$, $b_2 = 2$, $b_3 = 5, a_1 = 1, a_2 = 3$ y $a_3 = 7$, por ahora concentrese en las componentes b_i, $b_2 = 2 = 1 + 1 = a_1 + b_1$ ocurre lo mismo con $b_3 = 5 = 3 + 2 = a_2 + b_2$ de aquí se induce que $b_n = a_{n-1} + b_{n-1}$, ahora fíjese en las componentes a_i estas también se comportan similar, puede comprobar que $a_n = a_{n-1} + 2b_{n-1}$ en donde podemos concluir que una $u_n \in U_2$ se puede describir como

$$u_n = (a_{n-1} + 2b_{n-1}, a_{n-1} + b_{n-1})$$

Este es un claro ejemplo de lo que se quiere lograr en todos los $\boldsymbol{P_t}$**,** es conseguir una sucesión por recurrencia definida en dos variables las cuales me generen las unidades de componentes positivas, lo esperado es definir esta sucesión a partir del valor de t.

8.2 Sucesiones en dos variables definidas por recurrencia

Como se evidenció en la sección anterior se espera que las unidades en $\boldsymbol{P_t}$ se pueden describir a través de una sucesión definida por recurrencia en dos variables, donde estas variables serán las componentes de las unidades en cada $\boldsymbol{P_t}$. El estudio de este trabajo pretende caracterizar alguna sucesión para cada conjunto $\boldsymbol{P_t}$ **y** las denotaremos S_t**.**

Definición. Una sucesión S_t es una función que va de $\boldsymbol{N}$ en $\boldsymbol{N}$x$\boldsymbol{N}$ y esta se define por recurrencia de la siguiente manera:

$$s_0 = \quad a_0, b_0 \quad = (1,0)$$

$$s_n = (x_0 a_{n-1} + y_0 b_{n-1}, x_1 a_{n-1} + y_1 b_{n-1})$$

Como se ve en la definición anterior una sucesión de S_t está compuesta de 4 coeficientes llamados x_0, x_1, y_0 y y_1a partir de ellos y otras condiciones podremos ligar una sucesión S_t a un conjunto $\boldsymbol{P_t}$, ahora, para que una sucesión se pueda ligar al conjunto debe cumplir que:

1. Para toda $s_n \in S_t$, s_n es unidad en $\boldsymbol{P_t}$.

Como el cardinal de elementos de sucesión es el mismo del conjunto de los números Naturales si se encuentra una sucesión que cumpla la condición y que todos los elementos de S_t sean unidades de $\boldsymbol{P_t}$ entonces quedaría demostrado que el cardinal de las unidades con componentes positivas seria numerable, ahora, para una mayor facilidad de escritura de las sucesiones S_t utilizaremos una matriz que para representar una sucesión de estas.

Definición. Una ***matriz*** $\boldsymbol{M_t}$ es una matriz cuadrada de tamaño 2x2 que representa una sucesión S_t donde los coeficientes de la matriz serán $a_{1\,1} = x_0, a_{1\,2} = y_0, a_{2\,1} = x_1$ y $a_{2\,2} = y_1$, es decir la matriz:

$$M_t = \begin{matrix} x_0 & y_0 \\ x_1 & y_1 \end{matrix}$$

Representa la sucesión S_t:

$$s_0 = \ a_0, b_0 \ = (1,0)$$

$$s_n = (x_0 a_{n-1} + y_0 b_{n-1}, x_1 a_{n-1} + y_1 b_{n-1})$$

Ya con esta matriz definida se comenzará mostrando un algoritmo para hallar una sucesión S_t.

8.3 Cómo obtener una sucesión S_t

Nuevamente vamos a observar la tabla 1 y con los datos que están ahí vamos a construir las componentes x_0, x_1, y_0 y y_1 de la sucesión S_3, lo primero que se necesita es tener las unidades u_1 y u_2, para esto no hay un método diferente que “al tanteo”, así que por ello se hace uso del software para obtener estas primeras unidades, teniendo estas unidades se siguen los siguientes pasos para encontrar la sucesión:

1. Conocer u_0, u_1 y u_2.
2. Escribir a $u_1$en términos de u_0.

3. Escribir a u_2 en términos de u_1 utilizando los datos del paso 2.

Para mayor comprensión del lector se realizarán dichos pasos para el conjunto $\boldsymbol{P_3}$, se sabe que $u_0 = \ 1,0$ y con ayuda del software se obtiene $,u_1 = (2,1)$ y $u_2 = (7,4)$ teniendo así el paso uno, y ahora se procede con el paso 2.

En esta parte no sobra recordar que la sucesión debe tener la siguiente forma $s_n = x_0a_{n-1} + y_0b_{n-1}, x_1a_{n-1} + y_1b_{n-1}$, y que la finalidad es encontrar lo valores x_0, x_1, y_0 y y_1.

Como dice el paso 2 se escribe u_1 en términos de u_0: $u_1 = (x_0a_0 + y_0b_0, x_1a_0 + y_1b_0)$, como $u_0 = (1,0)$ y $u_1 = (2,1)$ reemplazando tenemos que $u_1 = ((x_0)1 + (y_0)0, (x_1)1 + (y_1)0)$,, es decir que:

$$a_1 = 2 = \ x_0 \ 1 + (y_0)0$$

$$b_1 = 1 = (x_1)1 + (y_1)0$$

Así que:

$$x_0 = 2$$

$$x_1 = 1$$

Ahora en el paso 3 se escribe $u_2 = (7,4)$ en términos de u_1: $u_2 = (x_0a_1 + y_0b_1, x_1a_1 + y_1b_1)$, pero como ya se tiene que $x_0 = 2$ y $x_1 = 1$, entonces:

$$u_2 = (2a_1 + y_0b_1, a_1 + y_1b_1)$$

Como $a_1 = 2$ y $b_1 = 1$ entonces:

$$u_2 = (4 + y_0, 2 + y_1)$$

Y por último como $u_2 = (7,4)$

$$a_2 = 7 = 4 + y_0$$

$$b_2 = 4 = 2 + y_1$$

$$y_0 = 3$$

$$y_1 = 2$$

Así encontrando los valores que buscábamos, $x_0 = 2, y_0 = 3, x_1 = 1$ y $y_1 = 2$, siendo entonces S_3:

$$s_0 = \left(a_0, b_0\right) = (1,0)$$

$$s_n = (2a_{n-1} + 3b_{n-1}, 1a_{n-1} + 2b_{n-1})$$

O de una forma más reducida

$$M_3 = \begin{pmatrix} 2 & 3 \\ 1 & 2 \end{pmatrix}$$

Ya con este ejemplo se puede pensar en una forma general de encontrar estas sucesiones utilizando el mismo algoritmo, como $u_0 = (1,0)$ para para cualquier t, entonces,

$$u_1 = \left((x_0)1 + (y_0)0,\ (x_1)1 + (y_0)0\right)$$

$$a_1 = (x_0)1 + (y_0)0$$

$$b_1 = (x_1)1 + (y_1)0$$

$$x_0 = a_1$$

$$x_1 = b_1$$

Y nuevamente escribiendo u_2 en términos de $u_1$se tiene que:

$$u_2 = \left(x_0 a_1 + y_0 b_1, x_1 a_1 + y_1 b_1\right)$$

Reemplazando ya en x_0 y x_1 queda que:

$$a_2 = a_1^2 + y_0 b_1$$

$$b_2 = b_1 a_1 + y_1 b_1$$

$$y_0 = (a_2 - a_1^2)/b_1$$

$$y_1 = (b_2 - b_1 a_1)/b_1$$

Quedando así x_0, x_1, y_0 y y_1 en términos de a_1, a_2, b_1 y b_2, esto sirvió para desarrollar un código que generara dichas sucesiones y así continuar con la indagación del problema.

8.4 Propiedades de S_t

Como se mención anteriormente se desarrolló un código que dado un valor para t hacia lo siguiente, primero calculaba las dos primeras unidades y con ellas establecía el valor de x_0, x_1, y_0 y y_1 como se mostró en la sección anterior, estos datos se organizaron en una tabla donde los valores de t van del 2 al 50, y omitiendo los valores donde t es un cuadrado, dicha tabla es la siguiente:

t	x_0	y_0	x_1	y_1
2	1	2	1	1
3	2	3	1	2
5	2	5	1	2
6	5	12	2	5
7	8	21	3	8
8	3	8	1	3
10	3	25	1	2
11	10	33	3	10
12	7	24	2	7
13	18	65	5	18
14	15	56	4	15
15	4	15	1	4
17	4	17	1	4
18	17	72	4	17
19	170	741	39	170
20	9	40	2	9
21	55	252	12	55
22	194	924	42	197
23	24	115	5	24
24	5	24	1	5
26	5	26	1	5
27	26	135	5	26
28	127	672	24	127
29	70	377	13	70
30	11	60	2	11
31	152	846	273	152

	0	3		0
32	17	96	3	17
33	23	132	4	23
34	35	204	6	35
35	6	35	1	6
37	6	37	1	6
38	37	228	6	37
39	25	156	4	25
40	19	120	3	19
41	32	205	5	32
42	13	84	2	13
43	348 2	228 33	531	348 2
44	199	132 0	30	199
45	161	108 0	24	161
46	243 35	165 048	358 8	243 35
47	48	329	7	48
48	7	48	1	7
50	7	50	1	7

Tabla 2. Tabla que muestra los valores de x_0, x_1, y_0 y y_1 para los primeros valores de t

Observando la Tabla 2 se evidencian las siguientes condiciones que cumplen estas primeras sucesiones:

1. Para todo valor de t se tiene que $x_0 = y_1$
2. Para todo valor de t se tiene que $\frac{y_0}{x_1} = t$ o $y_0 = x_1 t$

A partir de ello se puede concluir que para encontrar una sucesión S_t como y_0 y y_1 están escritos en términos de x_0, x_1 y t, la tarea para encontrar estas sucesiones se reduce a escribir x_0 y x_1 en términos de t, además, si comparamos los valores de la Tabla 1 con los de la Tabla 2, se puede conjeturar que:

3. Para todo valor de t se tiene que $x_0 = a_1$ y $x_1 = b_1$

Por esto a partir de ahora se trabajará solo con las sucesiones que sean de la forma S_t:

$$s_0 = a_0, b_0 = (1,0)$$

$$s_n = (x_0 a_{n-1} + t x_1 b_{n-1}, x_1 a_{n-1} + x_0 b_{n-1})$$

Y como la sucesión se redujo a dos incógnitas a partir de ahora $x_0 = x$ y $x_1 = y$, teniendo ahora para estudiar las sucesiones de la forma:

S_t=

$$s_0 = a_0, b_0 = (1,0)$$

$$s_n = (x a_{n-1} + t y b_{n-1}, y a_{n-1} + x b_{n-1})$$

Teorema 13. Dada la unidad $u_1 = a_1, b_1 \in \boldsymbol{P_t}$, esta genera a la matriz $M_t = \begin{matrix} a_1 & b_1(t) \\ b_1 & a_1 \end{matrix}$ describe una sucesión S_t ligada a $\boldsymbol{P_t}$.

Esto se demostrará por inducción:

$M_t = \begin{matrix} a_1 & b_1(t) \\ b_1 & a_1 \end{matrix}$ Describe por definición la sucesión S_t:

$$s_0 = a_0, b_0 = (1,0)$$

$$s_n = (a_1 a_{n-1} + b_1 \; t \; b_{n-1}, b_1 a_{n-1} + a_1 b_{n-1})$$

$$s_0 = 1,0$$

$$s_0 = |1^2 + 0^2| = 1 = 1$$

Así que s_0 es unidad

Suponga que $s_n = (a_n, b_n)$ es unidad eso implica que divide al neutro multiplicativo por tener inverso multiplicativo y por el teorema 3 que:

$$s_n = a_n^2 - t b_n^2 = 1 \; a_n^2 - t b_n^2 = 1$$

Según la sucesión $s_{n+1} = (a_1 a_n + b_1 \; t \; b_n, b_1 a_n + a_1 b_n)$

$$s_{n+1} \quad = | \ a_1 a_n + b_1 \ \ t \ \ b_n, \ \ ^2 - t \ \ \ b_1 a_n + a_1 b_n \ \ ^2|$$

$$s_{n+1} \quad = \ a_1^2 a_n^2 + 2a_1 a_n b_1 \ \ t \ \ b_n + b_1^2 \ \ t^2 \ \ b_n^2 - t(b_1^2 a_n^2 + 2b_1 a_n a_1 b_n + a_1^2 b_n^2 \ \ |$$

$$s_{n+1} \quad = |a_1^2 a_n^2 + 2a_1 a_n b_1 \ \ t \ \ b_n + b_1^2 \ \ t^2 \ \ b_n^2 - (t) b_1^2 a_n^2 - 2(t) b_1 a_n a_1 b_n - (t) a_1^2 b_n^2|$$

$$s_{n+1} \quad = |a_1^2 a_n^2 + 2a_1 a_n b_1 \ \ t \ \ b_n - 2(t) b_1 a_n a_1 b_n + b_1^2 \ \ t^2 \ \ b_n^2 - (t) b_1^2 a_n^2 - (t) a_1^2 b_n^2|$$

$$s_{n+1} \quad = |a_1^2 a_n^2 + b_1^2 \ \ t^2 \ \ b_n^2 - (t) b_1^2 a_n^2 - (t) a_1^2 b_n^2|$$

$$s_{n+1} \quad = |a_1^2 a_n^2 - (t) a_1^2 b_n^2 - (t) b_1^2 a_n^2 + b_1^2 \ \ t^2 \ \ b_n^2|$$

$$s_{n+1} \quad = |a_1^2 \ \ a_n^2 - \ \ t \ \ b_n^2 \ \ - \ \ t) b_1^2 (a_n^2 + \ \ t \ \ b_n^2 \ \ |$$

$$s_{n+1} \quad = |(a_1^2 - \ \ t) b_1^2 \ \ (a_n^2 + \ \ t \ \ b_n^2|$$

$$s_{n+1} \quad = |(a_1^2 - \ \ t) b_1^2 \ \ (a_n^2 + \ \ t \ \ b_n^2|$$

Ahora, recuerde que por hipótesis $a_n^2 - tb_n^2 \ = 1$y que $u_1$es unidad, implicando que $a_n^2 - tb_n^2 \ = 1$ y ahora reemplazamos obteniendo que:

$$s_{n+1} \quad = |(\pm 1)(\pm 1| = \ \pm 1 \ \ = 1$$

Y por el teorema 2 podemos concluir que s_{n+1} divide a la neutro multiplicativo y por ende es unidad, entonces todos los elementos de $S_t$son unidades, así que $M_t = \begin{matrix} a_1 & b_1(t) \\ b_1 & a_1 \end{matrix}$ describe la sucesión S_t ligada a $\boldsymbol{P_t}$.

■

Y de manera análoga se demuestra la siguiente afirmación, por tanto cual se dejará como corolario.

Corolario 10. Dada una unidad cualquiera de $u = (a, b) \in \boldsymbol{P_t}$ con componentes positivas, la matriz $M_t = \begin{matrix} a & tb \\ b & a \end{matrix}$ describe una sucesión S_t ligada a $\boldsymbol{P_t}$, a este proceso le llamará que la unidad u generó la matriz M_t y como M_t describe a una S_t también se puede decir que u generó a S_t.

Otra propiedad que se ve casi de inmediato es que S_t es creciente ya que todos sus elementos son parejas y cada componente de estas parejas son sumas de números Naturales.

Teorema 14. Una sucesión $\mathrm{S_t}$ es creciente.

Demostración:

Sean s_n y s_{n+1} dos elementos de S_t se tiene que $s_n = (a_n, b_n)$ y $s_{n+1} = a_{n+1}, b_{n+1}$, pero por la definición de S_t $s_{n+1} = \; a_1 \; a_n + t \; b_1 \; b_n, (b_1)a_n + (a_1)b_n$ y como estos números a_i y b_i son naturales se tienen dos casos:

Caso 1. Que $a_{n+1} = a_n$, si esto ocurre, entonces, $b_{n+1} \geq b_n$ por tanto $s_{n+1} \geq s_n$ por definición de orden léxico grafico concluyendo que S_t es creciente por definición de sucesión creciente.

Caso 2. Que $a_{n+1} > a_n$, si esto ocurre, entonces, $s_{n+1} \geq s_n$ concluyendo que S_t es creciente.

■

Por otro lado una matriz M_t generada por alguna unidad $u = (a, b)$, su determinante es $|M_t| = a^2 - tb^2$ y es evidente que esto tiene la forma de la cuasinorma de (a, b) y como esta pareja es unidad su cuasinorma es 1 concluyendo así que $|M_t| = \pm 1$, por esto hablará un poco de ellas.

1.1.1. Matrices M_t

Las matrices M_t generadas por una unidad, además, de solo representar sucesiones S_t también tiene relaciones con los elementos de $\boldsymbol{P_t}$, por ejemplo, del teorema 17 se sabe que los coeficientes a_{11}y a_{21} corresponden a las componentes a y b de alguna unidad respectivamente, ahora, piense en la matriz $M_t{}^2$ (refiriénse al producto entre matrices):

$$si \; M_t = \begin{matrix} a & tb \\ b & a \end{matrix}$$

$$entonces \;\; M_t{}^2 = \begin{matrix} a & tb \\ b & a \end{matrix} * \begin{matrix} a & tb \\ b & a \end{matrix} = \begin{matrix} a^2 + tb^2 & t(2ab) \\ 2ab & a^2 + tb^2 \end{matrix}$$

En los coeficientes de M_t se tiene que $a_{11} = a_{22}$ y que $(t)a_{21} = a_{12}$, esto mismo ocurre con los coeficientes de $M_t{}^2$, teniendo en cuenta esta regularidad se plantea el siguiente teorema.

Teorema 15. Dada una matriz M_t generada por una unidad entonces los coeficientes a_{11}, a_{12} de la matriz $M_t\ ^2$ son las componentes de una unidad $u_m = (a_{11}, a_{12}) \in P_t$

$$u_m = \ a^2 + tb^2, 2ab_1$$

$$u_m \ = \ \ a^2 + tb^2\ ^2 - t\ \ 2ab\ ^2$$

De la teoría del algebra lineal, dadas dos matrices A y B $\ A\ *\ B\ =\ A * B$, aplicándolo acá quedaría que $M_t\ ^2\ =\ M_t * M_t\ =\ M_t\ *\ M_t\ = \pm 1 * \pm 1 = 1$ y como la determinate de $M_t\ ^2 = \ a^2 + tb^2\ ^2 - t\ \ 2ab\ ^2$, tenemos que $a^2 + tb^2\ ^2 - t\ \ 2ab\ ^2$=1 y su vez $u_m\ \ = |\ a^2 + tb^2\ ^2 - t\ \ 2ab\ ^2|$

$$u_m\ \ =\ \ \ a^2 + tb^2\ ^2 - t\ \ 2ab\ ^2\ \ =\ \ 1$$

$$u_m\ \ =\ \ 1$$

$$u_m\ \ = 1$$

■

Como se cumple en $M_t\ ^2$ que $a_{11} = a_{22}$ y que $(t)a_{21} = a_{12}$ y además las a_{11} y a_{21} son las componentes de una unidad, está claro que la unidad (a_{11}, a_{21}) genera a $M_t\ ^2$ poe lo tanto $M_t\ ^2$ representa un sucesión ligada a P_t, y siendo más ambiciosos se espera que una matriz $M_t\ ^n$ represente una sucesión ligada a P_t.

Definición. Se dice que una matriz M_t está ligada a $\boldsymbol{P_t}$ si y solo si representa una sucesión ligada a $\boldsymbol{P_t}$**.**

Teorema 16. Si una matriz M_t fue generada por una unidad u entonces $M_t\ ^n$ está ligada a $\boldsymbol{P_t}$.y es generada por alguna unidad.

Demostración. M_t es una matriz generada por una unidad $u = (a, b)$

$$M_t\ ^2 = \begin{matrix} a & tb \\ b & a \end{matrix} * \begin{matrix} a & tb \\ b & a \end{matrix} = \begin{matrix} a^2 + tb^2 & t(2ab) \\ 2ab & a^2 + tb^2 \end{matrix}$$

Por el teorema 19 se tiene que a_{11}, a_{12} de la matriz $M_t\ ^2$ son las componentes de una unidad $u_m = (a_{11}, a_{12}) \in \boldsymbol{P_t}$, **c**omo se cumple en $M_t\ ^2$ que $a_{11} = a_{22}$ y que $(t)a_{21} = a_{12}$, está claro que la unidad (a_{11}, a_{21}) genera a $M_t\ ^2$ poe lo tanto $M_t\ ^2$ esta ligada a $\boldsymbol{P_t}$

Ahora, suponga que $M_t\ ^n$ esta ligada a $\boldsymbol{P_t}$ y es generada por una unidad (c, d) para concluir que $M_t\ ^{n+1}$ está ligada a $\boldsymbol{P_t}$

$$M_t^{\ n+1} = \begin{matrix} a & tb \\ b & a \end{matrix} * \begin{matrix} c & td) \\ d & c \end{matrix} = \begin{matrix} ac + tbd & tad + tbc \\ bc + ad & ac + tbd \end{matrix}$$

Se puede ver que $a_{11} = a_{22}$ y que $(t)a_{21} = a_{12}$ y que $(ac + tbd, bc + ad)$ si es unidad entonces genera a $M_t^{\ n+1}$.

$$|\ ac + tbd, bc + ad\ | = |\ \ a, b \quad c, d\ \ |$$

$$|\ ac + tbd, bc + ad\ | = |\ \ a, b\ || * ||\ c, d\ \ |$$

Y como (a, b) y (c, d) son unidades se tiene que:

$$ac + tbd, bc + ad \quad = 1 * 1$$

$$ac + tbd, bc + ad \quad = 1$$

Siendo así $(ac + tbd, bc + ad)$ una unidad, que además genera a $M_t^{\ n+1}$ por lo cual que demostrado el teorema.

■

Estos teoremas son necesarios para más adelante demostrar que existe una sucesión que genera a todas las unidades con componentes positivas ya que como se vio cada unidad genera una sucesión, pero adelantando, solo hay una sucesión que genera a todas las unidades con componentes positivas.

8.5 Relaciones entre las S_t ligadas a P_t.

Como se mostró en la sección anterior cada unidad genera una sucesión ligada a $\boldsymbol{P_t}$, los elementos de estas sucesiones son unidades, pero hasta ahora nada asegura que una sucesión de estas genere absolutamente todas las unidades, utilizando los visto hasta el momento de sucesiones y matrices ligadas a un $\boldsymbol{P_t}$ se pretende mostrar que hay una sucesión que genera todas las unidades, para ello, vamos se mostrarán algunos datos como medio de conjuración y dar respuesta a ¿cuál es la sucesión que me genera todas las unidades?

En este momento se agregará a la escritura lo siguiente: la matriz generada por la unidad u_n que está ligada a P_t se escribirá como $M_{t,n}$ y de la misma manera la sucesión generada por la unidad u_n que está ligada a P_t se escribirá como $S_{t,n}$, donde la unidad

u_n es la enésima unidad de las unidades de componentes positivas con el orden lexicográfico.

Observe la tabla 1 y céntrese conjunto P_2 y con las 3 primeras unidades (u_1, u_2 y u_3) se generarán las tres sucesiones ligadas a P_2 respectivamente.

Unidad u_i	**Matriz $M_{2,i}$**	**Sucesión $S_{2,i}$**	**Primeras unidades generadas por S_t, i**
$\boldsymbol{u_1 = (1,1)}$	$M_{2,1} = \begin{matrix} 1 & 2 \\ 1 & 1 \end{matrix}$	$s_0 = \ a_0, b_0 \ = (1{,}0)$ $s_n = (a_{n-1} + 2b_{n-1}, a_{n-1} + b_{n-1})$	$s_1 = \ 1{,}1$ $s_2 = \ 3{,}2$ $s_3 = \ 7{,}5$ $s_4 = \ 17{,}12$ $s_5 = \ 41{,}29$ $s_6 = (119{,}90)$
$\boldsymbol{u_2 = (3,2)}$	$M_{2,2} = \begin{matrix} 3 & 4 \\ 2 & 3 \end{matrix}$	$s_0 = \ a_0, b_0 \ = (1{,}0)$ $s_n = (3a_{n-1} + 4b_{n-1}, 2a_{n-1} + 3b_{n-1})$	$s_1 = \ 3{,}2$ $s_2 = \ 17{,}12$ $s_3 = \ 119{,}90$ $s_4 = \ 717{,}508$ $s_5 = \ 4183{,}2958$ $s_6 = (24381{,}17240)$
$\boldsymbol{u_3 = (7,5)}$	$M_{2,3} = \begin{matrix} 7 & 10 \\ 5 & 7 \end{matrix}$	$s_0 = \ a_0, b_0 \ = (1{,}0)$ $s_n = (7a_{n-1} + 10b_{n-1}, 5a_{n-1} + 7_1 b_{n-1})$	$s_1 = \ 7{,}5,$ $s_2 = \ 119{,}90$ $s_3 = \ 1733{,}1225$ $s_4 = \ 24381{,}17240$ $s_5 = \ 143067{,}242585$ $s_6 = (3427319{,}2413430)$

Tabla 3. Matrices y sucesiones ligadas a P_2 generadas por las 3 primeras unidades.

Esta tabla se puede evidenciar por ahora dos cosas, lo primero es que $M_{2,2} = (M_{2,1})^2$ y que $M_{2,3} = (M_{2,1})^3$, y lo mismo ocurre con P_3 y P_5 y lo mismo ocurre en las tablas 4 y 5 que salen a continuación:

Unidad u_i	**Matriz $M_{3,i}$**	**Sucesión $S_{2,i}$**	**Primeras unidades generadas por S_t, i**
$\boldsymbol{u_1 = (2,1)}$	$M_{2,1} = \begin{matrix} 2 & 3 \\ 1 & 2 \end{matrix}$	$s_0 = a_0, b_0 = (1,0)$ $s_n = (2a_{n-1} + 3b_{n-1}, a_{n-1} + 2b_{n-1})$	$s_1 = 2,1$ $s_2 = 7,4$ $s_3 = 26,15$ $s_4 = 97,56$ $s_5 = 362,209$ $s_6 = (1351,780)$
$\boldsymbol{u_2 = (7,4)}$	$M_{2,2} = \begin{matrix} 7 & 12 \\ 4 & 7 \end{matrix}$	$s_0 = a_0, b_0 = (1,0)$ $s_n = (7a_{n-1} + 12b_{n-1}, 4a_{n-1} + 7b_{n-1})$	$s_1 = 7,4$ $s_2 = 97,56$ $s_3 = 1351,780$ $s_4 = 18817,10864$ $s_5 = 262087,151316$ $s_6 = (3650401,2107560)$
$\boldsymbol{u_3 = (26,15)}$	$M_{2,3} = \begin{matrix} 26 & 30 \\ 15 & 26 \end{matrix}$	$s_0 = a_0, b_0 = (1,0)$ $s_n = (26a_{n-1} + 30b_{n-1}, 15a_{n-1} + 26_1 b_{n-1})$	$s_1 = 26,15$ $s_2 = 1351,780$ $s_3 = 70226,40545$ $s_4 = 3650401,2107560$ s_5 $= (189750626,109552575)$ s_6 $= (98633821515694626340)$

Tabla 4. Matrices y sucesiones ligadas a P_3 generadas por las 3 primeras unidades.

Unidad u_i	Matriz $M_{5,i}$	Sucesión $S_{2,i}$	Primeras unidades generadas por S_t, i
$\boldsymbol{u_1 = (2,1)}$	$M_{2,1} = \begin{matrix} 2 & 5 \\ 1 & 2 \end{matrix}$	$s_0 = a_0, b_0 = (1,0)$ $s_n = (2a_{n-1} + 5b_{n-1}, a_{n-1} + 2b_{n-1})$	$s_1 = 2,1$ $s_2 = 9,4$ $s_3 = 38,17$ $s_4 = 161,72$ $s_5 = 682,305$ $s_6 = (2889,1292)$
$\boldsymbol{u_2 = (9,4)}$	$M_{2,2} = \begin{matrix} 9 & 20 \\ 4 & 72 \end{matrix}$	$s_0 = a_0, b_0 = (1,0)$ $s_n = (3a_{n-1} + 4b_{n-1}, 2a_{n-1} + 3b_{n-1})$	$s_1 = 9,4$ $s_2 = 17,12$ $s_3 = 2889,1292$ $s_4 = 51841,23184$ $s_5 = 930249,416020$ $s_6 = (16692641,7465176)$
$\boldsymbol{u_3 = (38,17)}$	$M_{2,3} = \begin{matrix} 38 & 85 \\ 17 & 38 \end{matrix}$	$s_0 = a_0, b_0 = (1,0)$ $s_n = (7a_{n-1} + 10b_{n-1}, 5a_{n-1} + 7_1 b_{n-1})$	$s_1 = 38,17$ $s_2 = 2889,1292$ $s_3 = 219602,98209$ $s_4 = 16692641,7465176$ $s_5 = 1268860318,567451585$ $s_6 = (9.645E + 10,4.3134E + 10)$

Tabla 5.Matrices y sucesiones ligadas a $\boldsymbol{P_5}$ generadas por las 3 primeras unidades

Y dado esto nace la sospecha que si se organizan todas las unidades en orden lexicográfico la unidad enésima generará a $M_{t,1}{}^{n}$, es decir que $M_{t,n} = M_{t,1}{}^{n}$ pero antes de demostrar esto también se puede observar en las tablas 3, 4 y 5 que s_n de la sucesión $S_{t,2}$ el mismo s_{2n} de $S_{t,1}$ y que $s_n$de la sucesión $S_{t,3}$ es el mismo s_{3n} de $S_{t,1}$.

Teorema 17. Dada la matriz $M_{t,1}$se tiene que $s_n = u_n$ donde s_n es el enésimo término de la sucesión representada por $M_{t,1}$ y u_n es la enésima unidad de las unidades de componentes positivas (usando el orden lexicográfico).

Demostración: Sea $u_1 = (a_1, b_1)$ la primera unidad de componentes positivas en $\boldsymbol{P_t}$, en la sección de las unidades de $\boldsymbol{P_t}$ se demostró que si $u_1 = (a, b)$, entonces, la segunda unidad será $u_2 = (a^2 + tb^2, 2ab)$ y como $s_2 = (a_1\ a_1\ + tb_1\ b_1\ , b_1\ a_1\ + a_1(b_1) = a_1^2 + tb_1^2, 2a_1b_1\ =\ a, b\ \ a, b\ = u_1 * u_1 =\ u_1\ ^2$, quedando así demostrado que $u_2 =\ u_1\ ^2$, ahora si generamos la matriz $M_{t,1}$ con la unidad u_1 se tiene que $s_1 = u_1$ y $s_2 =\ a_1\ a_1\ + tb_1\ b_1\ , b_1\ a_1\ + a_1\ b_1\ =\ a_1^2 + tb_1^2, 2a_1b_1\ = u_2$, ahora supongamos que $s_n = u_n$ para concluir que $s_{n+1} = u_{n+1}$

Como $s_n = u_n = (a_n, b_n)$ se tiene que $s_{n+1} =\ a_1\ a_n\ + tb_1\ b_n\ , b_1\ a_n\ + a_1\ b_n$

$$s_{n+1} =\ a_1, b_1\ *\ a_n, b_n\ = u_1 * u_n$$

Por el teorema 13 se tiene que $u_n =\ u_1\ ^n$

$$s_{n+1} = u_1 *\ u_1\ ^n =\ u_1\ ^{n+1}$$

Y por el mismo teorema 13 se tiene que

$$s_{n+1} = u_{n+1}$$

■

Ahora, con lo que tenemos demostrado se puede afirmar que existe una sucesión que me genera a todos las unidades de componentes positivas y si recuerda el teorema 16, se concluye que por cada unidad de componentes positivas hay otras tres unidades, la sucesión generada por la primera unidad será la sucesión que genere todas las unidades, ya que si usamos otra sucesión generada por una unidad diferente a la primera esta generará unidades pero no todas, es decir, sabemos que toda unidad de componentes positivas es una potencia de u_1, u_n esta generara una sesión y dicha sucesión generar todas las unidades u_{mn}, si tiene la sucesión $S_{t,3}$, esta generará las unidades $u_3, u_6, u_9, \dots, u_{3m}, u_{3\ m+1\ ,\dots}$ y así sucesivamente, la demostración de esta afirmación se muestra a continuación.

Teorema 18. Sea s_n el enésimo término de la sucesión $S_{t,m}$ se tiene que $s_n = s_{nm}$ donde s_{nm} es el eneemesimo de la sucesión $S_{t,1}$

Demostración:

Se tiene la unidad $u_n = (a, b)$ y con ella se genera la matriz $M_{t,n}$ y esta a su vez describe la sucesión $S'_{t,n}$, se usará la demostración por inducción, $s'_1 =\ a_n\ 1\ + tb_n\ 0\ , b_n\ 1\ + a_n\ 0\ \ =\ a_n, b_n\ = u_n$ y $u_n = s_n$ de $s_{t,1}$.

Ahora, suponga que $s'_{m-1} = s_{n(m-1)}$ para concluir que $s'_m = s_{nm}$, por la definición de $S_{t,n}$, emésimo término de $S'_{t,n}$ es igual a

$$s'_m = \; a_n \; a_{m-1} \; + tb_n \; b_{m-1} \; , b_n \; a_{m-1} \; + a_n \; b_{m-1}$$

$$s'_m = \; a_n, b_n \; * \; a_{m-1}, b_{m-1}$$

$$s'_m = u_n * s'_{m-1}$$

$$s'_m = u_n * s_{n \; m-1} \; \textit{por hipotesis}$$

Por el teorema 22 $s_{n \; m-1} \; = u_{n \; m-1}$

$$s'_m = u_n * u_{n \; m-1}$$

Y por el teorema 13 $u_{n \; m-1} \; = (u_1)^{n \; m-1}$

$$s'_m = \; u_1 \;^{n} * (u_1)^{n \; m-1}$$

$$s'_m = \; u_1 \;^{n+n(m-1)} = \; u_1 \;^{n(1+ \; m-1 \;)} = \; u_1 \;^{nm}$$

$$s'_m = \; u_1 \;^{nm} = u_{nm} = s_{nm}$$

■

Teniendo en cuenta los demostrado hasta el momento es evidente que las matrices están relacionadas con las unidades de los súper-conjuntos $\boldsymbol{P_t}$, también quedó demostrado que cualquier unidad de componentes positivas es una potencia de la primera unidad de componentes positivas, que la enésima potencia de la primera unidad es la enésima unidad del conjunto de componentes positivas ordenadas con el orden lexicográfico, por ello la importancia de incluir el orden lexicográfico como método para ordenar unidades.

9 SOLUCIÓN DEL PROBLEMA PLANTEADO

En este capítulo se pretende mostrar como con la teoría planteada hasta el momento se puede saber cuál es la sucesión de dos variables definida por recurrencia como se mencionó en el planteamiento del problema que describe todas las unidades, también se mostrará para que casos ya se puede deducir el valor de la primera unidad de componentes positivas sin hacer uso del programa con el que se ha venido trabajando.

9.1 Sucesión que me genera todas las unidades

Recordando el problema de este trabajo se centraba en encontrar a través de sucesiones de dos variables definidas por recurrencia un método para describir las unidades de los conjuntos $\boldsymbol{P_t}$, hasta el momento está demostrado que hay tantas unidades con componentes positivas como números naturales, que cada unidad define una sucesión ligada a $\boldsymbol{P_t}$ pero que solo la sucesión generada por la primera unidad es aquella que genera todas las unidades de componentes positivas y que si se tiene una unidad de componentes positivas aparecen otras tres nuevas, así que la sucesión que genera absolutamente todas las unidades se llamará "***sucesión completa de unidades***".

La sucesión completa de unidades (SCU) deberá contemplar las unidades de componentes positivas, negativas y combinadas, para ello, será necesario utilizar la sucesión ligada a $\boldsymbol{P_t}$ que es generada por la primera unidad, es decir, $S_{t,1}$ ya que esta brindará absolutamente todas las unidades que tiene componentes positivas, ahora, la SCU deberá tomar en cuenta las unidades de la forma $-a,-b$, $a,-b$ $y\,(-a,b)$ de cada unidad (a,b) generada por $S_{t,1}$ con $a>0$ y $b>0$, a partir de aquí en esta unidad siempre que se hable de s_n se referirá directamente al enésimo término de la sucesión $S_{t,1}$ teniendo claro esto la SC se describirá de la siguiente forma, la SCU es una función cuyo dominio son los naturales y su rango serán las unidades de $\boldsymbol{P_t}$, si un elemento de dicho dominio es de la forma $4n$ su imagen será una unidad de componentes positivas, si es de la forma $4n+1$ su imagen tendrá la primera componente positiva o exclusivamente la segunda será negativa, si es de la forma $4n + 2$ será el inverso multiplicativo de la imagen de $4n + 1$ y $4n + 3$ su imagen tendrá ambas componentes negativas.

Si se tiene una unidad de componentes positivas su inverso multiplicativo será esa una unidad con las mismas componentes poro donde exclusivamente una de sus componentes será negativa como se demostró en el teorema 7, y si tenemos una unidad cualquiera para cambiar de signo ambas componentes basta con multiplicar dicha unidad con $(-1,0)$.

La SCU será dependiente de $S_{t,1}$ para así generar todas las unidades, la definición de la SCU es:

Definición. Dada una extensión cuadrática $\boldsymbol{P_t}$ se define la siguiente sucesión llamada ***sucesión completa de unidades (SCU):***

1. u_n es el enésimo término de la SCU si $n = 4m$ su imagen será s_m.
2. u_n es el enésimo término de la SCU si $n = 4m + 1$ su imagen será $s_m{}^{-1}$.
3. u_n es el enésimo término de la SCU si $n = 4m + 2$ su imagen será $s_m{}^{-1} * (-1,0)$.
4. u_n es el enésimo término de la SCU si $n = 4m + 3$ su imagen será $s_m * (-1,0)$.

Donde s_m es el emesimo término de la sucesión $S_{t,1}$.

Los teoremas de la sección anterior fueron necesarios para asegurar que hay una sucesión que describen todas las unidades con componentes positivas y así saber con seguridad que esta sucesión será la empleada para definir a la SCU, pero aunque ya se sabe que dicha sucesión existe, hay un limitante hasta ahora y es conocer las componentes de u_1 (la primera unidad de componentes positivas), así que es necesario conocer más acerca de esta primera unidad.

9.2 Primera unidad en un súper-conjunto P_t cuando $t = n^2 \pm c$

Para generar la SCU es necesario conocer a $S_{t,1}$ y para generar a $S_{t,1}$ es necesario conocer a u_1, esta es una de las tareas más relevantes de este trabajo, nuevamente con ayuda del software mencionado en el desarrollo de este documento se encontraron regularidades de cómo son las primeras unidades con respecto al valor de t, para ello se dará un corto resumen de las cosas relevantes que el lector debe tener en cuenta.

La matriz $M_{t,n}$ es una matriz que describe la sucesión ligada a $\boldsymbol{P_t}$ y la sucesión $S_{t,1}$ es la única sucesión que describe todas las unidades de componentes positivas, y además, las genera en orden lexicográfico. Las sucesiones S_t tienen 4 componentes que inicialmente se llamaron x_0, y_0, x_1 y y_1 que luego se redujeron a dos y que estas dos son las componentes de alguna unidad de componentes positivas de $\boldsymbol{P_t}$**,** pero para esta sección solo se tomará en cuenta la sucesión generada por la primera unidad de componentes positivas, en dado caso esta sucesión seria:

$$S_{t,1}:$$

$$s_0 = \ a_0, b_0 \ = \ 1,0 \ , u_1 = (a_1, b_1)$$

$$a_n = \ a_1 \ a_{n-1} \ + tb_1 \ b_{n-1} \quad , \quad b_n = (b_1 \ a_{n-1} \ + a_1 \ b_{n-1} \ )$$

$$s_n = (a_n, b_n)$$

Y la matriz que la representa es $M_{t,1} = \begin{matrix} a_1 & tb_1 \\ b_1 & b_1 \end{matrix}$, dado esto, solo interesa cómo encontrar dicha unidad u_1, nuevamente con uso del programa se generará la primera unidad de componentes positivas de los primeros 50 valores de t excluyendo los valores en que t es un cuadrado perfecto, estos valores se organizarán en la siguiente tabla:

Valor de t de P_t	a_1	b_1
2	1	1
3	2	1
5	2	1
6	5	2
7	8	3
8	3	1
10	3	1
11	10	3
12	7	2
13	18	5
14	15	4
15	4	1

17	4	1
18	17	4
19	170	39
20	9	2
21	55	12
22	194	42
23	24	5
24	5	1
26	5	1
27	26	5
28	127	24
29	70	13
30	11	2
31	1520	273
32	171	3
33	23	4
34	35	6
35	6	1
37	6	1
38	37	6
39	25	4
40	19	3
41	32	5
42	13	2
43	3482	531
44	199	30
45	161	24
46	24335	3588
47	48	7
48	7	1
50	7	1

Tabla 6. Componentes a_1*y* b_1 *de la unidad* u_1 *de* P_t *con respecto al valor de* t

La tabla 6 muestra lo siguiente, dado un valor de t el cual corresponde a la primera columna, se tienen las componentes a_1y b_1 que corresponden a la primera unidad de componentes positivas $u_1 = (a_1, b_1)$ para dicho valor t de $\boldsymbol{P_t}$lo primero que se puede observar de la tabla 6 es que cuando t es de la forma $n^2 \pm 1$ es sencillo deducir l forma de los valores de a_1 y b_1 en términos de n, por ejemplo cuando $t = 3$ o $t = 5$ se tiene que $u_1 = (2,1)$ o cuando $t = 8$ o $t = 10$ se tiene que $u_1 = \ 3,1$, y no solo que tiene la misma unidad si no que $b_1 = 1$ y $a_1 = n$ siempre que t sea de la forma $n^2 + 1$ o $n^2 - 1$, por lo que se concluye el siguiente teorema.

Teorema 19. Dado un súper-conjunto $\boldsymbol{P_t}$ si t es de la forma $n^2 + 1$ o $n^2 - 1$ con $n \in \boldsymbol{Z}^+$, entoces, la primera unidad de componentes positivas es $u_1 = (n, 1)$.

Demostración: se tiene el súper-conjunto $\boldsymbol{P_t}$ donde $t = n^2 + 1$ o $t = n^2 - 1$ donde $n \in \boldsymbol{Z}^+$ el elemento el elemento $(n, 1)$ es unidad ya que si $t = n^2 + 1$ tenemos que:

$$\begin{aligned} n,1 &= n^2 - t1^2 \\ n,1 &= n^2 - \ n^2 + 1 \ \ 1^2 \\ n,1 &= n^2 - \ n^2 + 1 \\ n,1 &= n^2 - n^2 - 1 \\ n,1 &= -1 \ = 1 \end{aligned}$$

Y si $t = n^2 - 1$ se tiene que:

$$\begin{aligned} n,1 &= n^2 - t1^2 \\ n,1 &= n^2 - \ n^2 - 1 \ \ 1^2 \\ n,1 &= n^2 - \ n^2 - 1 \\ n,1 &= n^2 - n^2 + 1 \\ n,1 &= 1 \ = 1 \end{aligned}$$

Mostrando que $(n, 1)$ es unidad en $\boldsymbol{P_t}$

Ahora solo falta demostrar que es la primera unidad, supongamos que la primera unidad es (c, d), esto significa que $\ c, d \ < (n, 1)$ si (c, d) es la primera unidad significa que la sucesión $S_{t,1}$, debe generar a $(n, 1)$, ahora vamos a decir que $(n, 1)$ es la enésima unidad de componentes positivas por lo que $s_m = \ n, 1 \ = u_m$, por el teorema.13 tenemos que $u_m = (u_1)^m = \; c,d \; * \; c,d \; ^{m-1}$ y sea $\; a,b \; = \; c,d \; ^{m-1}$, por lo que se obtiene $\; n,1 \; = \; c,d \; * \; a,b \; = (ca + tdb, da + cb)$ y al igualar la segunda componente $da + cb = 1$ dado que d, a, c y b son positivos enteros nos es posible encontrar 4 números positivos que cumplan la siguiente igualdad $da + cb = 1$, asi que $\; n,1 \; = u_1$ en $\boldsymbol{P_t}$ siempre que t sea de la forma $n^2 + 1$ o $n^2 - 1$.

■

Con esto ya no es necesario hacer uso de algún programa ya que si t es el sucesor o antecesor de un número cuadrado inmediatamente se obtiene a u_1 que generará a $S_{t,1}$ y con esta sucesión es posible generar la SCU que mostrara cuales serán todas las unidades de P_t.

Como ya se demostró para los valores de t de la forma $n^2 \pm 1$, se continua con los valores de la forma $t \pm 2$, fíjese de la tabla 6 en los valores de $t = n^2 + 2$, se puede ver que $b_1 = n$ y $a_1 = n^2 + 1$ y cuando $t = n^2 - 2$ se tiene que $b_1 = n$ y $a_1 = n^2 - 1$, lo cual permite postular los siguientes teoremas.

Teorema 20. Dado un súper-conjunto $\boldsymbol{P_t}$ si t es de la forma $n^2 + 2$ o con $n \in \boldsymbol{Z}^+$, entoces, la primera unidad de componentes positivas es $u_1 = (n^2 + 1, n)$.

Demostración: se tiene el súper-conjunto $\boldsymbol{P_t}$ donde $t = n^2 + 2$ donde $n \in \boldsymbol{Z}^+$ el elemento $(n^2 + 1, n)$ es unidad ya que si $t = n^2 + 2$ se tiene que:

$$\begin{aligned}
n^2 + 1, n \quad &= \; (n^2 + 1)^2 - tn^2 \\
n^2 + 1, n \quad &= \; n^4 + 2n^2 + 1 - \; n^2 + 2 \; n^2 \\
n^2 + 1, n \quad &= \; n^4 + 2n^2 + 1 - (n^4 + 2n^2) \\
n^2 + 1, n \quad &= \; (n^4 - n^4) + (2n^2 - 2n^2) + 1 \\
n^2 + 1, n \quad &= \; 1 \; = 1
\end{aligned}$$

Mostrando que $(n^2 + 1, n)$ es unidad en $\boldsymbol{P_t}$

Ahora solo falta demostrar que es la primera unidad, suponga que la primera unidad es (c, d), esto significa que $\; c,d \; < \; n^2 + 1, n \;$ si (c, d) es la primera unidad significa que la sucesión $S_{t,1}$, debe generar a $\; n^2 + 1, n \;$ ahora se dirá que $\; n^2 + 1, n \;$ es la emésima unidad de componentes positivas por tanto $s_m = (n^2 + 1, n) = u_m$, por el teorema 13 se concluye que $u_m = (u_1)^m = \; c,d \; * \; c,d \; ^{m-1}$, sea $\; a,b \; = \; c,d \; ^{m-1}$,reemplazando se obtiene $n^2+1, n = c, d * a, b = (ca+tdb, da+cb)$ y al igualar la primera componente daría que $ca+tdb=n^2+1$, y recordando que $t=n^2+2$ se tiene que $ca+(n^2+2)db=n^2+1$ pero esto no puede ser cierto ya que $n^2+2>n^2+1$, teneindo en cuenta que a, b, c y d son enteros positivos, $n^2+2\ db>n^2+1$, $ca+\ n^2+2\ db>n^2+1$, lo cual es contradicción ya que no puede ser posible que $ca+\ n^2+2\ db>n^2+1$ y al mismo tiempo $ca+(n^2+2)db=n^2+1$, concluyendo así que en $\boldsymbol{P_t}$ si t es de la forma n^2+2 con n $\in \mathbf{Z}^+$, entoces, la primera unidad de componentes positivas es $u_1=(n^2+1, n)$.

■

Teorema 21. Dado un súper-conjunto $\boldsymbol{P_t}$ si t es de la forma n^2-2 o con $n\in \boldsymbol{Z}^+$ **y** $\boldsymbol{n>2}$**,** entonces, la primera unidad de componentes positivas es $u_1=(n^2-1, n)$.

Demostración: se tiene el súper-conjunto $\boldsymbol{P_t}$ donde $t=n^2-2$ donde $n\in \boldsymbol{Z}^+$ el elemento el elemento (n^2+1, n) es unidad ya que si $t=n^2-1$ tenemos que:

$$
\begin{aligned}
n^2-1, n &= (n^2-1)^2-tn^2 \\
n^2-1, n &= n^4-2n^2+1-\ n^2-2\ \ n^2 \\
n^2-1, n &= n^4-2n^2+1-(n^4-2n^2) \\
n^2-1, n &= (n^4-n^4)+(2n^2-2n^2)+1 \\
n^2-1, n &= 1\ =1
\end{aligned}
$$

Ahora solo falta demostrar que es la primera unidad, suponga que la primera unidad es (c, d), esto significa que $c, d\ <\ n^2-1, n$ si (c, d) es la primera unidad significa que la sucesión $S_{t,1}$, debe generar a n^2-1, n por tanto se dirá que n^2-1, n es la emésima unidad de componentes positivas concluyendo que, $s_m=(n^2-1, n)=u_m$, por el teorema 13 $u_m=(u_1)^m=\ c, d\ *\ c, d\ ^{m-1}$ y sea $a, b\ =\ c, d\ ^{m-1}$, por lo que $n^2-1, n\ =\ c, d\ *\ a, b\ =(ca+tdb, da+cb)$ y al igualar la primera componente daría que $ca+tdb=n^2-1$, y recordando que $t=n^2-2$ se tiene que $ca+\ n^2-2\ db=n^2-1$, pero esto no puede ser cierto ya que para que se cumpla esta igualdad debe ser solo si

$db = ca = 1$ dado que $n^2 - 2, n^2 - 1, a, b, c$ y d son enteros positivos y para que esto ocurra se tiene que dar a su vez que $a = b = c = d = 1$ y por los corolarios 5 y 6 esto no puede ser cierto a menos que $t = 2$, pero para que eso ocurra debe ser porque $n = 2$ y como $n > 2$ por el enunciado del teorema queda demostrando que dado un súper-conjunto $\boldsymbol{P_t}$ si t es de la forma $n^2 - 2$ o con $n \in \boldsymbol{Z^+}$ **y** $\boldsymbol{n > 2}$**,** entonces, la primera unidad de componentes positivas es $u_1 = (n^2 - 1, n)$.

■

Con los resultados anteriores se pensaría en buscar ahora regularidades cuando t es de la forma $n^2 \pm 3$ pero si observa la tabla 6 cuanto $t = 22$ y $t = 28$ ya no se cumplen las igualdades en las componentes de la primera unidad, así que se empieza a observar en la tabla 6 cuáles tienen en común la segunda unidad, aunque se ve que para varios valores de t la segunda componente es la misma, se comenzó con las que su segunda componente es igual a 2, a continuación las verá en una tabla.

$\boldsymbol{t}$	$\boldsymbol{a_1}$	$\boldsymbol{b_1}$
6	5	2
12	7	2
20	9	2
30	11	2
42	13	2

Tabla 7. Valores de t donde el valor de la segunda componente de la primera unidad es igual a 2.

Se sabe que el valor de t es siempre de la forma $n^2 + c$ así que se observa en la siguiente tabla los valores de t de la tabla 7 para ver si también podemos escribir a c de una forma general.

$\boldsymbol{t}$	$\boldsymbol{n^2 + c}$
6	$2^2 + 2$
12	$3^2 + 3$

20	$4^2 + 4$
30	$5^2 + 5$
42	$6^2 + 6$

Tabla 7. Valores de t escritos de la forma $n^2 + c$

Con la tabla 7 y 6 se concluyen dos cosas, la primera es que si en un conjunto $\boldsymbol{P_t}$ la segunda componente de u_1 es 2, entonces, t es de la forma $n^2 + n$ y la segunda conclusión es que si t es de la forma $n^2 + n$ entonces la primera componenete de u_1 es $2n + 1$, por estas conclusiones se propone el siguiente teorema.

Teorema 22. Dado un súper-conjunto $\boldsymbol{P_t}$ si t es de la forma $n^2 + n$ con n entero y mayor que 1, entonces, la primera unidad de componentes positivas es $u_1 = (2n + 1{,}2)$.

***Demostración*:** al igual que el teorema 23 lo primero es demostrar que $(2\mathrm{n} + 1{,}2)$ es una unidad, para ello no se necesita más que mostrar que su cuasinorma es igual a 1.

$$2\mathrm{n} + 1{,}2 \quad = \quad 2n + 1 \;\; ^2 - t \;\; 2 \;\; ^2$$

$$2\mathrm{n} + 1{,}2 \quad = |4n^2 + 4n + 1 - 4t|$$

Pero como $t = n^2 + n$

$$2\mathrm{n} + 1{,}2 \quad = |4n^2 + 4n + 1 - 4(n^2 + n)|$$

$$2\mathrm{n} + 1{,}2 \quad = |4n^2 + 4n + 1 - 4n^2 - 4n)|$$

$$2\mathrm{n} + 1{,}2 \quad = \quad 4n^2 - 4n^2 \;\; + \;\; 4n - 4n \;\; + 1$$

$$2\mathrm{n} + 1{,}2 \quad = |1\;| = 1$$

Por lo que queda demostrado que $(2n + 1{,}2)$ es unidad, ahora se demostrará que es la primera unidad, suponga que la primera unidad es (c, d), esto significa que $c, d \;<\; (2n + 1{,}2)$ si (c, d) es la primera unidad significa que la sucesión $S_{t,1}$, debe generar a $(2n + 1{,}2)$, ahora se dirá que $(2n + 1{,}2)$ es la emésima unidad de componentes positivas, por lo que $s_m = \;\; 2n + 1{,}2 \;\; = u_m$, por el teorema 13 tenemos que $u_m = (u_1)^m = \;\; c, d \;\; *$

$c,d^{\ m-1}$ y sea $a,b = c,d^{\ m-1}$, por lo que se tendría $2n+1,1 = c,d * a,b = (ca+tdb, da+cb)$ y al igualar la segunda componente daría que $da+cb=2$ y dado que d,a,c y b son positivos enteros la única manera para que se cumpla esta igualdad es que $a=b=c=d=1$ por lo que daria que la primera unidad es $(1,1)$ y por el corolario 5 y 6 esto ocurriría si solo si $t=2$, por lo que si t es mayor que 2 se llegaría a una contradicción, y como $n>1$ si $t=n^2+n$ entonces $t>2$.

Quedado así demostrado que dado un súper-conjunto $\mathbf{P_t}$ si t es de la forma n^2+n con n entero y mayor que 1, entonces, la primera unidad de componentes positivas es $u_1=(2n+1,2)$

■

Si se observa la tabla 6 también hay valores para t en los que la segunda componente de la primera unidad es 4, por lo que se supone que cuando t tiene valores mayores a 50 se espera que también para lagunas t existan $b_1=4$ y para tratar de generalizar valores $b_1=8$, 16 ,32 etc. por lo cual se plantea la siguiente sección.

9.3 Primera unidad de un súper-conjunto P_t donde $t=n^2+\frac{n}{2^q}$

Unos de los objetivos de este trabajo es mostrar cómo generar un sucesión S_t a partir del valor de t, el medio para conseguirlo ha sido para algunos valores de t encontrar la primera unidad a través de la visualización de patrones encontrados de la tabla 6 y posteriormente conjeturando y demostrando cuál sería la primera unidad para dichos casos, ya con la primera unidad se genera dicha S_t y con ella se generan todas las unidades como se mostró en la sección 7.1.

Cuando se propuso este trabajo de grado en el departamento se pretendía mostrar la solución del problema para los súper-conjuntos $\boldsymbol{P_t}$ tales que t fuera de la forma $n^2+\frac{n}{2^q}$ donde que q es un número natural, está será enunciada a continuación pero no se demostrará ya que más adelante se demostrará otro teorema en donde este caso es un caso particular, lo primero es mostrar que patrones fueron los encontrados y a que conclusión permitió llegar. Se puede decir que t siempre $n^2 < t < \ n + 1 \ ^2$ para algún n natural, en la tabla 6 se ve que siempre para algún t se tiene que $b_1 = 2$ y cuando esto ocurre es porque t es de la forma $n^2 + n$ y que $a_1 = 2n + 1$ como se demostró en el teorema 26, luego de esta conjetura, se puede ver que para algunos valores de t $b_1 = 4$ y cuando ocurre esto es por que $n^2 < t < n^2 + n$ y más exactamente cuando t es de la forma $n^2 + \frac{n}{2}$ en dicho caso se tiene que $u_1 = (4n + 1{,}4)$, y así teniendo la siguiente conjetura:

Conjetura 2. Dado un súper conjunto $\boldsymbol{P_t}$ si t es de la forma $n^2 + \frac{n}{2}$, entonces, su primera unidad será $u_1 = (4n + 1{,}4)$.

Dadas esta conjetura y el teorema y el teorema 26 se piensa en generalizar al observar el siguiente patrón:

$\boldsymbol{t}$ **en términos de un** $\boldsymbol{n}$ **natural**	$\boldsymbol{u_1 = (a_1, b_1)}$
$\boldsymbol{n^2 + n = n^2 + \frac{n}{2^0}}$	$u_1 = (2n + 1{,}2)$
$\boldsymbol{n^2 + \frac{n}{2} = n^2 + \frac{n}{2^1}}$	$u_1 = (4n + 1{,}4)$
$\boldsymbol{n^2 + \frac{n}{2^q}}$	$u_1 = (2^{q+1}\,n + 1, 2^{q+1})$

Tabla 8. Patrones de la conjetura 2 y el teorema 26.

Y teniendo así siempre que t sea de la forma $\boldsymbol{n^2 + \frac{n}{2^q}}$ se conjetura que la primera unidad será $u_1 = (2^{q+1}\,n + 1, 2^{q+1})$, pero como se mencionó se desarrollará esta demostración como un caso particular de un teorema que se encuentra en la siguiente sección.

9.4 Primera unidad de un súper-conjunto P_t donde $t = n^2 + c$

Nuevamente se va a escribir a t como un cuadrado más un número positivo $(n^2 + c)$ pero esta vez se tendrán más cosas en cuenta, por ejemplo, dado que siempre se cumple que $n^2 < t < \ n+1\ ^2$ significa que $c < (n+1)^2 - n^2$, $c < 2n+1$, ahora, de los resultados de la sección 7.3 se tiene que este $c = \frac{n}{2^p}$, es decir es un entero que se obtiene a partir de una división y el valor de b_1 es el valor del divisor.

Como $n^2 < t < \ n+1\ ^2$ significa que entre n^2 y $(n+1)^2$ hay $2n$ posibles valores para t ya que el primer valor valido para t es n^2+1 asi que los valores posibles para t deben ser $\ n+1\ ^2 - (n^2+1) = n^2 + 2n + 1 - n^2 - 1 = 2n$, llámese esta diferencia f, es decir, f es la cantidad de valores que puede tomar t entre cada dos números cuadrados consecutivos, ahora, siguiendo la hipótesis del párrafo como $t = n^2 + c$ si $c|f$ y sea d en el entero positivo tal que $cd = f$, entoces, $b_1 = d$, ahora siguiendo el mismo patrón de la sección anterior se concluye que $a = dn + 1$.

Teorema 23. Dado un súper-conjunto $\boldsymbol{P_t}$ donde t es de la forma $n^2 + c$ con $c > 1$ y sea $f = n^2(n+1)^2 - \ n^2 + 1\ = 2n$, si $c|f$, entonces, la primera unidad de $\boldsymbol{P_t}$ es $u_1 = (dn+1, d)$ donde d es un entero talque $cd = f$.

Demostración: ya que d y n son positivos $dn+1, d \in \boldsymbol{Z}$ y eso hace que $\ dn+1, d\ \in \boldsymbol{P_t}$**,** para demostrar que es una unidad se calculara el valor de su cuasinorma para ver si da 1:

$$dn+1, d \quad = \quad dn+1\ ^2 - td^2$$

$$dn+1, d \quad = |\ dn\ ^2 + 2dn + 1 - td^2|$$

Pero recuerdes que $t = n^2 + c$

$$dn+1, d \quad = \quad dn\ ^2 + 2dn + 1 - \ n^2 + c\ d^2$$

$$dn+1, d \quad = |\ dn\ ^2 + 2dn + 1 - (n^2d^2 + cd^2)|$$

Como $cd = f$, se tiene que $cd^2 = cdd = fd$

$$dn+1, d \quad = |\ dn\ ^2 + 2dn + 1 - (n^2d^2 + fd)|$$

Ahora $f = 2n$

$$dn+1, d \quad = |\ dn\ ^2 + 2dn + 1 - (n^2d^2 + 2nd)|$$

$$dn+1, d \quad = \quad dn\ ^2 + 2dn + 1 - \quad dn\ ^2 + 2nd$$

$$dn+1, d \quad = \ 1$$

Quedando así demostrado que $(dn+1,d)$ es unidad de p_t, ahora se demostrará que es la primera unidad, suponga que la primera unidad es (e,g), esto significa que $e,g \ < (dn+1,d)$si (e,g) es la primera unidad significa que la sucesión $S_{t,1}$, debe generar a $(dn+1,d)$, ahora, se dirá que $(dn+1,d)$ es la emésima unidad de componentes positivas, por lo que $s_m = (dn+1,d) = u_m$, por el teorema 13 $u_m = (u_1)^m = \ e,g \ * \ e,g \ ^{m-1}$ y sea $\ a,b \ = \ e,g \ ^{m-1}$, concluyendo que $(dn+1,d) = \ e,g \ * \ a,b \ = (ea+tgb, ga+eb)$ al igualar la primera componente daría $ea+tgb = dn+1$, y esto no puede ser cierta ya que:

$$dc = f = 2n$$

Y como se tiene que $c > 1$

$$dc = 2n$$

$$d \leq n$$

$$dn \leq n^2$$

$$dn + 1 < n^2 + c$$

Como $bg > 1$

$$dn + 1 < \ n^2 + c \ bg$$

$$dn + 1 < \ n^2 + c \ bg + ea$$

$t = n^2 + c$ por tanto $dn + 1 < tbg + ea$ y al mismo tiempo $ea + tgb = dn + 1$ llegando aquí a una contradicción, por tanto, queda demostrado que dado un súper-conjunto $\boldsymbol{P_t}$ donde t es de la forma $n^2 + c$ con $c > 1$ y sea $f = n^2(n+1)^2 - \ n^2 + 1 \ = 2n$, si $c|f$, entonces, la primera unidad de $\boldsymbol{P_t}$ es $u_1 = (dn+1,d)$ donde d es un entero talque $cd = f$.

■

Recordando las conjeturas 2 y el teorema 26 $c = \frac{n}{2^q}$, y si multiplicas por un 1 convenientemente se tiene $c = \frac{n}{2^q} \ 1 \ = \frac{n}{2^q} \ \frac{2}{2} \ = \frac{2n}{2^{q+1}} = \frac{f}{2^{q+1}}$ si $t = n^2 + \frac{f}{2^{q+1}}$ significa que $c \in \boldsymbol{Z}$ es decir que para estos casos $c|f$ donde $d = 2^{q+1}$ por ello este resulta ser un caso particular del teorema 27.

Pero ahora la falta mirar los casos en que $t = n^2 + c$ pero c no divide a f, fíjese de nuevo en la tabla 6, y se citará un caso particular en el que no ocurre esto, cuanto $t = 33$ este se puede escribir como $t = 5^2 + 8$ y en este caso $f = 10$, es evidente que 8 no divide a 10 pero observe que la componente b_1 cuando $t = 33$ es la misma b_1 cuando $t = 39$, y a_1 cuando $t = 33$ es $a_1 - 2$ del a_1 cuando $t = 39$, y al reescribir estos dos valores de t en términos de un cuadrado quedaría que $33 = 5^2 + 8$ y $39 = 6^2 + 3$, pero es posible reescribir a $33 = 6^2 - 3$; fíjese que cuando $t = 39 = 6^2 + 3$ en este caso $f = 12$ y como 3 divide a 12 cuando $t = 39$ el teorema 27 funciona, esto mismo que se acabó de mencionar ocurre por ejemplo cuando $t = 79$ y $t = 83$ sólo que para estos valores tan altos no hay una tabla para observar así que la comprobación queda como opción para el lector, al igual, lo importante de esto es que se concluye el siguiente teorema.

Teorema 24. Dado un conjunto $\boldsymbol{P_{t_1}}$ donde $t_1 = n^2 + c_1$ y c_1 no divide $f_1 = 2n$ si existe un $t_2 = \ n + 1 \ ^2 + c_2$ donde $c_2 | f_2$, $f_2 = 2n + 2$ y $t_1 = \ n + 1 \ ^2 - c_2$ entonces $(d \ n + m \ - 1, d)$ es unidad donde $dc_2 = f_2$

Demostración: Como d, n son enteros se tiene que $(d(n+1) - 1, d) \in \boldsymbol{P_t}$, ahora su cuasinorma es:

$$\mathrm{d \ n+1 \ -1, d} \quad = \quad d \ n+1 \ -1 \ ^2 - t_1 d^2$$

$$(\mathrm{d(n+1)-1, d}) \quad = | \ dn + d - 1 \ ^2 - t_1 d^2 |$$

$$(\mathrm{d(n+1)-1, d}) \quad = | \ dn \ ^2 + d^2 + 1 + 2d^2 n - 2d - 2dn - t_1 d^2 |$$

Como $t_1 = \ \mathrm{n+1} \ ^2 - \mathrm{c_2}$

$$(\mathrm{d(n+1)-1, d}) \quad = | \ dn \ ^2 + d^2 + 1 + 2d^2 n - 2d - 2dn - (\ \mathrm{n+1} \ ^2 - \mathrm{c_2}) d^2 |$$

$$(\mathrm{d(n+1)-1, d}) \quad = | \ dn \ ^2 + d^2 + 1 + 2d^2 n - 2d - 2dn - (n^2 + 2n + 1 - \mathrm{c_2}) d^2 |$$

$$(\mathrm{d(n+1)-1, d}) \quad = | d^2 n^2 + d^2 + 1 + 2d^2 n - 2d - 2dn - (n^2 d^2 + 2nd^2 + d^2 - \mathrm{c_2} d^2) |$$

$$(\mathrm{d(n+1)-1, d}) \quad = | 1 - 2d - 2dn + \mathrm{c_2} d^2) |$$

Y recordemos que $c_2 d^2 = c_2 dd = f_2 d$ y $f_2 = 2n + 2$ se tiene que $c_2 d^2 = \ 2n + 2 \ d$

$$(\mathrm{d(n+1)-1, d}) \quad = | 1 - 2d - 2dn + \ \ 2n + 2 \ d) |$$

$$(\mathrm{d(n+1)-1, d}) \quad = | 1 - 2d - 2dn + 2nd + 2d |$$

$$(\mathrm{d}(\mathrm{n}+1)-1,\mathrm{d}) \quad = \ 1 \ = 1$$

Quedando demostrado el teorema 28.

■

Para dejar un poco más claro el uso de los teoremas 27 y 28 se va a mostrar ejemplo para cada caso, piense en el súper-conjunto P_{84} y se va a encontrar la SCU para este caso, lo primero es hallar cuál es el número cuadrado más grande que a su vez es menor que 84 y el número cuadrado más pequeño mayor que 84, estos números son número es 81 y 100 respectivamente, dado esto se reescribe a 84 como $81+3$ que es igual a 9^2+3, como la idea es mostrar a t en términos de un n^2+c en este caso $n=9$ y $c=3$, lo siguiente es encontrar a f recordando que es la cantidad de valores que puede tomar t entre 81 y 100, $f=100-82=18$, como en este caso $c|f$ existe $d=6$ talque $cd=f$, como ya se conoce el valor d se puede concluir la primera unidad ya que $u_1=(dn+1,d)$, así que la primera unidad será $(6*9+1{,}6)=(55{,}6)$.

Y así es como se aplicó el teorema 27, al conocer la primera unidad de P_{84} se genera la matriz ligada a este súper-conjunto,$M_{84,1} = \begin{matrix} 55 & 84*6 \\ 6 & 55 \end{matrix} = \begin{matrix} 55 & 504 \\ 6 & 55 \end{matrix}$, y esta matriz describe la sucesión $S_{84,1}$:

$$s_0 = \ a_0, b_0 \ = (1{,}0)$$

$$s_n = (55a_{n-1}+504b_{n-1}, 6a_{n-1}+55b_{n-1})$$

La cual describirá todas las unidades de componentes positivas y para obtener absolutamente todas las unidades ya teniendo $S_{84,1}$, se recurre a la SCU resolviendo así el problema para este caso, ahora se mostrará el ejemplo de cómo usar teorema 28.

Para este ejemplo usaremos a P_{78} y si replica el proceso de escribirlo en términos de n y c se tiene que $t=78=8^2+14$ en este caso $f=16$ y es evidente que 14 no divide a 16, así que se busca un t_2 de la forma $\ n+1\ ^2+c$ tal que $\ n+1\ ^2-c=78$ y que para este si se pueda aplicar el teorema 27, en este caso si existe y es 84 ya que $84 = \ 8+1\ ^2+3$ y a su vez $\ 8+1\ ^2-3=79$ y dado el ejemplo anterior a P_{84} si se le puede aplicar el teorema 27, si por ello se puede hacer uso el teorema 28, concluyendo que la unidad de P_{79} es $u_1=(d\ n+1\ -1,d)$ teniendo en cuenta que $d=6$ y para este caso $n=8$ así que la primera unidad de P_{79} es $u_1 = \ 6\ \ 8+1\ \ -1{,}6\ \ = (53{,}6)$ y ya con la primera unidad se replica el proceso del ejemplo anterior para obtener todas las unidades.

Hasta ahora estos son los casos para los cuales se ha encontrado la solución al problema faltando los casos a los cuales no se les puede aplicar el teorema 27 ni 28, quedando así abierto parte del problema, pero generando muchas herramientas para poder continuar abordándolo, ya que cada vez se encontraban soluciones para más casos pero por cuestiones de tiempo no se ha culminado para todos los casos.

10 CONCLUSIONES

Dado el problema abordado en este documento, aunque este estaba enmarcado en el estudio de una estructura algebraica y la teoría de números, no fue posible solucionar el problema usando solo dicha teoría por lo cual fue necesario hacer uso de la teoría de conjuntos y como herramientas fuertes y fundamentales el orden lexicográfico, teoría de sucesiones y teoría de matrices cuadradas $2x2$, abordando y justificando como se relacionaban dichos conceptos entre ellos y con las extensiones cuadráticas estudiadas para el desarrollo del trabajo la programación fue una herramienta muy útil debido a que permitió la exploración y por ende la elaboración de conjeturas y así mismo la demostración de teoremas que se encontraron de una manera inductiva; partiendo de patrones encontrados y así concluir los teoremas a demostrar y la segunda fue para realizar las cuantas necesarias para generar las tablas que se usaron en el documento con el ánimo de facilitar la comprensión del lector.

El objetivo general del trabajo fue cumplido ya que eran encontrar las sucesiones de dos variables recurrentes que generaban las unidades para los p_t cuando el valor de t era de la forma $n^2 + \frac{n}{2^q}$, este se logró encontrando una forma para t más general donde el caso mencionado en el objetivo general resultaba ser una caso particular, no sobra decir que el trabajo deja valores de t en los cuales no se ha hallado la primera unidad pero se considera que deja un marco teórico suficiente para desarrollar el problema por completo, ya que a medida que se continuaba con la exploración se solucionaban más casos, pero por cuestiones de tiempo no se logró terminar todos los casos.

Hallazgos importantes en el desarrollo del trabajo fueron encontrar que todas las unidades de componentes positivas resultan ser potencia de una la primera unidad de componentes positivas usando el orden lexicográfico, y además, que la enésima potencia de dicha unidad resulta ser la enésima unidad de componentes positivas, que las matrices también pueden ser medio para hallar dichas unidades usando la multiplicación usual entre matices y gracias a ellos se pudo concluir que aunque hay n sucesiones que describen unidades de P_t solo existe una sucesión que describe todas las unidades y además, que esta se puede generar utilizando la primera unidad, y por ello parte fundamental del trabajo fue hallar un método para encontrar la primera unidad en algunos P_t.

11 Bibliografía

Fraleigh, J. (1988). *Álgebra abstracta.* Wilmington, Delaware, E.U.A.: ADDISON-WESLEY IBEROAMERICANA.

Luque, C., Torres, J., & Mora, L. (2006). *Estructuras análogas a los números reales.* Bogotá, Colombia: Nomos S.A.

Muñoz, J. (2002). *Introducción a la teoría de conjuntos.* Bogotá, Colombia: Panamericana, Formas e Imperesos S:A:.

Rubiano, G., Gordillo, J., & Luis, J. (2004). *Teoría de números [para principiantes]*. Bogotá, Colombia: Universidad Nacional de Colombia.

Jimenez, H. (2006). *ESTUDIO ALGEBRAICO DE LOS NÚMEROS DUALES(Tesis para obtener titulo de pregrado)* . Universidad Pedagógica Nacional de Colombia.Bogota, Colombia.

Takeuchi, Y. (1976). *Sucesiones* . Mexico: Editorial Limusa.

Zuckerman, H., & Nieven, I. (1976). *Introducción a la teoría de números.* Mexico: Limusa.

MEN, M. D. (2006). *Estándares básicos de competencias en Lenguaje , Matemáticas, Ciencias y Ciudadanas*. Bogotá. Recuperado de: http://www. mineducacion. gov. co/1621/articles- 340021_recurso.

12 ANEXOS

12.1 Código del programa “divisores unidades y sucesiones de P_t)

Este es el código del programa utilizado para realizar las cuentas mencionadas durante el desarrollo de este trabajo con el fin de realizar exploraciones y conjeturas de los súper-conjuntos $\boldsymbol{P_t}$, dicho programa fue desarrollado para el programa “Free Pascal”.

```
program divisoresunidadesysucesionesdeP_t;
uses crt  ;
var
,a,b,c,d,e,f,g,h,i,j,k,l,z,t,n:longint;
x,y:array[1..3] of longint;
procedure uno;
 begin
 clrscr;
writeln('ha seleccionado la opcion 1');
writeln('escriba el valor de t, para el s£perconjunto P_t');
readln(t);
clrscr;
writeln('ahora escriba los valores a y b del a+bk del que desea conocer los
divisores');
readln(a,b);
writeln('usted a seleccionado buscar los divisores del nuemro ',a,'+',b,'k en p_',t);
i:=0;
for j:= 1 to 1000 do
for k:=1 to 1000 do
begin
c:=a*a-t*b*b ;
d:=j*j-t*k*k;
```

```
if (c mod d)=0 then
writeln ('(',j,'+',k,'k)');
end;
readln();
readln();
  end ;
  procedure dos;
 begin  clrscr;
writeln('seleccion¢ la opcion para conocer las 3 primeras unidades de P_t');
writeln('diga el valor de t');
readln(t);n:=1;
for j:= 1 to 1000 do
for k:=1 to 1000 do
begin
d:=j*j-t*k*k;
if( (d=1) and (n<4)) then
begin
writeln ('u_',n,'(',j,'+',k,'k)');n:=n+1;end;
  end ;
  readln();
  end;
  procedure tres;
 begin
   clrscr;
writeln('seleccion¢ la opcion para conocer las 15 primeras unidades de P_t');
writeln('diga el valor de t');
readln(t);n:=1;
for j:= 1 to 10000 do
for k:=1 to 10000 do
```

```
begin
   d:=j*j-t*k*k;
if( ((d=1)or(d=-1)) and (n<15)) then
begin
writeln ('u_',n,'(',j,'+',k,'k)');n:=n+1;end;
  end ;
  readln();
  end  ;
  procedure cuatro;
 begin
writeln('ha seleccionado la opcion para conocer la susecion recurrente que describe todas las unidades, dijite el valor de t');
readln(t);n:=0;
for j:= 1 to 1000 do
for k:=1 to 1000 do
begin
d:=j*j-t*k*k;
if( ((d=1)or(d=-1)) and (n<1)) then
begin
writeln('la sucesion definida por recurrencia que determina todas las unidades es:');
writeln ('x_0=',j,',','x_1=',k*t,',y_0=',k,',y_1=',j);n:=n+1;end;



  end ;
  readln();
readln();
  end  ;
begin
```

```
writeln('bienvenido,dijite el n£mero de lo que decea hacer seguido de la tecla enter');
writeln('1:conocer los divisores un un n£mero de un conjunto P_t');
Writeln('2:conocer las primeras 3 unidades de un conjunto P_t');
writeln('3:conocer las primera 30 unidades de un conjunto P_t');
writeln('4:conocer la matriz liagada P_t que describe todas las unidades');
readln(z);
case z of
 1:uno;
 2:dos;
 3:tres;
 4:cuatro;
end;
end.
```