Sobre las ecuaciones Diofánticas

William Benedicto Sarmiento Rondón

Universidad Industrial de Santander

Facultad de Ciencias

Escuela de Matemáticas

Bucaramanga

2004

Sobre las ecuaciones Diofánticas

William Benedicto Sarmiento Rondón

Trabajo de grado para optar al título de
Licenciado en Matemáticas

Director
Edilberto José Reyes González
Magíster en Matemáticas

Universidad Industrial de Santander
Facultad de Ciencias
Escuela de Matemáticas
Bucaramanga
2004

TABLA DE CONTENIDO

LISTA DE FIGURAS Y CUADROS

Pág

RESUMEN

TÍTULO: SOBRE LAS ECUACIONES DIOFÁNTICAS*

AUTOR: WILLIAM BENEDICTO SARMIENTO RONDÓN**

Palabras Claves:

- Ecuación Diofántica.
- Análisis Diofántico.
- Diofanto de Alejandría.
- Ecuación de Pell.
- Ecuación Lineal.

Contenido:

EL análisis diofántico es una rama de las matemáticas que se dedica exclusivamente a encontrar soluciones enteras positivas a ecuaciones de diferentes grados y variables, que aparecen de forma natural o como planteamiento de problemas.

Se llama análisis diofántico debido a que fue el matemático griego Diofanto de Alejandría quién se caracterizó por plantear problemas cuyas soluciones fuesen enteras y positivas; tales resultados se encuentran recopilados en su obra llamada "La Aritmética". Entre las ecuaciones típicas se encuentran la ecuación diofántica lineal de dos o más variables, la ecuación pitágorica, la ecuación de Pell. Para obtener la solución a dichas ecuaciones no existen métodos únicos, y dependen en gran manera de la intuición del ser humano. En el caso de la ecuación lineal se emplea el algoritmo de Euclides con el fin de encontrar una combinación lineal del máximo común divisor de los coeficientes que al multiplicarla por un factor c determinado es una solución.

Ésta monografía se basa primero en mostrar el origen del análisis diofántico por medio de la vida y obra de Diofanto, segundo en solucionar las ecuaciones diofánticas típicas por varios métodos y por último solucionar una ecuación diofántioca especial que se refiere a números poligonales.

---

* Tesis.

** Facultad de Ciencias. Licenciatura en matemáticas. Edilberto José Reyes González.

ABSTRACT

TITLE: ABOUT OF DIOPHANTINE EQUATIONS. *

AUTHOR: WILLIAM BENEDICTO SARMIENTO RONDÓN. **

Key words:

- Diophantine equation.
- Diophantine Analysis.
- Diophantus of Alexandria
- Pell equation.
- Lineal equation.

CONTENTS:

The diophantine analysis is one of the mathematies branches concerns mainly in finding positive integers solutions to equations of different grades and variables, that appear in a natural form or as a mathematical expression.

Diophantine comes from the name of a Greek mathematician Diophantus who is known for stating problems in which the solutions would be positive integers. Those results could be find in a collection called "Aritmethies". In the typical equations it is possible to find the linear diophantine equation of one or more incognits, the Pythagorean equation and Pell's equation. To obtain a solution for those equations it do not exist just one method, it depends on the ability of human being. In the case of the equation lineal it is used the Euclidean Algorithm in orden to will obtain a lineal combination of the greatest commom divisor of the coefficients which when being multiply by a c determined fact give us a solution.

This monography is based mainly in showing the Diophantine Analysis taking into account the biography and works of the Greek mathematicies . Then we proposed solutions to diophantine typical equations using different methods and finely we will give a solution of a diophantine special equation that refers to a polygonal numbers.

---

* Thesis.

** Faculty of Sciences, mathematics licenciature. Edilberto José Reyes González.

INTRODUCCIÓN

El estudio de los problemas diofánticos es una de las ramas más antiguas de las matemáticas, ya que los enteros positivos se han usado durante mucho tiempo, más que cualquier otro sistema numérico. Tal rama recibe actualmente el nombre de análisis diofántico, la cual se dedica a la búsqueda de soluciones enteras positivas de ecuaciones que aparecen en forma natural o planteadas. Aunque Diofánto recibe la autoría de la primera investigación sistemática de dichas ecuaciones, resultados parciales han sido obtenidos por griegos mucho antes.

Diofanto en el siglo III D.C., propuso y resolvió muchos problemas indeterminados acerca de cantidades y combinaciones relacionadas con los lados, áreas, perímetros de triángulos rectángulos, entre otros. Aunque la mayoría de los problemas de este dominio pueden ser enunciados en lenguaje libre de tecnicismos matemáticos, su investigación requirió ayuda de matemáticas avanzadas. Una mera referencia de materias que se usan frecuentemente en el análisis diofántico son funciones elípticas y enteras, series y productos infinitos, números complejos y algebraicos, etc.
Tales tipos de problemas fueron recopilados por este matemático en su libro llamado Aritmética. Diofanto, más que un cultor de la aritmética, y sobre todo de la geometría, como lo fueron los científicos griegos, debe considerársele un precursor de álgebra, a tal punto que es llamado el padre de ésta. En la solución a sus problemas aplica ingeniosos métodos, métodos que son totalmente diferentes para cada problema.

En el estudio de los números poligonales se generan situaciones relacionadas con características propias, tales como saber cuando un número es triangular y a la vez piramidal, por decir algo. Tales situaciones

han dado origen al planteamiento de problemas que se reducen a resolver una ecuación diofántica, y por lo tanto se convierten en una aplicación y hacen parte del análisis diofántico.

Gracias a Diofanto se generó un estudio por la matemática de parte de otros matemáticos para dar soluciones a este tipo de ecuaciones que supuestamente eran fáciles. Entre estos personajes se encuentra Fermat quién modificó un problema del libro de Aritmética y generó una ecuación, que fue la frustración de muchos matemáticos, la cual es $x^n + y^n = z^n$.

En la presente monografía se muestra un poco del trabajo de Diofanto, y la solución de algunas ecuaciones clásicas y especiales.

1. BREVE RESEÑA HISTÓRICA DE DIOFANTO Y SU OBRA.

1.1 Diofanto de Alejandría.

Matemático de la época helénica que más que un cultor de la aritmética, y sobre todo de la geometría, como lo fueron los científicos griegos, debe considerársele un precursor del álgebra y, en cierto sentido, más vinculado con la aritmética de los pueblos orientales que con la de los pueblos griegos. El nombre de Diofanto de Alejandría es inmortalizado en la designación de ecuaciones indeterminadas y la teoría de la aproximación. Sin embargo esta atribución es cuestionada debido a que Diofanto no inventó las ecuaciones indeterminadas puesto que Pitágoras (VI A.C) había encontrado la solución $x = 2n + 1,\ \ y = 2n^2 + 2n,\ \ z = 2n^2 + 2n + 1$ con $n \in Z^+$, para la ecuación $x^2 + y^2 = z^2$, y además por la existencia de un sin número de problemas antiguos indeterminados que ya existían. Diofanto, además no consideró el tipo de problema más común (ecuación lineal) como prioridad para desarrollar su trabajo o mejor dicho para solucionar en los enteros.

Los escritos disponibles permiten conocer que él fue, el primero en introducir procesos algebraicos sistemáticos para la solución de ecuaciones no lineales indeterminadas y además fue el primero en introducir notaciones algebraicas concretas y extensas que representaron un gran avance sobre los estilos verbales de sus predecesores y muchos sus sucesores. El hallazgo del libro *Aritmética* por fuentes Bizantinas ayudó en gran parte al renacimiento de la matemática al oeste de Europa y estimuló a muchos matemáticos a su estudio, de los cuales el más destacado fue Fermat.

Muchos de los trabajos de Fermat son conocidos por sus notas hechas en el libro de Diofanto.

De Diofanto como individuo no tenemos mucha información. Un famoso problema de la antología griega indica que él murió a los 84 años de edad, pero en qué año y en qué siglo es desconocido, él menciona a Hicicles y es citado por Theon el padre de Hipatía. En la introducción del libro XIV, el llamado libro de Euclides, Hicicles coloca a Diofanto más o menos en la generación de Apolonio de Pérgamo del cual sí se sabe con precisión en qué tiempo vivió. Así podemos colocar a Hicicles a mediados del siglo segundo A.C con razonable precisión. Por otro lado, Theon presenció el eclipse en el año 364 D.C. Con esta brecha de 500 años, los historiadores están en libre disposición de colocar a Diofanto donde les convenga según sus teorías del desarrollo histórico. La mayoría sigue las bases de una dudosa referencia por el *Byzantine Psellus,* asignándolo al siglo III D.C. Es así que Diofanto de Alejandría, vivió una época difícil de precisar, pero que probablemente debe situarse en el siglo tercero después de Cristo.

1.2 La Aritmética.

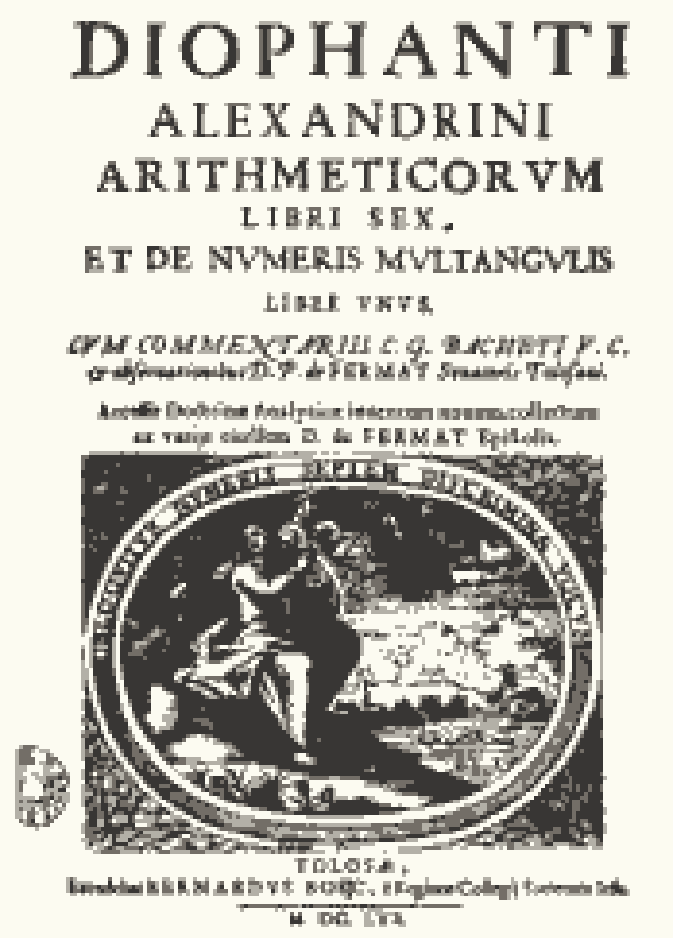
DIOPHANTI
ALEXANDRINI
ARITHMETICORVM
LIBRI SEX,
ET DE NVMERIS MVLTANGVLIS
LIBER VNVS.
CVM COMMENTARIIS C. G. BACHETI V. C.
& observationibus D. P. de FERMAT Senatoris Tolosani.
TOLOSÆ,

Figura 1. Carátula de la Aritmética de Diofanto.

El trabajo sobreviviente de Diofanto consiste en seis libros de la *Aritmética* y un fragmento *Sobre los números poligonales*. La introducción de la *Aritmética* promete trece libros de los cuales la posición y contenido de los siete libros perdidos es un misterio. Un libro corresponde a un pergamino que representa de *20* a *25* páginas ordinarias. Estos libros se pueden resumir así:

Libro I. Sistemas determinados de ecuaciones que involucran métodos lineales y cuadráticos.

Libros II-V. Ecuaciones y sistemas de ecuaciones, la mayoría de las cuales son indeterminaciones cuadráticas, aunque los libros IV y V contienen una selección de ecuaciones cúbicas determinadas e indeterminadas.
Libro VI. Ecuaciones que involucran triángulos rectos. [12]

La *Aritmética* es un libro interesante y original, que no contiene teoremas o proposiciones, sino problemas entre números abstractos, con excepción de los problemas del último libro, en el cual los datos y las incógnitas son elementos del triángulos rectángulos, y un problema con cantidades, único en toda la *Aritmética*, que trata de una compra de dos clases de vinos. Las características de esos problemas son:

1. Se trata de problemas, a veces determinados, pero la mayoría de los casos indeterminados, en los cuales las soluciones que Diofanto busca y encuentra son números racionales positivos (no enteros como la denominación actual del análisis diofántico).

2. En la solución de estos problemas se aplica cierto simbolismo bastante eficaz, semejante al nuestro, por lo menos en le tratamiento de los polinomios con una letra.

3. No aparece un orden, ni en lo que se refiere a la naturaleza de los problemas, ni en cuanto al método de resolución, aunque ellos pueden agruparse adoptando ciertos criterios de analogía.

Los métodos de la resolución aparecen diferentes en cada caso, pero la elección de estos métodos y los recursos auxiliares de los que Diofanto hecha mano, son tan ingeniosos y originales que confieren a este trabajo la fisonomía algebraica que lo caracteriza y distingue de los demás escritos

griegos. Esta habilidad e ingeniosidad se pone especialmente de manifiesto en los problemas de análisis indeterminado de primero, segundo y hasta de tercero y cuarto grados.

Esta habilidad no es casual; se funda sobre el conocimiento de una gran cantidad de propiedades aritméticas que los problemas de Diofanto revela; propiedades que no demuestra pero que aplica, por ejemplo el producto de dos números, cada uno de los cuales es una suma de dos cuadrados, puede expresarse de dos maneras distintas como suma de dos cuadrados; todo cubo puede expresarse como suma de tres cubos, etc. La demostración de la primera proposición es la siguiente:

Sea $a = x^2 + y^2,\ b = w^2 + z^2$ entonces

$$\begin{aligned} ab &= x^2w^2 + x^2z^2 + y^2w^2 + y^2z^2, \\ &= x^2w^2 + x^2z^2 + y^2w^2 + y^2z^2 - 2xywz + 2xywz, \\ &= (xw + yz)^2 + (xz - yw)^2 = (xw - yw)^2 + (xz + yz)^2. \end{aligned}$$

Por otro lado, el fragmento *Sobre los números poligonales* es un interesante escrito teórico sobre estos números, que encierran una importante generalización de la propiedad de los números triangulares de que si tomados ocho veces un número triangular y le sumamos la unidad se obtiene un número cuadrado. Diofanto demuestra que cualquier número poligonal de lado p, tomado tantas veces como indica el número $8(p - 2)$ y se le suma el cuadrado de $(p - 4)$, se obtiene un número cuadrado. El fragmento termina con el problema no resuelto de saber cuándo un número entero positivo es poligonal o no.

1.3 El epigrama de la antología griega.

Con el nombre Antología griega o Antología palatina (grupo de sabios de finales del siglo V o comienzos del siglo VI), se conoce una colección de

problemas de índole muy variado y que hoy se incluiría en la llamada matemática recreativa. En general, son problemas curiosos con enunciados pintorescos que se resuelven mediante simples raciocinios y a los sumo con ecuaciones de primer grado. La única excepción es precisamente un problema que figura en la *Aritmética* de Diofanto, único en el que Diofanto trata de cantidades y no de números racionales, ni de medidas, ni de elementos geométricos, que es un problema indeterminado de segundo grado. Este problema exige conocer las cantidades de dos vinos, cuyo costo es a *8* y *5* dracmas el congio respectivamente, tal que el valor sea un número cuadrado que sumado a *60* de el número total de congios al cuadrado. La solución que traen la *Antología* y Diofanto es *(59/12)* y *(79/12)* congios, respectivamente, cuya suma es *(23/2)* y cuyo cuadrado, disminuido de *60,* da el cuadrado de *(17/2); (289/4).* Haciendo la prueba de la respuesta se ve que cumple con las condiciones. El valor es

$$8\left(\frac{59}{12}\right)+5\left(\frac{79}{12}\right)=\frac{289}{4},\ \frac{289}{4}+60=\frac{529}{4}=\left(\frac{23}{2}\right)^2 \text{ y } \left(\frac{59}{12}\right)+\left(\frac{79}{12}\right)=\left(\frac{23}{2}\right).$$

El epigrama es un problema que se refiere a la edad en que Diofanto habría fallecido, pero es poco probable que ese epigrama tenga alguna finalidad informativa. El epigrama de la *Antología* que revela la edad en que murió Diofanto dice que éste transcurrió el sexto de su vida en la niñez, un doceavo en la adolescencia, y que después de transcurrir otro séptimo de su existencia se desposó, naciéndole un hijo después de cinco años de casado. Pero el hijo vivió la mitad de la vida del padre, y éste, afligido, buscó consuelo en la ciencia de los números y cuatro años después de la muerte del hijo, también falleció. Un cálculo simple da para la vida de Diofanto *84* años. Este cálculo se realizará más adelante. [8]

1.4 El simbolismo de Diofanto.

La notación numérica usada por Diofanto es por supuesto la notación helenística estándar la cual usa letras del alfabeto griego con tres letras arcaicas que sumadas dan *27* símbolos diferentes. Los primeros nueve símbolos para las unidades, los segundos para las decenas y los últimos para las centenas.

En el libro I de la *Aritmética* de Diofanto, se expone los signos (símbolos) que utilizará y sus reglas operatorias. Esos signos son: una letra para indicar la incógnita y también signos literales para indicar el cuadrado o el cubo de ella; para la cuarta, quinta y sexta potencia utilizaba oportunamente los dos signos anteriores; un signo especial agregado a los seis signos anteriores indicaba que se debía tomar la recíproca de esas seis potencias; un signo especial para indicar la sustracción y otro para la igualdad (la suma no tiene signo especial; los términos que se sumaban se escribían uno a continuación de otro). Las fracciones se representaron insertando la palabra "dividido por" entre expresiones numéricas en la misma línea. Los recíprocos de los enteros y las potencias negativas de la incógnita se designaron por un símbolo especial después del número o potencia.

Como la mayoría de los signos empleados por Diofanto (deformados, sin duda, por los copistas posteriores) parecen ser las iniciales de las palabras griegas para unidad, número, cuadrado, cubo, igual, etc., este simbolismo conduce a decir que si, con algún exceso de lenguaje, habláramos de un álgebra de Diofanto, deberíamos agregar que se trata de un "álgebra sincopada", es decir, en una etapa intermedia entre el álgebra retórica sin símbolos y el álgebra simbólica actual.

Por lo demás, el simbolismo de Diofanto es limitado, no dispone más que de una incógnita que obliga a ciertos recursos o artificios en el caso de tratarse de problemas de varias incógnitas, además sus potencias van, en lenguaje

moderno, desde el exponente -6 al exponente 6. Pero que a la final, le permite operar con potencias y polinomios. Estas operaciones incluyen las operaciones enteras con polinomios, combinadas con la transformación de las ecuaciones mediante el despeje de términos.

1.5 Los problemas de Diofanto.

En todos los problemas que resuelve, Diofanto adopta para las constantes valores numéricos particulares, pero el método que utiliza en general es independiente de esos valores. Claro que elige esos valores de manera que las soluciones sean posibles. Algunos ejemplos que se mostrarán más adelante darán idea del contenido y de los métodos de la *Aritmética* de Diofanto.

1. Problemas de primer grado con una incógnita.

El primer problema que trae la *Aritmética* es el de calcular dos números conociendo su suma y su diferencia. Si x es el menor, dice Diofanto, el mayor será $x + D$ (diferencia) y por tanto $x + x + D = S$ (suma), de donde

$$2x + D = S \quad \text{y} \quad 2x = S - D,$$

y los números serán

$$x = (S - D)/2, \qquad y = D + (S - D)/2.$$

Un problema interesante de la *Aritmética* de Diofanto es el siguiente: Dados dos números, buscar un tercero tal que los tres productos de cada uno de ellos por la suma de los otros dos, estén en progresión aritmética.

Diofanto plantea mediante desigualdades los tres casos que pueden presentarse y los resuelve. Considerando únicamente el caso en el que el producto del primer número dado, por la suma de los otros dos sea la media aritmética, es decir con símbolos actuales

$$2a(b + x) = (a + b)x + (a + x)b,$$

de donde,

$$x = (ab) / (2b - a).$$

Para que la solución sea positiva se debe cumplir que $2b > a$, y en efecto, los datos de Diofanto son $a = 5,\ b = 3$ y por consiguiente $x = 15$ tal que

$$60 = 3(5+15),\ 90 = 5(3+15),\ 120 = 15(3+5).$$

2. Sistemas lineales.

En los problemas que actualmente exigirían sistemas lineales para su solución, Diofanto los reduce, en general mediante la adecuada elección de una variable auxiliar. En otros problemas la elección es más acertada. Por ejemplo para calcular cuatro números, conociendo las cuatro diferencias entre la suma de tres de ellos y el cuarto, Diofanto toma como incógnita auxiliar la semisuma de los cuatro números, que se obtiene fácilmente de los datos mediante una ecuación de primer grado y con ella obtiene los cuatro números buscados. En efecto, si a, b, c, d son los datos y $x, y, z, u,$ los números buscados, es fácil ver que si v es la semisuma de éstos números entonces

$$x = v - (a/2),$$
$$y = v - (b/2),$$
$$z = v - (c/2),$$
$$u = v - (d/2),$$
$$2v = (v - a/2) + (v - b/2) + (v - c/2) + (v - d/2).$$

3. Ecuaciones de segundo grado.

En la solución aritmética de la ecuación de segundo grado, Diofanto completa los cuadrados y determina de ahí los valores de la incógnita. Veamos para ello la solución del problema de los vinos que lleva a un sistema indeterminado de segundo grado de la forma

$$8x + 5y = z^2;\ \ z^2 + 60 = (x + y)^2.$$

Diofanto empieza por tomar la suma $(x + y)$ como variable auxiliar, que lo lleva al nuevo sistema, haciendo $u = x + y$ tenemos

$$u^2 - 60 = 3x + 5u = 8u - 3y,$$

o a las inecuaciones

$$8u > u^2 - 60 > 5u.$$

Para resolver estas inecuaciones, primero deben resolverse las ecuaciones correspondientes, pero en este caso ambas tienen una sola raíz positiva. Diofanto llega a las mismas en la forma correspondiente $11 \leq u \leq 12$, pero como $u^2 - 60$ debe ser un cuadrado, Diofanto adopta como nueva incógnita un valor v tal que $u^2 - 60 = (u - v)^2$, de donde resultan las nuevas inecuaciones

$$22v \leq 60 + v^2 \leq 24v,$$

cuyas ecuaciones respectivas tienen ahora, en ambos casos, un par de raíces positivas.

Si Diofanto las hubiese tenido en consideración, había llegado a la limitación $3 \leq v \leq 21$, en cambio llega a $19 \leq v \leq 21$, que es la que se obtiene cuando de las dos raíces se toma únicamente la que corresponde al radical positivo. Diofanto en el problema toma $v = 20$, con lo cual $u = 23/2;\ x = 59/12;\ y = 79/12.$

También en el caso de sistemas de grado superior al primero busca y encuentra variables auxiliares adecuadas. Así en el problema de encontrar tres números x, y, z tales que se conocen los productos a, b, c de cada uno de ellos por la suma de los otros dos

$$x(y + z) = a;\quad y\,(z + x) = b;\quad z(x + y) = c,$$

adopta como nuevas incógnitas $u = xz,\ v = yz$ tal que se reduce a calcular dos números dadas la suma y la diferencia

$$u + v = c,\quad u - v = a - b,$$

y de ahí fácilmente los valores de los números buscados son

$$x^2v = u\,(a-u);\;\; y^2u = v\,(a-u);\;\; z^2(a-u) = uv.$$

Los problemas de Diofanto son formulados en términos de número pero el "número" siempre es positivo racional. Las soluciones son trabajadas en términos de ejemplos numéricos particulares. Las proposiciones generales no son enunciadas aún cuando la solución lo implica. Las restricciones a la elección de valores iniciales no son siempre dadas. La conclusión más razonable es que Diofanto no conocía como restringir o no como expresar los números que satisfacen la restricción.

Al igual que los babilonios, Diofanto no tenía inconvenientes para sumar áreas y longitudes, aunque para ser preciso, adicionaba el "número en el área" y "el número en la longitud". Su técnica en el álgebra es supremamente avanzada más allá de cualquier cosa que posean los babilonios, pues las ecuaciones cúbicas complicadas y de grado más alto no estaban aún sugeridas en el álgebra de Babilónica.

Aún en el caso cuadrático hay una buena diferencia. Cuando una ecuación cuadrática es solucionada, Diofanto hace el mayor esfuerzo para seleccionar la variable de tal forma que resulte una ecuación binomial; pero si esto no se realizara, entonces se usa la fórmula general cuadrática

Es inútil intentar adivinar que parte de los problemas avanzados y métodos son propios de Diofanto. La mayoría de los historiadores modernos postulan una continua tradición de los métodos algebraico orientales en la matemática griega, de una repentina invasión en el periodo romano; si esto es así, los textos y problemas dados debería ciertamente haber existido. Es probable que la *Aritmética* fuera una gran compilación de tal calidad que los predecesores no la tuvieron en estima. Hay rastros de la notación diofántica en otra parte por ejemplo, Heron (*60* D.C) usó el signo menos; pero ninguna evidencia existe que la notación semi-algebraica de los métodos generales permitidos fueran usados antes de la publicación de la *Aritmética*.

Para resumir, la aproximación básica algebraica de Diofanto es babilónica. La generalidad y la abstracción es griega. El trabajo puede ser visto como un episodio en la declinación de la matemática griega o como el más fino florecimiento del álgebra babilónica.

4. Sistemas indeterminados.

En la solución de estos sistemas es donde Diofanto muestra su habilidad "algebraica". Para las ecuaciones indeterminadas de primer grado Diofanto no muestra mayor dificultad, pues siendo los coeficientes racionales encuentra una solución de las tantas que existen o determina la que corresponde a un valor específico de una de las incógnitas. Pero en los sistemas de grado superior al primero, esto no puede hacerse y es necesario recurrir a soluciones especiales.

En algunos casos Diofanto habla de "expresión general"; por ejemplo, cuando se trata de encontrar dos números tales que su producto más (o menos) la suma, sea un número dado. Esa expresión general en esencia equivale a que si $xy \pm (x + y) = a,$ entonces $(x \pm 1)(y \pm 1) = a + 1,$ de manera que fijando uno de los factores se puede determinar el otro. Dada la naturaleza de las soluciones de Diofanto, es evidente que el problema consiste siempre en tratar de reducir las ecuaciones de grado superior a lineales, cosa que logra mediante adecuadas elecciones de variables auxiliares. Así, en los siguientes problemas indicamos a la derecha la sustitución adecuada:

- $x^2 + y^2 = a^2 + b^2;\ x = zu - a;\ y = zv - b.$
- $x^2 - y^2 = d;\ x = y + z.$

En algunos casos la solución es realmente genial. Así por ejemplo, en el caso de determinar cuatro números tales que sumando a cada uno de ellos el cuadrado de la suma se obtenga otro cuadrado. Para esto se aplica la propiedad de los triángulos rectángulos la cual dice: que el cuadrado de la

hipotenusa más cuatro veces el área, igual a un cuadrado (de la suma de los catetos); e identidades entre suma de cuadrados para tener cuatro triángulos rectángulos de igual hipotenusa. En efecto, de dos triángulos rectángulos de catetos $b,c;\ b',c'$ e hipotenusas a,a' respectivamente, se obtienen los cuatros triángulos rectángulos de catetos $ba',\ ca';\ b'a,\ c'a;\ bb'+cc',\ bc'-b'c$ y $bb'-cc',\ bc'+b'c$ todos de hipotenusa aa'. Aplicando la propiedad antes mencionada de los triángulos rectángulos, se obtienen cuatro números que sumados a un mismo cuadrado dan siempre cuadrados. Para satisfacer la condición del problema (el mismo cuadrado debe tener por base la suma de los cuatro números) basta introducir un factor indeterminado que se deduce imponiendo esa condición.

El último libro de *Aritmética*, con excepción del último problema, que es el de las dos clases de vino, está dedicado íntegramente a problemas de triángulos rectángulos de lados racionales, de ahí que todos esos problemas se resuelvan con sistemas de ecuaciones, una de las cuales es la pitagórica. Para resolverlos, o bien elige los números indeterminados que aparecen en la solución de la pitagórica de manera que satisfagan las condiciones del problema dado, o bien, por tanteos, busca un triángulo semejante al dado que cumpla con las condiciones del problema, y luego encuentra el factor de proporcionalidad.

Por ejemplo, determinar los lados de un triángulo rectángulo tal que el área más un cateto sea un cubo y su perímetro de un cuadrado. La solución parte de la solución de la ecuación pitagórica

$$x = (2u + 1) / (u + 1),\ y = 2u,\ z = (2u\,(u + 1) + 1) / (u + 1),$$

con u racional, de acuerdo a las condiciones del problema tenemos que

$$xy/2 + x = 2u + 1 = a^3, \qquad x + y + z = 2(2u + 1) = b^3,$$

obligando que $b^2 = 2a^3$ para $a = 2v^2$ y $b = 4v^3$, de donde $2u + 1 = 8v^6$ y la solución del problema es

$$x = 16\, v^6/(8\, v^6 + 1);\quad y = 8\, v^6 - 1;\quad z = ((8v^6 - 1)\,(8v^6 + 1) + 2) / (8v^6 + 1).$$

La solución de Diofanto es el triángulo de lados $16/9,\ 7$ y $65/9$, cuya área más un cateto es $72/9$ y cuyo perímetro es $\left(\frac{12}{3}\right)^2$ cuando $v = 1$.

Observemos el siguiente problema.

Determinar un triángulo rectángulo en el que el área más un cateto sea una cantidad dada (que Diofanto hace igual a 7). En este problema Diofanto adopta como una solución opcional un triángulo semejante a un triángulo dado, es decir, hace $x = bx_1,\ y = by_1,\ z = bz_1$, tal que $b \in Z$, y x_1, y_1, z_1 son valores que satisfacen a la ecuación pitagórica. Aplicando ésta solución provisoria a la condición del problema $a = xy/2 + x = (1/2)\, b^2 x_1 y_1 + bx_1$, y multiplicando por el coeficiente del cuadrado de b y completando el cuadrado, se llega a que

$$(\,(1/2)b\, x_1 y_1 + 1/2\ x_1)^{\,2} = (1/2)\, a\, x_1 y_1 + (1/4) x_1^2.$$

Si el segundo miembro fuese un cuadrado el problema estaría resuelto, pero con los valores adoptados no; luego, diríamos, que el triángulo buscado no es semejante al de lados x_1, y_1, z_1. [8]

5. Problemas indeterminados.

El problema 9 del libro II dice: Si $n = a^2 + b^2$, encontrar otras representaciones de n tal que sea la suma de dos cuadrados.

Primeros hacemos $a = (x + a)$ y $b = (\,rx - b)$, x es la incógnita y a, b, r son valores específicos dados, como $n = a^2 + b^2$ entonces

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

$$n = (r^2 + 1)x^2 + (2a - 2br)x + a^2 + b^2.$$

Por lo tanto $x = (2br - 2a)/(r^2 + 1)$ donde r puede ser cualquier racional tal que los valores pedidos sean positivos. La selección de $rx - b$ en vez de $b - rx$ fue dictada solamente para valores numéricos seleccionados de $b - rx$ que resulten ser negativos. Por ejemplo sea $13 = 2^2 + 3^2$, entonces busquemos otra forma de expresar 13 como la suma de dos cuadrados. De acuerdo a lo anterior $a = 2$, $b = 3$ y sea $r = 2$ entonces $x = \left(\frac{2*3*2-2*2}{4+1}\right) = \frac{8}{5}$ y por lo tanto

$13 = 2^2 + 3^2 = \left(\frac{8}{5} + 2\right)^2 + \left(2*\frac{8}{5} - 3\right)^2 = \left(\frac{18}{5}\right)^2 + \left(\frac{1}{5}\right)^2$ cuya suma es 13.

Euler escribió el planteamiento del problema como

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

la cual muestra la solución más apropiada, pero esta solución es extraña y bastante general. Aquí habría una oportunidad perfecta para enunciar una proposición en lugar de un problema. Y sería la siguiente: "Cualquier número que se pueda expresar como la suma de dos cuadrados, puede ser representado de infinitas de formas".

El problema 6 del libro III dice: Encontrar tres números tales que su suma sea un cuadrado y además que la suma de cualquiera dos de ellos sea un cuadrado, es decir

$$x + y + z = t^2,$$
$$x + y = u^2,$$
$$y + z = v^2,$$
$$x + z = w^2.$$

Aquí Diofanto asigna un valor fijo a w, que en notación moderna le permite jugar el papel de parámetro. Selecciona una incógnita r tal que

$$t = r + 1,\ u = r,\ v = r - 1,$$

entonces reemplazando obtenemos que

$$z = 2r + 1, \quad y = r^2 - 4r, \quad x = 4r, \quad w^2 = 6r + 1.$$

Por lo tanto $r = (w^2 - 1)/6$ donde w es un racional arbitrario mayor que 5 para que y sea positivo. Luego

$$x = (2w^2 - 2)/3, \; y = (w^2 - 1)(w^2 - 25)/36, \; z = (w^2 + 2)/3.$$

Este problema es seleccionado para ilustrar que Diofanto no estaba interesado en generalizar excepto como un algo inesperado. Una muestra del avance considerable en la generalidad puede ser obtenido del reemplazo por ejemplo de $r \pm 1$ por $r \pm s$; en un problema cualquiera.

Este problema es claramente equivalente a la ecuación $u^2 + v^2 + w^2 = 2t^2$, pues $x + y + y + z + x + z = u^2 + v^2 + w^2 = t^2 + t^2 = 2t^2$.

Usando métodos poco conocidos por Diofanto, que probablemente eran complicados en su notación se obtiene una solución mucho más general de la ecuación como se muestra en el sistema

$$(u, v, w, t) = ((w^2 - 1)/6, (w^2 - 7)/6, w, (w^2 + 5)/6).$$

Para obtener esta solución partimos de la solución dada por Euclides a la ecuación pitagórica la cual es $x = 2mn, y = m^2 - n^2, z = m^2 + n^2$.

Como $(x + y)^2 + (x - y)^2 = 2z^2$, y haciendo $p = x + y, q = x - y, z = k$ tenemos que $p = 2mn + m^2 - n^2, q = 2mn - m^2 + n^2, k = m^2 + n^2$ y por lo tanto $r = 2m + 2n$. Entonces la solución a la ecuación $u^2 + v^2 + w^2 = 2t^2$, es:

$$(u, v, w, t) = (s^2 + n^2 - 2mn - m^2, \; s^2 - n^2 - 2mn + m^2, \; 2s(n + m), \; s^2 + n^2 m^2).$$

La solución previa es obtenida escogiendo $m = 2, \; n = 1$ y dividiendo por 6.

El problema 24 del libro IV dice: Encontrar una solución de $x^4 + y^4 + z^4 = t^2$.

Sea $t^2 = (x^2 - m)^2$ y $x^2 = (m^2 - y^4 - z^4)/2m$. Entonces se debe encontrar un entero m tal que $(m^2 - y^4 - z^4)/2m$ sea un cuadrado. Si hacemos $m = y^2 + z^2$ entonces $x^2 = y^2 z^2 / (y^2 + z^2)$. Por lo tanto $y^2 + z^2$ debe ser un cuadrado digamos $(y + r)^2 = y^2$. Entonces igualando

$$y^2 + z^2 = (y + r)^2,$$

de donde

$$y = (z^2 - r^2)/2r,$$

y por lo tanto haciendo los reemplazos tenemos

$$(x, y, z, t) = ((z^3 - r^2z)/(z^2 + r^2),\ (z^2 - r^2)/2r,\ z,\ (z^8 + 14z^4r^4 + r^8)/(4r^2(z^2 + r^2)^2)),$$

es la solución del problema para $z,\ r \in Z$. Este ejemplo se ha seleccionado por dos razones.

La primera es de gran interés histórico. En este problema Fermat añadió lo siguiente "¿Por qué Diofanto no se preguntó si la suma de dos bicuadrados sería un cuadrado? De veras es imposible ..." Más tarde Euler conjeturó que también era imposible encontrar tres potencias cuartas tales que su suma no es una potencia cuarta. Pero este enunciado es falso puesto que Naom Elkies en *1988* encontró el siguiente contraejemplo:

$$2682440^4 + 15365639^4 + 18796760^4 = 20615673^4.$$

Segundo, el problema indica lo que sucede cuando la notación es insuficiente. Primero se selecciona a x como la incógnita $x;$ y m, y, z como parámetros. Pero, para obtener la solución completa el autor toma un subproblema en el cual y es la incógnita y entonces ésta deja de ser parámetro.

Miremos el siguiente problema: Encontrar un triángulo rectángulo tal que su área sumada a uno de sus catetos es un cuadrado, mientras que a su perímetro es un cubo.

Tenemos el triángulo de la forma $a = 2x+1,\ b = 2x^2 + 2x,\ c = 2x^2 + 2x + 1.$ El perímetro es $4x^2 + 6x + 2 = (4x + 2)(x + 1).$ Como es difícil pasar de un cuadrado a un cubo; consideremos de nuevo el triángulo

$$a_1 = (2x + 1)/(x + 1),\ b_1 = 2x,\ c_1 = (2x^2 + 2x + 1)/(x + 1),$$

obtenido al dividir por $(x + 1).$

El perímetro es de $4x+2$ y el área $(2x^2 + x)/(x + 1)$. Luego sumando el valor del área al cateto $(2x + 1)/(x + 1)$, tenemos $2x + 1$. Por lo tanto $4x + 2$ debe ser un cubo y $2x + 1$ un cuadrado. El valor obvio para $2x + 1$ es 4. Por lo tanto $x = 3/2$ y el triángulo es $8/5, 3, 17/5$ catetos e hipotenusa respectivamente. [12].

1.6 Un problema de aproximación.

En el problema 9 del libro V se necesita encontrar dos cuadrados mayores que 6, cuya suma sea 13.

En el primer problema de los problemas indeterminados se da un método general para descomponer un número dado en dos cuadrados cuando la partición es dada. Partiendo de que $13 = 2^2 + 3^2$ y escogiendo un r adecuado obtenemos los números con las condiciones pedidas. En este caso sería $r = 10$ y los números $\left(\frac{258}{101}\right)^2 + \left(\frac{275}{101}\right)^2 = 13$.

Por supuesto que Diofanto no podría haber hecho esto sin tener unos datos iniciales. Primero encuentra un número ligeramente más grande que $\sqrt{13/2}$, como $13/2 = 26/4$ escribe la siguiente desigualdad $2\sqrt{13/2} = \sqrt{26} < 5 + 1/x$, tal que $x^2 < 10x + 1$. En este caso toma $x = 10$ y obtiene una aproximación $\sqrt{13/2} \approx 51/20$. Luego $51/20 = 3 - 9/20 = 20 + 11/20$, y por lo tanto vemos que encuentra un número con una aproximación de $1/20$ tal que

$$(3 - 9y)^2 + (2 + 11y)^2 = 13.$$

Luego cuando $y = 5/101$ los cuadrados son precisamente los mencionados arriba. [12].

1.7 La vida de Diofanto.

La historia ha conservado pocos rasgos biográficos de Diofanto, notable matemático de la antigüedad. Lo que se conoce de él con respecto a su edad ha sido tomado de la dedicatoria que figura en su sepulcro, inscripción compuesta en forma de ejercicio matemático. El epitafio y su planteamiento se muestran en el siguiente cuadro:

En la lengua vernácula	En el idioma del álgebra:
¡Caminante! Aquí fueron sepultados los restos de Diofanto. Y los números pueden mostrar, ¡oh, milagro!, cuán larga fue su vida,	X
Cuya sexta parte constituyó su hermosa infancia.	$X / 6$
Había transcurrido además una duodécima parte de su vida, cuando de vello cubrióse su barbilla	$X / 12$
Y la séptima parte de su existencia transcurrió en un matrimonio estéril.	$X / 7$
Pasó un quinquenio más y le hizo dichoso el nacimiento de su precioso primogénito,	5
que entregó su cuerpo, su hermosa existencia, a la tierra, que duró tan sólo la mitad de la de su padre	$X / 2$
Y con profunda pena descendió a la sepultura, habiendo sobrevivido cuatro años al deceso de su hijo	4

Cuadro 1. Tabla de planteamiento del epitafio de Diofanto

En sí consiste resolver la siguiente ecuación

$$x / 6 + x / 12 + x / 7 + 5 + x / 2 + 4 = x.$$

Cuya solución es $x = 84$, y nos permite saber que Diofanto se casó a los 21 años, fue padre a los 38, perdió a su hijo a los 80 y murió a los 84 entre otros. [8].

1.8 Transmisión de Diofanto.

Cuando los árabes recorrieron al suroeste del Mediterráneo en el siglo VII, tomaron posesión de los manuscritos y trabajos relacionados con el álgebra, los cuales habían sido publicados en ediciones suficientemente grandes para que sobrevivieran a las guerras que sucedieron antes de la caída del imperio romano. Entre estos estaba la *Aritmética* o al menos una parte de ella. Las primeras traducciones y comentarios fueron publicados en árabe pero de estos no se conoce documento alguno, los únicos rastros están en las referencias de los bibliógrafos. Cuando los árabes formularon su propia álgebra aparentemente apelaron la tradición básica oriental. Los comienzos de una notación algebraica y de números abstractos no se ven por ningún lado. Además ningún problema de la *Aritmética* ha sido encontrado en el álgebra de Al-khwarizmi o hasta donde es conocido en cualquier otro texto de álgebra oriental. Probablemente los árabes encontraron a Diofanto poco práctico para sus matemáticas utilizadas; los hindúes lo vieron alguna vez en su *Aritmética* pero no se interesaron por su contenido pues no estaban estudiando temas relacionados con la teoría de problemas.

En otro lugar del conocimiento Bizantino, los manuscritos de Diofanto permanecieron casi intactos por más de ocho siglos. No conocemos cuando los libros faltantes fueron perdidos, pero la parte que existe escapó al saqueo de Constantinopla por los Cruzados en el año 1204 y posteriormente en el mismo siglo M. Planudes y G. Pachymeres escribían comentarios sobre la primera parte de la Aritmética.

En el periodo de la emigración de los sabios bizantinos, durante las conquistas turcas, las copias fueron enviadas a Italia entre los años *1461* y *1464*.

La primera traducción al latín fue hecha por W. Holzmann quién escribió bajo la versión griega de nombre X'ylander. Esta traducción fue publicada en el año *1575*. Mientras tanto Bombelli, en *1572* publicó cuatro libros de álgebra con problemas entre ellos algunos de su autoría.

Bachet, quién tomo prestado libremente a Bombelli y Holzmann hizo otra traducción en el año *1621* y publicó una segunda edición fue publicada en *1670* que incluía notas marginales de Fermat. En los siglos XVIII y XIX varias traducciones fueros hechas a todos los idiomas, basadas en las primeras ediciones mencionadas por Bachet y Holzmann. Finalmente en *1890* P. Tannery preparó un edición definitiva al texto griego.

Muchos de los problemas que resolvió Diofanto se originaron en la teoría de números y su propósito fue buscar soluciones enteras para las ecuaciones que generaban tales problemas.

Actualmente se llaman Ecuaciones Diofánticas a las ecuaciones con coeficientes enteros cuyas soluciones se buscan en el conjunto de los enteros positivos, y la parte de la teoría de números dedicada a tales ecuaciones se llama Análisis Diofántico. [12].

2. SOLUCIÓN DE ALGUNAS ECUACIONES DIOFÁNTICAS CLÁSICAS.

En este capitulo daremos las soluciones a tres tipos de ecuaciones diofánticas clásicas bien conocidas y otras que no lo son:

* La ecuación diofántica lineal.
* La ecuación de Pell.
* El triángulo pitágorico o la ecuación $x^2 + y^2 = z^2$

Empezaremos por estudiar la ecuación lineal y su generalización para n variables. Luego la ecuación $x^2 - dy^2 = 1$, llamada ecuación de Pell desde el siglo XVII, pero que sería más adecuado llamarla ecuación de Fermat, pues éste si contribuyó a su solución. Después estudiaremos la ecuación Pitagórica o $x^2 + y^2 = z^2$ cuya solución conocida desde la época griega pues, éstos se interesaron en encontrar triángulos rectángulos con catetos enteros; cada triángulo o mejor cada tripla de enteros (a, b, c) es llamada tripla pitagórica. Por último presentaremos la solución de algunos problemas curiosos y un pequeño comentario de el último teorema de Fermat.

2.1 La ecuación Diofántica Lineal.

Primero conozcamos que un problema se llama problema diofántico si se resuelve para enteros. En particular una ecuación de la forma $ax + by = c$ con $a,\ b \neq 0$ se llama ecuación lineal diofántica con dos variables si se resuelve para enteros.

Por ejemplo la ecuación $x + y = 1$ tiene infinitas soluciones enteras, mientras que la ecuación $6x + 8y = 7$ no tiene soluciones. Más adelante sabremos por qué estas afirmaciones.

Del curso de introducción a la teoría de números conocemos las condiciones y métodos para dar solución a este tipo de ecuación.

En esta sección presentaremos los teoremas necesarios para resolver tales ecuaciones, en algunos casos sin su demostración.

Sea la ecuación lineal

$$ax + by = c, \qquad (2.1)$$

entonces podemos enunciar los siguientes teoremas.

Teorema 2.1. La ecuación (2.1) tiene solución sí y solo sí $(a, b)|c$.

Demostración

i) Sea $d = (a, b)$ y supongamos que $d|c$ entonces existe un entero k tal que $c = kd$. Como d es una suma de múltiplos de a y de b, entonces $am + bn = d$. Esta combinación existe gracias al algoritmo de Euclides, cuya demostración se va hacer más adelante.

Multiplicando la última ecuación por k tenemos que $amk + bnk = c = dk$ y por lo tanto $x = mk$ y $y = nk$ es una solución.

ii) Supongamos que x_0 , y_0 es una solución de la ecuación.

Luego $ax_0 + by_0 = c$. Como $d|a$ y $d|b$ entonces $d|c$. De *i*) de *ii)* tenemos la demostración. ■ [10].

Teorema 2.2. Si $(a, b) = d$ en la ecuación (2.1) entonces existe una combinación lineal tal que

$$am + bn = d. \qquad m, n \in \mathbb{Z}. \qquad (2.2)$$

Demostración.

Supongamos que $a>b$ entonces por el algoritmo de la división tenemos que

$$a = bq_1 + r_1 , \qquad 0 < r_1 < b.$$

Si $r_1 = 0$ entonces b divide a y $(a, b) = b$. Si no, aplicamos nuevamente el algoritmo para obtener

$$b = r_1 q_2 + r_2, \qquad 0 < r_2 < r_1.$$

Si $r_2 = 0$ entonces $r_1 = (r_1, b) = (a, b)$. Si no, repetimos el proceso hasta llegar a lo sumo en b pasos, a un residuo cero; obteniendo las siguientes ecuaciones:

$$
\begin{aligned}
a &= bq_1 + r_1 && 0 < r_1 < b,\\
b &= r_1 q_2 + r_2 && 0 < r_2 < r_1,\\
r &= r_2 q_3 + r_3 && 0 < r_3 < r_2,\\
&\ldots\ldots\\
&\ldots\ldots\\
r_{k-3} &= r_{k-2} q_{k-3} + r_{k-1} && 0 < r_{k-1} < r_{k-2},\\
r_{k-2} &= r_{k-1} q_k + r_k && 0 < r_k < r_{k-1},\\
r_{k-1} &= r_k q_{k+1} + 0.
\end{aligned}
$$

EL M.C.D es el penúltimo residuo de todas las ecuaciones es decir r_k, el cual se puede expresar como combinación lineal de a y b por medio del reemplazo de cada una de los r_i y así se muestra que existen $m, n \in Z$ tal que $am + bn = d = r_k$, pues los r_i son enteros ■ [3].

Observemos que la prueba del teorema provee un método práctico para obtener la solución de la ecuación *(2.1),* pues se puede obtener una combinación lineal de $(a, b) = d$ y luego multiplicarla por el cociente de dividir c por d.

Ejemplo.

Resolver la ecuación diofántica

$$109x + 89y = 1$$

Solución:

Como $a = 109$ y $b = 89$, entonces aplicando el algoritmo tenemos

$$109 = 89*1 + \underline{20}$$

$$89 = \underline{20}*4 + \underline{9}$$

$$\underline{20} = \underline{9}*2 + \underline{2}$$
$$\underline{9} = \underline{2}*4 + \underline{1}$$

Los residuos son subrayados para no confundir los posibles reemplazos.

Para obtener la combinación empezamos por escribir

$$1 = \underline{9} - 4*\underline{2},$$

y sustituyendo de la tercera división

$$\underline{2} = \underline{20} - 2*\underline{9},$$

obtenemos

$$1 = 9*\underline{9} - 4*\underline{20},$$

ahora sustituyendo

$$\underline{9} = \underline{89} - 4*\underline{20},$$

de la segunda relación, obtenemos

$$1 = 9*\underline{89} - 40*\underline{20},$$

en el último paso usamos la primera división y escribimos

$$\underline{20} = \underline{109} - 89,$$

y así hemos llegado a la combinación

$$1 = 49*\underline{89} - 40*\underline{109} = 109*(-4)+89*\underline{(49),}$$

y por lo tanto una solución de la ecuación sería $x = -40 \;\; y = 49.$ [7].

El procedimiento que damos a continuación , conocido como el algoritmo extendido de Euclides, se puede programar fácilmente y permite hallar el M.C.D. de dos números a, b y escribirlo como combinación lineal de ellos.

Sea $(a, b) = d$ y supongamos que $0 < b < a$ entonces.

$$a = bq_1 + r_1 \qquad 0 < r_1 < b,$$
$$b = r_1 q_2 + r_2 \qquad 0 < r_2 < r_1,$$
$$r = r_2 q_3 + r_3 \qquad 0 < r_3 < r_2,$$
$$\ldots$$
$$\ldots$$
$$r_{k-3} = r_{k-2} q_{k-3} + r_{k-1} \qquad 0 < r_{k-1} < r_{k-2},$$

$$r_{k-2} = r_{k-1}\, q_k + r_k \qquad 0 < r_k < r_{k-1},$$

$$r_{k-1} = r_k\, q_{k+1} + 0.$$

Definimos $x_0=0,\ x_1=1,\ y_0=1,\ y_1 = -q_1$ y las fórmulas de recurrencia

$$x_i = x_{i-2} - x_{i-1}\, q_i\,,$$

$$y_i = y_{i-2} - y_{i-1}\, q.$$

Para $i = 2,3,\ldots,k.$

Por el algoritmo euclideano sabemos que $(a,b) = r_k$ y afirmamos que

$$r_k = a\, x_k + b\, y_k. \qquad x_k\,,\ y_k \in Z.$$

Teorema 2.3. Si $(a, b) = d$ y si x_0, y_0 es una solución de la ecuación *(2.1)* entonces la solución general es:

$$x = x_0 + \frac{kb}{d}, \quad y = y_0 - \frac{ka}{d} \quad k \in Z.$$

Demostración.

Sabemos que si k es un entero entonces $x_0 + \frac{kb}{d}\,,\ y_0 - \frac{ka}{d}$ es también una solución; solo resta mostrar que todas las soluciones son de esta forma.

Sea x_1, y_1 una solución de *(2.1)* entonces

$$ax_1 + by_1 = c = ax_0 + by_0\,,$$

$$a(x_1 - x_0) = -b(y_1 - y_0).$$

Como $(a, b) = d$, existe primos relativos a', b' tal que $a = da'\,,\ b = db'$, y reemplazando en lo anterior y dividiendo por d tenemos

$$a'(x_1 - x_0) = -b'(y_1 - y_0),$$

por lo tanto $b' | a'(x_1 - x_0)$ y como $(a', b') = 1$, tenemos que $b' | (x_1 - x_0)$ y entonces $x_1 - x_0 = kb'$ con $k \in Z$. Sustituyendo $(x_1 - x_0)$ en lo anterior tenemos $y_1 - y_0 = -ka'$ y por lo tanto

$$x_1 = x_0 + kb' = x_0 + \frac{kb}{d},$$

$$y_1 = \quad y_0 + \quad ka' = \mathrm{y}_0 - \frac{ka}{d},$$

ya que $x_1,\ y_1$ son soluciones al azar. ■ [10].

Es decir, si $x_0\ y\ y_0$ es una solución particular de *(2.1)* tenemos que

$$ax_0 + by_0 = c, \qquad (2.3)$$

entonces para hallar la solución general de x y y, restamos *(2.3)* de *(2.1)* y obtenemos

$$a(x - x_0) + b(y - y_0) = 0\ ,$$

la cual se puede escribir como

$$a(x - x_0) = -b(y - y_0). \qquad (2.4)$$

Esta ecuación muestra que el producto de a y $x - x_0$ es divisible por b de lo cual concluimos que

$$x - x_0 = \quad tb,$$

donde t es cualquier entero.

Cuando esto se sustituye en *(2.4)*, obtenemos

$$y - y_0 = -ta,$$

de lo cual concluimos que la solución general es

$$x = x_0 + tb\ , \qquad y = y_0 - ta\ , \qquad t \in \mathrm{Z}.$$

2.1.1 Método de Euler

Este método involucra un método simple que se repite varias veces. El proceso es fácil de aplicar, requiere un poco de división y las propiedades de los enteros bajo la suma y la resta.

Este proceso es más corto que el algoritmo de Euclides, en particular con ecuaciones de más de dos variables. [10].

Ejemplo

Resolver la siguiente ecuación diofántica

$$738x + 621y = 45$$

Solución:

La ecuación tiene solución pues el M.C.D $(728, 621) = 9$ y 9 divide 45.

Empecemos por despejar y,

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

como x, y deben ser enteros entonces $\frac{-117x + 45}{621} = t$, $t \in Z$. Luego

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

Haciendo lo mismo con x tenemos

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

ahora despejamos t tenemos

$t = \frac{-117u + 45}{36} = -3u + 1 + \frac{-9u + 9}{36} = -3u + 1 + v$, donde $v = \frac{-9u + 9}{36}$, $v \in Z$ y por lo tanto $u = -4v + 1$. Una solución podría ser cuando $v = 0$, y por consiguiente $u = 1, t = -2,$ de donde $x = 11, y = -13$ es una solución.

La solución general esta dada por

$$u = -4v + 1 \qquad t = -3u + 1 + v = 13v - 2$$
$$x = -5t + u = -69v + 11 \qquad y = -x + t = 82v - 13 \qquad t, u, v \in Z.$$

2.1.2 Método de fracciones continuas.

La ecuación (2.1) la podemos escribir de la siguiente manera

$$a'x + b'y = c'$$

donde $a = a'd, b = b'd, c = c'd, d = (a, b)$. A partir de esta ecuación podemos aplicar el método. Primero debemos encontrar la fracción continua $\frac{a'}{b'}$, con

$(a', b') = 1$. Como $\frac{a'}{b'}$, es racional, el último convergente C_n de la fracción continua simple finita que representa a $\frac{a'}{b'}$, es igual a $C_n = \frac{p_n}{q_n} = \frac{a'}{b'}$.

Si $(a, b) = 1$ entonces $p_n = a'$ y $q_n = b'$.

Por teoría de fracciones continuas tenemos $p_n q_{n-1} - p_{n-1} q_n = (-1)^n$ y por lo tanto $a' q_{n-1} - p_{n-1} b' = (-1)^n$. Multiplicando ambos miembros por $(-1)^n c' d$ obtenemos

$$da'((-1)^n c' q_{n-1}) + db'(-(-1)^n c' p_{n-1}) = dc' .$$

Por consiguiente una solución particular x_0 y y_0 de la ecuación diofántica lineal esta dada por

$$x_0 = (-1)^n c' q_{n-1} , \qquad y_0 = -(-1)^n c' p_{n-1} .$$

Y la solución general es:

$$x = x_0 + bt , \qquad y = y_0 - at , \qquad t \in \mathrm{Z} .$$

Como lo hemos dicho anteriormente. [10].

Ejemplo.

Resolver la ecuación diofántica lineal

$$18x + 5y = 7.$$

Solución:

Como $(18, 5) = 1$, entonces existen soluciones de la ecuación. La fracción continua de $\frac{18}{5}$ es $[3, 1, 1, 2]$ y por medio del siguiente cuadro se muestran los convergentes respectivos.

i	***-1***	***0***	***1***	***2***	***3***	***4***
a_i			3	1	1	2
p_i	0	1	3	4	7	18
q_i	1	0	1	1	2	5

Cuadro 2. Tabla de la solución de $18x + 5x = 7$

Donde $p_{-1} = 0,\ p_0 = 1,\ q_{-1} = 1, q_0 = 0, p_1 = a_1.$

Los convergentes correspondientes son $C_1 = 3,\ C_2 = 4,\ C_3 = 7/2,\ C_4 = 18/5.$

Así $p_4 = 18,\ q_4 = 5,\ p_3 = 7, q_3 = 2$. Como $n = 4$ entonces

$$p_4 q_3 - p_3 q_4 = (-1)^4$$

$$18q_3 - 5\, p_3 = 1$$

$$18q_3 + 5(-\, p_3) = 1$$

$$18(7q_3) + 5(-7\, p_3) = 7$$

$$18(14) + 5(-\, 49) = 7$$

Por lo tanto $x = 14$ y $y = -49$ es una solución particular y por lo tanto la solución general es $x = 14 + 5t\ \ y = -49 - 18t.$

2.1.3 Ecuaciones Diofánticas lineales con *n* incógnitas.

El método básico para tratar ecuaciones con n incógnitas es bastante parecido al método utilizado cuando es una ecuación de dos incógnitas. Para varias incógnitas nosotros formularemos el siguiente teorema.

Teorema 2.4. La ecuación $a_1x_1 + \ldots + a_nx_n = c$ tiene solución si y sólo si el M.C.D. de los a_i divida a c.

Demostración.

Sea $d = (a_1, a_2, \ldots a_n)$ el M.C.D de todos los números a_i, y supongamos que d divide a c, entonces existe un entero k tal que $c = kd$. Como d es una combinación lineal de de los a_i, entonces $a_1m_1 + \ldots + a_nm_n = d,\ m_i \in \mathbb{Z}$. Esta combinación existe gracias a algoritmo de Euclides. Multiplicando esta ecuación por k tenemos $a_1m_1k + \ldots + a_nm_nk = dk,$ y por lo tanto $x_i = m_ik$ es una solución para la ecuación. cada término y también a c pues la ecuación tiene solución. Por otra parte, supongamos que $x_1, x_2, x_3, \ldots x_n$ es una solución de la ecuación. Entonces $a_1x_1 + \ldots + a_nx_n = c$. Como d divide a_i entonces d divide a c. De esta manera tenemos la demostración.■ [7].

La existencia de la combinación lineal de d que nombramos anteriormente existe debido a el siguiente teorema.

Teorema 2.5. Si $a_1, a_2, \ldots, a_n$ es un conjunto de enteros con máximo común divisor, $d = (a_1, a_2, \ldots, a_n)$ entonces existen enteros $x_1, x_2, \ldots, x_n \in Z$ tal que

$$a_1x_1 + a_2x_2 + \ldots + a_nx_n = d.$$

Demostración.

La demostración se hará por inducción matemática. Para esto necesitamos observar que el resultado es verdadero para cuando $n = 1$, entonces $d = a_1$ y $x_1 = 1$. Si $n = 2$ es verdadero como se demostró anteriormente. La inducción consiste en suponer que el teorema es verdadero cuando existe $n - 1$ números a_i y luego para n números. Supongamos que

$$d_{n-1} = (a_1, \ldots, a_{n-1}),$$

el M.C.D. de $n - 1$ primeros números. De acuerdo a la condición podemos encontrar $n - 1$ números

$$y_1, y_2, \ldots, y_{n-1},$$

tal que

$$a_1y_1 + a_2y_2 + \ldots + a_{n-1}y_{n-1} = d_{n-1}.$$

Pero por propiedades de M.C.D. se tiene que si d es el M.C.D de los a_i es también el M.C.D de d_{n-1} y a_n

$$d = (d_{n-1}, a_n).$$

Esto significa que uno puede encontrar dos enteros t y x_n tal que

$$d_{n-1}\, t + a_nx_n = d,$$

y al reemplazar d_{n-1} obtenemos

$$a_1y_1\, t + \ldots + a_{n-1}y_{n-1}\, t + a_nx_n = d,$$

y esto es exactamente lo que buscamos haciendo

$$x_1 = y_1 t, \qquad x_2 = y_2 t, \quad \ldots \quad , \quad x_{n-1} = y_{n-1} t,$$

y de esta manera se concluye la prueba.■ [7].

Ejemplo.

Resolver la ecuación diofántica $100x_1 + 72x_2 + 90x_3 = 2.$

Solución:

Como $a_1 = 100,\ a_2 = 72,\ a_3 = 90$, y $(100, 72, 90) = 2 = d.$ Debemos encontrar x_1, x_2, x_3 enteros tal que

$$100x_1 + 72x_2 + 90x_3 = 2.$$

El $(100, 72) = 4 = d'.$ Por lo tanto debemos resolver la ecuación

$$100y_1 + 72y_2 = 4,$$

ó

$$25y_1 + 18y_2 = 1.$$

Por el método usual se encuentra que $y_1 = -5$ $y_2 = 7$ es una solución. Nuestro próximo paso para la solución es encontrar t, x_3 tal que

$$4t + 90x_3 = 2,$$

ó

$$2t + 45x_3 = 1.$$

Claramente una solución sería $x_3 = 1,\ t = -22$. Multiplicando y_1 y y_2 por -22 obtenemos una solución de la ecuación

$$x_1 = 110, \qquad x_2 = -154, \qquad x_3 = 1.$$

Otro ejemplo.

Hallar la solución general de la ecuación diofántica

$$100x_1 + 72x_2 + 90x_3 = 6.$$

Solución:

Cuando existe sólo dos incógnitas es bastante fácil derivar la solución general en cuanto se conocen una solución particular del conjunto de valores que satisfacen la ecuación.

Para varias incógnitas, la situación es más complicada. El método de más apropiado para encontrar la solución general es el siguiente:

Si dividimos la ecuación por *2* tenemos que

$$50x_1 + 36x_2 + 45x_3 = 3.$$

Y despejando

$$x_2 = \frac{3 - 50x_1 - 45x_3}{36} = -x_1 - x_3 + \frac{3 - 14x_1 - 9x_3}{36},$$

donde

$$t = \frac{3 - 14x_1 - 9x_3}{36},$$

debe ser un entero. Ahora despejando x_3 tenemos

$$x_3 = -4t - 2x_1 + \frac{(3 + 4x_1)}{9}.$$

Y por lo tanto

$$u = \frac{(3 + 4x_1)}{9},$$

debe ser un entero y despejando

$$x_1 = 2u + (u-3)/4.$$

Esto da finalmente que

$$v = \frac{(u - 3)}{4},$$

es un entero y $u = 4v+3$. Cuando sustituimos $u = 4v+3$ tenemos la solución general en términos de v.

$$x_1 = 9v + 6,$$

$$x_2 = 5t + 5v + 3,$$

$$x_3 = -4t - 14v - 9,$$

donde v, t son enteros arbitrarios.

2.1.4 Un método alternativo para la solución de esta ecuación.

Sea la ecuación

$$ax + by + cz = w, \qquad (2.5).$$

En este método de solución el algoritmo no es bastante claro, pero su efectividad es rápida. La idea fundamental es la siguiente: Supongamos que M.C.D de $(a, b, c) = 1$, entonces si podemos encontrar d, e, f, g, h, i enteros tales que el determinante

$$\begin{vmatrix} a & b & c \\ d & e & f \\ g & h & i \end{vmatrix} = 1$$

Formamos las ecuaciones

$$ax + by + cz = x',$$
$$dx + ey + fz = y',$$
$$gx + hy + iz = z'.$$

Como el determinante de los coeficientes es 1, las ecuaciones pueden resolverse para los enteros x, y, z en términos de x', y', z'. Haciendo $x' = d'$ y considerando a y', z' como parámetros, tenemos una solución general. La dificultad principal es encontrar el segundo y tercer renglón del determinante.

Sea $g' = (a, b)$ y $as - br = g'$. Como $(a, b, c) = 1$ implica que $(g', c) = 1$ y que existan enteros u, v tales que $g'u - cv = 1$. Por tanto hacemos el determinante de la siguiente

$$\begin{vmatrix} a & b & c \\ r & s & 0 \\ av/g' & bv/g' & u \end{vmatrix}.$$

El cual tiene por valor *1*, como lo podemos ver en el siguiente cálculo $c\left(\frac{rbv}{g'}-\frac{sav}{g'}\right)+u(as-rb)=cv\left(\frac{rb-sa}{g'}\right)+u(as-rb)=-cv+g'u=1.$ [1].

Ejemplo.

Resolver la ecuación diofántica

$$8x + 10y + 3z = 34.$$

Solución:

Note que $g' = (8, 10) = 2$ y $s = -1, r = -1$ es una solución de $8s - 10r = 2$, mientras que $u = 2, v = 1$ es una solución de $2u - 3v = 1.$ Por lo tanto, tenemos las ecuaciones

$$\begin{aligned} 8x + 10y + 3z &= x', \\ -x - y \quad\quad &= y', \\ 4x + 5y + 2z &= z'. \end{aligned}$$

Resolviendo en términos de x, y, z obtenemos las ecuaciones

$$\begin{aligned} x &= -2x' - 5y' + 3z', \\ y &= 2x' + 4y' - 3z', \\ z &= -x' + 2z', \end{aligned}$$

y haciendo $x' = 34$, tenemos la solución general en términos de los parámetros $y', z'.$

2.2. El triángulo pitagórico o la ecuación diofántica $x^2 + y^2 = z^2.$

Entre las tantas escuelas griegas de matemáticas y filosofía más viejas y venerables se encuentra la Pitagórica. Pitágoras nació alrededor del año *570* A.C., en la isla de Samos, se dice que viajó ampliamente y después instaló su escuela en Crotona al sureste de Italia, pero el fin no es hablar de quien era Pitágoras sino del teorema que afirma que en un triángulo rectángulo, el cuadrado de la hipotenusa es igual a la suma de los cuadrados de cada uno de sus catetos es decir

$$a^2 + b^2 = c^2, \qquad (2.6)$$

donde a, b son los catetos del triángulo y c es la hipotenusa.

Este resultado fue conocido con toda seguridad por los pitagóricos y ellos obtuvieron una demostración satisfactoria.

Una de las soluciones más conocidas del teorema ocurre cuando los lados del triángulo son

$$a = 3, \ b = 4, \ c = 5,$$

puesto que

$$3^2 + 4^2 = 5^2.$$

En los trabajos de la cultura China e Indú se encuentran otras soluciones por ejemplo

$$a = 5, \quad b = 12, \quad c = 13,$$
$$a = 8, \quad b = 15, \quad c = 17.$$

El pitagorismo considera al número como elemento primordial para el principio de todas las cosas o mejor dicho la omnipotencia y omnipresencia de este elemento en todo. Por esta causa se preocuparon por investigar las matemáticas y por resolver esta ecuación de manera general.

Una fórmula que genera soluciones para tal ecuación, la cual se atribuyó a Pitágoras es la siguiente:

$$a = 2n + 1, \qquad b = 2n^2 + 2n, \qquad c = 2n^2 + 2n + 1, \qquad (2.7)$$

donde n es un entero.

Se puede verificar que los valores de *(2.7)* satisfacen la ecuación. Por ejemplo para $n = 1, 2, 3$ tenemos las siguientes soluciones respectivamente

$$(3, 4, 5), \quad (5, 12, 13), \quad (7, 24, 25).$$

En la solución que Pitágoras muestra, podemos ver que tiene una propiedad especial, la cual es que la hipotenusa es una unidad más larga que uno de sus catetos.

También se les atribuye a los pitagóricos una solución particular dada por

$$x = \frac{n^2 - 1}{2},\ y = n,\ z = \frac{n^2 + 1}{2},$$

n impar. Es probable que ésta solución fuera deducida de la propiedad de que todo número cuadrado es la suma de n primeros números impares consecutivos, de modo que la diferencia entre dos cuadrados consecutivos es un número impar cuadrado.

La primera solución general del problema pitagórico es encontrada en el libro diez de los elementos de Euclides. Esta solución es

$$x = mn,\ y = \frac{m^2 - n^2}{2},\ z = \frac{m^2 + n^2}{2}, \qquad m, n \in \mathrm{Z}$$

Con $n = 1$ tenemos la solución anterior (Pitágoras).

Miremos ahora como podemos llegar a la solución general de la ecuación en enteros positivos.

La restricción de los enteros no es importante, si se encuentra una solución racional uno podría escribir los tres números con un común denominador

$$a = \frac{a_1}{m}, \qquad b = \frac{b_1}{m}, \qquad c = \frac{c_1}{m},$$

y se tiene que

$$a_1^2 + b_1^2 = c_1^2,$$

es una solución.

Primero se encuentra una solución entera primitiva de la ecuación, es decir, una solución en la cual no existe un factor común de a, b, c y además para cualquier par de los números a, b, c se tiene que son primos relativos.

Por ejemplo si a y b tienen a e como factor común, se cumple que e^2 divide a c^2, luego entonces c es divisible por e, contrario a la idea de que sea una solución primitiva.

El próximo paso es ver que en una solución primitiva a, b, c los números a, b no pueden ser ambos impares. Esta es una consecuencia del teorema de que todo número cuadrado es congruente con 0 o 1 módulo 4. Por lo tanto si ambos son impares se tendría que c^2 es congruente con $2 \pmod 4$, luego a, b no pueden ser ambos impares.

Supongamos ahora que a es par, entonces b y c son impares puesto que no tienen factores en común. Luego la ecuación *(2.6)* se podría escribir como

$$a^2 = c^2 - b^2 = (c - b)(c + b).$$

De acuerdo a lo anterior ambos miembros son divisibles por 4 y tenemos que

$$\left(\frac{a}{2}\right)^2 = \frac{c+b}{2} \bullet \frac{c-b}{2}. \qquad (2.7)$$

Aquí vemos que los dos factores enteros de la derecha son primos relativos, es decir no hay un factor común d que divida tanto la suma como la diferencia, además

$$\frac{c+b}{2} + \frac{(c-b)}{2} = c,$$

$$\frac{c+b}{2} - \frac{(c-b)}{2} = b,$$

y como b, c son primos relativos, se tiene que $d = 1$.

Cuando los dos números de la derecha *(2.7)* son primos relativos estos factores primos son diferentes, y entonces el producto no puede ser un cuadrado, a menos que cada uno de ellos sea un cuadrado.

Podemos, por lo tanto hacer

$$\frac{c+b}{2} = u^2, \quad \frac{c-b}{2} = v^2,$$

y sustituyendo en *(2.7)* tenemos

$$a = 2uv, \quad b = u^2 - v^2, \quad c = u^2 + v^2. \qquad (2.8)$$

Para asegurar que esta solución es primitiva, debemos observar que cualquier factor común de b y c debe dividir la suma y la diferencia de estos números. Pero como

$$c + b = 2u^2 , \quad c - b = 2v^2,$$

y como u, v son primos relativos, el único posible factor común es 2. Este factor se excluye cuando uno de los números u, v es par y el otro impar.

De la solución general primitiva *(2.8),* donde u y v son enteros sujetos a condiciones ya mencionadas, uno puede encontrar las soluciones de la ecuación por multiplicación de un entero cualquiera.

La solución general racional es obtenida por multiplicación de *(2.8)* por un número racional. Poco después, por medio de un problema Diofanto optó por buscar una solución general racional con fórmulas un poco diferentes a la obtenida. Al dividir la solución general *(2.8)* por v^2 obtenemos

$$a/v^2 = 2u/v, \quad b/v^2 = (u/v)^2 - 1, \quad c/v^2 = (u/v)^2 + 1.$$

Por lo tanto a partir de la solución *(2.8)* existe una solución racional

$$a_1 = 2t, \qquad b_1 = t^2 - 1, \qquad c_1 = t^2 + 1,$$

donde $t = u/v$. Cuando estos valores son multiplicados por algún número racional, obtenemos la solución general

$$a_0 = 2tr, \qquad b_0 = (t^2 - 1)r, \qquad c_0 = (t^2 + 1)r, \qquad (2.9)$$

donde r y t son racionales arbitrarios. [7].

Algunas de las soluciones enteras primitivas más pequeñas puede ser obtenida de *(2.8)* y se muestran en la siguiente tabla

u ***v***	***A***	***B***	***C***
u = 2 v = 1	*4*	*3*	*5*
u = 3 v = 2	*12*	*5*	*13*
u = 4 v = 1	*8*	*15*	*17*
u = 4 v = 3	*24*	*7*	*25*

Cuadro *3*. Tabla de soluciones de *(2.1)* por medio de *(2.8)*

Extensas tablas de triángulos pitagóricos enteros han sido calculadas.

Por ejemplo A. Martín da todos los triángulos primitivos para los cuales la hipotenusa es menor que 3000.

Existe un gran número de cuestiones que pueden ser preguntadas en consideración con los triángulos pitagóricos y que por siglos han sido la fuente de muchos problemas.

Por medio de las soluciones de la ecuación pitagórica se ha dado respuesta a problemas tales como:

1. ¿Cuándo la diferencia de la hipotenusa y uno de sus catetos es igual a uno?

Primero, no se puede tener que

$$c - b = 1,$$

puesto que cuando los valores de (2.8) son sustituidos en (2.6) se encuentra que la ecuación

$$2v^2 = 1,$$

no tiene solución en los enteros.

La otra posibilidad es que

$$c - a = 1,$$

y por lo tanto

$$u^2 + v^2 - 2uv = (u - v)^2 = 1,$$

de donde $u = v + 1$. Cuando esto es sustituido en (2.8) obtenemos

$$a = 2v^2 + 2v, \qquad b = 2v + 1, \qquad c = 2v^2 + 2v + 1,$$

que es la solución pitagórica.

2.2.1 El inradio de las triplas pitagóricas.

Consideremos las triplas (x, y, z) tal que $x^2 + y^2 = z^2;\ x, y, z \in \mathbf{Z}^+$ y sea r el radio del círculo inscrito en tal triángulo rectángulo, a cual llamaremos "inradio"

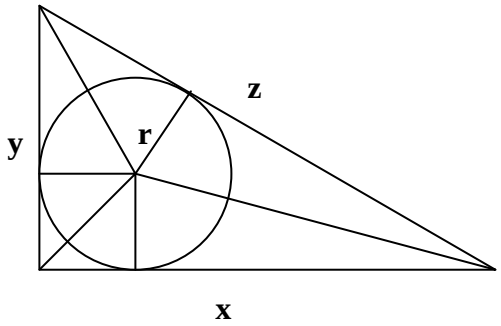

Figura 2. El inradio de un triángulo Pitagórico

Teorema 2.6. Dada la tripla pitagórica (x, y, z), entonces el inradio r es un número entero.

Demostración.

Hay dos maneras obvias para expresar el área A del triángulo

$$r(x + y + z) = 2A = xy\ ,$$

además, como todas las soluciones positivas de $x^2 + y^2 = z^2$ son de la forma

$$x = k2uv, \qquad y = k(u^2 - v^2), \qquad z = k(u^2 + v^2),$$

tal que $(u, v)=1$ y $k, u, v \in Z^+$.

Por sustitución en la ecuación mostrada obtenemos la relación

$$2rk(u^2 + uv) = 2k^2uv(u^2 - v^2),$$

la cual se reduce a

$$r = kv(u - v),$$

así se demuestra que r es un entero. ■

Por el teorema fundamental de la aritmética podemos escribir cualquier entero positivo r, de forma única de la siguiente manera

$$r = 2^{a} p_1^{a_1} p_2^{a_2} .....p_n^{a_n}, \qquad a \geq 0, \qquad n \geq 0, \qquad (2.10)$$

donde p_i es un primo impar $a_i \geq 1$, y $2 < p_1 < p_2 < ... < p_n$. Si $n = 0$, tenemos $r = 2^a$ y si $a = 0$, $r = 2^0 = 1$.

Sea la función $P(r)$ número-teórica que representa el número de tripletas pitagóricas primitivas positivas distintas, que tienen a r como inradio.

Teorema 2.7. Si r se representa como (2.10) entonces $P(r) = 2^n$.

Demostración.

Los enteros x, y, z usados en la demostración del teorema 2.6 son tripletas primitivas si y sólo si $k = 1$. Entonces la ecuación para r toma la forma $r = v(u - v)$, donde el segundo factor $(u - v)$ debe ser impar, puesto que u, v son no pares o impares a la vez. Como $(u, v) = 1$ se sigue que $(v, u - v) = 1$. De la misma forma, si $r = VU$ donde V, U son enteros positivos con U impar y $(V, U)=1$, entonces las ecuaciones $V = v$, $U = u - v$ tienen solución para $u = U + V$, $v = V$, donde u, v son enteros positivos tal que $u > v$, $(u, v) = 1$ y u, v no son pares o impares a la vez.

Por lo tanto todas las triplas pitagóricas primitivas positivas que tienen a r como inradio se encuentran factorizando r en todas las maneras posibles como un producto VU de dos factores primos relativos V, U con U impar.

Como U debe ser impar, $U = 1$ o U contiene factores primos impares. Si r es dado por (2.10), y si U tiene factores p_i, entonces U debe tener un factor p_i^a en orden tal que $r = VU$ con $(V, U) = 1$. Por lo tanto la selección de U, y el valor de $P(r)$ es exactamente el mismo que el número $\tau(r')$ de factores de $r' = p'_1, p'_2.... p'_n$ de donde

$$\tau(r') = (e_1 + 1)(e_2 + 1)....(e_n + 1) = 2^n,$$

dado que cada e_i en r' tiene valor 1 y como $P(r) = \tau\ (r')$, tenemos la demostración. ■

En particular, tenemos que mostrar que $P(r)$ es positivo para todo r y que el rango de $P(r)$ consiste exactamente de todas las potencias de 2 incluyendo $2^0 = 1$.

Como ejemplo consideremos $r = 15 = 2^0 3^1 5^1$ para el cual $n = 2$ y $P(15) = 4$. Las soluciones son

V	U	u	v	x	y	z
15	1	16	15	480	31	481
5	3	8	5	80	39	89
3	5	8	3	48	55	73
1	15	16	1	32	255	257

Cuadro 4. Tabla de soluciones de $P(15)$.

Ahora representemos $N(r)$ como el número total de triplas pitagóricas distintas positivas, no necesariamente primitivas que tienen a r como su correspondiente inradio.

Teorema 2.8. Si r es dado por (2.10) entonces

$$N(r) = (a + 1)(2a_1 + 1)(2a_2 + 1)\ldots\ldots(2a_n + 1).$$

Demostración.

De la fórmula $r = kv(u - v)$ en el teorema 2.6 vemos que k debe ser un divisor de r. Entonces $d = r/k$, y es el inradio de una tripla pitagórica primitiva. De la misma manera, si d es un divisor de r, decimos que $r = kd$, entonces la tripla pitagórica de inradio r puede ser encontrada por una magnífica tripla pitagórica primitiva de inradio d por un factor de proporcionalidad k; y soluciones distintas de d conducen a soluciones distintas para r, por lo tanto se sigue que la función $N(r)$ puede ser obtenida como

$$N(r) = \sum P(d),$$

Donde la sumatoria se extiende para todos los divisores d de r. Aplicando el teorema de multiplicidad de funciones podemos mostrar que $P(d)$ es una función multiplicativa.

Por el teorema *2.7* conocemos que $P(d) = 2^{v(d)}$, donde $v(d)$ es el número de enteros menores que d y primos relativos con d.

Si $(a, b) = 1$; tal que a, b pueden no tener factores primos impares, $a, b \in Z^+$.

Entonces $v(ab) = v(a) + v(b)$. Por consiguiente si $(a, b) = 1$ entonces

$$P(ab) = 2^{v(ab)} = 2^{v(a)+v(b)} = 2^{v(a)}\ 2^{v(b)} = P(a)\ P(b),$$

y así $P(d)$ es una función multiplicativa. Luego $N(r) = \sum P(d)$ es una función multiplicativa, y así para encontrar $N(r)$ necesitamos sólo investigar $N(p^a)$ para p primo.

Cuando $p = 2$, encontramos

$$N(2^a) = P(1) + P(2^1) + ... + P(2^a) = 2^0 + 2^0 + ...2^0 = a + 1.$$

Cuando p es impar, encontramos

$$N(p^a) = P(1) + P(p) + P(p^2) + ... + P(p^a) = 2^0 + 2^1 + 2^1 + ... + 2^1 = 2a + 1.$$

Combinando estos resultados con el hecho que $N(r)$ es multiplicativa completamos la demostración. ■ [11].

Ejemplo.

Tomemos $r = 15$ y $a = 0, a_1 = 1, a_2 = 1$, entonces

$$N(15) = (0 + 1)(2 + 1)(2 + 1) = 9.$$

Calculando tenemos que

$k = 15,\ d = 1, P(1) = 1$ con $(4, 3, 5)$ que llevan $(60, 45, 75)$.

$k = 5, d = 3,\ P(3) = 2$ con $(8, 15, 17)$ que llevan $(40, 75, 85)$ y con $(24, 7, 25)$ que llevan a $(120, 35, 125)$.

$k = 3,\ d = 5,\ P(5) = 2$ con $(12, 35, 37)$ que llevan $(36, 105, 111)$ y con $(60, 11, 61)$ que llevan a $(180, 33, 183)$.

$k = 1,\ d = 15,\ P(15) = 4$ llevan a las cuatro triplas primitivas dadas de los ejemplos anteriores.

2.3 El último teorema de Fermat.

Es el más famoso de todos sus teoremas. El problema 8 del libro II dice: Descomponer un cuadrado dado en dos cuadrados, es decir, sea c^2 el cuadrado dado y a, b los valores a encontrar tal que

$$c^2 = a^2 + b^2 . \qquad (2.11)$$

Este problema parece simple, pero no lo es. Los comentarios de Fermat con relación a este problema son de carácter constructivo y de consecuencias mayores. "Sin embargo, es imposible escribir un cubo como la suma de dos cubos, una cuarta potencia como la suma de dos cuartas potencias y en general cualquier potencia mayor que dos como una suma de dos potencias del mismo grado. Para esto he descubierto una prueba maravillosa pero el margen es tan pequeño para contenerla".

Este es el famoso teorema de Fermat, algunas veces llamado el último teorema de Fermat. En el cual los más prominentes matemáticos han puesto todos sus esfuerzos para resolverlo, desde el momento que se enunció. En el lenguaje algebraico, se requiere mostrar que la ecuación diofántica

$$x^n + y^n = z^n , \qquad (2.11)$$

no tiene solución en enteros x, y, z diferentes de cero, para $n \geq 3$. Un caso particular del teorema de Fermat para el cual no existe solución y que se demostrará más adelante es el siguiente

$$x^4 + y^4 = z^4 ,$$

tal ecuación se puede escribir $z^4 - y^4 = (x^2)^2$ y esta diferencia de dos cuartas potencias no puede ser un cuadrado. Es más si el exponente n de (2.11) es divisible por 4 entonces podemos escribir n como $n = 4m$ y la ecuación toma la forma $(x^m)^4 + (y^m)^4 = (z^m)^4$, de manera que se generaliza la demostración.

De manera similar podemos reducir la ecuación general *(2.11)* a el caso donde el exponente es primo impar. Supongamos que $n = mp,\ p > 2,\ p$ primo. Entonces la ecuación de Fermat se puede escribir

$$(x^m)^p + (y^m)^p = (z^m)^p,$$

así es suficiente probar que la ecuación es imposible para exponentes primos $p > 2$.

La cuestión de que Fermat tuviera una demostración de éste último problema sigue siendo un enigma. Fermat indudablemente poseía una de las más poderosas mentes en el campo investigativo de las leyes de los números, y por esto se le considera una razón para creer que Fermat lo demostró.

Además el comentario de que la margen fuese demasiado pequeña es quizá una excusa. El problema de Fermat ha sido notablemente activo durante toda su historia y sus resultados e investigaciones han sido publicadas frecuentemente en revistas de matemática y es el que más demostraciones erróneas ha generado. Además el teorema ha sido extremadamente importante como una meta y fuente constante de nuevos esfuerzos y por lo tanto de nuevos resultados en matemáticas.

Como hemos mencionado, Fermat da una prueba de este teorema cuando $n = 4$. Para el caso $n = 3$ lo presentó como un problema desafío para los matemáticos franceses e ingleses.

La primera prueba para el caso cúbico fue publicada por Euler en una traducción famosa de su álgebra. El caso $n = 5$ fue probado independiente por el matemático alemán Lejeune-Dirichlet y el francés Legendre en el año *1825* y en *1839* Lamé lo demostró para $n = 7$.

El más significante avance en las investigaciones de este problema fue hecha por el matemático alemán E. Kummer *(1810-1893).* Él extendió el dominio de la teoría de números para incluir no solamente los números

racionales sino los números algebraicos, es decir, números que satisfacen ecuaciones algebraica con coeficientes racionales.

En *1843* Kummer le dirigió a Lejeune-Dirichlet un manuscrito que contenía una prueba del teorema de Fermat basada en números algebraicos.
Dirichlet quién había trabajado por tener la demostración, inmediatamente encontró un error en su prueba; en el dominio de los números algebraicos el teorema fundamental no siempre representa un número de forma única como un producto de sus factores primos. Esta falla le causó a Kummer atacar el problema con mayor vigor y años más tarde encontró un sustituto para el teorema de factorización única en la teoría de ideales, una teoría que más tarde ganó importancia en varias las áreas de la matemática.
Por medio de los ideales, Kummer fue capaz de derivar una condición muy general para la insolubilidad del teorema de Fermat. Todos los avances para la solución de este problema se han basado principalmente en la idea de Kummer. Numerosos criterios fueron desarrollados por medio de la ecuación de Fermat; probada imposible para todos los exponentes menores a $n = 600$ con $n \neq 1,2$ [7].
Hasta 1995 se reconoció como acertada la demostración de Andrew Wiles de la conjetura de Shimura-Taniyama, conjetura que en 1986 Kibet había demostrado que es equivalente al teorema de Fermat, quedando éste comprobado por métodos altamente sofisticados. Queda aún la duda si Fermat realmente tenía una demostración de su sencilla aseveración.

2.4 La ecuación de Pell.

Sea la ecuación

$$x^2 - dy^2 = n\,, \qquad (2.12)$$

donde $d,\ n \in Z$. Cuando $d < 0$ y $n < 0$, la ecuación *(2.12)* no tiene solución. Cuando $d < 0$ y $n > 0$, existe a lo sumo un número finito de soluciones puesto que la ecuación *(2.12)* implica que $\left|x \le \sqrt{n}\right|$ y $\left|y \le \sqrt{n/|d|}\right|$. Además cuando $d = D^2,\ D \in Z$ tenemos que, $x^2 - dy^2 = x^2 - Dy^2 = (x - Dy)(x + Dy) = n$ y por consiguiente las soluciones serían las soluciones de $x + Dy = a,\ x - Dy = b,$ donde $a,\ b \in Z$ tal que $n = ab$. De manera que es más interesante encontrar la solución cuando $d \neq D^2$.

Un caso especial de la ecuación *(2.12)* sucede cuando $n = 1$, es decir

$$x^2 - dy^2 = 1, \qquad (2.13)$$

y se conoce como ecuación de Pell. Aunque la ecuación lleva su nombre, Pell no contribuyó a su solución; en cambio debería haberse llamado ecuación de Fermat, pues el sí dedicó esfuerzo y estudio para resolverla. La importancia de la ecuación de Pell radica principalmente en la investigación de números poligonales.

La principal idea o herramienta para dar solución a esta ecuación parte de que si $\sqrt{d}$ es un número irracional y $\frac{a}{b}$ es una aproximación racional de $\sqrt{d}$ entonces $\frac{a^2}{b^2}$ es una aproximación de d y por lo tanto $\frac{a^2}{b^2} - d = \frac{c}{b^2}$ es decir $a^2 - db^2 = c$.

Observe que si x, y es una solución de *(2.13)*, $x, -y; -x, y; -x, -y$, también lo son. Ahora si $y = 0$ entonces $x = \pm 1;$ si $x = 0$ no tendría soluciones excepto cuando $d = -1$, y por lo tanto $y = \pm 1$. Si la ecuación *(2.13)* tiene soluciones positivas y si x_1, y_1 hacen que $x_1 + y_1\sqrt{d}$ sea el mínimo valor entonces ésta solución se llama solución fundamental. [10].

Para la solución de la ecuación *(2.13)* utilizaremos algunos conceptos relacionados con las fracciones continuas, algunos de ellos sin su demostración pertinente.

Teorema 2.4.1. Si d es un entero positivo, $d \neq s^2,\ s \in Z$ tal que el desarrollo de $\sqrt{d}$ como fracción continua tiene una parte periódica con k términos, entonces x_k, y_k es una solución de *(2.13)*. [1].

Teorema 2.4.2. Si $\frac{x}{y}$ es una solución de la ecuación *(2.13)* con x, y enteros positivos primos entre si , entonces $\frac{x}{y}$ es un convergente en el desarrollo de $\sqrt{d}$ como fracción continua. [1].

Teorema 2.4.3. Si d es un entero positivo, $d \neq s^2,\ s \in Z$. Sea $\frac{x_\kappa}{y_\kappa}$ la *k*-ésima convergente de la fracción continua simple $\sqrt{d}$, $k = 1, 2, 3,...$ y sea n la longitud del periodo de la fracción continua. Entonces cuando n es par las soluciones positivas de la ecuación diofántica *(2.13)* son $x = x_{jn-1},\ y = q_{jn-1}$, $j = 1,2,3, \ldots ;$ cuando n es impar las soluciones positivas de la ecuación *(2.13)* son $x = x_{2jn-1},\ y = y_{2jn-1},\ j = 1,2,3, \ldots$ [9].

Por último sea x_0, y_0 una solución de *(2.13)* entonces podemos encontrar todas las soluciones positivas a partir de ella como se prueba en el siguiente teorema.

Teorema 2.4.4. Sea x_0, y_0 la solución fundamental de la ecuación *(2.13)* entonces todas las soluciones positivas x_k, y_k están dadas por:

$$(x_0 + y_0\sqrt{d}\,)^k = x_k + y_k\sqrt{d}$$

Demostración.

Supongamos que x_1, y_1 es una solución positiva. Entonces $x_1 + y_1\sqrt{d}$ está entre las potencias de $(x_0 + y_0\sqrt{d})$. Es decir para algún entero positivo m la siguiente desigualdad se cumple

$$(x_0 + y_0\sqrt{d})^m \leq x_1 + y_1\sqrt{d} \leq (x_0 + y_0\sqrt{d})^{m+1}. \qquad (2.14)$$

Haciendo $(x_0 + y_0\sqrt{d})^m = x_m + y_m\sqrt{d}$ y dividiendo la desigualdad *(2.14)* por esta cantidad, tenemos

$$1 \leq t + u\sqrt{d} \leq x_0 + y_0\sqrt{d},$$

donde

$$t + u\sqrt{d} = \frac{x_1 + y_1\sqrt{d}}{x_m + y_m\sqrt{d}} = (x_1 + y_1\sqrt{d})(x_m - y_m\sqrt{d}), \qquad (2.15)$$

y se tiene que $t = x_1 x_m - y_1 y_m d$, $u = x_m y_1 - y_m x_1$.

Sustituyendo $\sqrt{d}$ por $-\sqrt{d}$ *(2.15),* tenemos

$$t - u\sqrt{d} = (x_1 - y_1\sqrt{d})(x_m + y_m\sqrt{d}), \qquad (2.16)$$

multiplicando *(2.15)* y *(2.16)* tenemos

$$t^2 - du^2 = (x_1^2 - dy_1^2)(x_m^2 - dy_m^2) = 1.$$

Supongamos que t y u son positivos. Entonces

$$t^2 = 1 + du^2, \quad x_0^2 = 1 + d y_0^2,$$

nos demuestra que $t > x_0$, $u > y_0$ o de otro modo $t < x_0$, y $u < y_0$.

Las desigualdades *(2.14)* implican entonces que anterior se cumple y a la vez niega nuestra suposición de que x_0, y_0 es la solución positiva más pequeña o solución fundamental.

Por tanto, para completar la demostración necesitamos solamente mostrar que t y u son positivos.

Como

$$x_m^2 - y_m^2 d = 1 = x_1^2 - dy_1^2, \qquad (2.17)$$

implica que $x_1 > y_1\sqrt{d}$, $x_m > y_m\sqrt{d}$ y por lo tanto $t > 0$.

También u tiene el mismo signo que $(x_m y_1 - y_m x_1)(x_m y_1 + y_m x_1) = x_m^2 y_1^2 - y_m^2 x_1^2$. Sin embargo *(2.17)* implica que $x_m^2 y_1^2 = y_1^2 + y_m^2 y_1^2 d$, $y_m^2 x_1^2 = y_m^2 + d y_1^2 y_m^2$ y por tanto u no tiene el mismo signo que

$$x_m^2 y_1^2 - y_m^2 x_1^2 = y_1^2 - y_m^2 = (x_1^2 - x_m^2)/d. \qquad (2.18)$$

Sin embargo $x_m + y_m\sqrt{d} < x_1 + y_1\sqrt{d}$ implica que $x_m < x_1$ o que $y_m < y_1$. En el primer caso, la segunda igualdad *(2.18)* demuestra que u es positivo; en el último caso la primera igualdad *(2.18)* muestra que u es positivo. ■ [1].

Ejemplo. Solucionar la ecuación $x^2 - 13y^2 = 1$.

La fracción continua simple de $\sqrt{13}$ es $[3; \overline{1, 1, 1, 1, 6}]$. Entonces las soluciones a esta ecuación son los convergentes x_{10j-1}, y_{10j-1} para $j = 1,2,3,...$ donde $\frac{x_{10j-1}}{y_{10j-1}}$ es la $(10j-1)$ n-ésima convergente de la fracción continua $\sqrt{13}$. Se escoge la $(10j-1)$ n-ésima convergente, ya que como su periodo, $n = 5$, entonces las soluciones serán todos los convergentes $\frac{x_{10j-1}}{y_{10j-1}}$. De la siguiente tabla tenemos la solución:

i	***-2***	***-1***	***0***	***1***	***3***	***4***	***5***	***6***	***7***	***8***	***9***
a_i			*3*	*1*	*1*	*1*	*6*	*1*	*1*	*1*	*1*
p_i	*0*	*1*	*3*	*4*	*11*	*18*	*119*	*137*	*256*	*393*	*649*
q_i	*1*	*0*	*1*	*1*	*3*	*5*	*33*	*38*	*71*	*109*	*180*

Cuadro *5.* Tabla de la solución de $x^2 - 13y^2 = 1$.

De la tabla extraeremos la solución cuando $a_i = a_9$ porque su periodo es *5.*
Por lo tanto las soluciones son: $p_9 = x = 649$, $q_9 = y = 180$.

Ejemplo.

Resolver la ecuación

$$x^2 - 14y^2 = 1.$$

La fracción continua para $\sqrt{14}$ =[3, $\overline{1,2,1,6}$]. La longitud del periodo de la fracción es $n = 4$. Entonces la convergente que es solución de la ecuación es $\frac{p_{4j-1}}{q_{4j-1}}$. Entonces por medio de la siguiente tabla tenemos que en la columna $i = 3$ muestra la solución de la ecuación, $x = 15, y = 4$.

i	***-2***	***-1***	***0***	***1***	***2***	***3***	***4***
a_i			3	1	2	1	6
p_i	0	1	3	4	11	15	101
q_i	1	0	1	1	3	4	27

Cuadro 6. Tabla de la solución de $x^2 - 14y^2 = 1$

2.5 Otras ecuaciones diofánticas.

Puesto que existen métodos sistemáticos para resolver numerosas ecuaciones diofánticas, diferentes soluciones dependen del ingenio de quien las resuelve. Para demostrar cómo puede encontrarse tales soluciones consideremos los siguiente problemas.

a. En la fracción *16/64* se puede suprimir por error los seis y obtener *1/4;* que es el resultado correcto. Si $\overline{ab}$ representa al número de dos dígitos $10a + b$, y $\overline{bc}$ representa $10b + c$, ¿Para qué fracciones $\frac{\overline{ab}}{\overline{bc}}$ el cociente es igual a a/c, donde el numerador es un número de dos dígitos que son a, b, y el denominador es un número de dos dígitos que son b, c; $b > 0$? [1].

Para resolver este problema necesitamos encontrar los enteros positivos menores que *10,* tales que

$$\frac{10a+b}{10b+c} = \frac{a}{c},$$

es decir

$$10ac + bc = 10ab + ca,$$

de donde

$$10a(c - b) = c(a - b). \qquad (2.14)$$

Vemos que *10* es un divisor del segundo miembro de esta ecuación y no es divisor ni de c ni de $(a - b)$, ya que a, b, c son enteros positivos menores que *10*. En consecuencia, c es par y $a - b$ es divisible por *5, ó* $a - b$ es par y c es divisible por *5*.

Consideremos estos dos casos por separado

1. $a - b \equiv 0 \pmod 5$ y $c = 2c'$ para algún entero c'. Entonces $a - b = 0$ ó ± 5. En el primer caso *(2.14)* demuestra que $c = b$ y nuestra fracción es $\frac{\overline{aa}}{\overline{aa}}$. En el segundo *(2.14)* se reduce a

$$(b \pm 5)(2c' - b) = \pm c.$$

El primer miembro es par, ya que el primer factor, o el segundo, es par, si b es impar o par respectivamente. Entonces, como c' no debe ser mayor que *4* y como con el signo más, el primer miembro sería mayor que *4*, del doble signo debe tomarse el negativo. Entonces

$$a = b - 5 > 0,$$

y tenemos

$$(b - 5)(2c' - b) = -c', \qquad b>5,$$

de donde

$$b^2 - b(5 + 2c') + 9c' = 0.$$

Por tanto, si

$$c' = 2,\ b = 6,\ a = 1;\ si\ \ c' = 4,\ b = 9,\ a = 4,$$

y tenemos las fracciones

$$\frac{16}{64}, \quad \frac{49}{98}.$$

2. Supongamos ahora que $a - b = 2u,\ c = 5.$ Entonces la ecuación *(2.14)* nos da

$$2a(5 - b) = a - b.$$

Como a divide al primer miembro, debe dividir al segundo y, en consecuencia, es un divisor de b. Haciendo $b = ka$, y sustituyendo en la última ecuación se obtiene

$$9 = k(2a - 1),$$

lo que demuestra que k divide a 9 y por lo tanto es $1, 3, ó\ 9.$

En los casos respectivos obtenemos las fracciones

$$\frac{55}{55}, \quad \frac{26}{65}, \quad \frac{19}{95},$$

de este modo las únicas soluciones del problema son

$$\frac{\overline{aa}}{\overline{\overline{aa}}}, \quad \frac{16}{64}, \quad \frac{26}{65}, \quad \frac{19}{95}, \quad \frac{49}{98}.$$

b. El problema de Newton acerca de los toros. El problema, en realidad, no fue ideado por Newton, sino de origen popular.

"Tres prados cubiertos de hierba de una misma espesura y con el mismo grado de crecimiento, tienen un área de $3\ ^{1}/_{3}$ hectáreas, 10 hectáreas, y 24 hectáreas. La hierba del primero es comida por 12 toros durante 4 semanas; la del segundo, por 21 toros durante 9 semanas. ¿Cuántos toros comerán la hierba del tercero durante 18 semanas?"

Para la solución tomamos la incógnita auxiliar y, que significa la parte de la reserva inicial de hierba que crece en una hectárea durante una semana. En el primer prado crece durante la primera semana una cantidad de hierba igual a $3\ ^{1}/_{3} * y$; durante 4 semanas, $3\ ^{1}/_{3} * y\ * 4 = (40 / 3) * y$ de la reserva de

hierba que había inicialmente en una hectárea. Esto equivale a un crecimiento del área inicial del prado igual a: $3\,^{1}/_{3} + (40 / 3) * y$ hectáreas. En otras palabras: los toros comen tanta hierba como la que se necesita para cubrir un prado de $(3\,^{1}/_{3} + (40 / 3) * y)$ hectáreas. En una semana 12 toros se comen un cuarto de esta cantidad, y un toro come en una semana $1 / 48$, es decir, la reserva de hierba que hay en un área de

$$(3\,^{1}/_{3} + (40 / 3) * y) / 48 = (10 + 40\,y) / 144 \text{ hectáreas.}$$

De esa misma manera, con los datos del segundo prado, hallamos el área de éste que alimenta a un solo toro durante una semana: crecimiento de la hierba en 1 hectárea durante 1 semana lo asignamos con la incógnita y.
La superficie del sector que contiene hierba suficiente para alimentar 21 toros durante 9 semanas es igual a $10+90*y$.

El área necesaria para mantener un toro durante una semana será:

$$(10 + 90\,y) / 9 * 21 = (10 + 90\,y) / 189 \text{ hectáreas.}$$

Ambas normas de alimentación deben ser idénticas:

$$(10 + 40\,y) / 144 = (10 + 90\,y) / 189.$$

Al despejar la incógnita encontramos que $y = 1/12$. Veamos ahora cuál debe ser el área del prado con hierba suficiente para mantener un toro durante una semana:

$$(10 + 40 * y) / 144 = (10 + 40 / 12) / 144 = 5 / 54 \text{ hectáreas.}$$

Si representamos el número desconocido de toros con la x , tendremos:

$$(24 + (24 * 18 / 12)) / 18\,x = 5 / 54,$$

de donde $x = 36$.
El tercer prado puede mantener 36 toros durante 18 semanas.

c. Ahora miremos que la ecuación diofántica $x^4 + y^4 = z^2$ no tiene soluciones en x, y, z enteros diferentes de cero. [9].

Asumamos que la ecuación tiene soluciones enteras positivas $x, y, z \neq 0$.

Supongamos que $(x, y) = 1$, pero si $(x, y) = d$, entonces $x = dx_1$ y $y = dy_1$ con $(x_1,y_1) = 1$ donde x_1, y_1 son enteros positivos. Como $x^4 + y^4 = z^2$, tenemos que

$$(d\,x_1)^4 + (d\,y_1)^4 = z^2,$$

y factorizando

$$d^4(x_1^4 + y_1^4) = z^2,$$

Por lo tanto $d^4 \mid z^2$ y por consiguiente $d^2 \mid z$. Así que $z = d^2z_1$, donde z_1 es un entero positivo. Entonces

$$d^4(x_1^4 + y_1^4) = (d^2z_1)^2 = d^4z_1^2,$$

así que $x_1^4 + y_1^4 = z^2_1$. De esto concluimos que x_1, y_1, z_1 es una solución positiva con $(x_1,y_1)=1$ de $x^4 + y^4 = z^2$.

Ahora supongamos que $x = x_0,\ y = y_0, z = z_0$ es una solución de $x^4 + y^4 = z^2$ donde x_0, y_0, z_0 son enteros positivos con $(x_0, y_0) = 1$. Entonces se mostrará que existe otra solución en enteros positivos $x = x_1,\ y = y_1, z = z_1$ con $(x_1, y_1) = 1$ tal que $z_1 < z_0$.

Como $x_0^4 + y_0^4 = z^2_0$ tenemos que

$$(x_0^2)^2 + (y_0^2)^2 = z^2_0\,.$$

Luego x_0^2, y_0^2, z_0 es una tripla pitagórica y además $(x_0^2, y_0^2) = 1$, ya que si p es primo tal que $p \mid x_0^2$ y $p \mid y_0^2$, se tiene que $p \mid x_0$ y $p \mid y_0$; contradiciendo el hecho de que $(x_0, y_0) = 1$.

Por lo tanto x_0^2, y_0^2, z_0 es una tripla pitagórica primitiva y por la solución dada anteriormente a la ecuación pitagórica existen enteros m, n con $(m, n) = 1$, $m \not\equiv n\ x_0^2, y_0^2\ (mod\ 2)$ tal que

$$x_0^2 = m^2\text{-}n^2\,,$$
$$y_0^2 = 2mn,$$
$$z_0 = m^2 + n^2,$$

e intercambiar x_0^2, y_0^2 si es necesario para que y_0^2 sea par o viceversa.

De la ecuación x_0^2 vemos que

$$x_0^2 + n^2 = m^2.$$

Como $(m, n) = 1$, se sigue que x_0, n, m es una tripla pitagórica primitiva. De nuevo usando la premisa anterior existen r, s enteros con $(r, s) = 1$, $r \not\equiv s \pmod 2$ tal que

$$x_0 = r^2 - s^2,$$

$$n = 2rs ,$$

$$m = r^2 + s^2.$$

Como m es impar y $(m, n) = 1$ sabemos que $(m, 2n) = 1$. Veamos que $y_0^2 = 2mn$, entonces existen enteros positivo z, w tal que $m = z_1^2$ y $2n = w^2$, puesto que w es par, entonces $w = 2v$, $v \in Z$ se tiene que

$$v^2 = \frac{n}{2} = rs.$$

Como $(r, s) = 1$, por lo tanto existen x_1, y_1 tal que $r = x_1^2$, $s = y_1^2$ note que como $(r, s) = 1$ se sigue que $(x_1, y_1) = 1$ y por lo tanto $x_1^4 + y_1^4 = z_1^2$ donde x_1, y_1, z_1 son enteros positivos con $(x_1, y_1) = 1$. Además $z_1 < z_0$ porque

$$z_1 \leq z_1^4 = m^2 < m^2 + n^2 = z_0 .$$

Para completar la demostración, asumamos que $x^4 + y^4 = z^2$ tiene la mínima solución entera. Por la propiedad del buen orden sabemos que entre las soluciones positivas, existe una solución menor z_0 para la variable z. Sin embargo, mostramos que podemos encontrar otra solución z_0 menor;; induciendo una contradicción. Éste método de demostración se conoce con el nombre de método "de descenso al infinito".

Este método fue ideado por Fermat para resolver algunas de sus cuestiones de la teoría de los números, es una combinación de la inducción completa con la propiedad de que la sucesión de los números admite un mínimo. Una aplicación a las proposiciones "negativas", sería como por ejemplo que

ningún triángulo rectángulo de lados enteros tiene su área igual a un cuadrado. "Si hubiera algún triángulo rectángulo de lados enteros, cuya área fuera un cuadrado, habría otro triángulo menor que el anterior con igual propiedad. Si hubiera este segundo triángulo con tal propiedad, por el mismo raciocinio existiría un tercero menor que el anterior con la misma propiedad y luego un cuarto , un quinto etc..., hasta el infinito, descendiendo. Ahora bien, dado un número no existen infinitos números menores que el; luego es imposible que exista un triangulo de lados enteros... " Para las cuestiones afirmativas combina el método con la reducción al absurdo. Así, para demostrar que todo número primo es de la forma $4n+1$ es siempre suma de dos cuadrados, dice: " si no se compone de dos cuadrados, existirá otro número primo de la misma forma, menor que el anterior, que tampoco se compone de dos cuadrados, y luego un tercero etc... descendiendo hasta el infinito, hasta llegar al numero 5, que es menor de todos los números de este tipo y por lo tanto no sería suma de dos cuadrados.. Como esto es imposible, todos los números de esa naturaleza, están compuestos de esta manera. " [8].

3. SOLUCIÓN DE ALGUNAS ECUACIONES DIOFÁNTICAS ESPECIALES.

3.1 Números Cuadrados expresables como la suma de n cuadrados consecutivos.

En *1875* Edouard Lucas propuso el siguiente problema a partir de una situación en particular: ¿Cuándo una pirámide de bolas de cañón con base cuadrada contiene un número cuadrado?

Desde el punto de vista geométrico es encontrar todos los números que sean cuadrados piramidales y triangulares a la vez. Este problema es claramente equivalente a solucionar la ecuación diofántica

$$1^2 + 2^2 + \ldots x^2 = y^2. \qquad (3.1)$$

Lucas aseguró que la única solución no trivial es $x = 24, y = 70$.

La historia de la solución de esta ecuación empieza en *1876* cuando Moret-Blanc dió una prueba incompleta, pero aceptable para solucionar la ecuación. Moret dividió el problema en dos casos, cuando x es par y cuando x es impar.

En *1877* Lucas publicó una prueba para completar la de Moret, pero también presentó fallas. Lucas manejaba el caso con x par pero no con x impar.

En *1918* Watson manejó la falla de Lucas específicamente con la teoría Jacobiana de funciones elípticas y obtuvo la primera prueba completa de la proposición, era muy complicada para entender.

En *1952* Ljunggren, usó el método de Skolem's para dar una prueba simple desde el punto de vista aritmético

En *1966* Baker y Darenport usaron un teorema de los números transcendentales para solucionar simultáneamente las ecuaciones diofánticas $3x^2 - 2 = y^2$ y $8x - 7 = z^2$.

En *1975* Kanagasabapathy y Ponndurai dieron una solución elemental de las ecuaciones diofánticas anteriores.

En *1985*, De Gang Ma usó la teoría de los dos matemáticos anteriores para dar una solución elemental al problema de Lucas.

Para probar que la solución no trivial para la ecuación en estudio es $x = 24$ y $y = 70$ utilizaremos las ideas de De Gang Ma.

La ecuación *(3.1)* es equivalente a

$$x(x + 1)(2x + 1) = 6y^2.$$

Supongamos que x es par y con la ayuda de los siguientes tres lemas podremos dar solución a ella.

Lema 3.1. El área de un triángulo Pitagórico nunca es un cuadrado.

Demostración.

Supongamos que existen triángulos pitagóricos que tienen área cuadrada.

Sea w^2 el área más pequeña para tales triángulos. Sea x, y los lados del triángulo pitagórico con área w^2. Entonces $x^2 + y^2 = z^2$ y $\frac{xy}{2} = w^2$. Como w es mínima y x, y son primos relativos, (Tripla Pitagórica Primitiva). Además existen enteros positivos r, s tal que $(r, s) = 1$ y que $x = r^2 - s^2$ y $y = 2rs$, (fórmula de triángulo pitagórico).

Por lo tanto $(r^2 - s^2)rs = w^2$ y $\frac{s}{4} < s \leq w^2$, y como $r, s, r - s, r + s$, son primos dos a dos se tiene $(r - s)(r + s)rs = w^2$. Se sigue que hay enteros positivos a, b, c, d tal que $r = a^2$, $s = b^2$, $a^2 - b^2 = r - s = c^2$ y $a^2 + b^2 = r + s = d^2$. Note que $(c, d) = 1$ puesto que $(r - s, r + s) = 1$. Además que c, d son impares porque r, s no son pares e impares a la vez.

Sea $X = \frac{(c+d)}{2}$ y $Y = \frac{d-c}{2}$. Tal que $(X, Y) = 1$ y $X^2 + Y^2 = a^2$. Como X, Y no son pares e impares al a vez se tiene que $\frac{XY}{2} = \frac{d^2 - c^2}{8} = \frac{b^2}{4} = \frac{s}{4}$ es un cuadrado.

Como el triángulo con $X, Y, a;$ un es triángulo pitagórico con área $\frac{s}{4}$ entonces $w^2 \leq \frac{s}{4}$, lo cual es una contradicción. ■ [13].

Lema 3.2. No existe un entero positivo x tal que $2x^4 + 1$ es cuadrado.

Demostración.

La haremos por contradicción. Supongamos que (x, y) es la menor solución de $2x^4 + 1 = y^2$. Entonces para algún entero positivo s, $y = 2s + 1$ y $x^4 = 2s(s + 1)$. Si s es impar entonces $(s, 2(s + 1)) = 1$ tal que $s = u^4$, $v^4 = 2(s + 1)$ para enteros u, v. Luego $2(u^4 + 1) = v^4$ con u impar y v par.

Por lo tanto si $u = 1$ tenemos $2(1 + 1) \equiv 0 \pmod 8$ imposible; s no puede ser impar. Entonces s es par, $(2s, s + 1) = 1$ y $2s = u^4$, $s + 1 = v^4$ para enteros u, $v > 1$

Sea w un entero positivo tal que $u = 2w$. Sea a un entero positivo tal que $v^2 = 2a + 1$. Entonces $(u^4/2) + 1 = s + 1 = v^4$ así que $2w^4 = (v^4 - 1)/4 = a(a + 1)$. Como $v^2 = 2a + 1$ se sigue de la congruencia módulo 4 que a es par. Como $2w^4 = a(a + 1)$ se sigue que existe enteros positivos b, c tal que $a = 2b^4$ y $a + 1 = c^4$.

Sin embargo esto implica que $2b^4 + 1 = (c^2)^2$ y que $y \leq c^2$, por ser (x, y) la mínima. Por lo tanto $c^2 \leq a + 1 < v^2 \leq s + 1 < y$ es una contradicción. ■ [13].

Lema 3.3 Existe solamente un entero positivo a saber $x = 1$ tal que $8x^4 + 1$ es un cuadrado.

Demostración.

Supongamos que $8x^4 + 1 = (2s + 1)^2$. Entonces $2x^4 = s(s + 1)$. Si s es par entonces hay enteros u, v tal que $s = 2u^4$ y $s + 1 = v^4$. En este caso $2u^4+1 = s + 1 = v^4$ y por el Lema 3.2, $u = 0$ y por lo tanto $x = 0$. Si s es impar entonces existen enteros u, v tal que $s = u^4$ y $s + 1 = 2v^4$ en tal caso $u^4+ 1 = 2v^4$. Como u es impar se deriva que v es impar.

Elevando al cuadrado ambos lados $u^4 + 1 = 2v^4$ obtenemos $4v^8 - 4u^4 = u^8 - 2u^4+1$ y por lo tanto $(v^4 - u^2)(v^4 + u^2) = ((u^4 - 1)/2)^2$ es un entero cuadrado. Como $(v^4, u^2) =1$ se sigue que $(v^4 - u^2)/2$ y $(v^4 + u^2)/2$ son cuadrados.

Ahora

$$(v^2 - u\ )^2 + (v^2 + u\ )^2 = 4\frac{(v^4 + u^2)}{2} = A^2,$$

y

$$(v^2 - u\ )\frac{(v^2 + u)}{2} = \frac{(v^4 - u^2)}{2} = B^2.$$

Por el Lema 3.1 esto es imposible a menos de que $v^2 = \pm u$. Puesto que $u^4+ 1= 2v^4$ obtenemos $u^4 - 2u^2 + 1 = 0$ donde $u^2 = 1$, luego $s =1$ y $x = \pm 1$.■ [13].

Con los tres lemas anteriores podemos solucionar la ecuación diofántica

$$x(x + 1)(2x + 1) = 6y^2.$$

Supongamos que x es par. Entonces $x + 1$ es impar y por consiguiente $x, x + 1, 2x + 1$ son primos relativos dos a dos, y $x + 1$ ó $2x+1$ es un cuadrado o un triples cuadrado. Entonces $x+1 \not\equiv 2 \pmod 3$ y $2x+1 \not\equiv 2 \pmod 3$. Por lo tanto $x \equiv 0 \pmod 3$ y para algún entero no negativo p, q, r tenemos $x = 6q^2$, $x + 1= p^2$ y $2x+1 = r^2$. Así

$$6q^2 = (r - p)(r + p).$$

Puesto que p y r son ambos impares, 4 es factor de $(r - p)(r + p) = 6q^2$ y se tiene que q es par. Sea h un entero tal que $q = 2h$. Entonces

$6h^2 = \left(\frac{(r-p)}{2}\right)\left(\frac{(r+p)}{2}\right)$ y como $\left(\frac{(r-p)}{2}\right), \left(\frac{(r+p)}{2}\right)$ son primos relativos porque $(r^2, p^2) = 1$ obtenemos los siguientes dos casos:

Caso 1. Uno de los $\left(\frac{(r-p)}{2}\right)$ *ó* $\left(\frac{(r+p)}{2}\right)$, tiene la forma $6A^2$ y el otro B^2.

Entonces $p = \pm(6A^2 - B^2)$ y $q = 2AB$. Como $6q^2 + 1 = x+1 = p^2$, tenemos $24A^2B^2+1 = (6A^2 - B^2)$ ó $(6A^2 - 3B^2)^2 - 8B^4 = 1$. Por el Lema 3.3, $B = 0$ ó $B = 1$ por lo tanto $x = 6q^2=0$ *ó* $x = 24$.

Caso 2. Uno de los $\left(\frac{(r-p)}{2}\right)$ *ó* $\left(\frac{(r+p)}{2}\right)$, tiene la forma $3A^2$ y el otro $2B^2$.

Entonces $p = \pm(3A^2 - 2B^2)$ y $q = 2AB$. Así $24A^2B^2 + 1 = (3A^2 - 2B^2)$ y por lo tanto $(3A^2 - 6B^2)^2 - 2(2B)^4 = 1$. Por el Lema 3.2, $B = 0$ y por lo tanto $x = 6q^2 = 0$.
Así cuando x es par la única solución a la proposición de Lucas es $x = 24$.
Para el caso de x impar la demostración es más complicada, pero concluye que el único entero de la forma $x(x + 1)(2x + 1) = 6y^2$ es $x = 1$.
Por lo tanto que los únicos números cuadrados y a la vez cuadrados piramidales son 1 y 4900.

Un problema más general que parte de esta ecuación es el determinar el conjunto S de los valores de k, para el cual existe un cuadrado que es la suma de k cuadrados consecutivos, por ejemplo $600 \in S$ puesto que

$$25^2 + 26^2 + ...+ 623^2 + 624^2 = 9010^2.$$

Actualmente existe una tabla que contiene todos los elementos de S menores que 1000. Para encontrar este conjunto S daremos las condiciones y lemas necesarios.

Por convención escribimos $p^{\alpha} \| k$, si $p^{\alpha} | k$ pero $p^{\alpha+1} \nmid k$; α siempre es un entero estrictamente positivo.

Condiciones necesarias para que $k \in S$.

Se da el siguiente lema con el fin de conocer un resultado importante para las demás proposiciones.

Lema 3.4. Si $x^2 + y^2 \equiv 0 \pmod{2^{2n}}$, entonces $2^n \mid x$ y $2^n \mid y$

Demostración.

La proposición es trivial para $n = 1$. Supongamos que es verdadera para $n-1$, entonces $x^2 + y^2 \equiv 0 \pmod{2^{2n-2}}$. Por lo tanto $x = 2^{n-1}a$ y $y = 2^{n-1}b$, y reemplazando tenemos $2^{2n-2}a^2 + 2^{2n-2}b^2 \equiv 0 \pmod{2^{2n}}$. Dividiendo por 2^{2n-2}, obtenemos $a^2 + b^2 \equiv 0 \pmod 4$ por lo cual se deduce que a y b son pares. Por lo tanto $2^n \mid x$ y $2^n \mid y$. ■ [5].

Proposición 1. Sea k un elemento de S

1) Si $2^\alpha \| k$, entonces α es impar
2) Si $3^\alpha \| k$, entonces α es impar
3) Si p es un primo, $p>3$ y $p^\alpha \| k$ con α impar, entonces $p \equiv \pm 1 \pmod{12}$
4) Si p es un primo, $p>3$ y $p^\alpha \| k+1$ con $p \equiv 3 \pmod 4$, entonces α es par
5) Si $3^\alpha \| k+1$, entonces α es impar
6) $k \not\equiv 3 \pmod 9$
7) $k \not\equiv 2^\alpha - 1$ ó $2^\alpha \pmod{2^{\alpha+2}}$ para cualquier $\alpha \geq 2$

Demostración.

Como $k \in S$, existe $m, n \in \mathbf{N}$ tal que $\sum_{i=1}^{k} (n+i)^2 = m^2$. Esto puede escribirse de varias maneras

$$kn^2 + k(k+1)n + \frac{k(k+1)(2k+1)}{6} = m^2, \qquad (i)$$

$$kn(n + k + 1) + \frac{k(k+1)(2k+1)}{6} = m^2, \qquad (ii)$$

$$9k(2n + k + 1)^2 + 3k(k^2 - 1) = 36\, m^2 = j^2 \qquad (iii)$$

Demostración de *(iii)*.

Primero multiplicamos *(ii)* por *36* y tenemos

$$36kn(n + k + 1) + 6(k+1)(2k+1)k = 36m^2,$$

ahora sumamos cero en forma de $9k(k+1)^2 - 9k(k+1)^2$ y obtenemos

$$36kn(n + k + 1) + 9k(k+1)^2 - 9k(k+1)^2 + 6(k+1)(2k+1)k = 36m^2,$$

y factorizando se tiene que

$$9k(2n + k + 1)^2 + 3k(k^2 - 1) = 36\, m^2 = j^2 \ \blacksquare$$

1). Supongamos que $k = 2^\alpha r$ con α par $(\alpha \geq 2)$ y r impar. Entonces, por *(iii)*,

$$9*2^\alpha r(2n + 2^\alpha r + 1)^2 + 3*2^\alpha r(2^{2\alpha} r^2 - 1) = j^2,$$

y puesto que 2^α es cuadrado,

$$9r(2n + 2^\alpha r + 1)^2 + 3r(2^{2\alpha} r^2 - 1) = j^2.$$

Reduciendo módulo *4* tenemos que $2 \equiv j^2 \pmod 4$, contradicción.

2). Es similar. Supongamos que $k = 3^\alpha r$ con α par $(\alpha \geq 2)$ y $3 \nmid r$. Entonces por *(iii)*,

$$3^{\alpha+2} r(2n + 3^\alpha r + 1)^2 + 3^{\alpha+1} r(3^{2\alpha} r^2 - 1) = J^2,$$

y como 3^α es un cuadrado tenemos

$$9r(2n + 3^\alpha r + 1)^2 + 3r(3^{2\alpha} r^2 - 1) = J^2,$$

reduciendo módulo *9* tenemos que $6r \equiv j^2 \pmod 9$, contradicción puesto que $3 \nmid r$.

3). Sea $p>3$, p primo tal que $p^\alpha \| k$ con α impar. Puesto que α es impar y

$$k(9(2n + k + 1)^2 + 3(k^2 - 1)) = j^2,$$

p debe dividir el segundo factor del lado izquierdo, y así $9(2n + 1)^2 \equiv 3 \pmod{p}$. Puesto que $p \neq 3$, $3(2n + 1)^2 \equiv 1 \pmod{p}$ y por Legendre $(3/p) = 1$, que es $p \equiv \pm 1 \pmod{12}$.

4). Sea $p>3$, p primo tal que $p^{\alpha} \| k+1$ con $p \equiv 3 \pmod{4}$. Entonces $k + 1 = ap^{\alpha}$ con $p \nmid a$, y así

$$(ap^{\alpha} - 1)(9(2n + ap^{\alpha})^2 + 3ap^{\alpha}(ap^{\alpha} - 2)) = j^2,$$

de la cual se sigue que $-(6n)^2 \equiv m^2 \pmod{p}$. Si $p \nmid n$, entonces $(-1/p) = 1$ (puesto que $p \nmid 6$) contradiciendo que $p \equiv 3 \pmod{4}$. Por lo tanto, $n = bp^{\beta}$ con $p \nmid b$ y $\beta > 0$ y

$$(ap^{\alpha} - 1)(9(2bp^{\beta} + ap^{\alpha})^2 + 3ap^{\alpha}(ap^{\alpha} - 2)) = j^2 \qquad (3.2)$$

Si $\alpha < 2\beta$, entonces

$$(ap^{\alpha} - 1)\, p^{\alpha}(9(4b^2p^{2\beta - \alpha} + 4abp^{\beta} + a^2p^{\alpha}) + 3a(ap^{\alpha} - 2)) = j^2,$$

en este producto, el único factor divisible por p es p^{α}, por lo tanto α es par. Si $\alpha = 2\beta$, entonces α es obviamente par. Supongamos ahora que $\alpha > 2\beta$; y si dividimos (3.2) por $p^{2\beta}$ obtenemos

$$(ap^{\alpha} - 1)\,(9(2b + ap^{\alpha - \beta})^2 + 3ap^{\alpha - 2\beta}\,(ap^{\alpha} - 2)) = j^2,$$

reduciendo módulo p, llegamos a $-(6b)^2 \equiv j^2 \pmod{p}$. Puesto que $p \nmid 6b$, tenemos $(-1/p) = 1$, de nuevo contradicción, $p \equiv 3 \pmod{4}$, y así $\alpha > 2\beta$ no es posible.

5). Sea $k + 1 = 3^{\alpha}a$ donde $3 \nmid a$ y $\alpha \geq 2$. Entonces

$$(3^{\alpha}a - 1)\,((2n + 3^{\alpha}a)^2 + 3^{\alpha - 1}a\,(3^{\alpha}a - 2)) = j^2,$$

de la cual deducimos que $-(2n)^2 \equiv j^2 \pmod{3}$ y así $n = 3^{\beta}b$, donde $3 \nmid b$ y $\beta > 0$. Por los tanto

$$(3^{\alpha}a - 1)((2 * 3^{\beta}b + 3^{\alpha}a)^2 + 3^{\alpha - 1}a(3^{\alpha}a - 2)) = j^2.$$

Haciendo $\alpha' = \alpha - 1$, y aplicando el mismo argumento como en ***4)*** (comparando α' y 2β) mostramos que α' es par, y así α es impar.

6). Empezamos por la igualdad *(ii).* Supongamos que

$$4kn(n + k + 1) + \frac{2k(k+1)(2k+1)}{3} = m^2,$$

donde $k = 9\mu + 3$. Entonces, reduciendo módulo 3, tenemos

$$2(3\mu + 1)(9\mu + 4)(18\mu + 7) \equiv m^2 \pmod 3,$$

que es $2 \equiv m^2 \pmod 3$, contradicción.

7). Supongamos que

$$9kn(n + k + 1) + \frac{3k(3k+1)(2k+1)}{2} = m^2,$$

donde $k = 2^\alpha + \mu 2^{\alpha+2}$ $(\alpha \geq 2)$, reduciendo módulo $2^{\alpha+1}$, tenemos $3*2^{\alpha-1} \equiv m^2 \pmod{2^{\alpha+1}}$. Si α es impar, entonces $\alpha - 1$ es impar y $3 \equiv m^2 \pmod 4$. Si α es par, entonces dividiendo por $2^{\alpha-2}$ se obtiene $6 \equiv m^2 \pmod 8$. En cada caso tenemos una contradicción.

El segundo caso de **7)** es decir $k = 2^\alpha - 1 + \mu 2^{\alpha+2}$ da $3*2^{\alpha-1} - 9n^2 \equiv m^2 \pmod{2^{\alpha+1}}$.

Supongamos entonces que $m^2 + 9n^2 \equiv 3*2^{\alpha-1} \pmod{2^{\alpha+1}}$, lo cual implica $m^2 + 9n^2 \equiv 0 \pmod{2^{\alpha-1}}$. Si α es impar, por el Lema 3.4 tenemos $m = 2^{(\alpha-1)/2}a$ y $n = 2^{(\alpha-1)/2}b$ y así

$$2^{\alpha-1}a^2 + 9*2^{\alpha-1}b^2 \equiv 3*2^{\alpha-1} \pmod{2^{\alpha+1}},$$

de lo cual deducimos que $a^2 + b^2 \equiv 3 \pmod 4$, contradicción. Si $\alpha = 2$, entonces $m^2 + n^2 \equiv 6 \pmod 8$, contradicción. Si α es par y $\alpha > 2$, tenemos que $m^2 + 9n^2 \equiv 0 \pmod{2^{\alpha-2}}$, y así $m = 2^{(\alpha-2)/2}a$ y $n = 2^{(\alpha-2)/2}b$ lo cual da $2^{\alpha-2}a^2 + 9*2^{\alpha-2}b^2 \equiv 3*2^{\alpha-1} \pmod{2^{\alpha+1}}$ y $a^2 + b^2 \equiv 6 \pmod 8$, otra contradicción. ■ [5].

Observemos que la condición 7), excluye inmediatamente 910 valores de $k \leq 1000$. De los 90 valores restantes 88 se dan en la tabla. Sin embargo $k = 25$ y $k = 842$ cumplen la condición 7), pero no son solución de la ecuación.

Para demostrar que $\{25, 842\} \notin S$, se hará con una aplicación de la ecuación de Pell a la ecuación $(n + 1)^2 + ... + (n + x)^2 = y^2$.
Tales teoremas serán enunciados y no se darán todas las demostraciones.

Sea la siguiente ecuación

$$x^2 - ky^2 = a \qquad (3.3)$$

llamada ecuación de Pell, donde $k \in \mathrm{N}$ y $a \in \mathbf{Z}$. Aceptaremos como únicas soluciones de (3.3), aquellas de las cuales x, y son enteros positivos.
Consideremos primero el caso cuando k es un cuadrado. Entonces $(x - \sqrt{ky})(x + \sqrt{ky}) = a$, tiene un número finito de soluciones. Para cada par de u, v de enteros tal que $uv = a$, $u \geq v$ y $2\sqrt{k} \mid (u - v)$ produce una solución $x = \dfrac{(u + v)}{2}$, $y = \dfrac{(u - v)}{2\sqrt{k}}$.

Ejemplo.

Encontrar todos los números cuadrados que se pueden expresar como la suma de 49 cuadrados consecutivos.
Solución:
Para ello debemos resolver la ecuación diofántica $49n^2 + 2450n + 40425 = m^2$ (ver igualdad (i)). Haciendo $m = 7x$, tenemos $n^2 + 50n + 825 = x^2$, la cual se reduce a la ecuación $x^2 - y^2 = 200$, (ecuación de Pell), haciendo $y = n + 25$. Las soluciones son las parejas $(x, y) \in \{(15, 5), (27, 23), (51, 49)\}$. Como n debe ser positivo, y $y \geq 25$ y así la única solución es $n = 24$ y $m = 357$; la cual

muestra la suma de 49 cuadrados consecutivos que es igual a un cuadrado es decir,

$$25^2 + 26^2 + \ldots + 73^2 = 357^2.$$

Ahora para mostrar que no hay un cuadrado, el cual sea la suma de 25 cuadrados consecutivos, primero escribiremos la ecuación $25n^2 + 650n + 5525 = m^2$, de *(i)* la cual se reduce a $x^2 - y^2 = 52$, haciendo $m = 5x,\ y = n + 13$. Entonces se concluye fácilmente que la última ecuación no tiene solución con $n \geq 0$.

Supongamos ahora que k no es cuadrado. Si (x_1, y_1) y (x_2, y_2), son dos soluciones diferentes de *(3.3)*, escribiremos $(x_1, y_1) < (x_2, y_2)$ si $x_1 < x_2$ y $y_1 < y_2$.

Lema 3.5. Las soluciones de *(3.3)* pueden ser ordenadas

Demostración.

Sea (x_1 , y_1) y (x_2 , y_2) dos soluciones diferentes de *(3.10)*.

Entonces $x_1^2 - ky_1^2 = x_2^2 - ky_2^2 = a$, lo cual implica $x_1^2 - x_2^2 = k(y_1^2 - y_2^2)$ y por lo tanto $x_1 - x_2$ y $y_1 - y_2$ son ambos positivos o ambos negativos. Así se tiene

$$(x_1 , y_1) < (x_2 , y_2) \quad \text{ó} \quad (x_2 , y_2) < (x_1 , y_1)$$ ■

Lema 3.6 La ecuación $x^2 - ky^2 = 1$ tiene siempre una solución diferente de $(1, 0)$.

Demostración.

Por lo menos $(-1, 0)$ es solución. ■

Lema 3.7. Sea (λ, μ) la solución más pequeña o fundamental de $x^2 - ky^2 = 1$ diferente de $(1, 0)$ y sea M la matriz

$$\begin{bmatrix} \lambda & k\mu \\ \mu & \lambda \end{bmatrix}.$$

Entonces, si (x, y) es una solución de (3.3), $M^k(x, y)$ es también una solución para cualquier $k \in Z$, donde M^0 es una matriz idéntica $2x2$.

Demostración.

Como $M(x, y) = \begin{pmatrix} \lambda x + k\mu y \\ \mu x + \lambda y \end{pmatrix}$ y

$$M^{-1}\begin{bmatrix} x \\ y \end{bmatrix} = \begin{bmatrix} \lambda & -k\mu \\ -\mu & \lambda \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} = \begin{bmatrix} \lambda x - k\mu y \\ -\mu x + \lambda y \end{bmatrix},$$

tenemos que probar solamente que $\begin{pmatrix} \lambda x + \varepsilon\, k\mu y \\ \varepsilon\, \mu x + \lambda y \end{pmatrix}$ con $\varepsilon = \pm 1$ es una solución de (3.3), lo cual es bastante fácil. ■

Lema 3.8. Si $(x_1, y_1) < (x_2, y_2)$ entonces $M(x_1, y_1) < M(x_2, y_2)$ y $M^{-1}(x_1, y_1) < M^{-1}(x_2, y_2)$

Demostración.

$$M = \begin{pmatrix} \lambda & \kappa\mu \\ \mu & \lambda \end{pmatrix} \quad \text{y}$$

$$M.(x_1, y_1) = \begin{pmatrix} \lambda & \kappa\mu \\ \mu & \lambda \end{pmatrix} (x_1, y_1) = \begin{pmatrix} \lambda x_1 + k\mu y_1 \\ \mu x_1 + \lambda y_1 \end{pmatrix},$$

$$M.(x_2, y_2) = \begin{pmatrix} \lambda & \kappa\mu \\ \mu & \lambda \end{pmatrix} (x_2, y_2) = \begin{pmatrix} \lambda x_2 + k\mu y_2 \\ \mu x_2 + \lambda y_2 \end{pmatrix}.$$

Ahora estableciendo la relación menor y por la hipótesis de inducción tenemos

$$M(x_1, y_1) < M(x_2, y_2). \blacksquare$$

Lema 3.9. $M^{-1}(x, y) < (x, y) < M(x, y)$.

Demostración.

$$M^{-1}(x, y) = \begin{pmatrix} \lambda x - k\mu y \\ -\mu x + \lambda y \end{pmatrix},$$

$$M(x, y) = \begin{pmatrix} \lambda x + k\mu y \\ \mu x + \lambda y \end{pmatrix}.$$

Comparando tenemos que

$$M^{-1}(x, y) < (x, y) < M(x, y). \blacksquare$$

Los resultados anteriores sugieren el siguiente método para resolver *(3.3).*

Primero, si $a > 0$, la solución real más pequeña de *(3.10)* es $(\sqrt{a}, 0)$. Como

$$M(\sqrt{a}, 0) = \sqrt{a}\ (\lambda, \mu),$$

y si podemos encontrar todas las soluciones enteras de *(3.3)* entre $(\sqrt{a}, 0)$ y $\sqrt{a}\ (\lambda, \mu)$, decimos que $(x_1, y_1), \ldots, (x_r, y_r)$, es el conjunto de todas las soluciones de *(3.3)* y es dado por $\{M^{\alpha}(x_i, y_i) \mid \alpha \in \mathbf{N}, i = 1...r\}$. Igualmente, si $a < 0$, es suficiente determinar todas las soluciones (x_i, y_i) entre

$$(0, \sqrt{-a/k})\ \ y\ \ M(0, \sqrt{-a/k}) = \sqrt{-a/k}\ (k\mu, \lambda).$$

El orden para aplicar este método, es determinar las solución no trivial (λ, μ) de $x^2 - ky^2 = 1$, la cual puede ser encontradas usando fracciones continuas.

Ejemplo.

Encontrar un cuadrado el cual pueda ser expresado como la suma de *11* cuadrados consecutivos.

De *(i)* tenemos la ecuación $11n^2 + 132n + 506 = m^2$. Haciendo $m = 11$, $x = n + 6$, obtenemos $x^2 - 11y^2 = -10$, para $k = 11$ tenemos por medio de fracciones continuas que $\lambda = 10$, $\mu = 3$ es la menor solución y así es suficiente encontrar todas la soluciones entre

$$\sqrt{10/11}\,(0, 1) \quad \text{y} \quad \sqrt{10/11}\,(33, 10),$$

es decir las soluciones (x, y) con $1 \le y \le 9$, son $(1, 1)$ y $(23, 7)$. Todas las otras soluciones son dadas por

$$\begin{bmatrix} x \\ y \end{bmatrix} = \begin{bmatrix} 10 & 33 \\ 3 & 10 \end{bmatrix}^{\alpha} \begin{bmatrix} 1 \\ 1 \end{bmatrix},$$

y

$$\begin{bmatrix} x \\ y \end{bmatrix} = \begin{bmatrix} 10 & 33 \\ 3 & 10 \end{bmatrix}^{\alpha} \begin{bmatrix} 23 \\ 7 \end{bmatrix}.$$

Ahora para mostrar que no hay un cuadrado el cual es la suma de 842 cuadrados consecutivos se hace lo siguiente:

Debemos resolver la ecuación de *(i)*

$$842n^2 + 709806n + 199337185 = m^2.$$

Haciendo $x = 2n + 843,\ m = 421y,$ tenemos

$$x^2 - 842y^2 = -236321.$$

Para $k = 842$ tenemos $\lambda = 1683$ y $\mu = 58$, (por fracciones continuas) así es suficiente encontrar las soluciones (x, y) con $0 \le x \le 818154$ y $17 \le y \le 28195$ pero es fácil observar con ayuda de programa computacional que no existen soluciones en este intervalo (este chequeo se puede hacerse muy rápido porque $x^2 \equiv 281 \pmod{842}$, y así $x \equiv \pm 165 \pmod{842}$ por lo cual se sigue que solamente los enteros x de la forma $842t \pm 165$ con $0 \le t \le 971$ deben ser considerados). [5].

Tabla de los elementos de S menores que 1000.

Para cada uno de los valores de x, el valor más pequeño es $(n + 1)$, para que $(n+1)^2 + (n + 2)^2 .....+.....+ (n + x)^2 = y$

x	n+1	x	n+1	x	n+1	x	n+1
1	1	184	7	383	9985	625	301
2	3	191	4493	393	802	649	38
11	18	193	83342	407	183	673	177
23	7	194	83	409	71752	674	126031
24	1	218	65	431	10123	698	322
26	25	239	899	443	16806	722	131
33	7	241	3807	457	94707486	753	197
47	539	242	64	458	1081	767	6665193
49	25	249	556	479	7989	793	516232
50	7	289	20	481	1663	794	1122
59	22	297	106	491	11476	841	1678
73	442	299	132	506	1778	856	8617
74	225	311	2277	529	255	863	23172625
88	192	312	15	537	68680	864	65
96	13	313	1788	539	172	866	12116
97	15	337	5063	554	25	887	413
107	20914	338	27	568	443	897	454
121	244	347	11320	577	167065	913	688013
122	50	352	280	578	3	914	3480
146	5552	361	358	587	310097726	961	3
169	30	362	1805	599	2927	971	51958
177	553	376	210	600	25	983	9977

Cuadro 7. Tabla de los elementos de S<1000

BIBLIOGRAFÍA

[1] BURTON W. Jones. Teoria de números. F Trillas, 1969.

[2] D.T. Walter. "On the diophantine equation $mX^2 - nY^2 = \pm 1$". Amer. Math. Monthly. Mayo 1967, 504-513.

[3] JIMÉNEZ Rafael, RUBIANO Gustavo. Teoria de Números. Unibiblos. Santa Fé de Bogotá. 1999.

[4] NIVEN I, ZUCKERMAN H. S. An introduction to the theory of numbers. Wiley, 1980.

[5] LAURENT Beeckmans. "Squares Expressibles as Sum of Consecutive Squares" Amer. Math. Monthly. Mayo 1994, 437-442.

[6] LAUB Moshe. "Squares expressible as a Sum of n consecutives Squares" Amer. Math. Monthly 97 (1990) , 662-625.

[7] ORE Oystein. *Number Theory and its History*. Dover Publications, New York, 1948.

[8] REY Pastor J, BABINI J. *Historia de la matemática*. Espasa –Calpe, Buenos Aires, 1951.

[9] ROSEN Kenneth. Elementary number theory and applications. Addison-Wesley Publishing Company, New Jersey.

[10] SHOCKLEY James, Introduccion of Number Theory. Holt Rinehart and Winston. New York 1967.

[11] STEWART B. M. *Theory of numbers*. Mac Millan, New York, 1952.

[12] SWIFT J.D. "Diophantus of Alexandria" Amer. Math. Monthly. V 43, 1956, 163-170.

[13] W. S. Anglin. "The square Pyramid Puzzle." Amer. Math. Monthly 97, 1990, 120-124.