Neiva,10 de Noviembre de 2020

Señores

CENTRO DE INFORMACIÓN Y DOCUMENTACIÓN

UNIVERSIDAD SURCOLOMBIANA

Ciudad Neiva

Los suscritos:

Carlos Alberto Ortiz García, con C.C. No. 1079181006

Brayan Artunduaga Fajardo, con C.C. No. 1078777724,

Autores del trabajo de grado titulado**:**
"Ecuaciones Diofánticas Lineales y Ecuaciones Diofánticas de Orden Dos"
Presentado y aprobado en el año 2020 como requisito para optar al título de Licenciado en Matemáticas

Autorizamos al CENTRO DE INFORMACIÓN Y DOCUMENTACIÓN de la Universidad Surcolombiana para que, con fines académicos, muestre al país y el exterior la producción intelectual de la Universidad Surcolombiana, a través de la visibilidad de su contenido de la siguiente manera:

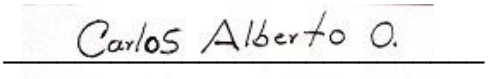
- Los usuarios puedan consultar el contenido de este trabajo de grado en los sitios web que administra la Universidad, en bases de datos, repositorio digital, catálogos y en otros sitios web, redes y sistemas de información nacionales e internacionales "open access" y en las redes de información con las cuales tenga convenio la Institución.

- Permita la consulta, la reproducción y préstamo a los usuarios interesados en el contenido de este trabajo, para todos los usos que tengan finalidad académica, ya sea en formato Cd-Rom o digital desde internet, intranet, etc., y en general para cualquier formato conocido o por conocer, dentro de los términos establecidos en la Ley 23 de 1982, Ley 44 de 1993, Decisión Andina 351 de 1993, Decreto 460 de 1995 y demás normas generales sobre la materia.

- Continúo conservando los correspondientes derechos sin modificación o restricción alguna; puesto que, de acuerdo con la legislación colombiana aplicable, el presente es un acuerdo jurídico que en ningún caso conlleva la enajenación del derecho de autor y sus conexos.

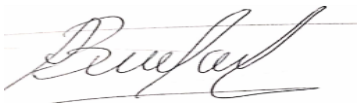
De conformidad con lo establecido en el artículo 30 de la Ley 23 de 1982 y el artículo 11 de la Decisión Andina 351 de 1993, “Los derechos morales sobre el trabajo son propiedad de los autores” , los cuales son irrenunciables, imprescriptibles, inembargables e inalienables.

EL AUTOR/ESTUDIANTE:



Firma: Carlos Alberto Ortiz García

EL AUTOR/ESTUDIANTE:



Firma: Brayan Artunduaga Fajardo

TÍTULO COMPLETO DEL TRABAJO: Ecuaciones Diofánticas Lineales y Ecuaciones Diofánticas de Orden Dos.

AUTOR O AUTORES:

Primero y Segundo Apellido	Primero y Segundo Nombre
Artunduaga Fajardo Ortiz García	Brayan Carlos Alberto

DIRECTOR Y CODIRECTOR TESIS:

Primero y Segundo Apellido	Primero y Segundo Nombre
Gutiérrez Hoyos Ayala Plazas	Hernando Julio Cesar

ASESOR (ES):

Primero y Segundo Apellido	Primero y Segundo Nombre
Gutiérrez Hoyos	Hernando

PARA OPTAR AL TÍTULO DE: Licenciados en Matemáticas

FACULTAD: Educación

PROGRAMA O POSGRADO: Licenciatura en Matemáticas

CIUDAD: Neiva **AÑO DE PRESENTACIÓN:** 2020 **NÚMERO DE PÁGINAS: 72**

TIPO DE ILUSTRACIONES (Marcar con una **X**)**:**

Diagramas___ Fotografías _X_ Grabaciones en discos___ Ilustraciones en general _X_
Grabados___ Láminas___ Litografías___ Mapas___ Música impresa___ Planos___
Retratos___ Sin ilustraciones___ Tablas o Cuadros__

SOFTWARE requerido y/o especializado para la lectura del documento: Ninguno

MATERIAL ANEXO: Ninguno

PREMIO O DISTINCIÓN *(En caso de ser LAUREADAS o Meritoria)*: Ninguno

PALABRAS CLAVES EN ESPAÑOL E INGLÉS:

Español	Inglés
1. Ecuación diofántica	diophantine equation
2. Métodos	methods
3. Nota histórica	historic note
4. Terna pitagórica	Pythagorean triples
5. Fracciones continuas	continued fractions
6. Congruencias	Congruences

RESUMEN DEL CONTENIDO: (Máximo 250 palabras)

Se realizó un estudio sobre las ecuaciones Diofánticas lineales y ecuaciones Diofánticas de orden Dos de la forma $\boldsymbol{ax + by = c}$ y $\boldsymbol{x^2 + y^2 = z^2}$ respectivamente. De acuerdo a lo anterior, se tuvo en cuenta una nota histórica sobre las Ecuaciones Diofánticas, posteriormente se recopiló los siguientes métodos: Ecuaciones Diofánticas mediante el algoritmo de Euclides, Fracciones continuas y Congruencias modulares. Dichos métodos permiten desarrollar estas ecuaciones Diofánticas haciendo uso de unos conceptos previos relacionados con la teoría de números. Por otro lado, se realizó un aplicativo web que permite encontrar las soluciones de un problema practico basado en una ecuación Diofántica lineal. Por último, se estudió una posible hipótesis de cómo pudieron haber sido obtenidas las ternas pitagóricas según los Babilónicos, y así mismo se relacionó a Diofanto con las ternas pitagóricas.

Este trabajo surge por el interés en estudiar e identificar algunos métodos de solución a ecuaciones diofánticas en el conjunto de los números enteros. En este trabajo las ecuaciones se toman como un elemento de estudio clave tanto en lo matemático como en lo histórico. Dentro del estudio de las ecuaciones, es importante reconocer el conjunto en el

que se están planteando las ecuaciones y en el conjunto de valores que se consideran puedan ser solución de la ecuación, ya que esto determinará de una manera u otra, las técnicas y métodos utilizados para encontrar o determinar el conjunto solución de las mismas.

Finalmente, este trabajo deja la satisfacción de haber indagado hechos históricos como el desarrollo de la matemática antigua que con certeza resalta las diferentes maneras de cómo los matemáticos con sus impresionantes habilidades de pensar abordaban los problemas matemáticos de la época, aportando resultados interesantes como las ecuaciones diofánticas.

ABSTRACT: (Máximo 250 palabras)

A study was carried out on the linear Diophantine equations and Diophantine equations of order 2 of the form $\boldsymbol{ax + by = c}$ and $\boldsymbol{x^2 + y^2 = z^2}$ respectively. According to the above, a historical note on Diophantine Equations was taken into account, later the following methods were compiled: Diophantine Equations using the Euclid algorithm, Continuous fractions and Modular Congruence's. These methods allow to develop these Diophantine equations making use of previous concepts related to number theory. On the other hand, a web application was created that allows finding solutions to a practical problem based on a linear Diophantine equation. Finally, a possible hypothesis of how the Pythagorean triples could have been obtained according to the Babylonians was studied, and Diophantus was also related to the Pythagorean triples.

This work arises from the interest in studying and identifying some methods for solving Diophantine equations in the set of integers. In this work, equations are taken as a key element of study both mathematically and historically. Within the study of equations, it is important to recognize the set in which the equations are being proposed and in the set of values that are considered to be a solution to the equation, since this will determine in one way or another, the techniques and methods used to find or determine the solution set of them.

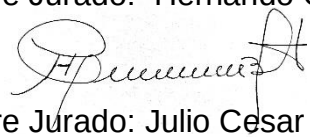
Finally, this work leaves the satisfaction of having investigated historical facts such as the development of ancient mathematics that certainly highlights the different ways in which mathematicians with their impressive thinking skills approached the mathematical problems of the time, providing interesting results such as equations Diophantine.

APROBACION DE LA TESIS

Nombre Presidente Jurado: Julio Cesar Duarte

Firma: 

Nombre Jurado: Hernando Gutiérrez Hoyos

Firma: 

Nombre Jurado: Julio Cesar Ayala Plazas

Firma: 

Universidad Surcolombiana

Facultad de Educación

Programa de Licenciatura en Matemáticas

Ecuaciones Diofánticas Lineales y Ecuaciones Diofánticas de Orden 2

Brayan Artunduaga Fajardo
Carlos Alberto Ortiz García

Neiva, Huila
2020

Universidad Surcolombiana

Facultad de Educación

Programa de Licenciatura en Matemáticas

Ecuaciones Diofánticas Lineales y Ecuaciones Diofánticas de Orden 2

Trabajo presentado como requisito de grado para optar al título de Licenciados en Matemáticas

Brayan Artunduaga Fajardo
20151136594
Carlos Alberto Ortiz García
20152143484

Asesor:
Profesor. Hernando Gutiérrez Hoyos

Neiva, Huila
2020

Nota de Aceptación

_____

_____

_____

_____

_____

Jefe de Programa

_____

Asesor

_____

Segundo Lector

Neiva, Noviembre de 2020

AGRADECIMIENTOS

En principio, queremos agradecer a cada docente de la Licenciatura en Matemáticas quienes con su apoyo y enseñanzas nos brindaron sus diversos conocimientos, especialmente en el campo de las matemáticas y los temas que corresponde a nuestra profesión razón por la cual, constituyeron la base de nuestra formación como profesionales. Seguidamente, queremos expresar con gratitud y agradecimiento sincero al Profesor. Hernando Gutiérrez Hoyos, quien ha sido parte de nuestro proceso académico-formativo como profesor de asignatura y hoy como tutor de nuestro trabajo de grado el cual, representa la última etapa que vivimos como estudiantes de la Licenciatura en Matemáticas. De igual forma, agradecemos toda su paciencia y capacidad para orientar y organizar las ideas de donde surgierón aportes invaluables.

YO, Brayan Artunduaga Fajardo
Quiero agradecer a mi madre Violeth, a ella le debo la vida y le estaré eternamente agradecido por eso, me enorgullece ser su hijo, siempre resaltaré que eres una madre ejemplar que en todo momento ha querido lo mejor para sus hijos, infinitamente gracias madre, te amo. Agradecer a mis hermanos Carlos, Dagoberto y Fabián y a mi hermana Diana por ser también parte de mi motivación de sacar en adelante esta carrera.

También quiero agradecer a Paola por su apoyo y colaboración incondicional, por haber compartido conmigo esta experiencia con cariño, respeto y amabilidad, estaré plenamente agradecido y tenga la certeza que eres una mujer muy importante para mi vida.

A mis compañeros, de la licenciatura especialmente a Liliana, Luisa y Nicolás por ser esos compañeros que fueron de gran apoyo en circunstancias difíciles, que siempre estuvieron conmigo compartiendo momentos de alegría y enojo.

YO, Carlos Alberto Ortiz García
Quiero agradecer a mis padres, Sonia y Folmar, por su ejemplo de lucha y honestidad; a mi hermano Andrés por su paciencia, inteligencia y responsabilidad que, de forma incondicional, entendieron todo este proceso durante todos estos años. Sin su apoyo y colaboración habría sido imposible cumplir mis objetivos que significan alegría y orgullo para mi y también para ellos.

También quiero agradecer a todos mis compañeros de grupo, de la licenciatura, en especial a Jefferson, Tatiana y David quienes tengo sólo palabras de agradecimiento, ya que con ellos se vivieron y compartieron momentos inolvidables. Seguidamente agradezco su gran apoyo moral y humano, necesarios en los momentos difíciles de este trabajo y esta profesión.

Finalmente, queremos agradecer a la Universidad Surcolombiana, la cual nos sentimos profundamente orgullosos, debido a que nos brindaron una educación de excelente calidad.

Gracias a todas las personas que siempre nos apoyaron y creyeron en la realización de este trabajo de grado.

ÍNDICE GENERAL

INTRODUCCIÓN

Las ecuaciones diofánticas, que aparecen por primera vez en uno de los libros mas importante de las dos obras de Diofanto. De Diofanto sólo sabemos que vivió en Alejandría hacia el año (250), y que murió a los 84 años. La *Aritmética* comprendía originalmente de trece libros, de los que únicamente solo se conocen los seis primeros.

Ésta joya fue traducida al árabe por Qustá ibn Lúgá a mediados de la segunda mitad del siglo *IX*. De las ediciones modernas, una de las más famosas fue la de Bachet (1621), que publicó por primera vez el texto griego con traducción latina; esta fue la famosa edición utilizada por Fermat para dejar en ella enunciada su misteriosa demostración de teorema o conjetura.

La *Aritmética* de Diofanto, los ejemplos y problemas son todos de teoría de números; Sin embargo, aún cuando es de enorme interés su estudio, nos vamos a referir solamente a las ecuaciones diofánticas lineales y ecuaciones diofánticas de orden 2, esto es, a ecuaciones con coeficientes y soluciones que son numeros enteros, de la forma $ax + by = c$ y $x^2 + y^2 = z^2$.

Este trabajo surge por el interés en estudiar e identificar algunos métodos de solución a ecuaciones diofánticas en el conjunto de los números enteros. En este trabajo las ecuaciones se toman como un elemento de estudio clave tanto en lo matemático como en lo histórico. Dentro del estudio de las ecuaciones, es importante reconocer el conjunto en el que se están planteando las ecuaciones y en el conjunto de valores que se consideran puedan ser solución de la ecuación, ya que esto determinará de una manera u otra, las técnicas y métodos utilizados para encontrar o determinar el conjunto solución de las mismas.

Es por ello que se necesita que el lector este familiarizado con resultados básicos teniendo noción de algunos conceptos de la teoría de números, que traten de llamar la atención en como se fue abarcando dicho proceso por contenidos que establezca como hipótesis que los métodos de solución a las ecuaciones se cumpliran siempre y cuando en la estructura algebraica que se trabaje sea posible establecer algunas propiedades claves en el conjunto de los números enteros.

El presente trabajo está estructurado de la siguiente manera:

Capitulo I. Nociones Preliminares
En este capitulo se expone algunos conceptos básicos de la teoría de números, en este análisis se establecen propiedades de divisibilidad, máximo común divisor, números primos, algoritmo de Euclides y otros que servirán para el desarrollo de los métodos en el estudio de las ecuaciones diofánticas lineales y de orden 2.

Capitulo II. Métodos de Solución de las Ecuaciones Diofánticas Lineales
En este capitulo se muestran algunos métodos para la solución de las ecuaciones diofánticas lineales de la forma $(ax + by = c)$ en el conjunto de los números enteros. Dando así a conocer alternativas para el desarrollo de las ecuaciones mediante la aplicación del Algoritmo de Euclides, de las Fracciones Continuas y de las Congruencias Lineales mostrando así diferentes ejemplos y formas para solucionar problemas.

Seguidamente se desarrolló una aplicación pensando en utilizar uno de los métodos para la solución de la ecuación diofántica lineal haciendo uso del ALGORTIMO DE EUCLIDES, el cual consiste en adivinar o calcular la fecha de cumpleaños de una persona.

Capitulo III. Ecuaciones Diofánticas de Orden 2
En este capitulo se trata de dar una buena idea en como los babilonios llegaron a construir ternas pitagóricas que aparecen en la tablilla Plimton 322, teniendo en cuenta el estudio de Diofanto y las Ternas Pitagóricas.

JUSTIFICACIÓN

El presente trabajo nace del interés de consultar temas interesantes dentro de la teoría de números, rama de la matemática encargada de estudiar el conjunto de los números enteros, de aquí que se optó por indagar acerca de las ecuaciones diofánticas particularmente las lineales y las de segundo grado de la forma $ax + by = c$ y $x^2 + y^2 = z^2$ respectivamente. Este trabajo se enfocará en consultar fuentes de información acerca del desarrollo de las ecuaciones diofánticas y en la clasificación de métodos de solución de dichas ecuaciones, de manera que se logre hacer una recopilación y así poder contribuir en aspectos históricos y metodológicos útiles a otro tipo de investigaciones o simplemente puede ser utilizado como base para mejorar tipos de trabajos referentes a las ecuaciones diofánticas lineales y de orden 2.

Con este trabajo se pretende atender temas importantes dentro de las matemáticas como las ecuaciones diofánticas, de igual manera resaltar que el aprendizaje de las mismas. En cuanto a lo procedimental ayuda a fortalecer los conocimientos teóricos en relación a la teoría de números y potenciar las habilidades en aspectos aritméticos y algebraicos. De otro lado, exaltar las implicaciones prácticas que conllevan las ecuaciones diofánticas lineales en contextos cotidianos basado en problemas, los cuales se desarrollan en base a unas condiciones dadas para poder encontrar dichas soluciones. Del mismo modo, destacar la genialidad que contaron los antiguos matemáticos para buscar soluciones a este tipo de ecuaciones, garantizando que las mismas estén en el conjunto de los números enteros positivos, como único conjunto numérico disponible de la época. En este sentido, valorar el esfuerzo y la creatividad con que disponían los matemáticos para desarrollar métodos de solución a este tipo de ecuaciones, recurriendo de artificios procedentes de la habilidad del pensamiento, fomentando así de manera involuntaria la denominada hoy en día teoría de números

Por otra parte, este trabajo permite poner en práctica los aprendizajes adquiridos durante la trayectoria universitaria y así mismo contribuir con el desarrollo profesional despertando interés por la investigación hacia la literatura matemática.

OBJETIVOS

Objetivo General

- Compilar, identificar y establecer algunos métodos de solución a ecuaciones diofánticas lineales de la forma $(ax + by = c)$ y de las ecuaciones de orden 2 de la forma $\left(x^2 + y^2 = z^2\right)$.

Objetivos Específicos

- Enunciar distintos métodos y procedimientos algebraicos para la solución a ecuaciones diofánticas lineales mediante el Algoritmo de Euclides, de las Fracciones Continuas y de las Congruencias Lineales y de las segundo orden teniendo en cuenta el estudio de Diofanto y las ternas Ternas Pitagóricas de la forma $ax + by = c$ y $x^2 + y^2 = z^2$ respectivamente.
- Mostrar la solución de problemas prácticos en relación a las ecuaciones diofánticas lineales de la forma $ax + by = c$.
- Diseñar un aplicativo web que permita encontrar la solución a una ecuación diofántica lineal basada en un problema practico.

CONTEXTUALIZACIÓN HISTÓRICA

Las Ecuaciones Diofánticas son ecuaciones con coeficientes enteros, cuyas soluciones se buscan en el conjunto de los números enteros.

Este tipo de ecuaciones se conocen en matemáticas desde la antigüedad por civilizaciones como los bábilonios y los mesopotámicos, pero fue tras la obra del matemático griego Diofanto de Alejandría (*siglo III d.c. 210–290*) que comenzarón a llamarse Ecuaciones Diofánticas. Fue en este siglo que Diofanto publicó su "Aritmética"; un tratado de 13 libros, del que solo se conocen los seís primeros, en el cual se trata de una forma rigurosa no solo las ecuaciones de primer grado, sino también las de segundo.

En este tratado propone y resuelve problemas sobre cantidades y combinaciones relacionadas con las medidas de lados, áreas, perímetros de triángulos y sumas de cuadrados que son resueltos de forma numérica. Problemas como: ¿Qué números son suma de dos números cuadrados? ¿Qué números son suma de tres números cúbicos?. Estas ecuaciones son las que tanto sus coeficientes como soluciones se encuentran en el conjunto de los números enteros. una de estas ecuaciones es la ecuación pitagórica, la cual esta dentro de nuestros objetos de estudio.

Diofanto de Alejandría es considerado el algebrista griego mas importante; su trabajo en este campo se destaca por encima de sus contemporáneos. Una de sus contribuciones más importantes es la introducción, un poco incipiente por cierto del simbolismo en el álgebra. Particularmente para la igualdad y para las operaciones suma y producto con entidades numéricas. Debido a esta combinación del simbolismo con el lenguaje usual, el álgebra de Diofanto se llama sincopada. El algebra anterior a Diofanto indica las operaciones y la igualdad en el lenguaje escrito usual; esta álgebra se llama retórica.

Los griegos clásicos no consideraban productos con mas de tres factores ya que no tenían ningún significado geométrico para ellos, ya que x^2 era el área de un cuadrado y x^3 el volumen de un cubo. Diofanto consideró potencias como x^4, x^5 etc.

Hay indicios de influencia babilónica, pero no hay prueba alguna de que haya una conexión directa entre los trabajos de Diofanto y el álgebra babilónica, pues sus números son completamente abstractos y no se refieren a situaciones particulares y/o específicas de la cotidianidad como era el caso de egipcios y babilonios.

Sin duda muchos de los problemas que resolvio Diofanto se originaron en la teoría de números y su propósito fue buscar soluciones enteras para las ecuaciones que generaban tales problemas, estudio que posteriormente llevo al surgimiento de la rama de la teoría de números dedicada al trabajo con tales ecuaciones, conocido actualmente como analisís Diofantico. Dicho trabajo llevo a matemáticos como Fermat y Euler a desarrollar métodos enfocados a buscar soluciones enteras para las ecuaciones $ax + by = c$ y; $ax^2 + bx + cy + dy^2 = e$

CAPÍTULO 1

NOCIONES PRELIMINARES

Para poder entender ó hacerle un seguimiento a los desarrollos teóricos en relación con el estudio de las Ecuaciones Diofánticas, es necesario tener conocimientos previos de una serie de elementos que se recogen actualmente en la denominada Teoría de Números que esta relacionada, primordialmente, con las propiedades de los números naturales, $1, 2, 3, 4, \ldots,$. También llamados enteros positivos. A continuación se relacionan algunos de los recursos de esta teoría, considerado básicos para iniciar el estudio de las Ecuaciones Diofánticas.

1.1. Orden en los Números Naturales

Definición 1.1.1 (**Orden en los Números Naturales**). *Dados dos números naturales m y n, decimos que $m \leq n$ si y solo si existe un número natural p de tal manera que $n = m + p$.*

Simbólicamente:

$$m \leq n \Leftrightarrow \exists p \in \mathbb{N} \text{ Tal que } n = m + p,$$

Esta relación define un orden en los Números Naturales.

1.1.1. Propiedades del Orden en $\mathbb{N}$

Teorema 1.1.2. *El orden definido en $\mathbb{N}$ satisface las siguientes propiedades:*

i) Para todo $m \in \mathbb{N}$, $m \leq m$.

ii) Para $m, n \in \mathbb{N}$, si $n \leq m$ y $m \leq n$, entonces $m = n$.

iii) Para $m, n, r \in \mathbb{N}$, si $m \leq n$ y $n \leq r$, entonces $m \leq r$.

Demostración:

i) $m \leq m$, pues $m = m + 0$ y $0 \in \mathbb{N}$.

ii) Si $n \leq m$, $\exists p \in \mathbb{N}$ Tal que $m = n + p$,
Si $m \leq n$, $\exists q \in \mathbb{N}$ Tal que $n = m + q$.
Luego:

$$\begin{aligned} m &= n + p \\ &= (m + q) + p \\ &= m + (p + q) \end{aligned}$$

Por lo tanto, $p + q = 0$ y, en consecuencia, $p = q = 0$, lo que implica $m = n$.

iii) Si $m \leq n$, $\exists p \in \mathbb{N}$ Tal que $n = m + p$,
Si $n \leq r$, $\exists q \in \mathbb{N}$ Tal que $r = n + q$.
Luego:

$$\begin{aligned} r &= n + q \\ &= (m + p) + q \\ &= m + (p + q) \end{aligned}$$

Así que $m \leq r$. □

Definición 1.1.3. *Si $n, m \in \mathbb{N}$, diremos que $n < m$ si $n \leq m$ y $n \neq m$.*

Observación:

$$\begin{aligned} n < m &\Leftrightarrow n \leq m \text{ y } n \neq m \\ &\Leftrightarrow \exists p \in \mathbb{N} \text{ Tal que. } m = n + p \text{ y } n \neq m. \end{aligned}$$

Como $n \neq m$, entonces $p \neq 0$. □

Teorema 1.1.4 (**Ley de la Tricotomía**). *Dados $m, n \in \mathbb{N}$, se verifica una y solo una de las siguientes relaciones,*

$$m < n,\ n = m,\ n < m.$$

La demostración requiere la prueba del siguiente lema.

Lema 1.1.5. *Si $m, n \in \mathbb{N}$, todas las siguientes afirmaciones son falsas:*

a) $m < n$ *y* $m = n$.

b) $n < m$ *y* $n = m$.

c) $m < n$ *y* $n < m$.

Nota. *Para esta demostración se hace uso de el tercer Axioma de Peano que dice:*

AP–3 *Si $\forall n \in \mathbb{N}$, entonces $n^* \neq 0$.*

Demostración:

a) Si tuviéramos simultáneamente $m < n$ y $m = n$, tendríamos $n = m + p^*$, donde $p \in \mathbb{N}$ y $m = n$, lo que implicaría que $p^* = 0$. Esto contradice el tercer Axioma de Peano. Por tanto (a) es falso.

b) Si tuviéramos simultáneamente $n < m$ y $n = m$, tendríamos $m = n + q^*$, donde $q \in \mathbb{N}$ y $n = m$, lo que implicaría que $q^* = 0$. Esto contradice el tercer Axioma de Peano. Por tanto (b) es falso.

c) Si $m < n$ y $n < m$, tendríamos $n = m + p^*$ y $m = n + q^*$ lo que implicaría

$$n = (n + q^*) + p^* = n + (q^* + p^*) = n + (q^* + p)^*,$$

en consecuencia $(q^* + p)^* = 0$, lo que contradice el tercer Axioma de Peano. Por tanto (c) es falso. □

1.1.2. Principio de Buena Ordenación

Definición 1.1.6 (**Elemento Mínimo de un Conjunto**). *Sea $S \subseteq \mathbb{N}$, $S \neq \phi$. Un número natural m es el mínimo de S se nota $m = min\ S$ si cumple las dos condiciones siguientes:*

a) $m \in S$

b) $m \leq s, \forall s \in S$

Teorema 1.1.7 (**Principio de Buena Ordenación**). *Todo subconjunto no vacío S de números naturales tiene un elemento mínimo.*

Nota. *Para esta demostración se hace uso de el quinto Axioma de Peano que dice:*

AP–5 Si $A \neq \mathbb{N}$ y $0 \in A$, entonces $\exists m \in A$ de tal manera que $m + 1 \notin A$.

Demostración: Sea $A = \{n \in \mathbb{N} : n \leq s, \forall s \in S\}$.

Se tiene que $0 \in A$, pues $0 \leq s$, $\forall s \in \mathbb{N}$, así que $0 \leq s$, $\forall s \in S$ además $A \neq \mathbb{N}$, en efecto: como $S \neq \phi$, sea $s \in S$, luego $s < s + 1$, lo que significa que $s + 1 \notin A$.

Por el postulado quinto de Peano, entonces $\exists m \in A$ de manera que $m + 1 \notin A$. Vamos a probar que $m = min\ S$

Como $m \in A$, entonces $m \leq s, \forall s \in S$ y se está cumpliendo la propiedad (b) de la definición anterior. Falta probar que $m \in S$. Procedemos por contradicción:

Si $m \notin S$, entonces como $m \in A$, debe tenerse que $m < s, \forall s \in S$, o sea que $m + 1 \leq s, \forall s \in S$, lo cual significa que $m + 1 \in A$, lo cual es contradictorio pues en este caso $A = \mathbb{N}$.

Así que $m \in S$ y $m = min\ S$. □

1.1.3. Múltiplos y Divisores de un Número Entero

Si $a \in \mathbb{Z}$, siendo $a \neq 0$ y $b = a \cdot q$ para algún $q \in \mathbb{Z}$, diremos que a divide a b. De igual manera podemos decir que a es un divisor de b, a es un factor de b, b es múltiplo de a. Si a divide a b lo notaremos como $a \mid b$.
A manera de ilustración vemos que: -3 divide a 12 puesto que $12 = (-3) \cdot (-4)$, y 6 no divide a 21 puesto que no existe ningún entero q tal que $6 \cdot q = 21$.

1.1.4. Conjunto de Múltiplos y Divisores de un Número Entero

Si $a \in \mathbb{Z}$, el conjunto $M_a = \{a \cdot q \mid q \in \mathbb{Z}\}$ se llamará el conjunto de los múltiplos de a. El conjunto $D_a = \{b \in \mathbb{Z} \mid b/a\}$ se llamará el conjunto de los divisores de a.

A manera de ilustración: Si $a = 6$

$$M_6 = \{6 \cdot q \mid q \in \mathbb{Z}\} = \{0, \pm 6, \pm 12, \pm 18, \dots\}$$
$$D_6 = \{b \in \mathbb{Z} \mid b/6\} = \{\pm 1, \pm 2, \pm 3, \pm 6\}$$

En cualquier caso D es finito, pero M puede ser finito ó infinito. Si $a \neq 0$, D es finito, si $a = 0$ entonces M es finito.

1.2. Algoritmo de la División

Teorema 1.2.1 (**El Algoritmo de la División**). *Si a es un número natural y b es un número entero, existen enteros únicos q, r tales que $b = aq + r$, con $0 \leq r < a$.*

Demostración: De la igualdad $b = at + r$, se obtiene $r = b - at$. Sea el conjunto

$$S = \{b - at, t \in \mathbb{Z}\} \subseteq \mathbb{Z}.$$

Consideremos $b \geq 0$, como t recorre el conjunto de los enteros, sea $t = 0$. En este caso $b - at \geq 0$. Supongamos que $b < 0$ por idéntica razón hagamos $t = b$. En dicho caso,

$$b - at = b - ab = b\,(1 - a)\,.$$

Pero, $1 \leq a$ entonces, $b\,(1 - a) \geq 0$ es decir, $b - at \geq 0$, lo que permite afirmar que el conjunto S posee elementos no negativos. Sea $D \subseteq S$ formado por los elementos no negativos de S. Por el Principio de Buena Ordenación, D tiene un elemento mínimo. Tomando r como este número y a q como el mayor entero que satisface la condición $b - aq \geq 0$, se deduce que, $r = b - aq \geq 0$. Restando $\boldsymbol{a}$ a ambos miembros y factorizando,

$$r - a = b - aq - a = b - a\,(q + 1)\,.$$

Pero, $q + 1 > q$ y por la selección de q debe tenerse que

$$b - a\,(q + 1) < 0$$

o sea,

$$r - a < 0$$

de donde se concluye que $r < a$ lo que permite escribir

$$0 \leq r < a$$

Para **demostrar** la **unicidad** supongamos que q y r no son únicos. Sean q_1 y r_1 enteros tales que $b = aq_1 + r_1$, con $0 \leq r_1 < a$. Por la propiedad transitiva de la igualdad,

$$aq_1 + r_1 = aq + r.$$

Supongamos que $r > r_1$, entonces $r - r_1 > 0$. Trasponiendo términos y factorizando,

$$0 < r - r_1 = a\,(q_1 - q)$$

de donde se tiene que $a \mid (r - r_1)$.
Pero $0 \leq r_1 < a$, implica que $-a < -r_1 \leq 0$ y como $0 \leq r < a$ se pueden sumar miembro a miembro estas desigualdades dando como resultado

$$-a < (r - r_1) < a$$

o sea,

$$(r - r_1) < a.$$

Como $a \mid (r - r_1)$, necesariamente $a < (r - r_1)$; lo cual es una contradicción. Por lo tanto, r no es mayor que r_1. Suponer que r_1 es mayor que r conduce a una contradicción similar, de donde se deduce que r_1 no es mayor que r, quedando como única posibilidad, $r = r_1$.
De la expresión $r - r_1 = a\,(q_1 - q)$ observamos que $0 = a\,(q_1 - q)$ y como a es diferente de cero se concluye que $(q_1 - q) = 0$ y por lo tanto, $q = q_1$. En síntesis la unicidad del cociente y el residuo quedan **demostrados**. □

1.3. Máximo Común Divisor

En esta sección analizaremos el problema de determinar el mayor de los factores comunes a dos enteros. Mediante el empleo del algoritmo de la división al igual que el desarrollo y utilización de las fracciones continuas mediante una escritura apropiada de los números racionales e irracionales a partir de dicho algoritmo.

Si se toman dos enteros a, b puede ocurrir que ambos sean iguales a cero y en este caso cualquier entero es un divisor común de ellos. Si al menos uno es diferente de cero, los divisores comunes son finitos; uno de los cuales siempre es 1, deduciéndose que existe alguno mayor que todos y debe ser positivo.

Definición 1.3.1. *Dados dos enteros* $a,\ b,\ a^2 + b^2 \neq 0$, *entonces* $d \in \mathbb{Z} - \{0\}$ *se llama común divisor de* a *y* b *si y solo si* $d \mid a$ *y* $d \mid b$.

Nota. *el siguiente teorema garantiza la existencia y unicidad del máximo común divisor.*

Teorema 1.3.2. *Dados dos enteros* a *y* $b,\ a^2 + b^2 \neq 0$, *existe un entero único* g, *tal que*

1. $g > 0$.
2. $g \mid a$ *y* $g \mid b$.
3. $g = min\{ax + by > 0, x,\ y,\ \in \mathbb{Z}\}$.
4. Si d es cualquier entero tal que $d \mid a$ *y* $d \mid b$, entonces $d \mid g$.

Nota. *Este número* g *es, precisamente, el máximo común divisor de* a *y* b.

Demostración: Considérese a *y* b positivos, donde $a > b$. Por el **Algoritmo de la División** existen enteros $r_1,\ q_1$ únicos tales que

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

Si $r_1 = 0$, entonces b es un común divisor de a *y* b . Podemos tomar $g = b$.

1. $g > 0$.
2. $g \mid a$ *y* $g \mid b$.

Tomemos el conjunto

$$H = \{ax + by > 0,\ x,\ y\ \in \mathbb{Z}\} \subseteq \mathbb{Z}.$$

Si $x < 0$, necesariamente $y > 0$ entonces $by > 0$. Debido a que

$$ax + by > 0$$

debe tenerse

$$|ax| < by.$$

Pero cero es el mínimo natural que verifica esta última desigualdad, luego $x = 0$, entonces el mínimo valor para y deber ser 1, por tanto

$$b = a \cdot (0) + b \cdot (1) > 0$$

es un elemento de H.
Similarmente si $y \leq 0$ hallamos $y = 0,\ x = 1$ como valores mínimos, o sea

$$a = a \cdot (1) + y \cdot (0) > 0$$

pertenece también a H, pero $b < a$.
Si $x > 0,\ y > 0,\ ax > a,\ by > y;$ entonces $ax + by > a + b > b$.

En síntesis,

$$b = g = min\{ax + by > 0,\ x,\ y\ \in \mathbb{Z}\}$$

dado por demostrado (3).
(4). Si existe d tal que $d \mid a\ ,\ d \mid b$, debe tenerse que $d \mid g$ puesto que $g = b$. Si $r_1 \neq 0$, la aplicación repetida del algoritmo de la división demuestra la existencia de parejas únicas $q_i,\ r_i,\ 2 \leq i \leq k+1,\ 0 < r_i < r_{i-1}$, tales que

$$\begin{aligned} a &= bq_1 + r_1 \\ b &= r_1q_2 + r_2 \\ r_1 &= r_2q_3 + r_3 \\ &\vdots \\ r_{k-2} &= r_{k-1}q_k + r_k \\ r_{k-1} &= r_kq_{k+1} + 0. \end{aligned}$$

Aquí confrontamos cada etapa con la posibilidad de tener cero por residuo; pero suponemos que esto no sucede sino hasta el K-ésimo paso de la división, o diciéndolo en otra forma, definimos a k como el número de la etapa en la cual aparece cero como residuo. En esta parte el proceso debe de detenerse porque la división por cero no esta definida. Por otro lado, eventualmente debe aparecer un cero como residuo puesto que $b > r_1 > r_2 > \ldots > r_k$ es una sucesión finita estrictamente decreciente de naturales; y como existen $b-1$ enteros positivos menores que b, después de a lo más $b-1$ divisiones debe obtenerse el esperado cero como residuo.
En conclusión, si b no divide a a existe siempre un sistema finito de ecuaciones de la clase anterior y un k-ésimo residuo diferente de cero. Aseguramos que para satisfacer las condiciones $(1)\,,\ (2)\,,\ (3)\,,\ (4)$ podemos tomar $g = r_k$.
De la última ecuación observamos que $r_k \mid r_{k-1}$ entonces

$$\begin{aligned} r_{k-2} &= r_{k-1} + r_k \\ &= (r_kq_{k+1})\, q_k + r_k \\ &= r_k\,(q_{k+1}q_k + 1) \end{aligned}$$

o sea que $r_k \mid r_{k-2}$.
Siguiendo el proceso vemos de las dos primeras ecuaciones que $r_k \mid a,\ y\ r_k \mid b$, luego r_k es un divisor común $a\ y\ b$. Expresando los residuos sucesivos se obtiene

$$\begin{aligned} r_1 &= a - bq_1 \\ r_2 &= b - r_1q_2 \\ &= b - (a - bq_1)\, q_2 \\ &= b - aq_2 + bq_1q_2 \\ &= a\,(-q_2) + b\,(1 + q_1q_2)\,. \end{aligned}$$

La forma de estas igualdades indica que r_k puede obtenerse por reemplazos sucesivos como una combinación lineal de $a\ y\ b$ con coeficientes enteros en cuya expresión intervienen los q_i, o sea,

$$r_k = ax + by.$$

Como $r_k > 0$, por el principio de la buena ordenación existe un elemento mínimo en el conjunto H. Sea h tal elemento, luego para algunos enteros $x_0,\ y_0$ se establece la igualdad

$$h = ax_0 + by_0 > 0.$$

Supongamos que h no divide a a, entonces existen enteros únicos q, r tales que

$$a = hq + r,\ 0 < r < h$$

Luego

$$\begin{aligned} r &= a - hq \\ &= a - (ax_0 + by_0)q \\ &= a\,(1 - x_0 q) + (-y_0 q)\,. \end{aligned}$$

Como $r < h$, implicaría que h no es el mínimo, llegando a una contradicción; por consiguiente $h \mid a$.
Similarmente $h \mid b$ y de aquí, $h \mid (ax + by)$, o sea, $h \mid r_k$.
Por la propiedad (3) de divisibilidad $h < r_k$. Pero $r_k \mid a$ y $r_k \mid b$ implica que $r_k \mid (ax_0 + by_0)$ y en consecuencia $r_k = h$. por la misma propiedad $r_k \leq h$, concluyendo que $r_k = h$.
En síntesis, r_k es el mínimo del conjunto de los $ax + by > 0$.

Sea d tal que $d \mid a$ y $d \mid b$, entonces $d \mid (ax + by)$, es decir dr_k.
como r_k cumple las cuatro condiciones del teorema, es posible afirmar que $r_k = g = (a, b)$.
Si $a < b$, intercabiamos los roles .
Si $a < 0$ y $b < 0$ determinar g correspondiente a los respectivos valores absolutos.
Si $a = 0$, entonces $|b| = g = (a, b)$.

Para demostrar la unicidad, tomemos g, g_1 dos enteros que satisface las condiciones del teorema, entonces $g \mid a$ y $g \mid b$ implica $g \mid g_1$.
Por otra parte $g_1 \mid a$ y $g_1 \mid b$ implica $g_1 \mid g$ y como consecuencia $g < g_1$ y $g_1 \leq g$ determinándose que implica $g = g_1$. □

Nota. *El Máximo Común Divisor entre a y b es el* ***<u>ultimo residuo</u>*** *distinto de cero, en el algoritmo de las divisiones sucesivas de Euclides.*

Ejemplo 1.1. *Mediante el Algoritmo de la División calculamos el máximo común divisor de* 141 *y* 96 *(que evidentemente es* 3*) con el fin de expresarlo, de una vez, como una combinación lineal de dichos números.*

Solución:

$$\begin{array}{r|l} 141 & 96 \\ \hline 45 & 1 \end{array} \qquad 141 = 1 \cdot 96 + 45 \qquad 0 \leq 45 < 96$$

$$\begin{array}{r|l} 96 & 45 \\ \hline 6 & 2 \end{array} \qquad 96 = 2 \cdot 45 + 6 \qquad 0 \leq 6 < 45$$

$$\begin{array}{r|l} 45 & 6 \\ \hline 3 & 7 \end{array} \qquad 45 = 7 \cdot 6 + 3 \qquad 0 \leq 3 < 6$$

$$\begin{array}{r|l} 6 & 3 \\ \hline 0 & 2 \end{array} \qquad 6 = 2 \cdot 3 + 0$$

Luego: $(141, 96) = 3$. Ahora,

$$\begin{aligned} 3 &= 45 - 7 \cdot 6 \\ &= 45 - 7 \cdot (96 - 2 \cdot 45) \\ &= 45 - 7 \cdot 96 + 14 \cdot 45 \\ &= 15 \cdot 45 - 7 \cdot 96 \\ &= 15 \cdot (141 - 1 \cdot 96) - 7 \cdot 96 \\ &= 15 \cdot 141 - 15 \cdot 96 - 7 \cdot 96 \\ &= 141 \cdot (15) + 96 \cdot (-22) \end{aligned}$$

Expresado 3 como una combinación lineal de 141 y 96, donde intervienen 15 y -22 □

Ejemplo 1.2. *Mediante el Algoritmo de la División calculamos el máximo común divisor de* 356 *y* 260 *(que evidentemente es* 4*) con el fin de expresarlo, de una vez, como una combinación lineal de dichos números.*

Solución:

$$\begin{array}{r|l} 356 & 260 \\ \hline 96 & 1 \end{array} \qquad 356 = 1 \cdot 260 + 96 \qquad 0 \leq 96 < 260$$

$$\begin{array}{r|l} 260 & 96 \\ \hline 68 & 2 \end{array} \qquad 260 = 2 \cdot 96 + 68 \qquad 0 \leq 68 < 96$$

$$\begin{array}{r|l} 96 & 68 \\ \hline 28 & 1 \end{array} \qquad 96 = 1 \cdot 68 + 28 \qquad 0 \leq 28 < 68$$

$$\begin{array}{r|l} 68 & 28 \\ \hline 12 & 2 \end{array} \qquad 68 = 2 \cdot 28 + 12 \qquad 0 \leq 12 < 28$$

$$\begin{array}{r|l} 28 & 12 \\ \hline 4 & 2 \end{array} \qquad 28 = 2 \cdot 12 + 4 \qquad 0 \leq 4 < 12$$

$$\begin{array}{r|l} 12 & 4 \\ \hline 0 & 3 \end{array} \qquad 12 = 3 \cdot 4 + 0$$

Luego: $(356, 260) = 4$. Ahora,

$$\begin{aligned} 4 &= 28 - 2 \cdot 12 \\ &= 28 - 2 \cdot (68 - 2 \cdot 28) \\ &= 28 - 2 \cdot 68 + 4 \cdot 28 \\ &= 5 \cdot 28 - 2 \cdot 68 \\ &= 5 \cdot (96 - 1 \cdot 68) - 2 \cdot 68 \\ &= 5 \cdot 96 - 5 \cdot 68 - 2 \cdot 68 \\ &= 5 \cdot 96 - 7 \cdot 68 \\ &= 5 \cdot 96 - 7 \cdot (260 - 2 \cdot 96) \\ &= 5 \cdot 96 - 7 \cdot 260 + 14 \cdot 96 \\ &= 19 \cdot 96 - 7 \cdot 260 \\ &= 19 \cdot (356 - 1 \cdot 260) - 7 \cdot 260 \\ &= 19 \cdot 356 - 19 \cdot 260 - 7 \cdot 260 \\ &= 356 \cdot (19) + 260 \cdot (-26) \end{aligned}$$

Expresado 4 como una combinación lineal de 356 y 260, donde intervienen 19 y -26 □

Ejemplo 1.3. *El máximo común divisor de tres enteros a, b, c se define como $(a, b, c) = ((a, b), c) = (a, (b, c))$. Mediante el Algoritmo de la División calculamos el máximo común divisor de 4410, 1404 y 8712 con el fin de expresarlo, de una vez, como una combinación lineal de dichos números.*

Solución: $(4410, 1404, 8712) = (4410, (1404, 8712))$.

Tenemos que $(1404, 8712)$

$$\begin{array}{r|l} 8712 & 1404 \\ \hline 288 & 6 \end{array} \qquad 8712 = 6 \cdot 1404 + 288 \qquad 0 \leq 288 < 1404$$

$$\begin{array}{r|l} 1404 & 288 \\ \hline 252 & 4 \end{array} \qquad 1404 = 4 \cdot 288 + 252 \qquad 0 \leq 252 < 288$$

$$\begin{array}{r|l} 288 & 252 \\ \hline 36 & 1 \end{array} \qquad 288 = 1 \cdot 252 + 36 \qquad 0 \leq 36 < 252$$

$$\begin{array}{r|l} 252 & 36 \\ \hline 0 & 7 \end{array} \qquad 252 = 7 \cdot 36 + 0$$

Luego: $(1404, 8712) = 36$. Ahora,

$$\begin{aligned} 36 &= 288 - 1 \cdot 252 \\ &= 288 - 1 \cdot (1404 - 4 \cdot 288) \\ &= 288 - 1 \cdot 1404 + 4 \cdot 288 \\ &= 5 \cdot 288 - 1 \cdot 1404 \\ &= 5 \cdot (8712 - 6 \cdot 1404) - 1 \cdot 1404 \\ &= 5 \cdot 8712 - 30 \cdot 1404 - 1 \cdot 1404 \\ &= 1404 \cdot (-31) + 8712 \cdot (5) \end{aligned}$$

Luego: $(4410, 36)$. Tenemos que,

$$\begin{array}{r|l} 4410 & 36 \\ \hline 18 & 122 \end{array} \qquad 4410 = 122 \cdot 36 + 18 \qquad 0 \leq 18 < 36$$

$$\begin{array}{r|l} 36 & 18 \\ \hline 0 & 2 \end{array} \qquad 36 = 2 \cdot 18 + 0$$

Luego: $(4410, 36) = 18$. Ahora,

$$\begin{aligned} 18 &= 4410 - 122 \cdot 36 \\ &= 4410 - 122 \cdot (1404 \cdot (-31) + 8712\,(5)) \\ &= 4410 + 1404 \cdot (3782) - 8712 \cdot (610) \\ &= 4410 \cdot (1) + 1404 \cdot (3782) + 8712 \cdot (-610) \end{aligned}$$

Expresado 18 como una combinación lineal de 4410, 1404 y 8712, donde intervienen 1, 3782 y -610 □

1.3.1. Propiedades del Máximo Común Divisor

Hemos mostrado que si $g = (a, b)$ entonces existen x_0, y_0 enteros tales que $g = ax_0 + by_0$. El siguiente teorema muestra el único caso en el que se da la equivalencia de las afirmaciones.

Teorema 1.3.3. *Sean a, b enteros no ambos nulos. Entonces, $(a, b) = 1$ si y solo si existen enteros s, t tales que $1 = sa + bt$.*

Demostración: Si $(a, b) = 1$, se sabe que existe $s, t \in \mathbb{Z}$ tales que $1 = sa + bt$. Recíprocamente si existen enteros s, t tales que $1 = sa + tb$; como $(a, b) \mid a$ y $(a, b) \mid b$, entonces $(a, b) \mid 1$ y en consecuencia $(a, b) = 1$. □

Teorema 1.3.4. *Si $m \in \mathbb{Z}^+$, $(ma, mb) = m\,(a, b)$.*

Demostración: El resultado se obtiene de multiplicar todas las igualdades en el Algoritmo de Euclides por m:

$$\begin{aligned} ma &= mbq_1 + mr_1 \quad ;\ 0 \le mr_1 < mb \\ mb &= mr_1q_2 + mr_2 \ ;\ 0 \le mr_2 < mr_1 \\ &\vdots \\ mr_{k-1} &= mr_kq_{k+1} + 0 \\ (ma, mb) &= (mb, mr_1) = \ldots = (mr_{k-1}, mr_k) = mr_k = m\,(a, b)\,. \end{aligned}$$

□

Definición 1.3.5. *Dos números enteros a y b se llaman primos relativos si $(a, b) = 1$.*

Teorema 1.3.6. *Si $(a, b) = 1$ y $b \mid ac$, entonces $b \mid c$*

Demostración: si $(a, b) = 1$, existen entonces $s, t \in \mathbb{Z}$ tales que $1 = sa + tb$. Luego, $C = (cs)\,a + (ct)\,b$, ó $C = (ac)\,s + (bc)\,t$. Por hipótesis $b \mid ac$ y es claro que $b \mid bc$, luego $b \mid c$. □

Teorema 1.3.7. *Si $(a, b) = 1$ y $(a, c) = 1$, entonces $(a, bc) = 1$.*

Demostración: Puesto que $(a, b) = 1$ y $(a, c) = 1$ tenemos que, $1 = ax + by$ y también $1 = ar + cs$ con x, y, r, s enteros y por lo tanto,

$$\begin{aligned} 1 &= (ax + by)\,(ar + cs) \\ &= a\,(xar + xsc + byr) + bc\,(ys) \\ &= ap + bcq \text{ con } p, q \in \mathbb{Z}, \end{aligned}$$

por tanto $(a, bc) = 1$ □

1.4. Números Primos

Definición 1.4.1. *Un número entero $p > 1$ es primo si y solo si tiene dos divisores positivos:* 1 *y el mismo p. Un número $a > 1$, que tenga fuera del* 1 *y de si mismo otros divisores se llama compuesto. Los primeros números primos son:* $2, 3, 5, 7, 11, 13, \ldots$
Algunas propiedades elementales de los números primos:

Teorema 1.4.2.

i) Sea $a \in \mathbb{Z}$, $a > 1$. El menor divisor de a, distinto de 1*, es número primo.*

ii) Sea $a \in \mathbb{Z}$ un número compuesto, sea p el divisor menor de a distinto de la unidad. Entonces $p \leq \sqrt{a}$.

iii) El conjunto de los números primos es infinito.

Demostración:

i) Sea q el menor divisor de a; $q \neq 1$. Si q fuera compuesto, digamos $q = q_1 * r$ con $q \in \mathbb{Z}$ y $1 < q_1 < q$, como $q \mid a$ y $q_1 \mid q$, tendríamos que $q_1 \mid a$, lo cual no es posible pues $q_1 < q$ y q es el divisor más pequeño de a.

ii) $a \in \mathbb{Z}$, p el divisor menor de a, p es primo. Como $p \mid a$, entonces $a = q \cdot p$, donde $p \leq q$ o sea que $p^2 \leq q \cdot p$. Luego $p^2 \leq a$ ó $p \leq \sqrt{a}$.

iii) Supongamos que existe un numero primo p que sea el mayor de todos. Sea n el productos de todos los primos, menores o iguales que p. Entonces

$$n + 1 = (2 \cdot 3 \cdot 5 \cdot 7 \cdots p) + 1 > p.$$

Nótese que n no es divisible entre 2, 3, 5 o bien p. De aquí que cualquier divisor primo p de n es un primo distinto de $2, 3, 5, 7, 13, \ldots, p$. Ahora si $n + 1$ es un primo, entonces p no es el mayor de ellos. si $n + 1$ es compuesto, entonces debe contener mayores primos que p, ya que la división de $n + 1$ por primos menores o iguales que p deja como resto 1. Por lo tanto, en ningún caso existe un primo que sea el mayor de ellos; esto es, el número de primo es finito.

Nota. *la parte ii) del Teorema 1.4.2 da una técnica para probar si un número es o no primo. A manera de ejemplo: $a = 79$. La raíz de 79 esta entre* 8 *y* 9 *: $8 < \sqrt{79} < 9$. Basta probar si entre los primos menores que* 9 *hay divisores* $2, 3, 5, 7$. *Como ningúno es divisor,* 79 *es primo.* □

Teorema 1.4.3.

i) Sea p un número primo dado. Si a es un entero cualquiera entonces $(a, p) = 1$ ó $p \mid a$.

ii) si p es primo y $p \mid a \cdot b$, entonces $p \mid a$ ó $p \mid b$.

iii) Si p, q, son primos y $p \mid q$ entonces $p = q$.

Demostración:

i) Supongamos que $(a, p) \neq 1$, como p solo tiene dos divisores (p y 1), luego, debe existir un número entero positivo distinto de 1 que divida simultáneamente a a, y p, pero p solo tiene dos posibilidades que son dos divisores 1 y p, entonces $(a, p) = p$ por lo tanto $p \mid a$.

ii) Supongamos que $p \nmid a$. Por lo tanto $p \mid b$. Análogamente si suponemos que $p \nmid b$, entonces $p \mid a$.

iii) Como p y q son dos primos tales que $p \mid q$, entonces $p = 1$ ó $p = q$. Como p es primo, excluimos el caso $p = 1$. Por lo tanto $p = q$. □

1.5. Fracciones Continuas

Las Fracciones Continuas son uno de los temas más interesantes dentro de la teoría de números, así como también de los temas más antiguos. Tienen sus primeros antecedentes en los trabajos de Euclides, dado que el algoritmo para hallar el máximo común divisor entre dos enteros provee un método para hallar una fracción continua. Este algoritmo se presenta en el libro *VII* de los elementos de Euclides a través de las siguientes proposiciones:

Proposición 1.5.1.

i) Dados dos números desiguales y restándose sucesivamente el menor del mayor, si el que queda no mide nunca al anterior hasta que quede la unidad, los números iniciales serán primos entre si.

ii) Dados dos números no primos entre si, hallar su medida común máxima.

Posteriormente, en el siglo *XVI*, se pueden mencionar los resultados de Bombelli y Cataldi quienes emplearon un método para encontrar aproximaciones de raíces cuadradas. Unas décadas después, John Wallis en su obra la aritmética de los infinitesimales presenta una pequeña teoría acerca de las fracciones continuas y una interesante representación de $4/\pi$ conocido hoy en día como el producto de Wallis. Seguidamente, en el siglo *XVIII*, se destacaron los trabajos realizados por Leonhard Euler en sus obras: introducción al análisis del infinito y sobre fracciones continuas y, entre lineas, se puede intuir en su sentido actual una construcción de los reales en términos de fracciones continuas.

1.5.1. Fracciones Continuas Simples

Dada cualquier fracción racional $\frac{u_0}{u_1}$, en su más simple expresión de manera que $(u_0, u_1) = 1$ y $u_1 > 0$, aplicamos el algoritmo de Euclides tal y como se formulo en el teorema 1.2.1.

Vemos que:

$$\begin{aligned}
u_0 &= u_1 a_0 + u_2 && ;\ 0 \leq u_2 < u_1 \\
u_1 &= u_2 a_1 + u_3 && ;\ 0 \leq u_3 < u_2 \\
u_2 &= u_3 a_2 + u_4 && ;\ 0 \leq u_4 < u_3 \\
&\vdots && \vdots \\
u_{j-1} &= u_j a_{j-1} + u_{j+1} && ;\ 0 \leq u_{j+1} < u_j \\
u_j &= u_{j+1}\, a_j
\end{aligned}$$

□

Nota. *La notación se ha alterado a la dada en el teorema 1.2.1, reemplazando a, b por u_0, u_1; $r_1, r_2, \ldots, r_j$ por $u_2, u_3, \ldots, u_{j+1}$ y $q_1, q_2, \ldots, q_{j+1}$ por $a_0, a_1, \ldots, a_j$. La forma de la expresión anterior es un poco más apropiada para nuestros propósitos actuales.*

Posteriormente la expresión mencionada anteriormente las podemos transformar en:

$$\frac{u_0}{u_1} = a_0 + \frac{u_2}{u_1} = a_0 + \frac{1}{\frac{u_1}{u_2}} \quad ;\ \frac{u_1}{u_2} = a_1 + \frac{u_3}{u_2}$$

$$\frac{u_0}{u_1} = a_0 + \frac{1}{a_1 + \frac{u_3}{u_2}} = a_0 + \frac{1}{a_1 + \frac{1}{\frac{u_2}{u_3}}} \quad ;\ \frac{u_2}{u_3} = a_2 + \frac{u_4}{u_3}$$

$$\frac{u_0}{u_1} = a_0 + \frac{1}{a_1 + \frac{1}{a_2 + \frac{u_4}{u_3}}} = a_0 + \frac{1}{a_1 + \frac{1}{a_2 + \frac{1}{\frac{u_3}{u_4}}}}$$

Continuando este proceso finitamente hasta a_j, obtenemos lo siguiente:

$$\frac{u_0}{u_1} = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{\cdots \\ \ddots \\ a_{j-1} + \cfrac{1}{a_j}}}}$$

Definición 1.5.2. *Se denominan convergentes ó reducidos de una fracción continua simple* $[a_1, a_2, \ldots, a_j]$ *a las fracciones continuas simples finitas.*

$$\begin{aligned}
c_1 &= [a_1] = a_1 \\
c_2 &= [a_1, a_2] = a_1 + \frac{1}{a_2} \\
c_3 &= [a_1, a_2, a_3] = a_1 + \cfrac{1}{a_2 + \cfrac{1}{a_3}} \\
&\vdots \qquad\qquad\qquad \vdots \\
c_j &= [a_1, a_2, \ldots, a_j] = a_1 + \cfrac{1}{a_2 + \cfrac{1}{a_3 + \cfrac{1}{\cdots \\ \ddots \\ a_{j-1} + \cfrac{1}{a_j}}}}
\end{aligned}$$

Se dice que tal fracción continua finita es simple si todos los $c_i, (i \in \mathbb{N})$ son enteros.

Teorema 1.5.3. *Toda fracción continua simple finita representa un número racional y recíprocamente, todo número racional representa una fracción continua simple finita.*

Demostración: Veamos que para todo número racional, $\frac{p}{q} \in \mathbb{Q},\ p > q$ y $q \neq 0$ existe una fracción continua simple finita $[a_1, a_2, \ldots, a_j]$ que lo representa:

$$p = qa_0 + r_0 \ \Rightarrow\ \frac{p}{q} = a_0 + \frac{r_0}{q},\ \text{con } a_0 < \frac{p}{q}\ ;\ 0 \leq r_0 < q$$

análogamente:

$$\begin{aligned}
\frac{q}{r_0} &= a_1 + \frac{r_1}{r_0} \qquad \text{con } a_1 < \frac{q}{r_0} \quad ;\ 0 \leq r_1 < r_0 \\
\frac{r_0}{r_1} &= a_2 + \frac{r_2}{r_1} \qquad \text{con } a_2 < \frac{r_0}{r_1} \quad ;\ 0 \leq r_2 < r_1 \\
&\vdots \qquad\qquad\qquad \vdots \qquad\qquad\qquad \vdots \\
\frac{r_{n-2}}{r_{n-1}} &= a_n + \frac{r_n}{r_{n-1}}\ \text{con } a_n < \frac{r_{n-2}}{r_{n-1}}\ ;\ 0 \leq r_n < r_{n-1}
\end{aligned}$$

En consecuencia, aparece una sucesión decreciente de enteros positivos menores que el entero q: $[r] = [r_0, r_1, \ldots, r_{n-1} - r_n]\,,\ r_0 > r_1 > \ldots > r_{n-1} > r_n$ y como solamente existe un número finito, de enteros menores que q, el proceso ha de terminar tras un número finito de pasos, por lo que resulta:

$$\frac{p}{q} = a_0 + \frac{r_0}{q} = a_0 + \frac{1}{\frac{q}{r_0}} = a_0 + \cfrac{1}{a_1 + \frac{r_1}{r_0}} = \ldots$$

$$\ldots = a_0 + \cfrac{1}{a_1 + \cfrac{1}{\cfrac{r_0}{r_1}}} = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{\cfrac{r_1}{r_2}}}} = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{\ddots \\ a_{j-1} + \cfrac{1}{a_j}}}}$$ □

Nota. *En la expresión anterior se supuso que la fracción racional $\frac{u_0}{u_1}$ tenía denominador positivo u_1, pero no puede hacerse una suposición semejante respecto a u_0. De aquí que a_0 puede ser positivo, negativo o bien cero. No obstante, supuesto que $0 \leq u_2 < u_1$, se nota que el cociente a_1 es positivo y, de modo semejante, los cocientes subsecuentes $a_2, a_3, \ldots, a_j$ son enteros positivos. En el caso de que $j \geq 1$ esto es, si el conjunto contiene más de una ecuación, entonces $a_i = \frac{a_j}{a_{j+1}}$ y $0 \leq u_{j+1} < u_j$ implica que $a_j > 1$.*

En los siguientes ejemplos ilustraremos el procedimiento para expresar un número racional como una fracción continua simple:

Ejemplo 1.4. *Expresar $\frac{95}{43}$ como una fracción continua simple.*

Solución: Por el Algoritmo de Euclides se tiene que:

$$\begin{array}{r|l} 95 & 43 \\ \hline 9 & 2 \end{array} \qquad 95 = 2 \cdot 43 + 9 \qquad 0 \leq 9 < 43$$

$$\begin{array}{r|l} 43 & 9 \\ \hline 7 & 4 \end{array} \qquad 43 = 4 \cdot 9 + 7 \qquad 0 \leq 7 < 9$$

$$\begin{array}{r|l} 9 & 7 \\ \hline 2 & 1 \end{array} \qquad 9 = 1 \cdot 7 + 2 \qquad 0 \leq 2 < 7$$

$$\begin{array}{r|l} 7 & 2 \\ \hline 1 & 3 \end{array} \qquad 7 = 3 \cdot 2 + 1 \qquad 0 \leq 1 < 2$$

$$\begin{array}{r|l} 2 & 1 \\ \hline 0 & 2 \end{array} \qquad 2 = 2 \cdot 1 + 0$$

Luego: Lo expresamos como una fracción continua. Ahora,

$$\begin{aligned} \frac{95}{43} &= 2 + \frac{9}{43} = 2 + \cfrac{1}{\cfrac{43}{9}} = 2 + \cfrac{1}{4 + \cfrac{7}{9}} \\ &= 2 + \cfrac{1}{4 + \cfrac{1}{\cfrac{9}{7}}} = 2 + \cfrac{1}{4 + \cfrac{1}{1 + \cfrac{2}{7}}} \\ &= 2 + \cfrac{1}{4 + \cfrac{1}{1 + \cfrac{1}{\cfrac{7}{2}}}} = 2 + \cfrac{1}{4 + \cfrac{1}{1 + \cfrac{1}{3 + \cfrac{1}{2}}}} \end{aligned}$$

La representación de $\frac{95}{43}$ como una fracción continua no es única. Existe una excepción trivial, ya que el último término 2 puede ser expresado como $1 + \frac{1}{1}$ de aquí que:

$$= 2 + \cfrac{1}{4 + \cfrac{1}{1 + \cfrac{1}{3 + \cfrac{1}{2}}}} = 2 + \cfrac{1}{4 + \cfrac{1}{1 + \cfrac{1}{3 + \cfrac{1}{1 + \cfrac{1}{1}}}}}$$

□

Ejemplo 1.5. *Evaluar la fracción continua simple* $[3, 4, 7, 4, 8]$.

Solución:

$$[3,4,7,4,8] = 3 + \cfrac{1}{4 + \cfrac{1}{7 + \cfrac{1}{4 + \cfrac{1}{8}}}} = 3 + \cfrac{1}{4 + \cfrac{1}{7 + \cfrac{1}{\frac{33}{8}}}}$$

$$= 3 + \cfrac{1}{4 + \cfrac{1}{7 + \cfrac{8}{33}}} = 3 + \cfrac{1}{4 + \cfrac{1}{\frac{239}{3}}}$$

$$= 3 + \cfrac{1}{4 + \frac{39}{239}} = 3 + \cfrac{1}{\frac{989}{239}} = 3 + \frac{239}{989} = \frac{3206}{989}$$

Algunas veces es conveniente escribir una fracción continua simple, tal como se muestra en el Ejemplo anterior, esta escrita en forma abreviada. □

Ejemplo 1.6. *Expresar* $-\frac{16}{9}$ *como una fracción continua simple.*

Solución: Por el Algoritmo de Euclides se tiene que:

$$\begin{array}{r|l} -16 & 9 \\ \hline 2 & -2 \end{array} \qquad -16 = (-2)\cdot 9 + 2 \qquad 0 \le 2 < 9$$

$$\begin{array}{r|l} 9 & 2 \\ \hline 1 & 4 \end{array} \qquad 9 = 4\cdot 2 + 1 \qquad 0 \le 1 < 2$$

$$\begin{array}{r|l} 2 & 1 \\ \hline 0 & 2 \end{array} \qquad 2 = 2\cdot 1 + 0$$

Luego: Lo expresamos como una fracción continua. Ahora,

$$-\frac{16}{9} = -2 + \frac{2}{9} = -2 + \cfrac{1}{\frac{9}{2}} = -2 + \cfrac{1}{4 + \frac{1}{2}}$$

Por lo tanto, $-\frac{16}{9} = [-2, 4, 2]$ se escogió -2 para el entero a_1 con el fin de que los términos restantes pudieran ser enteros positivos. □

Nota. *El siguiente teorema es necesario para el desarrollo del método de las fracciones continuas que corresponde resolver ecuaciones diofánticas lineales mediante una técnica muy practica, ya que permite hallar una solución particular de la ecuación de la forma $ax + by = c$.*

Teorema 1.5.4. *Dada la fracción continua simple $[a_1, a_2, \ldots, a_j]$, cuyos convergentes podemos representar por:*

$$c_1 = [a_1] = \frac{p_1}{q_1}, c_2 = [a_1, a_2] = \frac{p_2}{q_2}, \ldots, c_j = [a_1, a_2, \ldots, a_j] = \frac{p_j}{q_j}$$

Se cumple que:

$$p_j q_{j-1} - q_j p_{j-1} = (-1)^j$$

O bien:

$$c_j - c_{j-1} = \frac{(-1)^j}{q_j q_{j-1}}$$

Demostración: Utilizando el método de inducción matemática.

En efecto, supongamos que es valido para $j = 2$.

$$c_2 = [a_1, a_2] = a_1 + \frac{1}{a_2} = \frac{a_1 a_2 + 1}{a_2}$$

Luego,

$$p_2 q_1 - q_2 p_1 = (a_1 a_2 + 1) \cdot 1 - a_1 a_2 = 1 = (-1)^2$$

Vemos que el resultado anterior es valido para $j = 2$.

Supongamos que es valido para $j = k$:

$$p_k q_{k-1} - q_k p_{k-1} = (-1)^k$$

Ahora, supongamos que es valido para $j = k + 1$:

$$\begin{aligned} p_{k+1} q_k - p_k q_{k-1} &= (a_{k+1} p_k + p_{k-1}) \cdot q_k - p_k \cdot (a_{k+1} q_k + q_{k-1}) \\ &= a_{k+1} p_k q_k + p_{k-1} q_k - p_k a_{k+1} q_k - p_k q_{k-1} \\ &= -(p_k q_{k-1} - p_{k-1} q_k) \\ &= -(-1)^k \\ &= (-1)^{k+1} \end{aligned}$$

En consecuencia, se verifica que para todo entero positivo j: $p_j q_{j-1} - q_j p_{j-1} = (-1)^j$ y la segunda expresión $c_j - c_{j-1} = \frac{(-1)^j}{q_j q_{j-1}}$ es inmediata, pues dividiendo por $q_j q_{j-1}$ tenemos lo siguiente:

$$\frac{p_j q_{j-1} - q_j p_{j-1}}{q_j q_{j-1}} = \frac{p_j q_{j-1}}{q_j q_{j-1}} - \frac{q_j p_{j-1}}{q_j q_{j-1}} = \frac{p_j}{q_j} - \frac{p_{j-1}}{q_{j-1}}$$

Ahora,

$$\frac{p_j}{q_j} - \frac{p_{j-1}}{q_{j-1}} = c_j - c_{j-1} = \frac{(-1)^j}{q_j q_{j-1}}$$

□

1.6. Congruencias Modulares

Definición 1.6.1. *Sean $a, b, m \in \mathbb{Z}$, con $m > 1$. se dice que a es congruente con b módulo m si y solo si $m/(a-b)$ y se denota por $a \equiv b \pmod{m}$. Expresión que fué ideada por Gauss.*
Cuando a y b no sean congruentes módulo m, se denota por $a \not\equiv b \pmod{m}$, en tal caso; $m \nmid (a-b)$.
Otra manera de interpretar la congruencia módulo m entre a y b es observando que los residuos de dividir a y b por m coinciden. Recordar que los posibles residuos de dividir por m, son: $0, 1, 2, \ldots, m-1$.

Ejemplo 1.7. *Se tiene que $27 \equiv 19 \pmod{4}$ por Definición 1.6.1. Se observa que:*

Solución:

$$\begin{array}{r|l} 27 & 4 \\ 3 & 6 \end{array} \quad ; \quad 27 = 6 \times 4 + 3 \quad \text{y} \quad \begin{array}{r|l} 19 & 4 \\ 3 & 4 \end{array} \quad ; \quad 19 = 4 \times 4 + 3$$

Luego tenemos que $4/(27-19)$ entonces, $\begin{array}{r|l} 8 & 4 \\ 0 & 2 \end{array}$; $8 = 2 \times 4 + 0$

Otra forma de verlo, es observando que 27 y 19 tienen el mismo residuo al dividir por 4. □

Notar que si $a \equiv b \pmod{m}$ esto se puede expresar de las siguientes maneras:

i) $m/(a-b)$.

ii) $a - b = km$, donde k es un entero.

iii) $a = km + b$.

Teorema 1.6.2. *Sean a y b enteros arbitrarios. Entonces $a \equiv b \pmod{m}$ si y solo si a y b dejan el mismo residuo al ser divididos por m.*

Demostración: ($\Rightarrow$) Suponga que $a \equiv b \pmod{m}$ entonces existe un entero k tal que $a = km + b$. Como b y m son enteros, por el Algoritmo de la División Teorema 1.2.1 existen enteros q y r tales que:

$$b = qm + r \ ; \text{ con } \ 0 \leq r < m$$

es decir, r es el resto cuando b es dividido por m.
Ahora, debemos ver que r es el resto cuando a es dividido por m.
Como $a = km + b$, luego $a = (qm + r) + km$ o sea que, $a = qm + km + r = (q + k)\, m + r$ como $(q + k)$ es un entero, es decir, r es también el resto de la división de a por m.

($\Leftarrow$) Suponga que a y b dejan el mismo residuo al ser divididos por m, es decir:

$$a = q_1 m + r \ \text{ y } \ b = q_2 m + r \ , \ 0 \leq r < m$$

restando se obtiene $a - b = (q_1 - q_2)\, m$, como $(q_1 - q_2)\, m$ es un entero, $m/(a-b)$, es decir, $a \equiv b \pmod{m}$. □

Definición 1.6.3. *La congruencia módulo m es una* ***relación de equivalencia*** *puesto que se verifican las siguientes propiedades:*

i) **Reflexiva**: $a \equiv a \pmod{m}$, para todo $a \in \mathbb{Z}$.

ii) **Simétrica**: $a \equiv b \pmod{m}$ entonces $b \equiv a \pmod{m}$, para todo par de enteros a y b.

iii) **Transitiva**: $a \equiv b \pmod{m}$ y $b \equiv c \pmod{m}$ entonces $a \equiv c \pmod{m}$, para toda terna de enteros a, b y c.

Seguidamente, se presenta la demostración de la Transitividad.

Demostración: Como $a \equiv b \pmod{m}$ y $b \equiv c \pmod{m}$, $m/(a-b)$ y $m/(b-c)$, luego existen $p, q \in \mathbb{Z}$ tales que:

$$a - b = mp \text{ y } b - c = mq$$

respectivamente. Sumando se obtiene:

$$a - c = mp + mq = (p+q)\, m$$

Como $(p+q)$ es un entero, $m/(a-c)$; es decir $a \equiv c \pmod{m}$. □

Definición 1.6.4. *Dado un entero a se denomina **clase de equivalencia** asociada con a respecto a la congruencia módulo m, a todos lo enteros que sean congruentes con a módulo m. Esta clase se denota por $[a]_m$. Es decir:*

$$[a]_m = \{a' \in \mathbb{Z} \mid a' \equiv a \pmod{m}\}$$

Otras presentaciones para la clase de equivalencia de a son las siguientes:

$$[a]_m = \{a + mk \mid k \in \mathbb{Z}\}$$
$$[a]_m = \{b \text{ en } \mathbb{Z} \mid a = km + b,\ k \in \mathbb{Z}\}$$

Ejemplo 1.8. *Mediante la relación de congruencia módulo 4, las clases de equivalencia del $0, 1, 2, 3$ son respectivamente las siguientes:*

Comencemos con la clase del 0:

$$[0]_4 = \{0 + 4k \mid k \in \mathbb{Z}\} = \{\ldots, -8, -4, 0, 4, 8, \ldots\},$$

Vamo con la clase del 1:

$$[1]_4 = \{1 + 4k \mid k \in \mathbb{Z}\} = \{\ldots, -9, -5, 1, 5, 9, \ldots\},$$

Vamo con la clase del 2:

$$[2]_4 = \{2 + 4k \mid k \in \mathbb{Z}\} = \{\ldots, -10, -6, 2, 6, 10, \ldots\},$$

Por ultimo con la clase del 3:

$$[3]_4 = \{3 + 4k \mid k \in \mathbb{Z}\} = \{\ldots, -11, -7, 3, 7, 11, \ldots\}.$$

En este caso el conjunto $\mathbb{Z}$ es partido en 4 subconjuntos disjuntos o clases de equivalencia que corresponden a los 4 conjuntos determinados por los residuos 0, 1, 2 y 3. Entonces a los enteros los agrupamos con los que tengan residuo 0, los que tengan residuo 1, los que tengan residuo 2 y los que tengan residuo 3. Todos los que tengan residuo cero son equivalentes entre si porque son congruentes módulo 4, a si mismo, todos los que tengan residuo 1, 2 y 3 son equivalentes entre si bajo la relación de congruencia módulo 4.

Estas clases de equivalencia reciben el nombre de **clases residuales** porque para que dos elementos esten en la misma clase de equivalencia se requieren que tengan el mismo residuo.

En general, lo anterior permite agrupar a los enteros en conjuntos disjuntos de manera que dos números enteros son congruentes módulo m si y solo si están en la misma clase residual. Por otro lado, toda relación de equivalencia determina una partición del conjunto donde se define, es decir, los divide en subconjuntos que no son vacíos, son disjuntos dos a dos y eso reproduce todo el conjunto. A esta partición del conjunto se le denomina **conjunto cociente** y se designa por $\mathbb{Z}/R$.

Donde R es la congruencia modulo 4 definida mediante la condición $a \equiv b \pmod{4}$.

$$\mathbb{Z}/R = \{\,[0], [1], [2], [3]\,\}$$

por Definición 1.6.3 se deducen las siguientes propiedades relativas a la relación de congruencia definida en el conjunto de los enteros.

Teorema 1.6.5. *Sean* $a \equiv b \pmod{m}$ *y* $a' \equiv b' \pmod{m}$. *Entonces:*

a) Si $a \equiv b \pmod{m}$ y $a' \equiv b' \pmod{m}$, entonces $a + a' \equiv b + b' \pmod{m}$.

b) Si $a \equiv b \pmod{m}$ y $a' \equiv b' \pmod{m}$, entonces $a - a' \equiv b - b' \pmod{m}$.

c) Si $a \equiv b \pmod{m}$ y $a' \equiv b' \pmod{m}$, entonces $aa' \equiv bb' \pmod{m}$.

d) Si $a \equiv b \pmod{m}$ y c es un entero, entonces $a + c \equiv b + c \pmod{m}$.

e) Si $a \equiv b \pmod{m}$ y c es un entero, entonces $ac \equiv bc \pmod{m}$.

f) Si $ac \equiv bc \pmod{m}$ y $(c, m) = 1$, entonces $a \equiv b \pmod{m}$.

g) Si $a \equiv b \pmod{m}$ y d/m, entonces $a \equiv b \pmod{d}$.

h) Sea $c \neq 0$, $ac \equiv bc \pmod{m}$ y $(c, m) = d$, entonces $a \equiv b \pmod{m/d}$.

Demostración: Teorema 1.6.5

a) Como $a \equiv b \pmod{m}$, entonces existe un entero k tal que $a = km + b$, de la misma manera, como $a' \equiv b' \pmod{m}$, entonces existe un entero q tal que $a' = qm + b'$. Luego,

$$\begin{aligned} a + a' &= km + b + qm + b' \\ &= (b + b') + km + qm \\ &= (b + b') + (k + q)\, m \end{aligned}$$

Como $(k + q)$ es un entero, por definición de relación de congruencia se tiene que:

$$\boldsymbol{a + a' \equiv b + b' \pmod{m}}$$

b) Como $a \equiv b \pmod{m}$, entonces existe un entero k tal que $a = km + b$, de la misma manera, como $a' \equiv b' \pmod{m}$, entonces existe un entero q tal que $a' = qm + b'$. Luego,

$$\begin{aligned} a - a' &= km + b - (qm + b') \\ &= km + b - qm - b' \\ &= (b - b') + (k - q)\, m \end{aligned}$$

Como $(k - q)$ es un entero, por definición de relación de congruencia se tiene que:

$$\boldsymbol{a - a' \equiv b - b' \pmod{m}}$$

c) Como $a \equiv b \pmod{m}$, entonces existe un entero k tal que $a = km + b$, de la misma manera, como $a' \equiv b' \pmod{m}$, entonces existe un entero q tal que $a' = qm + b'$. Luego,

$$\begin{aligned} aa' &= (km + b)\,(qm + b') \\ &= kmqm + kmb' + bqm + bb' \\ &= bb' + (bq + kb' + kqm)\, m \end{aligned}$$

Como $(bq + kb' + kqm)$ es un entero, por definición de relación de congruencia se tiene que:

$$\boldsymbol{aa' \equiv bb' \pmod{m}}$$

d) Como $a \equiv b \pmod{m}$, entonces existe un entero k tal que $a = km + b$. Luego,

$$\begin{aligned} a + c &= km + b + c \\ &= (b + c) + km \end{aligned}$$

Por definición de relación de congruencia se tiene que:

$$\boldsymbol{a + c \equiv b + c \pmod{m}}$$

e) Como $a \equiv b \pmod{m}$, entonces existe un entero k tal que $a = km + b$. Luego,

$$\begin{aligned} ac &= (km + b)\, c \\ &= bc + kmc \\ &= bc + (kc)\, m \end{aligned}$$

Como (kc es un entero, por definición de relación de congruencia se tiene que:

$$\boldsymbol{ac \equiv bc \pmod{m}}$$

f) Como $ac \equiv bc \pmod{m}$, entonces por Definición 1.6.1 $m/(ac - bc)$; esto es, $m/c\,(a - b)$. Por hipótesis como $(c, m) = 1$, por el Teorema 1.3.6 sigue que $m/(a - b)$. Por lo tanto, $a \equiv b \pmod{m}$.

Nota. *Se deduce que* ***f)*** *se puede dividir sin problema en congruencias modulares por un número, siempre y cuando este sea* ***primo relativo*** *con el módulo.*

g) Como $a \equiv b \pmod{m}$, entonces existe un entero k tal que $a - b = km$. Por hipótesis d/m, entonces existe un entero q tal que $m = qd$. Luego,

$$a - b = k\,(qd) = (kq)\, d$$

Como (kq) es un entero, en consecuencia $d/(a - b)$, por definición de relación de congruencia se tiene que:

$$\boldsymbol{a \equiv b \pmod{d}}$$

h) Como $ac \equiv bc \pmod{m}$, entonces por Definición 1.6.1 $m/(ac - bc)$; esto es, $m/c\,(a - b)$. Por hipótesis el $(c, m) = d$, entonces existen números enteros k y q tal que $c = dk$ y $m = dq$ respectivamente. Luego tenemos que,

$$dq/dk\,(a - b)$$

$$q/k\,(a - b)$$

donde $(q, k) = 1$, por el Teorema 1.3.6 se tiene que $q/(a - b)$.
Por tanto, por relación de congruencia $a \equiv b \pmod{q}$ como $m = dq$, luego $\boldsymbol{a \equiv b \pmod{m/d}}$. □

A manera de ilustración del Teorema 1.6.5 veamos que:

Ejemplo 1.9. *Sea las siguientes relaciones de congruencia* $22 \equiv 14 \pmod{4}$*;* $11 \equiv 7 \pmod{4}$ *y* $c = 5$*, entonces.*

Solución:

a) Tenemos las relaciones de congruencia $22 \equiv 14 \pmod{4}$ y $11 \equiv 7 \pmod{4}$.

$$\begin{aligned} 22 + 11 &\equiv 14 + 7 \pmod{4} \\ 33 &\equiv 21 \pmod{4} \end{aligned}$$

c) Tenemos las relaciones de congruencia $22 \equiv 14 \pmod{4}$ y $11 \equiv 7 \pmod{4}$.

$$\begin{aligned} (22)\,(11) &\equiv (14)\,(7) \pmod{4} \\ 242 &\equiv 98 \pmod{4} \end{aligned}$$

e) Tenemos las relaciones de congruencia $22 \equiv 14 \pmod{4}$ y $c = 5$.

$$\begin{aligned} (22)\,(5) &\equiv (14)\,(5) \pmod{4} \\ 110 &\equiv 70 \pmod{4} \end{aligned}$$

g) Se tiene que $22 \equiv 14 \pmod{4}$; $(22, 14) = 2$ y $22 \equiv 14 \pmod{2}$. □

1.6.1. Inverso Multiplicativo Modular

Definición 1.6.6. *Un elemento a es invertible módulo m si existe a' en $\mathbb{Z}$ tal que $a \cdot a' \equiv 1 \pmod{m}$. En este caso se dice que a' es el inverso de a mediante la congruencia modulo m.*

Teorema 1.6.7. *Un entero a es invertible módulo m si y solo si $(a, m) = 1$. Si a posee inverso entonces este es único.*

Demostración: Como a es invertible módulo m, entonces existe un entero a' tal que $a \cdot a' \equiv 1 \pmod{m}$; por tanto hay un entero k tal que $a \cdot a' + mk = 1$; de ahí que por el Teorema 1.3.3 $(a, m) = 1$. Recíprocamente, como $(a, m) = 1$ entonces existen enteros s, t tales que $as + mt = 1$, de donde $as \equiv 1 \pmod{m}$; por tanto $s = a'$. La **unicidad** módulo m significa que si $a \cdot a' \equiv 1 \pmod{m}$ y $a \cdot a'' \equiv 1 \pmod{m}$ entonces $a' \equiv a'' \pmod{m}$.
Suponga que $a \cdot a' \equiv 1 \pmod{m}$ y $a \cdot a'' \equiv 1 \pmod{m}$, entonces existen k y k' tales que $a \cdot a' + mk = 1$ y $a \cdot a'' + mk' = 1$ respectivamente. Luego restando se obtiene:

$$a\,(a' - a'') + m\,(k - k') = 0$$

Como $(k - k')$ es un entero, por relación de congruencia $a\,(a' - a'') \equiv 0 \pmod{m}$, o bien, $m/a\,(a' - a'')$ pero como $(a, m) = 1$ entonces $m/\,(a' - a'')$. Por tanto $a' \equiv a'' \pmod{m}$. □

Ejemplo 1.10. *Encontrar el inverso multiplicativo de 24 para la siguiente congruencia modular,* $24 \equiv 17 \pmod{7}$.
*Para este caso, se debe encontrar un entero a' tal que $a' \cdot 24 \equiv 1 \pmod{7}$. Luego, $24a' + 7k = 1$ para algún $k \in \mathbb{Z}$. Como $(7, 24) = 1$, entonces se puede encontrar los valores de a' y k, ya que por medio del **Algoritmo de Euclides** $(7, 24) = 1$ se puede expresar como una combinación lineal de dichos números.*

Solución:

$$\begin{array}{r|l} 24 & 7 \\ \hline 3 & 3 \end{array} \qquad 24 = 3 \cdot 7 + 3 \qquad 0 \leq 3 < 7$$

$$\begin{array}{r|l} 7 & 3 \\ \hline 1 & 2 \end{array} \qquad 7 = 2 \cdot 3 + 1 \qquad 0 \leq 1 < 3$$

$$\begin{array}{r|l} 3 & 1 \\ \hline 0 & 3 \end{array} \qquad 3 = 3 \cdot 1 + 0$$

Luego: $(7, 24) = 1$. Ahora,

$$\begin{aligned} 1 &= 7 - 2 \cdot 3 \\ &= 7 - 2 \cdot (24 - 3 \cdot 7) \\ &= 7 - 2 \cdot 24 + 6 \cdot 7 \\ &= 7 \cdot 7 - 2 \cdot 24 \\ &= 7 \cdot (7) + 24 \cdot (-2) \end{aligned}$$

Así que el inverso multiplicativo de 24 mediante la relación de congruencia módulo 7 es -2, obsérvese que cualquier otro entero equivalente a -2 módulo 7 es un inverso multiplicativo de 24.
Para mayor claridad se tiene la siguiente ilustración:

$$5 \equiv -2 \pmod{7}\ ;\ 5 \cdot 24 \equiv 1 \pmod{7}\ ;\ 120 \equiv 1 \pmod{7}$$

de la misma manera,

$$12 \equiv -2 \pmod{7}\ ;\ 12 \cdot 24 \equiv 1 \pmod{7}\ ;\ 288 \equiv 1 \pmod{7}$$

nos damos cuenta que 5 y 12 también son inversos multiplicativos de 24.

Nota. *Normalmente se escoge como inverso multiplicativo modular el menor entero positivo de la clase. Claramente se observa que el inverso multiplicativo no es un número, es toda una clase.*
Así se tiene que el inverso multiplicativo elegido de 24 en $\mathbb{Z}$ mediante la relación de congruencia módulo 7 es 5. □

1.6.2. Congruencias Lineales

Definición 1.6.8. *Una congruencia lineal módulo m es un enunciado de la forma $ax \equiv b \pmod{m}$, donde $m \nmid a$.*

Teorema 1.6.9. *Si $(a, m) = 1$, entonces $ax \equiv 1 \pmod{m}$ tiene solución única $x \equiv a^{-1} \pmod{m}$.*

Demostración: Como la congruencia lineal $ax \equiv 1 \pmod{m}$ es equivalente a resolver la ecuación $ax + km = 1$ con $k \in \mathbb{Z}$. Si $(a, m) = 1$ entonces existen a' y k' enteros tal que $a \cdot a' + m \cdot k' = 1$, con lo que tenemos la solución $x = a'$ para la ecuación $ax \equiv 1 \pmod{m}$.

La unicidad módulo m significa que si $a \cdot a' \equiv 1 \pmod{m}$ y $a \cdot a'' \equiv 1 \pmod{m}$ tendremos lo siguiente $a' \equiv a'' \pmod{m}$. Para verificar que la solución es única módulo m, supongamos que $a \cdot a'' \equiv 1 \pmod{m}$, luego, restando tenemos $a(a' - a'') \equiv 0 \pmod{m}$ entonces $m \mid a(a' - a'')$ pero como $(a, m) = 1$ luego $m \mid (a' - a'')$ por tanto $a' \equiv a'' \pmod{m}$. □

Teorema 1.6.10. *La congruencia lineal $ax \equiv b \pmod{m}$ tiene exactamente d soluciones, donde $(a, m) = d$, si y solo si $d \mid b$. Si $d \nmid b$ entonces la congruencia lineal no tiene solución.*

Demostración: Por definición, la congruencia lineal $ax \equiv b \pmod{m}$ implica $ax = b + km$, donde $k \in \mathbb{Z}$; o bien, $ax + km = b$. En consecuencia cualquier divisor de a y m debe dividir a b. Por lo tanto, si $(a, m) = d$, no existe solución si $d \nmid b$.

Si $d \mid b$ entonces

$$a = d \cdot a',\ m = d \cdot m' \text{ y } b = d \cdot b'$$

donde $(a', m') = 1$ por el teorema 1.6.5 (h) como $(m, d) = d$.

$$a'x \equiv b' \pmod{m'}$$

Como $(a', m') = 1$ por el teorema 1.6.9 existe exactamente una solución $x \equiv x_0 \pmod{m'}$ de esta congruencia lineal 1.6.9 es también solución de la congruencia lineal:

$$ax \equiv b \pmod{m}$$

Las soluciones de la congruencia lineal 1.6.9 son de la forma:

$$x = x_0 + km' \pmod{m'}, \text{ donde } k \in \mathbb{Z}$$

como $m' = \frac{m}{d}$, las soluciones de la congruencia lineal $ax \equiv b \pmod{m}$ son de la forma:

$$x = x_0 + k\frac{m}{d}, \text{ donde } 0 \leq k < d$$

o bien,

$$x_0, x_0 + \frac{m}{d}, x_0 + 2\frac{m}{d}, \ldots, x_0 + (d-1)\frac{m}{d}$$ □

Para resolver las ecuaciones en congruencias modulares se pueden utilizar dos métodos que incluso, se pueden manejar simultáneamente.

1) Utilizando la relación de congruencia modular y sus propiedades.

2) Convirtiéndolos en ecuaciones de la forma $ax + km = b$, donde k es un número entero.

Para ilustrar los Teoremas anteriores se consideran las siguientes congruencias modulares:

a) Resolver $5x \equiv 3 \pmod 7$.
Primero calculamos el máximo común divisor de 5 y 7 y luego lo expresamos como una combinación lineal, (para ello hacemos uso del Algoritmo de la División).

$$\begin{array}{r|l} 7 & 5 \\ 2 & 1 \end{array} \qquad 7 = 1 \cdot 5 + 2 \qquad 0 \leq 2 < 5$$

$$\begin{array}{r|l} 5 & 2 \\ 1 & 2 \end{array} \qquad 5 = 2 \cdot 2 + 1 \qquad 0 \leq 1 < 2$$

$$\begin{array}{r|l} 2 & 1 \\ 0 & 2 \end{array} \qquad 2 = 2 \cdot 1 + 0$$

Luego: $(5, 7) = 1$. según el teorema 1.6.9 la ecuación $5x \equiv 3 \pmod 7$ tiene solución única. Ahora,

$$\begin{aligned} 1 &= 5 - 2 \cdot 2 \\ &= 5 - 2 \cdot (7 - 1 \cdot 5) \\ &= 5 - 2 \cdot 7 + 2 \cdot 5 \\ &= 3 \cdot 5 - 2 \cdot 7 \\ &= 5 \cdot (3) + 7 \cdot (-2) \end{aligned}$$

Así que, lo siguiente corresponde:

$$\begin{aligned} x &= (3) \cdot 3 \pmod 7 \\ x &= 9 \pmod 7 \\ x &= 2 \end{aligned}$$

decimos que 9 mód 7 es el residuo obtenido de la división de 9 entre 7, luego 9 mód $7 = 2$.

$$\begin{aligned} 5 \cdot (2) &\equiv 3 \pmod 7 \\ 10 \text{ mód } 7 &= 3 \text{ mód } 7 \\ 3 &= 3 \end{aligned}$$

El inverso de 5 mód 7 es **3**.

Multiplicando a ambos lados de la congruencia tenemos que:

$$\begin{aligned} 5 \cdot (3)\, x &\equiv 3 \cdot (3) \pmod 7 \\ 15x &\equiv 9 \pmod 7 \\ x &\equiv 9 \pmod 7 \\ x &= 2 \end{aligned}$$

vemos que 15 mód 7 es el residuo obtenido de la división de 15 entre 7, luego 15 mód $7 = 1$.

Por lo tanto, la solución para la ecuación $5x \equiv 3 \pmod 7$ es $x = 2$.

b) Resolver $14x \equiv 11 \pmod 5$.
Primero calculamos el máximo común divisor de 14 y 5 y luego lo expresamos como una combinación lineal, (para ello hacemos uso del Algoritmo de la División).

$$\begin{array}{r|l} 14 & 5 \\ \hline 4 & 2 \end{array} \qquad 14 = 2 \cdot 5 + 4 \qquad 0 \leq 4 < 5$$

$$\begin{array}{r|l} 5 & 4 \\ \hline 1 & 1 \end{array} \qquad 5 = 1 \cdot 4 + 1 \qquad 0 \leq 1 < 4$$

$$\begin{array}{r|l} 4 & 1 \\ \hline 0 & 4 \end{array} \qquad 4 = 4 \cdot 1 + 0$$

Luego: $(14, 5) = 1$. según el teorema 1.6.9 la ecuación $14x \equiv 11 \pmod 5$ tiene solución única. Ahora,

$$\begin{aligned} 1 &= 5 - 1 \cdot 4 \\ &= 5 - 1 \cdot (14 - 2 \cdot 5) \\ &= 5 - 1 \cdot 14 + 2 \cdot 5 \\ &= 3 \cdot 5 - 1 \cdot 14 \\ &= 14 \cdot (-1) + 5 \cdot (3) \end{aligned}$$

Así que, lo siguiente corresponde:

$$\begin{aligned} x &= (-1) \cdot 11 \pmod 5 \\ x &= -11 \pmod 5 \\ x &= 4 \end{aligned}$$

decimos que -11 mód 5 es el residuo obtenido de la división de 11 entre 5, luego -11 mód $5 = 4$. Observemos que a mód b es el residuo obtenido de la división de a entre b, $\frac{a}{b}$ = Cociente+Residuo si $a < 0$, a mód $b = b -$ Residuo. Como $a = -11$, $b = 5$ el Residuo=1 si $-11 < 0$, por lo tanto -11 mód $5 = 5 - 1 = 4$

$$\begin{aligned} 14 \cdot (4) &\equiv 11 \pmod 5 \\ 56 \text{ mód } 5 &= 11 \text{ mód } 5 \\ 1 &= 1 \end{aligned}$$

El inverso de 14 mód 5 es **-1**.

Multiplicando a ambos lados de la congruencia tenemos que:

$$\begin{aligned} 14 \cdot (-1)\, x &\equiv 11 \cdot (-1) \pmod 5 \\ -14x &\equiv -11 \pmod 5 \\ x &\equiv -11 \pmod 5 \\ x &= 4 \end{aligned}$$

vemos que -14 mód 5 es el residuo obtenido de la división de 14 entre 5, luego -14 mód $5 = 1$.

Por lo tanto, la solución para la ecuación $14x \equiv 11 \pmod 5$ es $x = 4$.

c) Resolver $8x \equiv 16 \pmod{12}$.
Primero calculamos el máximo común divisor de 8 y 12 y luego lo expresamos como una combinación lineal, (para ello hacemos uso del Algoritmo de la División).
como el $(8, 12) = 4$; $4 \mid 16$ entonces la ecuación tiene 4 soluciones, vemos que nuestra ecuación $2x \equiv 4 \pmod{3}$, luego calculamos el máximo común divisor de 2 y 3.

$$\begin{array}{r|l} 3 & 2 \\ \hline 1 & 1 \end{array} \qquad 3 = 1 \cdot 2 + 1 \qquad 0 \leq 1 < 2$$

$$\begin{array}{r|l} 2 & 1 \\ \hline 0 & 2 \end{array} \qquad 2 = 2 \cdot 1 + 0$$

Luego: $(2, 3) = 1$. Ahora,

$$\begin{aligned} 1 &= 3 - 1 \cdot 2 \\ &= 2 \cdot (-1) + 3 \cdot (1) \end{aligned}$$

Así que, lo siguiente corresponde:

$$\begin{aligned} x &= (-1) \cdot 4 \pmod{3} \\ x &= -4 \pmod{3} \\ x &= 2 \end{aligned}$$

decimos que -4 mód 3 es el residuo obtenido de la división de 4 entre 3, luego -4 mód $3 = 2$. Observemos que a mód b es el residuo obtenido de la división de a entre b, $\frac{a}{b}$ = Cociente+Residuo si $a < 0$, a mód $b = b -$ Residuo. Como $a = -4$, $b = 3$ el Residuo=1 si $-4 < 0$, por lo tanto -4 mód $3 = 3 - 1 = 2$

$$\begin{aligned} 2 \cdot (2) &\equiv 4 \pmod{3} \\ 4 \text{ mód } 3 &= 4 \text{ mód } 3 \\ 1 &= 1 \end{aligned}$$

El inverso de 2 mód 3 es $\mathbf{-1}$.

Multiplicando a ambos lados de la congruencia tenemos que:

$$\begin{aligned} 2 \cdot (-1)\, x &\equiv 4 \cdot (-1) \pmod{3} \\ -2x &\equiv -4 \pmod{3} \\ x &\equiv -4 \pmod{3} \\ x &= 2 \end{aligned}$$

vemos que -2 mód 3 es el residuo obtenido de la división de 2 entre 3, luego -2 mód $3 = 1$.

Observemos que $x = x_0 + 3k$; $3 \mid (x - 2)$, por lo tanto $3k = x - 2$ $k \in \mathbb{Z}$ luego:

$$x = 2 + 3k \ ; \ 0 \leq k < 4$$

Si $k = 0$, se obtiene la solución $x = 2$.
Si $k = 1$, se obtiene la solución $x = 5$.
Si $k = 2$, se obtiene la solución $x = 8$.
Si $k = 3$, se obtiene la solución $x = 11$.

d) Resolver $16x \equiv 4 \pmod{21}$.
Como $(16, 21) = 1$, la ecuación $16x \equiv 4 \pmod{21}$ tiene única solución, por el Teorema 1.6.10 y el Algoritmo de Euclides se tiene que:

$$16s + 21t = 1, \text{ donde } s, t \text{ son enteros}$$

Resolviendo,

$$\begin{array}{r|l} 21 & 16 \\ \hline 5 & 1 \end{array} \qquad 21 = 1 \cdot 16 + 5 \qquad 0 \leq 5 < 16$$

$$\begin{array}{r|l} 16 & 5 \\ \hline 1 & 3 \end{array} \qquad 16 = 3 \cdot 5 + 1 \qquad 0 \leq 1 < 5$$

$$\begin{array}{r|l} 5 & 1 \\ \hline 0 & 5 \end{array} \qquad 5 = 5 \cdot 1 + 0$$

Luego: $(16, 21) = 1$. Ahora,

$$\begin{aligned} 1 &= 16 - 3 \cdot 5 \\ &= 16 - 3 \cdot (21 - 1 \cdot 16) \\ &= 16 - 3 \cdot 21 + 3 \cdot 16 \\ &= 4 \cdot 16 - 3 \cdot 21 \\ &= 16 \cdot (4) + 21 \cdot (-3) \end{aligned}$$

Así que, $s = 4$ y obsérvese que s es el inverso multiplicativo de 26. Luego,

$$\begin{aligned} (4)(16)\, x &\equiv (4)(4) \pmod{21} \\ x &\equiv 16 \pmod{21} \end{aligned}$$

Por tanto, la solución de la ecuación $16x \equiv 4 \pmod{21}$ es $x = 16$.

e) Resolver $12x \equiv 98 \pmod{20}$.
Como $(12, 20) \nmid 98$. Por tanto la ecuación de congruencia $12x \equiv 98 \pmod{20}$ no tiene solución, así que $12x \not\equiv 98 \pmod{20}$.

CAPÍTULO 2

MÉTODOS DE SOLUCIÓN DE LAS ECUACIONES DIOFÁNTICAS LINEALES

2.1. Ecuaciones Diofánticas Lineales Mediante el Algoritmo de Euclides

2.1.1. Nota Histórica

Brahmagupta nació (posiblemente) en Ujjain, India, en el 598; y murió también en la india en el 670. Brahmagupta amaba la matemática, al igual que muchos de sus colegas. Cabe admirar aún más su actitud matemática al descubrir que él fue aparentemente el primero que dio una solución general de la Ecuación Diofántica Lineal $ax + by = c$, con a, b, c enteros. Para que esta ecuación tenga soluciones enteras, el máximo común divisor entre a y b debe dividir a c, Brahmagupta sabía que si a y b son primos entre si, entonces todas las soluciones de la ecuación vienen dadas por $x = x_0 + \frac{b}{g}t$, $y = y_0 - \frac{a}{g}t$, siendo $g = (a, b)$, g/c, y la pareja (x_0, y_0) una solución particular de la ecuación y t es un entero arbitrario.
El mérito de Brahmagupta está en haber hallado la formula para generar todas las soluciones enteras de la Ecuación Diofántica Lineal, mientras que su precursor Diofanto solo llego a una solución particular.

2.1.2. Introducción

Las ecuaciones diofánticas que abordaremos en nuestro trabajo de grado son las del siguiente tipo:

$$ax + by = c \text{ y } ax^2 + bx + cy + dy^2 = e$$

Lineales y cuadráticas respectivamente.

Empezaremos con el caso más simple que son las ecuaciones diofánticas lineales de dos y tres variables:

$$ax + by = c \text{ y } ax + by + cz = d \text{ con } a, b, c, d \in \mathbb{Z}$$

Teorema 2.1.1. *La ecuación diofántica lineal $ax + by = c$, tiene soluciones enteras si y solo si g/c, donde $g = (a, b)$.*

Demostración: ($\Rightarrow$) Supongamos que la pareja $(x_0, y_0) \in \mathbb{Z}$ es una solución de $ax + by = c$, vemos que g/c, donde $g = (a, b)$. Como g/a y g/b, entonces g/ax_0 y g/by_0 luego $g/ax_0 + by_0$ o sea que g/c.

($\Leftarrow$) Supongamos que g/c, donde $g = (a, b)$ y veamos que la ecuación $ax + by = c$ admite solución. En efecto: $g = sa + tb$ (por ser g/c y $g = (a, b)$), luego:

$$c = kg = k(sa + tb) = a(ks) + b(kt)$$

esto quiere decir que los valores: $x = ks$ y $y = kt$ forman una solución de la ecuación. □

Cuando una ecuación diofántica tiene solución, es fácil hallar una solución particular usando el Algoritmo de Euclides.

Ejemplo 2.1. *Determinar una solución particular de la ecuación diofántica lineal.*

$$11x + 27y = 4$$

Solución: Mediante el Algoritmo de la División hallamos el máximo común divisor de 11 y 27 (que evidentemente es 1) con el fin de expresarlo, de una vez, como una combinación lineal de dichos números.

$$\begin{array}{r|l} 27 & 11 \\ \hline 5 & 2 \end{array} \qquad 27 = 2 \cdot 11 + 5 \qquad 0 \leq 5 < 11$$

$$\begin{array}{r|l} 11 & 5 \\ \hline 1 & 2 \end{array} \qquad 11 = 2 \cdot 5 + 1 \qquad 0 \leq 1 < 5$$

$$\begin{array}{r|l} 5 & 1 \\ \hline 0 & 5 \end{array} \qquad 5 = 5 \cdot 1 + 0$$

Luego: $(11, 27) = 1$ como $1/4$: $4 = 1 \cdot 4$. Ahora,

$$\begin{aligned} 1 &= 11 - 2 \cdot 5 \\ &= 11 - 2 \cdot (27 - 2 \cdot 11) \\ &= 11 - 2 \cdot 27 + 4 \cdot 11 \\ 1 \cdot (4) &= 11 \cdot (5 \cdot 4) + 27 \cdot (-2 \cdot 4) \\ 4 &= (11) \cdot (20) + (27) \cdot (-8) \end{aligned}$$

Por lo tanto una solución particular de la ecuación diofántica lineal $11x+27y = 4$ corresponde a la pareja $(20, -8)$. □

Ejemplo 2.2. *Determinar una solución particular de la ecuación diofántica lineal.*

$$39x + 26y = 105$$

Solución: Como el máximo común divisor de 39 y 26 es 13 y, ademas, $13 \nmid 105$, la ecuación diofántica lineal $39x + 26y = 105$ no tiene soluciones enteras. □

Teniendo en cuenta lo anterior podemos hallar una **solución general** de la ecuación diofántica lineal. En efecto: tomamos la ecuación diofántica lineal $ax + by = c$, y suponemos que g/c, donde $g = (a, b)$ entonces hay solución. Consideremos la ecuación $ax + by = 0$ denominada la ecuación homogénea correspondiente a la ecuación diofántica lineal $ax + by = c$. la ecuación homogénea podemos escribirla así:

$$\frac{a}{g}x + \frac{b}{g}y = 0 \ ; \ (g \neq 0)$$

Esta ecuación homogénea tiene dos soluciones inmediatas que son:

1. La **primera** solución seria $x = 0$ y $y = 0$ (evidente).

2. La **segunda** la pareja $\left(\frac{b}{g}, \frac{-a}{g}\right)$.

En efecto:

$$a\left(\frac{b}{g}\right) + b\left(\frac{-a}{g}\right) = \frac{ab}{g} - \frac{ab}{g} = \frac{ab - ab}{g} = 0$$

Nota. *Cualquier múltiplo de esta solución, también es solución es decir la pareja* $\left(\frac{b}{g}t, \frac{-a}{g}t\right)$; $t \in \mathbb{Z}$.

En efecto:

$$a\left(\frac{b}{g}t\right) + b\left(\frac{-a}{g}t\right) = \frac{abt}{g} - \frac{abt}{g} = \frac{abt - abt}{g} = 0$$

A las soluciones del tipo $x = \left(\frac{b}{g}\right)t$ y $y = \left(\frac{-a}{g}\right)t$ *con* $t \in \mathbb{Z}$ se les conoce como **solución general** de la ecuación diofántica lineal homogénea.

De otra parte si la pareja (x_0, y_0) son una solución particular de la ecuación diofántica lineal $ax+by = c$ entonces $ax_0 + by_0 = c$.

Luego se tiene que: $ax + by = ax_0 + by_0$,
Agrupamos los términos:

$$ax - ax_0 = by_0 - by,$$
$$a(x - x_0) = b(y_0 - y),$$

entonces,

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

Lo cual significa que $(x - x_0)$ y $(y - y_0)$ son solución de la ecuación homogénea. así que:

$$x - x_0 = \left(\frac{b}{g}\right)t \text{ y } y - y_0 = \left(\frac{-a}{g}\right)t \text{ con } t \in \mathbb{Z}$$

así que:

$$x = x_0 + \left(\frac{b}{g}\right)t \text{ y } y = y_0 - \left(\frac{a}{g}\right)t \text{ con } t \in \mathbb{Z}$$

Resumiendo lo anterior, se ha demostrado el siguiente teorema que dice:

Teorema 2.1.2. *Si* $g = (a, b)$, g/c *y la pareja* (x_0, y_0) *es una solución particular de la ecuación diofántica lineal* $ax + by = c$ *entonces la pareja* (x, y) *esta dada por las ecuaciones:*

$$x = x_0 + \left(\frac{b}{g}\right)t \text{ y } y = y_0 - \left(\frac{a}{g}\right)t \text{ con } t \in \mathbb{Z}$$

Ejemplo 2.3. *Determinar las soluciones enteras y positivas de la ecuación diofántica lineal.*

$$18x + 5y = 48$$

Solución: Mediante el Algoritmo de la División hallamos el máximo común divisor de 18 y 5 (que evidentemente es 1) con el fin de expresarlo, de una vez, como una combinación lineal de dichos números.

$$\begin{array}{r|l} 18 & 5 \\ \hline 3 & 3 \end{array} \qquad 18 = 3 \cdot 5 + 3 \qquad 0 \leq 3 < 5$$

$$\begin{array}{r|l} 5 & 3 \\ \hline 2 & 1 \end{array} \qquad 5 = 1 \cdot 3 + 2 \qquad 0 \leq 2 < 3$$

$$\begin{array}{r|l} 3 & 2 \\ \hline 1 & 1 \end{array} \qquad 3 = 1 \cdot 2 + 1 \qquad 0 \leq 1 < 2$$

$$\begin{array}{r|l} 2 & 1 \\ \hline 0 & 2 \end{array} \qquad 2 = 2 \cdot 1 + 0$$

Luego: $(18, 5) = 1$ como $1/48$: $48 = 1 \cdot 48$. Ahora,

$$\begin{aligned} 1 &= 3 - 1 \cdot 2 \\ &= 3 - 1 \cdot (5 - 1 \cdot 3) \\ &= 3 - 1 \cdot 5 + 1 \cdot 3 \\ &= 2 \cdot 3 - 1 \cdot 5 \\ &= 2 \cdot (18 - 3 \cdot 5) - 1 \cdot 5 \\ &= 2 \cdot 18 - 6 \cdot 5 - 1 \cdot 5 \\ &= 18 \cdot 2 - 5 \cdot 7 \\ 1 \cdot (48) &= 18 \cdot (2 \cdot 48) + 5 \cdot (-7 \cdot 48) \\ 48 &= 18 \cdot (96) + 5 \cdot (-336) \end{aligned}$$

Por lo tanto una solución particular de la ecuación diofántica lineal $18x + 5y = 48$ corresponde a la pareja $(96, -336)$.

Teniendo en cuenta que la ecuación homogénea correspondiente es:

$$18x + 5y = 0,$$

una solución es: $x = 5$ y $y = -18$.

La solución general de la homogénea es: $x = 5t$ y $y = -18t$ con $t \in \mathbb{Z}$

Por lo tanto la solución general de la no homogénea ($ax + by = c$) esta dada por:

$$x = 96 + (5)\, t \text{ y } y = -336 - (18)\, t \text{ con } t \in \mathbb{Z}$$

Como se ha solicitado hallar las soluciones positivas, estas se pueden obtener o pueden ser obtenidas considerando el sistema de desigualdades.

$$\begin{cases} 96 + 5t > 0 \\ -336 - 18t > 0 \end{cases}$$

Como $96 + 5t > 0$ si $t \geq -19$ y $-336 - 18t > 0$ si $t \leq -19$ entonces el sistema es positivo para $-19,2 < t < -18,6$ como $t \in \mathbb{Z}$ entre el intervalo $-19,2 < t < -18,6$ luego el único entero en este intervalo es $t = -19$.

Reemplazando $t = -19$, tenemos que $x = 96 + 5\,(-19) = 1$ y $y = -336 - 18\,(-19) = 6$ por lo tanto la única solución entera positiva de la ecuación diofántica lineal $18x + 5y = 48$ es la pareja $(1, 6)$. □

2.1.3. Problemas de Aplicación

Ejemplo 2.4. *Una compañia compró cierto número de reliquias falsas a* \$17 *cada una, y vendió algunas de ellas a* \$49 *cada una. si la cantidad comprada originalmente es mayor que* 50 *y menor que* 100*, y la compañia tuvo una ganancia de* \$245*, ¿Cuántas reliquias faltan por vender?*

Sean:

$$x = \textit{número de reliquias falsas compradas}$$
$$y = \textit{número de reliquias vendidas}$$

La cantidad comprada originalmente es mayor que 50 *y menor que* 100 *y la compañia tuvo una ganancia de* \$245*.*

Luego, la ecuación diofántica lineal correspondiente es:

$$-17x + 49y = 245$$

Solución: Mediante el Algoritmo de la División hallamos el máximo común divisor de 17 y 49 (que evidentemente es 1) con el fin de expresarlo, de una vez, como una combinación lineal de dichos números.

$$\begin{array}{r|l} 49 & 17 \\ \hline 15 & 2 \end{array} \qquad 49 = 2 \cdot 17 + 15 \qquad 0 \leq 15 < 17$$

$$\begin{array}{r|l} 17 & 15 \\ \hline 2 & 1 \end{array} \qquad 17 = 1 \cdot 15 + 2 \qquad 0 \leq 2 < 15$$

$$\begin{array}{r|l} 15 & 2 \\ \hline 1 & 7 \end{array} \qquad 15 = 7 \cdot 2 + 1 \qquad 0 \leq 1 < 2$$

$$\begin{array}{r|l} 2 & 1 \\ \hline 0 & 2 \end{array} \qquad 2 = 2 \cdot 1 + 0$$

Luego: $(17, 49) = 1$ como $1/245$: $245 = 1 \cdot 245$. Ahora,

$$\begin{aligned} 1 &= 15 - 7 \cdot 2 \\ &= 15 - 7 \cdot (17 - 1 \cdot 15) \\ &= 15 - 7 \cdot 17 + 7 \cdot 15 \\ &= 8 \cdot 15 - 7 \cdot 17 \\ &= 8 \cdot (49 - 2 \cdot 17) - 7 \cdot 17 \\ &= 8 \cdot 49 - 16 \cdot 17 - 7 \cdot 17 \\ &= 8 \cdot 49 - 23 \cdot 17 \\ 1 \cdot (245) &= (-17) \cdot (23 \cdot 245) + (49) \cdot (8 \cdot 245) \\ 245 &= (-17) \cdot (5635) + (49) \cdot (1960) \end{aligned}$$

Por lo tanto una solución particular de la ecuación diofántica lineal $-17x + 49y = 245$ corresponde a la pareja $(5635, 1960)$.

Teniendo en cuenta que la ecuación homogénea correspondiente es:

$$-17x + 49y = 0,$$

una solución es: $x = 49$ y $y = 17$.

La solución general de la homogénea es: $x = 49t$ y $y = 17t$ con $t \in \mathbb{Z}$

Por lo tanto la solución general de la no homogénea ($ax + by = c$) esta dada por:

$$x = 5635 + (49)\,t \text{ y } y = 1960 + (17)\,t \text{ con } t \in \mathbb{Z}$$

Como se ha solicitado hallar cuántas reliquias faltan por vender, estas se pueden obtener o pueden ser obtenidas considerando el sistema de desigualdades.

$$\begin{cases} 5635 + 49t > 0 \\ 1960 + 17t > 0 \end{cases}$$

La cantidad comprada originalmente es mayor que 50 y menor que 100.

$$50 < x < 100$$

Como $50 < 5635 + 49t < 100$ entonces el sistema es positivo para $-113,9 < t < -112,9$ como $t \in \mathbb{Z}$ entre el intervalo $-113,9 < t < -112,9$ luego el único entero en este intervalo es $t = -113$.

Reemplazando $t = -113$, tenemos que $x = 5635 + 49\,(-113) = 98$ y $y = 1960 + 17\,(-113) = 39$ por lo tanto la única solución entera positiva de la ecuación diofántica lineal $-17x + 49y = 245$ es la pareja $(98, 39)$.

Luego, la cantidad originalmente comprada es de 98 reliquias y la cantidad vendida es de 39 reliquias, entonces la cantidad de reliquias que faltan por vender son de 59 reliquias. □

Ejemplo 2.5. *Pídale a un estudiante que multiplique el día de su cumpleaños por* 12 *y el número del mes en que nació por* 31 *y dígale que sume los resultados.*

*Primero tomaremos la fecha de cumpleaños, (*27 *de Septiembre), ahora haremos lo siguiente:*

1. *Multiplicaremos el día de cumpleaños, que en este caso es* 27 *por 12.*
2. *Luego multiplicaremos el número del mes, que en este caso es* 9 *por 31.*

Sean:

$$x = \textit{día de su cumpleaños}$$
$$y = \textit{número del mes de cumpleaños}$$

Luego sumando estos resultados $324 + 279 = 603$. *La idea es hallar la fecha de cumpleaños conociendo esta suma.*

La ecuación diofántica lineal correspondiente es:

$$12x + 31y = 603$$

Solución: Mediante el Algoritmo de la División hallamos el máximo común divisor de 12 y 31 (que evidentemente es 1) con el fin de expresarlo, de una vez, como una combinación lineal de dichos números.

$$\begin{array}{r|l} 31 & 12 \\ \hline 7 & 2 \end{array} \qquad 31 = 2 \cdot 12 + 7 \qquad 0 \leq 7 < 12$$

$$\begin{array}{r|l} 12 & 7 \\ \hline 5 & 1 \end{array} \qquad 12 = 1 \cdot 7 + 5 \qquad 0 \leq 5 < 7$$

$$\begin{array}{r|l} 7 & 5 \\ \hline 2 & 1 \end{array} \qquad 7 = 1 \cdot 5 + 2 \qquad 0 \leq 2 < 5$$

$$\begin{array}{r|l} 5 & 2 \\ \hline 1 & 2 \end{array} \qquad 5 = 2 \cdot 2 + 1 \qquad 0 \leq 1 < 2$$

$$\begin{array}{r|l} 2 & 1 \\ \hline 0 & 2 \end{array} \qquad 2 = 2 \cdot 1 + 0$$

Luego: $(12, 31) = 1$ como $1/603$: $603 = 1 \cdot 603$. Ahora,

$$\begin{aligned}
1 &= 5 - 2 \cdot 2 \\
&= 5 - 2 \cdot (7 - 1 \cdot 5) \\
&= 5 - 2 \cdot 7 + 2 \cdot 5 \\
&= 3 \cdot 5 - 2 \cdot 7 \\
&= 3 \cdot (12 - 1 \cdot 7) - 2 \cdot 7 \\
&= 3 \cdot 12 - 3 \cdot 7 - 2 \cdot 7 \\
&= 3 \cdot 12 - 5 \cdot 7 \\
&= 3 \cdot 12 - 5 \cdot (31 - 2 \cdot 12) \\
&= 3 \cdot 12 - 5 \cdot 31 + 10 \cdot 12 \\
&= 13 \cdot 12 - 5 \cdot 31 \\
1 \cdot (603) &= (12) \cdot (13 \cdot 603) + (31) \cdot (-5 \cdot 603) \\
603 &= (12) \cdot (7839) + (31) \cdot (-3015)
\end{aligned}$$

Por lo tanto una solución particular de la ecuación diofántica lineal $12x + 31y = 603$ corresponde a la pareja $(7839, -3015)$.

Teniendo en cuenta que la ecuación homogénea correspondiente es:

$$12x + 31y = 0,$$

una solución es: $x = 31$ y $y = -12$.

La solución general de la homogénea es: $x = 31t$ y $y = -12t$ con $t \in \mathbb{Z}$

Por lo tanto la solución general de la no homogénea ($ax + by = c$) esta dada por:

$$x = 7839 + (31)\, t \text{ y } y = -3015 - (12)\, t \text{ con } t \in \mathbb{Z}$$

Como se ha solicitado hallar el día y mes de cumpleaños de cualquier persona, estas se pueden obtener o pueden ser obtenidas considerando el sistema de desigualdades.

$$\begin{cases} 7839 + 31t > 0 \\ -3015 - 12t > 0 \end{cases}$$

Como $7839 + 31t > 0$ si $t \geq -252,8$ y $-3015 - 12t > 0$ si $t \leq -251,2$ entonces el sistema es positivo para $-252,8 < t < -251,2$ como $t \in \mathbb{Z}$ entre el intervalo $-252,8 < t < -251,2$ luego el único entero en este intervalo es $t = -252$.

Reemplazando $t = -252$, tenemos que $x = 7839 + 31\,(-252) = 27$ y $y = -3015 - 12\,(-252) = 9$ por lo tanto la única solución entera positiva de la ecuación diofántica lineal $12x + 31y = 603$ es la pareja $(27, 9)$.

Por lo tanto, la fecha de cumpleaños de esta persona es el día 27 del mes 9 que hace referencia a septiembre. □

2.1.4. Ecuaciónes Diofántica en tres Variables

A Continuación trabajaremos sobre la solución de la ecuación diofántica lineal en tres variables.

Para tal efecto consideremos la ecuación:

$$ax + by + cz = d, \text{ con } a, b, c, d \in \mathbb{Z} \text{ y } g \mid d, \text{ donde } g = (a, b, c)$$

Comenzaremos haciendo $g_1 = (a, b)$ (eligiendo a y b no se pierde generalidad).

Considerando la siguiente ecuación: $ax + by = g_1$, sabemos que toda solución de la pareja (x, y) esta dada por las ecuaciones:

$$x = x_0 + \left(\frac{b}{g_1}\right) t \text{ y } y = y_0 - \left(\frac{a}{g_1}\right) t$$

donde la pareja (x_0, y_0) es una solución particular de la ecuación homogénea y $t \in \mathbb{Z}$.

Ahora, planteamos la ecuación:

$$g_1 s + cz = d,$$

entonces toda solución esta dada por las relaciones:

$$s = s_0 + \left(\frac{c}{g}\right) u \text{ y } z = z_0 - \left(\frac{g_1}{g}\right) u$$

donde la pareja (s_0, z_0) es una solución particular de la ecuación homogénea y $u \in \mathbb{Z}$.

Como $s = s_0 + \left(\frac{c}{g}\right) u$ se tienen finalmente que la solución general de la ecuación diofántica lineal de tres variables esta dada por la tripleta:

$$x = x_0 \left(s_0 + \frac{c}{g}u\right) + \frac{b}{g_1}t \; ; \; y = y_0 \left(s_0 + \frac{c}{g}u\right) - \frac{a}{g_1}t \text{ y } z = z_0 - \frac{g_1}{g}u \text{ con } t, u \in \mathbb{Z}$$

Comprobemos que efectivamente estos valores de x, y y z satisfacen la ecuación $ax + by + cz = d$.

$$\begin{aligned}
ax + by + cz &= a\left(x_0 s_0 + x_0 \frac{c}{g}u + \frac{b}{g_1}t\right) + b\left(y_0 s_0 + y_0 \frac{c}{g}u - \frac{a}{g_1}t\right) + c\,(z) \\
&= \left(ax_0 s_0 + ax_0 \frac{c}{g}u + \frac{ab}{g_1}t\right) + \left(by_0 s_0 + by_0 \frac{c}{g}u - \frac{ba}{g_1}t\right) + c\,(z) \\
&= ax_0 s_0 + by_0 s_0 + ax_0 \frac{c}{g}u + by_0 \frac{c}{g}u + \cancel{\frac{ab}{g_1}t} - \cancel{\frac{ba}{g_1}t} + c\,(z) \\
&= (ax_0 + by_0)\, s_0 + (ax_0 + by_0)\, \frac{c}{g}u + c\,(z) \\
&= (ax_0 + by_0)\left(s_0 + \frac{c}{g}u\right) + c\,(z) \\
&= g_1 s + cz \\
&= d
\end{aligned}$$

Ejemplo 2.6. *Determinar las solución general de la ecuación diofántica lineal.*

$$21x + 14y + 5z = 1$$

Solución: Mediante el Algoritmo de la División hallamos el máximo común divisor de 21 y 14 (que evidentemente es 7) con el fin de expresarlo, de una vez, como una combinación lineal de dichos números.

$$\begin{array}{cc|c} 21 & 14 & \\ 7 & 1 & \end{array} \qquad 21 = 1 \cdot 14 + 7 \qquad 0 \leq 7 < 14$$

$$\begin{array}{cc|c} 14 & 7 & \\ 0 & 2 & \end{array} \qquad 14 = 2 \cdot 7 + 0$$

Luego: $g_1 = (21, 14) = 7$. Ahora,

$$\begin{aligned} 7 &= 21 - 1 \cdot 14 \\ &= 21 \cdot (1) + 14 \cdot (-1) \end{aligned}$$

Una solución particular de la ecuación diofántica corresponde a la pareja $(1, -1)$.

Ahora debemos obtener una solución particular de la siguiente ecuación diofántica lineal que corresponde a la siguiente:

$$7s + 5z = 1$$

Mediante el Algoritmo de la División hallamos el máximo común divisor de 7 y 5 (que evidentemente es 1) con el fin de expresarlo, de una vez, como una combinación lineal de dichos números.

$$\begin{array}{cc|c} 7 & 5 & \\ 2 & 1 & \end{array} \qquad 7 = 1 \cdot 5 + 2 \qquad 0 \leq 2 < 5$$

$$\begin{array}{cc|c} 5 & 2 & \\ 1 & 2 & \end{array} \qquad 5 = 2 \cdot 2 + 1 \qquad 0 \leq 1 < 2$$

$$\begin{array}{cc|c} 2 & 1 & \\ 0 & 2 & \end{array} \qquad 2 = 2 \cdot 1 + 0$$

Luego: $g = (7, 5) = 1$ como $1/1$: $1 = 1 \cdot 1$. Ahora,

$$\begin{aligned} 1 &= 5 - 2 \cdot 2 \\ &= 5 - 2 \cdot (7 - 1 \cdot 5) \\ &= 5 - 2 \cdot 7 + 2 \cdot 5 \\ &= 3 \cdot 5 - 2 \cdot 7 \\ 1 &= 7 \cdot (-2) + 5 \cdot (3) \end{aligned}$$

Por lo tanto una solución particular de la ecuación diofántica lineal $7s + 5z = 1$ corresponde a la pareja $(-2, 3)$.

Por lo tanto la solución general de la no homogénea ($ax + by + cz = d$) esta dada por:

$$\left\{ \begin{array}{rcl} x &=& (1) \cdot \left(-2 + \dfrac{5}{1} u \right) + \dfrac{14}{7} t \\ y &=& (-1) \cdot \left(-2 + \dfrac{5}{1} u \right) - \dfrac{21}{7} t \\ z &=& 3 - \dfrac{7}{1} u \end{array} \right. \Longrightarrow \left\{ \begin{array}{rcl} x &=& -2 + 5u + 2t \\ y &=& 2 - 5u - 3t \\ z &=& 3 - 7u \end{array} \right.$$

□

Ejemplo 2.7. *Determinar las solución general de la ecuación diofántica lineal.*

$$8x + 14y + 5z = 11$$

Solución: Mediante el Algoritmo de la División hallamos el máximo común divisor de 8 y 14 (que evidentemente es 2) con el fin de expresarlo, de una vez, como una combinación lineal de dichos números.

$$\begin{array}{r|l} 14 & 8 \\ \hline 6 & 1 \end{array} \qquad 14 = 1 \cdot 8 + 6 \qquad 0 \leq 6 < 8$$

$$\begin{array}{r|l} 8 & 6 \\ \hline 2 & 1 \end{array} \qquad 8 = 1 \cdot 6 + 2 \qquad 0 \leq 2 < 6$$

$$\begin{array}{r|l} 6 & 2 \\ \hline 0 & 3 \end{array} \qquad 6 = 3 \cdot 2 + 0$$

Luego: $g_1 = (8, 14) = 2$. Ahora,

$$\begin{aligned} 2 &= 8 - 1 \cdot 6 \\ &= 8 - 1 \cdot (14 - 1 \cdot 8) \\ &= 8 - 1 \cdot 14 + 1 \cdot 8 \\ &= 2 \cdot 8 - 1 \cdot 14 \\ &= 8 \cdot (2) + 14 \cdot (-1) \end{aligned}$$

Una solución particular de la ecuación diofántica corresponde a la pareja $(2, -1)$.

Ahora debemos obtener una solución particular de la siguiente ecuación diofántica lineal que corresponde a la siguiente:

$$2s + 5z = 11$$

Mediante el Algoritmo de la División hallamos el máximo común divisor de 2 y 5 (que evidentemente es 1) con el fin de expresarlo, de una vez, como una combinación lineal de dichos números.

$$\begin{array}{r|l} 5 & 2 \\ \hline 1 & 2 \end{array} \qquad 5 = 2 \cdot 2 + 1 \qquad 0 \leq 1 < 2$$

$$\begin{array}{r|l} 2 & 1 \\ \hline 0 & 2 \end{array} \qquad 2 = 2 \cdot 1 + 0$$

Luego: $g = (2, 5) = 1$ como $1/11$: $1 = 1 \cdot 11$. Ahora,

$$\begin{aligned} 1 &= 5 - 2 \cdot 2 \\ 1 \cdot (11) &= 2 \cdot (-2 \cdot 11) + 5 \cdot (1 \cdot 11) \\ 11 &= 2 \cdot (-22) + 5 \cdot (11) \end{aligned}$$

Por lo tanto una solución particular de la ecuación diofántica lineal $2s + 5z = 11$ corresponde a la pareja $(-22, 11)$.

Por lo tanto la solución general de la no homogénea ($ax + by + cz = d$) esta dada por:

$$\left\{ \begin{array}{rcl} x &=& (2) \cdot \left(-22 + \dfrac{5}{1} u \right) + \dfrac{14}{2} t \\ y &=& (-1) \cdot \left(-22 + \dfrac{5}{1} u \right) - \dfrac{2}{8} t \\ z &=& 11 - \dfrac{2}{1} u \end{array} \right. \Longrightarrow \left\{ \begin{array}{rcl} x &=& -44 + 10u + 7t \\ y &=& 22 - 5u - 4t \\ z &=& 11 - 2u \end{array} \right.$$

□

2.2. Ecuaciones Diofánticas Lineales Mediante Fracciones Continuas

2.2.1. Nota Histórica

Los primeros rastros de la idea de una fracción continua es algo confusa, para muchos resultados aritméticos antiguos que sugieren estas fracciones, pero no hubo un desarrollo sistemático del tema. ya hemos visto que el método de Euclides para encontrar el M.C.D de dos números es esencialmente el de convertir una fracción en una fraccón continua. Este es quizás el primer paso importante (c. 300 B.C.) en el desarrollo del concepto de fracción continua.
Una referencia a las fracciones continuas se encuentra en las obras del matemático indio Aryabhata, que murió alrededor del 550 A.D. Su trabajo contiene uno de los primeros intentos de la solución general de una ecuación lineal indeterminada de la forma $ax + by = c$ donde a, b, c son números enteros, mediante el uso de fracciones continuas.

2.2.2. Introducción

El siguiente método mostrará cómo la teoría de las fracciones continuas pueden ser aplicado para resolver tales ecuaciones:

Usando el teorema 1.5.4 podemos encontrar soluciones particulares de una ecuación diofántica lineal en dos variables, de la forma:

$$ax + by = c \text{ con } a, b, c \in \mathbb{Z},$$

el teorema 2.1.1 proporciona una solución particular denotada por la pareja (x_0, y_0); ası, para aplicar dicho teorema es necesario conocer o determinar una solución.

Cuando una ecuación diofántica tiene solución, es facil hallar una solución particular usando el método de fracciones continuas.

Este método consiste en calcular la fracción continua asociada a la fracción $\frac{a}{b}$, donde a y b son los coeficientes de la ecuación diofántica lineal. Se sabe que si $\frac{a}{b} = [a_1, a_2, \ldots, a_j]$ para los convergentes $C_k = \frac{p_k}{q_k}$ se tiene que:

$$C_j = \frac{a}{b} = \frac{p_j}{q_j}$$

Volvamos ahora a la resolución de la ecuación $ax + by = c,\ (a, b) = 1$

Expresemos la proporción del teorema 1.5.4 como sigue:

$$\frac{a}{b} - \frac{p_{j-1}}{q_{j-1}} = \frac{(-1)^j}{bq_{j-1}}$$

Reduciendo esta proporción a un denominador común y omitiéndolo, nos resulta $aq_{j-1} - bp_{j-1} = (-1)^j$.

Multiplicando la relación obtenida por $(-1)^j c$, tenemos:

$$a\left[(-1)^j cq_{j-1}\right] + b\left[(-1)^{j+1} cp_{j-1}\right] = c$$

De aquí se deduce que la pareja (x_0, y_0), donde $x_0 = (-1)^j cq_{j-1}$ y $y_0 = (-1)^{j+1} cp_{j-1}$.

Es una solución de la ecuación $(ax + by = c,\ (a, b) = 1)$, conforme con el teorema 2.1.2, la solución general de esta ecuación tiene la siguiente forma:

$$x = x_0 + \left(\frac{b}{g}\right) t \text{ y } y = y_0 - \left(\frac{a}{g}\right) t \text{ con } t \in \mathbb{Z}$$

Ejemplo 2.8. *Determinar una solución particular de la siguiente ecuación diofántica lineal haciendo uso de las fracciones continuas.*

$$88x + 25y = 2$$

Solución: Mediante el Algoritmo de la División hallamos el máximo común divisor de 88 y 25 (que evidentemente es 1), quiere decir que existen soluciones en la ecuación diofántica lineal.

$$\begin{array}{cc|c} 88 & 25 & \\ 13 & 3 & \end{array} \qquad 88 = 3 \cdot 25 + 13 \qquad 0 \leq 13 < 25$$

$$\begin{array}{cc|c} 25 & 13 & \\ 12 & 1 & \end{array} \qquad 25 = 1 \cdot 13 + 12 \qquad 0 \leq 12 < 13$$

$$\begin{array}{cc|c} 13 & 12 & \\ 1 & 1 & \end{array} \qquad 13 = 1 \cdot 12 + 1 \qquad 0 \leq 1 < 12$$

$$\begin{array}{cc|c} 12 & 1 & \\ 0 & 12 & \end{array} \qquad 12 = 12 \cdot 1 + 0$$

Luego, lo expresamos como una fracción continua. Ahora,

$$\frac{88}{25} = 3 + \frac{13}{25} = 3 + \frac{1}{\frac{25}{13}} = 3 + \frac{1}{1 + \frac{13}{25}} = 3 + \frac{1}{1 + \frac{1}{\frac{25}{13}}} = 3 + \frac{1}{1 + \frac{1}{1 + \frac{1}{12}}}$$

Suprimiendo el último término de esta fracción, o sea $\frac{1}{12}$, transformamos la fracción continua que acabamos de hallar en una fracción ordinaria y la restamos de la fracción inicial: $\frac{88}{25}$.

$$3 + \frac{1}{1 + \frac{1}{1}} = 3 + \frac{1}{2} = \frac{7}{2}, \text{ restando se obtiene que: } \frac{88}{25} - \frac{7}{2} = \frac{88 \cdot 2 - 25 \cdot 7}{25 \cdot 2} = \frac{1}{25 \cdot 2}$$

Reduciendo, acontinuación, la expresión obtenida a un denominador común y suprimiendo este denominador, obtenemos:

$$\begin{aligned} 88 \cdot (2) - 25 \cdot (7) &= 1 \\ 88 \cdot (2) + 25 \cdot (-7) &= 1 \end{aligned}$$

Multiplicamos la relación obtenida por 2:

$$\begin{aligned} 88 \cdot (2 \cdot 2) + 25 \cdot (-7 \cdot 2) &= 1 \cdot (2) \\ 88 \cdot (4) + 25 \cdot (-14) &= 2 \end{aligned}$$

Por lo tanto una solución particular de la ecuación diofántica lineal $88x + 25y = 2$ corresponde a la pareja $(4, -14)$.

Otra manera de encontrar esta misma solución particular asociada a la fracción continua finita que corresponde a la fracción $\frac{88}{25}$, la podemos obtener mediante la aplicación del teorema 1.5.4 al desarrollo de $[3, 1, 1, 12]$. En efecto:

$$C_1 = [a_1] = \frac{a_1}{1};\ C_1 = [3] = \frac{3}{1} = 3;\ C_1 = 3$$

$$C_2 = [a_1, a_2] = a_1 + \frac{1}{a_2};\ C_2 = [3,1] = 3 + \frac{1}{1} = 3 + 1 = 4;\ C_2 = 4$$

$$C_3 = [a_1, a_2, a_3] = a_1 + \frac{1}{a_2 + \frac{1}{a_3}};\ C_3 = [3,1,1] = 3 + \frac{1}{1 + \frac{1}{1}} = 3 + \frac{1}{1+1} = 3 + \frac{1}{2} = \frac{7}{2};\ C_3 = \frac{7}{2}$$

$$C_4 = [a_1, a_2, a_3, a_4] = a_1 + \frac{1}{a_2 + \frac{1}{a_3 + \frac{1}{a_4}}};\ C_4 = [3,1,1,12] = 3 + \frac{1}{1 + \frac{1}{1 + \frac{1}{12}}} = \frac{88}{25};\ C_4 = \frac{88}{25}$$

Así que: $p_4 = 88$, $q_4 = 25$, $p_3 = 7$ y $q_3 = 2$ por el teorema 1.5.4, tenemos que:

$$\begin{aligned}
p_4 \cdot q_3 - q_4 \cdot p_3 &= (-1)^4 \\
88 \cdot (q_3) - 25 \cdot (p_3) &= 1 \\
88 \cdot (q_3) + 25 \cdot (-p_3) &= 1 \\
88 \cdot (2 \cdot q_3) + 25 \cdot (-2 \cdot p_3) &= 2 \cdot 1 \\
88 \cdot (2 \cdot q_3) + 25 \cdot (-2 \cdot p_3) &= 2 \\
88 \cdot (2 \cdot 2) + 25 \cdot (-2 \cdot 7) &= 2 \\
88 \cdot (4) + 25 \cdot (-14) &= 2
\end{aligned}$$

Por lo tanto una solución particular de la ecuación diofántica lineal $88x + 25y = 2$ corresponde a la pareja $(4, -14)$. □

Ejemplo 2.9. *Determinar una solución general de la siguiente ecuación diofántica lineal haciendo uso de las fracciones continuas.*

$$37x - 11y = 23$$

Solución: Mediante el Algoritmo de la División hallamos el máximo común divisor de 37 y 1 (que evidentemente es 1), quiere decir que existen soluciones en la ecuación diofántica lineal.

$$\begin{array}{r|l} 37 & 11 \\ \hline 4 & 3 \end{array} \qquad 37 = 3 \cdot 11 + 4 \qquad 0 \leq 4 < 11$$

$$\begin{array}{r|l} 11 & 4 \\ \hline 3 & 2 \end{array} \qquad 11 = 2 \cdot 4 + 3 \qquad 0 \leq 3 < 4$$

$$\begin{array}{r|l} 4 & 3 \\ \hline 1 & 1 \end{array} \qquad 4 = 1 \cdot 3 + 1 \qquad 0 \leq 1 < 3$$

$$\begin{array}{r|l} 3 & 1 \\ \hline 0 & 3 \end{array} \qquad 3 = 3 \cdot 1 + 0$$

Con base en lo anterior podemos expresar el desarrollo de la fracción $\frac{37}{11}$ mediante fracción continua simple finita por el siguiente arreglo $[3, 2, 1, 3]$. acontinuación, hacemos uso del teorema 1.5.4 y obtenemos que:

$$C_1 = [3] = \frac{3}{1} = 3$$

$$C_2 = [3,2] = 3 + \frac{1}{2} = \frac{6+1}{2} = \frac{7}{2}$$

$$C_3 = [3,2,1] = 3 + \frac{1}{2+\frac{1}{1}} = 3 + \frac{1}{2+1} = 3 + \frac{1}{3} = \frac{9+1}{3} = \frac{10}{3}$$

$$C_4 = [3,2,1,3] = 3 + \frac{1}{2+\frac{1}{1+\frac{1}{3}}} = 3 + \frac{1}{2+\frac{1}{\frac{4}{3}}} = 3 + \frac{1}{2+\frac{3}{4}} = 3 + \frac{1}{\frac{8+3}{4}} = 3 + \frac{1}{\frac{11}{4}} = 3 + \frac{4}{11} = \frac{37}{11}$$

Así que: $p_4 = 37$, $q_4 = 11$, $p_3 = 10$ y $q_3 = 3$ luego, tenemos que:

$$\begin{aligned} p_4 \cdot q_3 - q_4 \cdot p_3 &= (-1)^4 \\ 37 \cdot (q_3) - 11 \cdot (p_3) &= 1 \\ 37 \cdot (23 \cdot q_3) - 11 \cdot (23 \cdot p_3) &= 23 \cdot 1 \\ 37 \cdot (23 \cdot q_3) - 11 \cdot (23 \cdot p_3) &= 23 \\ 37 \cdot (23 \cdot 3) - 11 \cdot (23 \cdot 10) &= 23 \\ 37 \cdot (69) - 11 \cdot (230) &= 23 \end{aligned}$$

Por lo tanto una solución particular de la ecuación diofántica lineal $37x - 11y = 23$ corresponde a la pareja $(69, 230)$.

Teniendo en cuenta que la ecuación homogénea correspondiente es:

$$37x - 11y = 0,$$

una solución es: $x = -11$ y $y = -37$.

La solución general de la homogénea es: $x = -11t$ y $y = -37t$ con $t \in \mathbb{Z}$

Por lo tanto la solución general de la no homogénea ($ax + by = c$) esta dada por:

$$x = 69 - (11)\, t \text{ y } y = 230 - (37)\, t \text{ con } t \in \mathbb{Z}$$

□

2.2.3. Problemas de Aplicación

Ejemplo 2.10. *Pídale a un estudiante que multiplique el día de su cumpleaños por* 12 *y el número del mes en que nació por* 31 *y dígale que sume los resultados.*

*Primero tomaremos la fecha de cumpleaños, (*27 *de Septiembre), ahora haremos lo siguiente:*

1. Multiplicaremos el día de cumpleaños, que en este caso es 27 *por 12.*

2. Luego multiplicaremos el número del mes, que en este caso es 9 *por 31.*

Sean:

$$x = \textit{día de su cumpleaños}$$
$$y = \textit{número del mes de cumpleaños}$$

Luego sumando estos resultados $324 + 279 = 603$. *La idea es hallar la fecha de cumpleaños conociendo esta suma.*

La ecuación diofántica lineal correspondiente es:

$$12x + 31y = 603$$

Solución: Mediante el Algoritmo de la División hallamos el máximo común divisor de 12 y 31 (que evidentemente es 1).

$$\begin{array}{r|l} 31 & 12 \\ \hline 7 & 2 \end{array} \qquad 31 = 2 \cdot 12 + 7 \qquad 0 \leq 7 < 12$$

$$\begin{array}{r|l} 12 & 7 \\ \hline 5 & 1 \end{array} \qquad 12 = 1 \cdot 7 + 5 \qquad 0 \leq 5 < 7$$

$$\begin{array}{r|l} 7 & 5 \\ \hline 2 & 1 \end{array} \qquad 7 = 1 \cdot 5 + 2 \qquad 0 \leq 2 < 5$$

$$\begin{array}{r|l} 5 & 2 \\ \hline 1 & 2 \end{array} \qquad 5 = 2 \cdot 2 + 1 \qquad 0 \leq 1 < 2$$

$$\begin{array}{r|l} 2 & 1 \\ \hline 0 & 2 \end{array} \qquad 2 = 2 \cdot 1 + 0$$

Con base en lo anterior podemos expresar el desarrollo de la fracción $\frac{31}{12}$ mediante fracción continua simple finita por el siguiente arreglo $[2, 1, 1, 2, 2]$. acontinuación, hacemos uso del teorema 1.5.4 y obtenemos que:

$$C_1 = [2] = \frac{2}{1} = 2$$

$$C_2 = [2,1] = 2 + \frac{1}{1} = 2 + 1 = 3$$

$$C_3 = [2,1,1] = 2 + \frac{1}{1 + \frac{1}{1}} = 2 + \frac{1}{1+1} = 2 + \frac{1}{2} = \frac{4+1}{2} = \frac{5}{2}$$

$$C_4 = [2,1,1,2] = 2 + \frac{1}{1 + \frac{1}{1 + \frac{1}{2}}} = 2 + \frac{1}{1 + \frac{1}{\frac{3}{2}}} = 2 + \frac{1}{1 + \frac{2}{3}} = 2 + \frac{1}{\frac{3+2}{3}} = 2 + \frac{1}{\frac{5}{3}} = 2 + \frac{3}{5} = \frac{13}{5}$$

$$C_5 = [2,1,1,2,2] = 2 + \frac{1}{1 + \frac{1}{1 + \frac{1}{2 + \frac{1}{2}}}} = 2 + \frac{1}{1 + \frac{1}{1 + \frac{1}{\frac{5}{2}}}} = 2 + \frac{1}{1 + \frac{1}{1 + \frac{2}{5}}} = \cdots = 2 + \frac{7}{12} = \frac{31}{12}$$

Así que: $p_5 = 31$, $q_4 = 12$, $p_4 = 13$ y $q_4 = 5$ luego, tenemos que:

$$\begin{aligned}
p_5 \cdot q_4 - q_5 \cdot p_4 &= (-1)^5 \\
31 \cdot (q_4) - 12 \cdot (p_4) &= -1 \\
-31 \cdot (q_4) + 12 \cdot (p_4) &= 1 \\
12 \cdot (p_4) - 31 \cdot (q_4) &= 1 \\
12 \cdot (p_4) + 31 \cdot (-q_4) &= 1 \\
12 \cdot (603 \cdot p_4) + 31 \cdot (-603 \cdot q_4) &= 603 \cdot 1 \\
12 \cdot (603 \cdot p_4) + 31 \cdot (-603 \cdot q_4) &= 603 \\
12 \cdot (603 \cdot 13) + 31 \cdot (-603 \cdot 5) &= 603 \\
12 \cdot (7839) + 31 \cdot (-3015) &= 603
\end{aligned}$$

Por lo tanto una solución particular de la ecuación diofántica lineal $12x + 31y = 603$ corresponde a la pareja $(7839, -3015)$.

Teniendo en cuenta que la ecuación homogénea correspondiente es:

$$12x + 31y = 0,$$

una solución es: $x = 31$ y $y = -12$.

La solución general de la homogénea es: $x = 31t$ y $y = -12t$ con $t \in \mathbb{Z}$

Por lo tanto la solución general de la no homogénea ($ax + by = c$) esta dada por:

$$x = 7839 + (31)\, t \text{ y } y = -3015 - (12)\, t \text{ con } t \in \mathbb{Z}$$

Como se ha solicitado hallar el día y mes de cumpleaños de cualquier persona, estas se pueden obtener o pueden ser obtenidas considerando el sistema de desigualdades.

$$\begin{cases} 7839 + 31t > 0 \\ -3015 - 12t > 0 \end{cases}$$

Como $7839 + 31t > 0$ si $t \geq -252,8$ y $-3015 - 12t > 0$ si $t \leq -251,2$ entonces el sistema es positivo para $-252,8 < t < -251,2$ como $t \in \mathbb{Z}$ entre el intervalo $-252,8 < t < -251,2$ luego el único entero en este intervalo es $t = -252$.

Reemplazando $t = -252$, tenemos que $x = 7839 + 31\,(-252) = 27$ y $y = -3015 - 12\,(-252) = 9$ por lo tanto la única solución entera positiva de la ecuación diofántica lineal $12x + 31y = 603$ es la pareja $(29, 9)$.

Por lo tanto, la fecha de cumpleaños de esta persona es el día 29 del mes 9 que hace referencia a septiembre. □

2.3. Ecuaciones Diofánticas Lineales Mediante Congruencias Lineales

2.3.1. Nota Histórica

Podemos mencionar las congruencias lineales. Primero, Carl Freidrich Gauss consideró las congruencias y desarrolló congruencias. Gauss lo notó; cuando intenta resolver las ecuaciones diofánticas lineales $(ax + by = c)$; si $m/(a - b)$, entonces escribimos $a \equiv b \pmod{m}$, donde a es congruente con b modulo m.

2.3.2. Introducción

Las congruencias lineales pueden ser usadas para obtener soluciones, si ellas existen, de las ecuaciones diofánticas lineales en dos variables, de la forma:

$$ax + by = c \text{ con } a, b, c \in \mathbb{Z},$$

determinar las soluciones de esta ecuaciíon diofántica lineal que equivale a hallar las soluciones de la congruencia lineal:

$$ax \equiv c \pmod{b}$$

Según el teorema 1.6.10, si $g = (a, b)$, entonces existe una solución de esta congruencia lineal cuando g/c. Toda solución de la congruencia lineal $(ax \equiv c \pmod{b})$ es de la forma: $x = x_0 + \left(\frac{b}{g}\right) t$, donde x_0 es una solución particular y t es un entero. Sustituyendo $x_0 + \left(\frac{b}{g}\right) t$ en la ecuación diofántica lineal $(ax + by = c)$, obtenemos los valores de y que satisfacen la ecuación diofántica: $a\left(x_0 + \frac{b}{g}t\right) + by = c$ Por lo tanto,

$$\begin{aligned}
by &= c - a\left(x_0 + \frac{b}{g}t\right) \\
y &= \frac{c - a\left(x_0 + \frac{b}{g}t\right)}{b} \\
y &= \frac{c - ax_0 - \frac{ab}{g}t}{b} \\
y &= \frac{c - ax_0}{b} - \frac{\frac{ab}{g}t}{b} \\
y &= \frac{\cancel{ax_0} + by_0 - \cancel{ax_0}}{b} - \frac{a\cancel{b}}{g\cancel{b}}t \\
y &= \frac{\cancel{b}y_0}{\cancel{b}} - \frac{a}{g}t \\
y &= y_0 - \left(\frac{a}{g}\right) t
\end{aligned}$$

donde y_0 es el complemento de la solución particular de la pareja (x_0, y_0) de la ecuación $ax + by = c$.

En consecuencia las parejas (x, y) que constituyen soluciones de la ecuación diofántica lineal $ax+by = c$ están relacionadas mediante las siguientes ecuaciones:

$$x = x_0 + \left(\frac{b}{g}\right) t \text{ y } y = y_0 - \left(\frac{a}{g}\right) t \text{ con } t \in \mathbb{Z}$$

Ejemplo 2.11. *Determinar una solución particular de la ecuación diofántica lineal dada, haciendo uso de las congruencias lineales.*

$$48x + 7y = 17$$

Solución: Mediante el Algoritmo de la División hallamos el máximo común divisor de 48 y 7 (que evidentemente es 1) con el fin de expresarlo, de una vez, como una combinación lineal de dichos números.

$$\begin{array}{r|l} 48 & 7 \\ 6 & 6 \end{array} \qquad 48 = 6 \cdot 7 + 6 \qquad 0 \leq 6 < 7$$

$$\begin{array}{r|l} 7 & 6 \\ 1 & 1 \end{array} \qquad 7 = 1 \cdot 6 + 1 \qquad 0 \leq 1 < 6$$

$$\begin{array}{r|l} 6 & 1 \\ 0 & 6 \end{array} \qquad 6 = 6 \cdot 1 + 0$$

Luego: $g = (48, 7) = 1$. Ahora,

$$\begin{aligned} 1 &= 7 - 1 \cdot 6 \\ &= 7 - 1 \cdot (48 - 6 \cdot 7) \\ &= 7 - 1 \cdot 48 + 6 \cdot 7 \\ &= 7 \cdot 7 - 1 \cdot 48 \\ &= 48 \cdot (-1) + 7 \cdot (7) \end{aligned}$$

Para atender la petición del ejercicio transformamos la ecuación diofántica lineal dada, en una ecuación equivalente en forma de congruencia lineal. En tal sentido la ecuación $48x + 7y = 17$, la escribimos de la siguiente manera:

$$48x \equiv 17 \pmod 7$$

para hallar una solución particular de esta ecuación diofántica $48x + 7y = 17$ se obtiene, haciendo uso del inverso multiplicativo.

Así que el inverso multiplicativo de 48 mediante la relación de congruencia módulo 7 es -1.

Multiplicando a ambos lados de la congruencia obtenemos lo siguiente:

$$\begin{aligned} 48\,(-1)\,x &\equiv 17\,(-1) \pmod 7 \\ -48x &\equiv -17 \pmod 7 \\ x &\equiv 4 \pmod 7 \\ x &= 4 \end{aligned}$$

Observemos que -48 mód 7 es el residuo obtenido de la división de 48 entre 7, como $-48 < 0$ el residuo de la división es igual a 6, por lo tanto -48 mód $7 = 7 - 6 = 1$.

De igual manera para -17 mód 7 es el residuo obtenido de la división de 17 entre 7, como $-17 < 0$ el residuo de la división es igual a 3, por lo tanto -17 mód $7 = 7 - 3 = 4$.

Por ultimo 4 mód 7 es el residuo obtenido de la división de 4 entre 7 la solución para esta división es 0 con residuo 4, por lo tanto 4 mód $7 = 4$.

Ahora, sustituyendo 4 en la ecuación diofántica lineal $48x + 7y = 17$, obtenemos:

$$48x + 7y = 17\ ;\ 48\,(4) + 7y = 17\ ;\ 192 + 7y = 17\ ;\ 7y = 17 - 192\ ;\ 7y = -175\ ;\ y = \frac{-175}{7} = -25$$

Por lo tanto una solución particular de la ecuación diofántica (obtenida mediante el uso de las congruencias lineales) corresponde a la pareja $(4, -25)$. □

Ejemplo 2.12. *Determinar una solución general de la ecuación diofántica lineal dada, haciendo uso de las congruencias lineales.*

$$61x - 11y = 81$$

Solución: Mediante el Algoritmo de la División hallamos el máximo común divisor de 61 y 11 (que evidentemente es 1) con el fin de expresarlo, de una vez, como una combinación lineal de dichos números.

$$\begin{array}{r|l} 61 & 11 \\ \hline 6 & 5 \end{array} \qquad 61 = 5 \cdot 11 + 6 \qquad 0 \leq 6 < 11$$

$$\begin{array}{r|l} 11 & 6 \\ \hline 5 & 1 \end{array} \qquad 11 = 1 \cdot 6 + 5 \qquad 0 \leq 5 < 6$$

$$\begin{array}{r|l} 6 & 5 \\ \hline 1 & 1 \end{array} \qquad 6 = 1 \cdot 5 + 1 \qquad 0 \leq 1 < 5$$

$$\begin{array}{r|l} 5 & 1 \\ \hline 0 & 5 \end{array} \qquad 5 = 5 \cdot 1 + 0$$

Luego: $g = (61, 11) = 1$. Ahora,

$$\begin{aligned} 1 &= 6 - 1 \cdot 5 \\ &= 6 - 1 \cdot (11 - 1 \cdot 6) \\ &= 6 - 1 \cdot 11 + 1 \cdot 6 \\ &= 2 \cdot 6 - 1 \cdot 11 \\ &= 2 \cdot (61 - 5 \cdot 11) - 1 \cdot 11 \\ &= 2 \cdot 61 - 10 \cdot 11 - 1 \cdot 11 \\ &= 2 \cdot 61 - 11 \cdot 11 \\ &= 61 \cdot (2) - 11 \cdot (11) \end{aligned}$$

Para atender la petición del ejercicio transformamos la ecuación diofántica lineal dada, en una ecuación equivalente en forma de congruencia lineal. En tal sentido la ecuación $61x - 11y = 81$, la escribimos de la siguiente manera:

$$-11y \equiv 81 \pmod{61}$$

para hallar una solución particular de esta ecuación diofántica $61x - 11y = 81$ se obtiene, haciendo uso del inverso multiplicativo.

Así que el inverso multiplicativo de -11 mediante la relación de congruencia módulo 61 es 11.

Multiplicando a ambos lados de la congruencia obtenemos lo siguiente:

$$\begin{aligned} -11\,(11)\,y &\equiv 81\,(11) \pmod{61} \\ -121y &\equiv 891 \pmod{61} \\ y &\equiv 37 \pmod{61} \\ y &= 37 \end{aligned}$$

Observemos que -121 mód 61 es el residuo obtenido de la división de 121 entre 61, como $-121 < 0$ el residuo de la división es igual a 60, por lo tanto -121 mód $61 = 61 - 60 = 1$.

De igual manera para 891 mód 61 es el residuo obtenido de la división de 891 entre 61, entonces el residuo de la división es igual a 37.

Por ultimo 37 mód 61 es el residuo obtenido de la división de 37 entre 61 la solución para esta división es 0 con residuo 37, por lo tanto 37 mód $61 = 37$.

Ahora, sustituyendo 37 en la ecuación diofántica lineal $61x - 11y = 81$, obtenemos:

$$61x - 11y = 81 \; ; \; 61x - 11\,(37) = 81 \; ; \; 61x - 407 = 81 \; ; \; 61x = 81 + 407 \; ; \; 61x = 488 \; ; \; x = \frac{488}{61} = 8$$

Por lo tanto una solución particular de la ecuación diofántica (obtenida mediante el uso de las congruencias lineales) corresponde a la pareja $(8, 37)$.

Teniendo en cuenta que la ecuación homogénea correspondiente es:

$$61x - 11y = 0,$$

una solución es: $x = 11$ y $y = 61$.

La solución general de la homogénea es: $x = 11t$ y $y = 61t$ con $t \in \mathbb{Z}$

Por lo tanto la solución general de la no homogénea ($ax + by = c$) esta dada por:

$$x = 8 + (11)\,t \text{ y } y = 37 + (61)\,t \text{ con } t \in \mathbb{Z}$$

□

2.3.3. Problemas de Aplicación

Ejemplo 2.13. *La entrada a un cierto museo vale* \$7,200 *para adultos y* \$3,000 *para niños. Cierto día en que asistieron más adultos que niños se recaudaron* \$360,000. *¿Cuántos adultos y cuántos niños asistieron al museo? (Determinar una solución de la ecuación diofántica lineal dada, haciendo uso de las congruencias lineales).*

$$x = \textit{número de adultos que ingresaron al museo}$$
$$y = \textit{número de niños que ingresaron al museo}$$

La ecuación diofántica lineal correspondiente es:

$$7,200x + 3,000y = 360,000 \; \textit{Ó sea que} : \; 12x + 5y = 600$$

Solución: Mediante el Algoritmo de la División hallamos el máximo común divisor de 12 y 5 (que evidentemente es 1) con el fin de expresarlo, de una vez, como una combinación lineal de dichos números.

$$\begin{array}{r|l} 12 & 5 \\ 2 & 2 \end{array} \qquad 12 = 2 \cdot 5 + 2 \qquad 0 \leq 2 < 5$$

$$\begin{array}{r|l} 5 & 2 \\ 1 & 2 \end{array} \qquad 5 = 2 \cdot 2 + 1 \qquad 0 \leq 1 < 2$$

$$\begin{array}{r|l} 2 & 1 \\ 0 & 2 \end{array} \qquad 2 = 2 \cdot 1 + 0$$

Luego: $g = (12, 5) = 1$. Ahora,

$$\begin{aligned} 1 &= 5 - 2 \cdot 2 \\ &= 5 - 2 \cdot (12 - 2 \cdot 5) \\ &= 5 - 2 \cdot 12 + 4 \cdot 5 \\ &= 12 \cdot (-2) + 5 \cdot (5) \end{aligned}$$

Para atender la petición del ejercicio transformamos la ecuación diofántica lineal dada, en una ecuación equivalente en forma de congruencia lineal. En tal sentido la ecuación $12x + 5y = 600$, la escribimos de la siguiente manera:

$$12x \equiv 600 \pmod 5$$

para hallar una solución particular de esta ecuación diofántica $12x + 5y = 600$ se obtiene, haciendo uso del inverso multiplicativo.

Así que el inverso multiplicativo de 12 mediante la relación de congruencia módulo 5 es -2.

Multiplicando a ambos lados de la congruencia obtenemos lo siguiente:

$$\begin{aligned} 12\,(-2)\,x &\equiv 600\,(-2) \pmod 5 \\ -24x &\equiv -1200 \pmod 5 \\ x &\equiv -1200 \pmod 5 \\ x &= -1200 \end{aligned}$$

Observemos que -24 mód 5 es el residuo obtenido de la división de 24 entre 5, como $-24 < 0$ el residuo de la división es igual a 4, por lo tanto -24 mód $5 = 5 - 4 = 1$.

Ahora, sustituyendo -1200 en la ecuación diofántica lineal $12x + 5y = 600$, obtenemos:

$$12x + 5y = 600\ ;\ 12\,(-1200) + 5y = 600\ ;\ -14400 + 5y = 600\ ;\ 5y = 600 + 14400\ ;\ y = \frac{15000}{5} = 3000$$

Por lo tanto una solución particular de la ecuación diofántica (obtenida mediante el uso de las congruencias lineales) corresponde a la pareja $(-1200, 3000)$.

Teniendo en cuenta que la ecuación homogénea correspondiente es:

$$12x + 5y = 0,$$

una solución es: $x = 5$ y $y = -12$.

La solución general de la homogénea es: $x = 5t$ y $y = -12t$ con $t \in \mathbb{Z}$

Por lo tanto la solución general de la no homogénea ($ax + by = c$) esta dada por:

$$x = -1200 + (5)\,t \text{ y } y = 3000 - (12)\,t \text{ con } t \in \mathbb{Z}$$

Como se ha solicitado hallar cuántos adultos y cuántos niños asistieron al museo, estas se pueden obtener o pueden ser obtenidas considerando el sistema de desigualdades.

$$\begin{cases} -1200 + 5t > 0 \\ 3000 - 12t > 0 \end{cases}$$

Como $-1200 + 5t > 0$ si $t \geq 240$ y $3000 - 12t > 0$ si $t \leq 250$ entonces el sistema es positivo para $240 < t < 250$ como $t \in \mathbb{Z}$ entre el intervalo $240 < t < 250$ los posibles valores de t en este intervalo son $t = 241, 242, 243, 244, 245, 246, 247, 248, 249$.

Nuevamente con base en la información dada en el problema tenemos que $y < x$ ya que ingresaron más adultos que niños.

Como $3000 - 12t < -1200 + 5t$ si $t \leq 247,05$ como $t \in \mathbb{Z}$ entre el intervalo $247,05 < t < 250$ luego los dos únicos enteros en este intervalo son 248 y 249.

Cuando $t = 248$: $x = 40$ y $y = 24$, es decir ingresaron 40 adultos y 24 niños.

Cuando $t = 249$: $x = 45$ y $y = 12$, es decir ingresaron 45 adultos y 12 niños.

Otra manera de encontrar esta misma solución asociada a la congruencia lineal haciendo uso de las propiedades, la podemos obtener mediante la aplicación del teorema 1.6.5. En efecto:

$$x = \text{número de adultos que ingresaron al museo}$$
$$y = \text{número de niños que ingresaron al museo}$$

La ecuación diofántica lineal correspondiente es:

$$7,200x + 3,000y = 360,000$$

Mediante el Algoritmo de la División hallamos el máximo común divisor de 7200 y 3000.

$$\begin{array}{r|l} 7200 & 3000 \\ \hline 1200 & 2 \end{array} \qquad 7200 = 2 \cdot 3000 + 1200 \qquad 0 \leq 1200 < 3000$$

$$\begin{array}{r|l} 3000 & 1200 \\ \hline 600 & 2 \end{array} \qquad 3000 = 2 \cdot 1200 + 600 \qquad 0 \leq 600 < 1200$$

$$\begin{array}{r|l} 1200 & 600 \\ \hline 0 & 2 \end{array} \qquad 1200 = 2 \cdot 600 + 0$$

Luego: $(7200, 3000) = 600$ como $600/360000$. Ahora,

Para atender la petición del ejercicio transformamos la ecuación diofántica lineal dada, en una ecuación equivalente en forma de congruencia lineal. En tal sentido la ecuación $7200x + 3000y = 360000$, la escribimos de la siguiente manera:

$$7200x \equiv 360000 \pmod{3000}$$

Así que por el teorema 1.6.5, tenemos que:

Por la propiedad h): Sea $c \neq 0$, $ac \equiv bc \pmod{m}$ y $(c, m) = d$, entonces $a \equiv b \pmod{m/d}$.

$$12\,(600)\,x \equiv 600\,(600) \pmod{\tfrac{3000}{600}}$$

se obtiene que:

$$12x \equiv 600 \pmod{5}$$

Ahora, por la propiedad f): Si $ac \equiv bc \pmod{m}$ y $(c, m) = 1$, entonces $a \equiv b \pmod{m}$.

$$1\,(12)\,x \equiv 50\,(12) \pmod{5}$$

se obtiene que:

$$x \equiv 50 \pmod{5}$$

Ahora, sustituyendo 50 en la ecuación diofántica lineal $7200x + 3000y = 360000$, obtenemos:

$$y = \frac{7200 \cdot (50) - 360000}{3000} \; ; \; y = 0$$

Por lo tanto una solución particular de la ecuación diofántica (obtenida mediante el uso de las propiedades de congruencias modular) corresponde a la pareja $(50, 0)$.

Teniendo en cuenta que la ecuación homogénea correspondiente es:

$$12x + 5y = 0,$$

una solución es: $x = 5$ y $y = -12$.

La solución general de la homogénea es: $x = 5t$ y $y = -12t$ con $t \in \mathbb{Z}$

Por lo tanto la solución general de la no homogénea ($ax + by = c$) esta dada por:

$$x = 50 + (5)\, t \text{ y } y = -12t \text{ con } t \in \mathbb{Z}$$

Como se ha solicitado hallar cuántos adultos y cuántos niños asistieron al museo, estas se pueden obtener o pueden ser obtenidas considerando el sistema de desigualdades.

$$\begin{cases} 50 + 5t > 0 \\ -12t > 0 \end{cases}$$

Como $50 + 5t > 0$ si $t \geq -10$ y $-12t > 0$ si $t \leq 0$ entonces el sistema es positivo para $-10 < t < 0$ como $t \in \mathbb{Z}$ entre el intervalo $-10 < t < 0$ los posibles valores de t en este intervalo son $t = -9, -8, -7, -6, -5, -4, -3, -2, -1$.

Nuevamente con base en la información dada en el problema tenemos que $y < x$ ya que ingresaron más adultos que niños.

Como $-12t < 50 + 5t$ si $t \leq -2,94$ como $t \in \mathbb{Z}$ entre el intervalo $-2,94 < t < 0$ luego los dos únicos enteros en este intervalo son -2 y -1.

Cuando $t = -2$: $x = 40$ y $y = 24$, es decir ingresaron 40 adultos y 24 niños.

Cuando $t = -1$: $x = 45$ y $y = 12$, es decir ingresaron 45 adultos y 12 niños. □

APLICACIÓN WEB PARA CALCULAR LA FECHA DE CUMPLEAÑOS

Introducción

Las herramientas tecnológicas que se dan en forma permanente, han permitido los diversos procesos que se desarrollan en la vida diaria, en nuestro contexto actual, ya que permite importantes desarrollos de sistemas de información basadas en la realización de una página web es en esencia un documento que viaja desde el servidor web donde se encuentra guardado (Hosting), hasta tu navegador donde se muestra como tal la página web en función de la información dada por el servidor.

Los programas y lenguajes que intervienen en el desarrollo de la aplicación web para adivinar ó calcular la fecha de cumpleaños son las siguientes:

- PHP: PHP (acrónimo de "PHP: Hypertext Preprocessor") es un lenguaje "open source" interpretado de alto nivel embebido en páginas HTML y ejecutado en el servidor.
- HTML: Es el lenguaje con el que se estructura el documento base con toda la información que viaja desde el servidor web hasta el navegador.
- CSS: Es un lenguaje que define el color, tamaño y estructura de la web en lo que apariencia se refiere, y el cual tiene que interpretar el navegador para mostrar la web del modo esperado por el desarrollador web.
- JS (JavaScript): Es otro lenguaje de programación como PHP, pero cuyo código se manda directamente insertado en el documento base HTML o en ficheros separados para que se interprete y ejecute por parte del navegador web.
- Apache HTTP Server: Un servidor web como su nombre lo indica, es un software instalado en el equipo con todas las condiciones necesarias para servir o entregar páginas web que le sean solicitadas por un navegador, asegurando que se muestren y representen todos los elementos necesarios para su correcto funcionamiento y visualización. Existen varios tipos de servidores web, Apache es un software de código abierto, libre de uso y totalmente configurable, es en este momento el más utilizado en la red, ya sea en plataformas Linux o Windows.

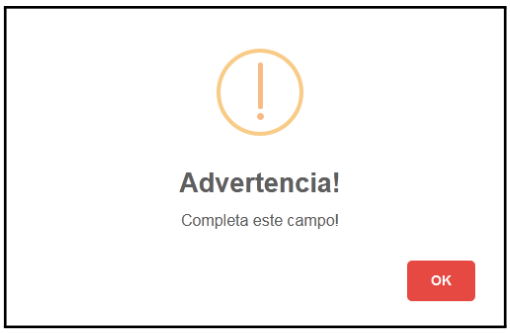
Aplicación Web para Calcular la Fecha de Cumpleaños

La siguiente aplicación web se desarrolló pensando en aplicar unos de los métodos para la solución de la ecuación diofántica lineal por medio del ALGORITMO DE EUCLIDES, en la cual consiste en adivinar o calcular la fecha de cumpleaños de una persona con dicho programa.

A continuación, mostraremos el funcionamiento de la aplicación web:

(a) Figura 1.

Como primera medida se hará la presentación de la aplicación web, donde para la interfaz se tuvo en cuenta el logotipo de la universidad surcolombiana como se puede observar en la Figura 1. Seguidamente a medida que se va interactuando con la aplicación por medio de unos botones que dicen Mostrar en cual, este desplegará un enunciado mostrando la dinámica del ejercicio y otro botón que dice calcular donde saldrán en pantalla una serie de enunciados que depende exclusivamente del resultado ingresado en la casilla de texto.



(b) Figura 2.

Este mensaje de advertencia significa que si la persona al dar Click en el botón CALCULAR, sin haber ingresado el resultado mostrará la siguiente alerta como se muestra en la Figura 2. La persona deberá ingresar en la casilla de texto el resultado en este caso solo ingresará como máximo tres números y no podrá ingresar texto ya que la aplicación cuenta con unas validaciones estrictas.

(c) Figura 3.

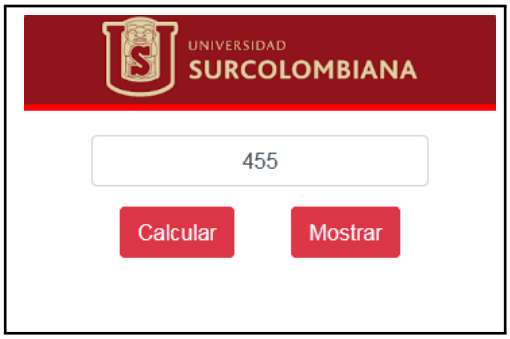
Al dar Click en el botón MOSTRAR automáticamente aparecerá un mensaje, ver Figura 3.

Pídale a un estudiante que multiplique el día de su cumpleaños por 12 y el número del mes en que nació por 31 y dígale que sume los resultados.

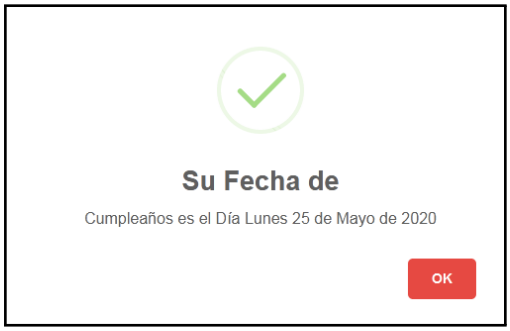
Primero tomaremos la fecha de cumpleaños, (25 de Mayo), ahora haremos lo siguiente:

- Multiplicaremos el día de cumpleaños, que en este caso es 25 por 12.
- Luego multiplicaremos el número del mes, que en este caso es 5 por 31.

Al obtener el resultado de esta suma que evidentemente es (455), procedemos a ingresar el resultado en la casilla para verificar si exactamente es el día y mes de cumpleaños como se muestra en la Figura 4.

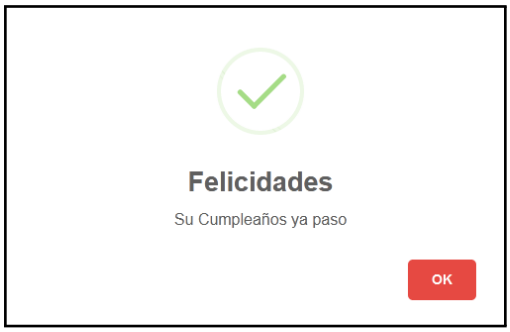


(d) Figura 4.



(e) Figura 5.

En la Figura 5, se muestra como tal el resultado del día y mes de cumpleaños de dicha persona.



(f) Figura 6.

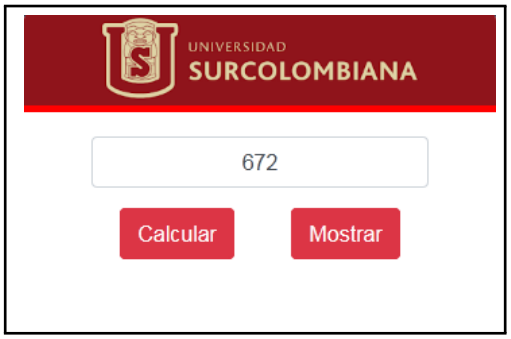
Seguidamente en la Figura 6, se muestra si la persona cumplió o esta próximo a cumplir años.

Pídale a un estudiante que multiplique el día de su cumpleaños por 12 y el número del mes en que nació por 31 y dígale que sume los resultados.

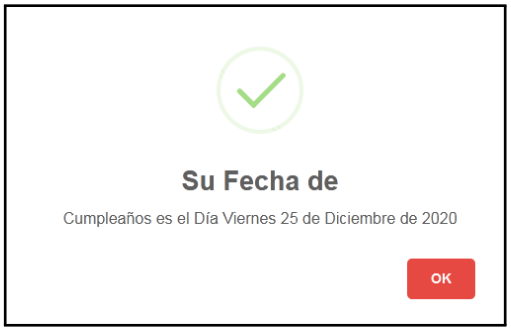
Primero tomaremos la fecha de cumpleaños, (25 de Diciembre), ahora haremos lo siguiente:

- Multiplicaremos el día de cumpleaños, que en este caso es 25 por 12.
- Luego multiplicaremos el número del mes, que en este caso es 12 por 31.

Al obtener el resultado de esta suma que evidentemente es (672), procedemos a ingresar el resultado en la casilla para verificar si exactamente es el día y mes de cumpleaños como se muestra en la Figura 7.



(g) Figura 7.



(h) Figura 8.

En la Figura 8, se muestra como tal el resultado del día y mes de cumpleaños de dicha persona.

(i) Figura 9.

Seguidamente en la Figura 9, se muestra que a la persona le faltan 120 días para su cumpleaños.

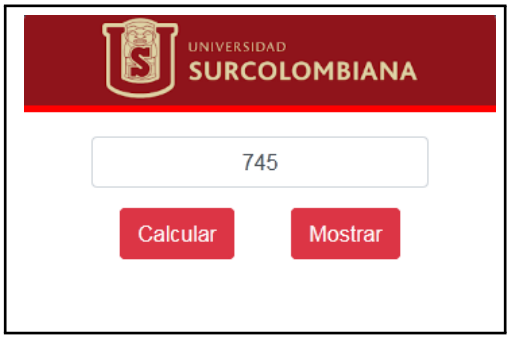
En la siguiente ilustración se muestra que al ingresar un resultado distinto y sin tener en cuenta lo que pide el ejercicio en el siguiente enunciado:

Pídale a un estudiante que multiplique el día de su cumpleaños por 12 y el número del mes en que nació por 31 y dígale que sume los resultados.

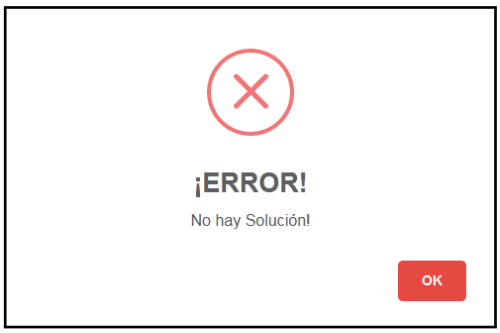
Primero tomaremos la fecha de cumpleaños, (31 de Diciembre), ahora haremos lo siguiente:

- Multiplicaremos el día de cumpleaños, que en este caso es 31 por 12.
- Luego multiplicaremos el número del mes, que en este caso es 12 por 31.

Al obtener el resultado de esta suma que evidentemente es (744), al ingresar un resultado distinto al del procedimiento en la casilla de texto para verificar si exactamente es el día y mes de cumpleaños como se muestra en la Figura 10.



(j) Figura 10.



(k) Figura 11.

Sabiendo bien los valores del intervalo permitido para el ejercicio de aplicación, para tal caso que una persona ingrese un valor que no este dentro del intervalo establecido en el ejercicio, como lo muestra en la Figura 10, la pantalla mostrara un mensaje de error diciendo no hay solución como se muestra en la Figura 11.

CAPÍTULO 3

ECUACIONES DIOFÁNTICAS DE ORDEN 2

3.1. Nota Histórica

La ecuación $x^2 + y^2 = z^2$ es tal vez una de la mas antigua e importante que se conoce, sin embargo, hoy en día se denomina ecuación pitagórica y una terna de números (x, y, z) que satisfacen la ecuación $x^2+y^2 = z^2$ se le llama terna pitagórica. Cuando x, y y z son números reales positivos podemos asociar la ecuación con el resultado obtenido del teorema de pitágoras donde los valores x, y y z corresponden a las medidas de los catetos y la hipotenusa de un triangulo rectángulo respectivamente. Ademas, si el Máximo Común Divisor de $(x, y, z) = 1$ se dice que es una terna pitagórica primitiva.

Uno de los documentos más antiguos que hace referencia al manejo de esta tripleta de números relacionados por $x^2+y^2 = z^2$ es una tablilla de arcilla que parece ser originada en la cultura babilonica y que actualmente se encuentra en la Universidad de Columbia, Nueva York, la cual fue donada por el editor neoyorquino George Arthur Plimton en 1936 después de su muerte.

Esta tablilla de arcilla denominada Plimton 322 datada al rededor de $1900 - 1800$ A.C mide $12,7 \times 8,8$ cm y tiene aproximadamente un grosor de 2 cm y fue escrita con la ayuda de dos símbolos, una cuña vertical en forma de flecha que representa la unidad y una cuña horizontal con la misma forma para el número **diez**, a este tipo de escritura se le denomina cuneiforme, ademas los números aparecen escritos en 15 filas y 4 columnas en un sistema sexagesimal.

Por otro lado, según estudios realizados por Neugebauer y Abrahan Sanchs y otros investigadores en 1945, encontraron que se tratan de ternas pitagóricas donde seguramente se cree que los babilónicos debieron de utilizar un método para construir las ternas pitagóricas que aparecen en la tablilla.

3.2. Forma o técnica de interpretación de como pudieron haber sido obtenidas las ternas pitagóricas

A continuación se presenta una "posible" hipotesis segun los investigadores Neugebauer y Sanchs en el libro mathematical cuneiform texts (1945), de como los babilonios llegaron a construir ternas pitagóricas que aparecen en la tablilla Plimton 322.

Con base en la ecuación $x^2 + y^2 = z^2$ la idea consiste en simplificar esta expresión dividiendo por alguno de los términos cuadráticos. A manera de ejemplo, dividamos ambos miembros de la igualdad por x^2:

$$\begin{cases} \dfrac{x^2}{x^2} + \dfrac{y^2}{x^2} &= \dfrac{z^2}{x^2} \\ 1 + \dfrac{y^2}{x^2} &= \dfrac{z^2}{x^2} \end{cases} \Longrightarrow \begin{cases} 1 &= \dfrac{z^2}{x^2} - \dfrac{y^2}{x^2} \\ 1 &= \left(\dfrac{z}{x}\right)^2 - \left(\dfrac{y}{x}\right)^2 \end{cases}$$

Si hacemos cambio de variable $b = \frac{y}{x}$ y $c = \frac{z}{x}$ se obtiene que:

$$\begin{aligned} 1 &= c^2 - b^2 \\ b^2 &= c^2 - 1 \\ b^2 &= (c-1)(c+1) \\ b \cdot b &= (c-1)(c+1) \end{aligned}$$

Visto de otra manera,

$$\frac{b}{c-1} = \frac{c+1}{b} = t$$

Luego $t = \frac{b}{c-1}$ y $t = \frac{c+1}{b}$, siendo $t = \frac{p}{q}$ donde $p, q \in \mathbb{Z}$ con $q \neq 0$ y $p > q$.

$$\begin{cases} t &= \dfrac{c+1}{b} \\ t &= \dfrac{b}{c-1} \end{cases} \Longrightarrow \begin{cases} c &= tb - 1 \\ b &= t(c-1) \end{cases}$$

Resolviendo lo anterior obtenemos que:

$$\begin{cases} b &= t(c-1) \\ b &= t([tb-1]-1) \\ b &= t(tb-2) \\ b &= t^2 b - 2t \end{cases} \Longrightarrow \begin{cases} b + 2t &= t^2 b \\ 2t &= t^2 b - b \\ 2t &= \left(t^2 - 1\right) b \\ b &= \dfrac{2t}{t^2 - 1} \end{cases}$$

Como $t = \frac{p}{q}$ reemplazando t en $b = \frac{2t}{t^2-1}$ nos queda lo siguiente:

$$\begin{aligned} b &= \frac{2t}{t^2-1} = \frac{2\left(\dfrac{p}{q}\right)}{\left(\dfrac{p}{q}\right)^2 - 1} \\ &= \frac{\dfrac{2p}{q}}{\dfrac{p^2}{q^2} - 1} = \frac{\dfrac{2p}{q}}{\dfrac{p^2 - q^2}{q^2}} \\ b &= \frac{2pq^{\not 2}}{\not q(p^2 - q^2)} = \frac{2pq}{p^2 - q^2} \end{aligned}$$

$$\begin{cases} c &= tb-1 \\ c &= t\left(\dfrac{2t}{t^2-1}\right)-1 \\ c &= \dfrac{2t^2}{t^2-1}-1 \end{cases} \Longrightarrow \begin{cases} c &= \dfrac{2t^2-1\left(t^2-1\right)}{t^2-1} \\ c &= \dfrac{2t^2-t^2+1}{t^2-1} \\ c &= \dfrac{t^2+1}{t^2-1} \end{cases}$$

Como $t=\frac{p}{q}$ reemplazando t en $c=\frac{t^2+1}{t^2-1}$ nos queda lo siguiente:

$$\begin{aligned} c &= \frac{t^2+1}{t^2-1} = \frac{\left(\frac{p}{q}\right)^2+1}{\left(\frac{p}{q}\right)^2-1} \\ &= \frac{\frac{p^2}{q^2}+1}{\frac{p^2}{q^2}-1} = \frac{\frac{p^2+q^2}{q^2}}{\frac{p^2-q^2}{q^2}} \\ c &= \frac{\left(p^2+q^2\right)\cancel{q^2}}{\cancel{q^2}\left(p^2-q^2\right)} = \frac{p^2+q^2}{p^2-q^2} \end{aligned}$$

Como $b=\frac{y}{x}$ y $c=\frac{z}{x}$, por lo tanto la terna pitagórica es:

$$\left(p^2-q^2,\ 2pq,\ p^2+q^2\right),\ \text{siendo } p>q\ ;\ p,\ q\in\mathbb{Z}$$

Comprobemos que definitivamente estos valores $x=p^2-q^2$, $y=2pq$ y $z=p^2+q^2$ satisfacen la ecuación $x^2+y^2=z^2$.

$$\begin{aligned} x^2+y^2 &= \left(p^2-q^2\right)^2+(2pq)^2 \\ &= p^4-2p^2q^2+q^4+4p^2q^2 \\ &= p^4+2p^2q^2+q^4 \\ &= \left(p^2+q^2\right)^2 \\ &= z^2 \end{aligned}$$

Ejemplo 3.1. *Suponga que $p=2$ y $q=1$, entonces los números:.*

$$p^2-q^2=2^2-1^2=3,\ 2pq=2\cdot 2\cdot 1=4,\ p^2+q^2=2^2+1^2=5$$

Solución: definen una terna pitagórica, en efecto:

$$\begin{aligned} (3)^2+(4)^2 &= (5)^2 \\ 9+16 &= 25 \\ 25 &= 25 \end{aligned}$$

Así que la terna pitagórica esta dada por la tripleta $(3,4,5)$. □

3.3. Diofanto y las Ternas Pitagóricas

El problema número 8 del libro II de la aritmética de Diofanto plantea: "descomponer un cuadrado en dos cuadrados perfectos" para ello se realiza un procedimiento deductivo, que se desarrolla de la siguiente manera:

Suponga que se quiere descomponer el número 16 en dos cuadrados. Siendo x^2 el primer número, entonces el segundo debe ser $16-x^2$, el cual también debe ser un cuadrado es decir, $16-x^2=y^2$. Luego, Diofanto identifica al número y^2 con una expresión del tipo $\left(mx-\sqrt{16}\right)^2$, donde m es un racional mayor que uno. Igualando a ambos lados, resulta:

$$\begin{cases} 16-x^2 &= \left(mx-\sqrt{16}\right)^2 \\ 16-x^2 &= (mx-4)^2\text{, resolviendo} \\ 16-x^2 &= m^2x^2-8mx+16 \\ 8mx &= m^2x^2+x^2 \\ 8mx &= x^2\left(m^2+1\right)\text{, como } x>0 \\ \textit{queda, } x &= \dfrac{8m}{m^2+1} \end{cases} \Longrightarrow \begin{cases} \textit{Así que, } y^2 &= 16-\left(\dfrac{8m}{m^2+1}\right)^2 \\ &= \dfrac{16\left(m^2-1\right)^2}{\left(m^2+1\right)^2}\text{, como } y>0 \text{ y } m>1 \\ \textit{entonces, } y &= \dfrac{4\left(m^2-1\right)}{m^2+1} \end{cases}$$

De esta manera, el número 16 se puede descomponer como:

$$16=x^2+y^2 \Longrightarrow 16=\left(\frac{8m}{m^2+1}\right)^2+\left(\frac{4\left(m^2-1\right)}{m^2+1}\right)^2$$

Por ejemplo, para $m=3$ se tiene que:

$$16=\left(\frac{12}{5}\right)^2+\left(\frac{16}{5}\right)^2$$

En general, si se quiere descomponer el cuadrado $n^2, n\in\mathbb{N}$, como suma de dos cuadrados: $n^2=x^2+y^2$, se sigue el procedimiento anterior:

$$\begin{aligned} y^2 &= n^2-x^2 = \left(mx-\sqrt{n^2}\right)^2 \\ &= n^2-x^2 = (mx-n)^2 \\ &= n^2-x^2 = m^2x^2-2mnx+n^2 \\ &= 2mnx = x^2\left(m^2+1\right) \\ x &= \frac{2mn}{m^2+1}\text{ pues, } x>0 \end{aligned}$$

Luego, como $y^2=n^2-x^2$ entonces:

$$\begin{aligned} y^2 &= n^2-\left(\frac{2mn}{m^2+1}\right)^2 = \frac{n^2\left(m^2-1\right)^2}{\left(m^2+1\right)^2} \\ y &= \frac{n\left(m^2-1\right)}{m^2+1}\text{ pues, } m>1 \text{ y } n>0 \end{aligned}$$

Es decir, los números $x = \frac{2mn}{m^2+1}$ y $y = \frac{n\left(m^2-1\right)}{m^2+1}$ satisface que: $n^2 = x^2 + y^2$. Por lo tanto, esto genera la terna:

$$\left(\frac{2mn}{m^2+1},\ \frac{n\left(m^2-1\right)}{m^2+1},\ n\right) \text{ con } m \text{ un número racional mayor que uno y } n \in \mathbb{N}$$

Sin embargo, se tiene el inconveniente de que los números x e y no son enteros para infinitos valores de m. Como la idea de Diofanto (tal vez por los recursos de la época) era de obtener ternas pitagóricas de números enteros positivos y compuesta por enteros positivos únicamente, entonces pudo haber trabajado el problema de la siguiente manera:

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

Si m es entero entonces se multiplica por $\frac{\left(m^2+1\right)^2}{n^2}$ a ambos lados de la igualdad anterior,

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

Así se tiene la terna pitagórica $\left(2m,\ m^2-1,\ m^2+1\right)$, para m entero positivo.

En caso que m sea racional no entero, entonces $m = \frac{p}{q},\ q \neq 0$. Se tiene,

$$\begin{aligned}
\left(m^2+1\right)^2 &= (2m)^2 + \left(m^2-1\right)^2 \\
\left(\left(\frac{p}{q}\right)^2+1\right)^2 &= \left(2\frac{p}{q}\right)^2 + \left(\left(\frac{p}{q}\right)^2-1\right)^2 \\
\left(\frac{p^2+q^2}{q^2}\right)^2 &= \left(\frac{2p}{q}\right)^2 + \left(\frac{p^2-q^2}{q^2}\right)^2
\end{aligned}$$

Si se multiplica a ambos lados de la igualdad anterior por q^4 se tiene:

$$\left(p^2+q^2\right) = (2pq)^2 + \left(p^2-q^2\right)$$

Así se tiene la terna pitagórica:

$$\left(2pq,\ p^2-q^2,\ p^2+q^2\right),\ \text{siendo } p > q\ ;\ p,\ q \in \mathbb{Z}$$

Ejemplo 3.2. *Suponga que $p = 6$ y $q = 4$, entonces los números:.*

$$2pq = 2 \cdot 6 \cdot 4 = 48,\ p^2 - q^2 = 6^2 - 4^2 = 20,\ p^2 + q^2 = 6^2 + 4^2 = 52$$

Solución: definen una terna pitagórica, en efecto:

$$\begin{aligned}
(52)^2 &= (48)^2 + (20)^2 \\
2704 &= 2304 + 400 \\
2704 &= 2704
\end{aligned}$$

Así que la terna pitagórica esta dada por la tripleta $(48, 20, 52)$. □

Conclusiones

El resultado de este trabajo es un recurso que integra saberes que pueden mejorar y fortalecer habilidades aritméticas y algebraicas, contribuyendo al desarrollo y estudio para la solución de problemas. Lo siguiente permite concluir que:

1. Al momento de analizar y estudiar los métodos de solución a las ecuaciones diofánticas en el conjunto de los números enteros, se puede observar que existen diferentes formas de abordar un problema aplicando conceptos previos al desarrollo algebraico que tienen los enteros que abre la posibilidad de realizar estudios acerca de estos métodos.
2. En el estudio y estructura de los números enteros ($\mathbb{Z}$), cabe destacar que se permitió abordar conceptos interesantes como Teoremas y sus Propiedades, Algoritmo de Euclides, M.C.D, Números Primos., entre otros, que fueron fundamentales en el desarrollo de este trabajo, lo que permite abordar temas de la teoría de números.
3. Sin duda, la recopilación de este trabajo deja la satisfacción de haber indagado hechos históricos como el desarrollo de la matemática antigua que con certeza resalta las diferentes maneras de cómo los matemáticos con sus impresionantes habilidades de pensar abordaban los problemas matemáticos de la época, aportando resultados interesantes como las ecuaciones diofánticas.
4. En cuanto a las contribuciones que hicieron los antiguos matemáticos respecto a las ecuaciones diofánticas lineales de la forma ($ax + by = c$), las primeras civilizaciones trabajaban este tipo de ecuaciones buscando solución única y sólo fue hasta el estudio de Diofanto y Brahmagupta que empezaron a buscar soluciones infinitas como también emplearon diferentes métodos de encontrar dichas soluciones.

BIBLIOGRAFÍA

[1] GUSTAVO N. RUBIANO O. TEORÍA DE NÚMEROS [PARA PRINCIPIANTES], 2A. EDICIÓN. Universidad Nacional de Colombia, Sede Bogotá. Facultad de Ciencias, 2004.

[2] RÓBINSON CASTRO PUCHE. ÁLGEBRA MODERNA e introducción al álgebra geométrica, 1A. EDICIÓN. Bogotá: Ecoe Ediciones, 2013 (Ciencias exactas. Matemáticas).

[3] ANTHONY J. PETTOFREZZO, DONALD R. BYRKIT. INTRODUCCIÓN A LA TEORÍA DE LOS NÚMEROS, Copyright © 1972 por Editorial Prentice–Hall Internacional, Englewood Cliffs, New Jersey.

[4] AUGUSTO SILVA SILVA. INTRODUCCIÓN A LA TEORÍA DE NÚMEROS (Universidad Surcolombiana).

[5] BELTRÁN SOSA, PABLO ANDRES. Las ecuaciones en el mundo discreto: Un estudio sobre las Ecuaciones Diofánticas. Bogotá, Universidad Pedagógica Nacional, 2014.

[6] WALTER MORA F. INTRODUCCIÓN A LA TEORÍA DE LOS NÚMEROS Ejemplo y Algoritmos, Copyright © Revista digital Matemática Educación e Internet. 1ra ed. – Escuela de Matemática, Instituto Tecnológico de Costa Rica. 2010. 217 pp.

[7] A. O. Guelfond. RESOLUCIÓN DE ECUACIONES EN NÚMEROS ENTEROS – LECCIONES POPULARES DE MATEMÁTICAS, Segunda edición. EDITORIAL MIR MOSCÚ.

[8] MANUEL FEITO GUZMÁN, CARLOS J. SANDOVAL RUIZ. MATEMÁTICAS Y COMPETENCIAS BÁSICAS A PARTIR DE LA TABLILLA PLIMPTON 322 (1). ARTÍCULOS Noviembre 2014.

[9] JOSÉ WILLIAM PORRAS. TERNAS PITAGÓRICAS. Centro de Investigaciones Científicas, Escuela Naval de Cadetes "Almirante Padilla", Isla Manzanillo, Cartagena de Indias, Colombia. ARTÍCULO Diciembre 2017.

[10] JUAN JOSÉ FALLAS. Ternas Pitagóricas: métodos para generarlas y algunas curiosidades. Instituto Tecnológico de Costa Rica (Escuela de Matemáticas). Derechos Reservados © 2009 Revista Digital Matemática, Educación e Internet.