UNIVERSIDAD SAN FRANCISCO DE QUITO
USFQ

Colegio de Ciencias e Ingenierías

Tres Identidades de Liouville para Teoría Analítica de Números

José Gabriel Castillo Flores

Matemática

Trabajo de fin de carrera presentado como requisito
para la obtención del título de

Matemático

Quito, 19 de mayo de 2025

UNIVERSIDAD SAN FRANCISCO DE QUITO
USFQ

Colegio de Ciencias e Ingenierías

HOJA DE CALIFICACIÓN
DE TRABAJO DE FIN DE CARRERA

Tres Identidades de Liouville para Teoría Analítica de Números

José Gabriel Castillo Flores

Director: John R. Skukalek, Ph.D. _____

Codirector: David F. Hervas, Ph.D. _____

Quito, 19 de mayo de 2025

© DERECHOS DE AUTOR

Nombres y apellidos: José Gabriel Castillo Flores

Código: 00322044

C.I.: 0107329377

Fecha: Quito, 19 de mayo de 2025

ACLARACIÓN PARA PUBLICACIÓN

Nota: El presente trabajo, en su totalidad o cualquiera de sus partes, no debe ser considerado como una publicación, incluso a pesar de estar disponible sin restricciones a través de un repositorio institucional. Esta declaración se alinea con las prácticas y recomendaciones presentadas por el Committee on Publication Ethics COPE descritas por Barbour et al. (2017) Discussion document on best practice for issues around theses publishing, disponible en `http://bit.ly/COPETheses`.

UNPUBLISHED DOCUMENT

Note: The following capstone project is available through Universidad San Francisco de Quito USFQ institutional repository. Nonetheless, this project – in whole or in part – should not be considered a publication. This statement follows the recommendations presented by the Committee on Publication Ethics COPE described by Barbour et al. (2017) Discussion document on best practice for issues around theses publishing available on `http://bit.ly/COPETheses`.

Resumen

Se presentan tres identidades desarrolladas por el matemático francés Joseph Liouville en el ámbito de la teoría analítica de números. De esta manera, se detalla el tiempo y lugar en el que habitó Liouville, se introducen definiciones y teoremas fundamentales de la aritmética que permiten demostrar cada identidad en su totalidad, se aborda funciones aritméticas y ecuaciones diofánticas que constituyen el bastidor de las identidades, y se describen aplicaciones de cada una de ellas. En consecuencia, se produce la inserción de problemas clásicos relacionados con la representación de un entero como suma de dos cuadrados y sumas de convolución; cuyo resultado involucra el trabajo de otros matemáticos como Fermat, Girard, Euler, Dirichlet, Legendre y Jacobi. En definitiva, se concibe una disertación en formato de libro que expresa el quehacer de un matemático puro.

Palabras clave: Liouville, aritmética, número, matemática, identidad, representación, convolución, teorema

Abstract

Three identities developed by the French mathematician Joseph Liouville are presented in the context of analytic number theory. For this reason, the time and place where Liouville lived are detailed; definitions and fundamental theorems of arithmetic are introduced, which allow each identity to be proved completely; number-theoretic functions and Diophantine equations are addressed, which constitute the frame of the identities; and application of each one of them are described. In consequence, the insertion of classic problems that are related to the representation of an integer as the sum of two squares and convolution sums is produced, whose result involves the work of other mathematicians like Fermat, Girard, Euler, Dirichlet, Legendre and Jacobi. In short, a dissertation in book format is conceived that expresses the task of a pure mathematician.

Keyword: Liouville, arithmetic, number, mathematics, identity, representation, convolution, theorem

Agradecimiento

Para empezar, quiero agradecer a Dios por haberme dado la sabiduría y fortaleza, por brindarme la vida para ver realizado este sueño y por ser siempre la luz de mi sendero.

También doy infinitas gracias a mis padres Fausto Castillo y Alicia Flores, las dos personas más importantes en mi vida, por siempre creer en mí desde un principio, por todo el cariño y apoyo recibido a lo largo de estos años, pese al tiempo y la distancia, por darme la oportunidad de estudiar esta carrera, por ser el eje de todos mis logros y éxitos y el sustento en mis horas más difíciles, por el sacrificio que hicieron para que pueda formarme como profesional. De igual forma, agradezco a mi abuelo Fausto Flores, por todo lo realizado y vivido en estos años universitarios, puesto que su compañía y cuidado han sido mi soporte constante e invaluable durante esta etapa de mi vida.

A continuación, pongo en manifiesto mi más sincero agradecimiento a mis profesores de carrera. En primer lugar, a mi director de tesis, John Skukalek, por compartir conmigo sus conocimientos y enseñanzas a lo largo de toda la carrera; fue un completo honor haber sido alumno suyo los nueve semestres en diferentes cursos, entre ellos teoría de números, materia que me apasionó y que representa el dominio de este trabajo, y por haber sido el pionero en sumergirme en este apasionante viaje que gira en torno a la matemática, aun sin conocerlo en persona en la época en que las clases eran virtuales. Después, a mi codirector, David Hervas, por mostrarme la belleza de una demostración, por brindarme la oportunidad de despertar mi ingenio y creatividad para la creación de problemas, y por darme consejos basados en su experiencia para ser un mejor matemático. Gracias por todo su apoyo, orientación y tiempo durante todo este proyecto.

Adicionalmente, me gustaría agradecer a mi profesor Pedro Espinoza, quien me introdujo por primera vez a los concursos de matemática, lo que me permitió descubrir mi verdadera vocación. Gracias a él, me encuentro aquí, por todas sus lecciones y por haber puesto su confianza en mí desde un principio.

Por último, agradezco a mis profesores de mi subespecialización que, pese a no ser de mi carrera, me recibieron en sus clases de brazos abiertos y dejaron una importante huella, no solo en mi formación profesional, sino también en mi experiencia universitaria, entre ellos Eduardo Holguín, Luis Miguel Prócel, Dennis Cazar y Marco Herrera.

Dedicatoria

A Dios, por permitirme culminar esta etapa de mi vida satisfactoriamente.

A mis padres Fausto y Alicia, por su amor incondicional, por creer siempre en mi capacidad de salir adelante frente a cualquier adversidad, darme la libertad de escoger mi profesión y afrontar el vacío de mi partida para que yo pueda volar y cumplir mis sueños.

A mi abuelo Fausto, por su presencia y cuidado inmensurable en estos últimos años, por su paciencia y comprensión en mis arduas jornadas de estudio.

A mi profesor Pedro Espinoza, por ser mi mentor, puesto que este logro es también fruto de su trabajo.

A Joseph Liouville en homenaje póstumo, cuya obra como matemático fue la inspiración para esta disertación.

Índice general

CAPÍTULO 1

Prólogo

«Tant que vous n'aurez pas déployé vos ailes, vous n'aurez aucune ideée de la distance à laquelle vous pouvez voler.»

Hasta que no extiendas tus alas, no tendrás idea de qué tan lejos puedes volar.

Napoleón Bonaparte

Seguramente, se puede interrogar acerca del contenido que aguarda en las siguientes páginas de esta disertación y sobre el impacto que pueda generar la misma. En efecto, el término purista dentro de la matemática para una audiencia abierta y general, pudiese significar una posible aversión o despertar una intriga, como todo lo desconocido lo hace. A veces los acontecimientos impredecibles son los que mayor huella dejan cuando existe predisposición por parte del receptor. En este contexto, se pretende aclarar que si bien no se descarta la existencia de aplicaciones dentro de la vida "real", el propósito de este trabajo se fundamenta dentro de la misma matemática, donde se invita a conectar y seguir eslabones de razonamiento deductivo que desencadenan en el producto final que, para un matemático, se denomina demostración.

Cuando se escucha algún tópico relacionado con la matemática, tristemente se lo suele asociar con cálculos numéricos que se desglosan en operaciones complicadas y confusas, sin sentido aparentemente. Si leyó el título correctamente, en él se menciona la rama que se abordará en esta disertación, teoría de números. A priori, esto puede resultar contradictorio con la premisa anterior; si tiene que ver con números, por supuesto contendrá operaciones numéricas. De hecho, la intuición es correcta, mas no es completa, y lo que realmente se busca es brindar una oportunidad de sumergirse en el apasionante mundo de las demostraciones a partir de los conceptos más elementales y contemplar su belleza.

Como desafío y contribución personal, se incluyeron todas las definiciones, proposiciones y teoremas básicos que constituyen el eje central de esta investigación desde una perspectiva propia y detalles a rajatabla, claro que se otorga el respectivo crédito al autor cuando se lo requiere. En el sumario, pudo observar que se destina un capítulo entero a los fundamentos de la aritmética para que el contenido esté accesible tanto a un público que cuenta con experiencia en la materia como también aquel que no.

En lo referente al contenido y meta última, el lector podrá esperar una breve síntesis del trabajo del matemático francés Joseph Liouville en el campo de la teoría de números, así como algunos de sus resultados más sorprendentes y su relación intrínseca con problemas clásicos dado que se conciben como herramientas alternativas que pueden emplearse para su resolución. La principal motivación radica en profundizar el contexto histórico y entablar vínculos entre la riqueza de las ideas de Liouville junto con el trabajo de otros matemáticos dentro de la aritmética. En definitiva, todos estos componentes promueven la investigación científica y fijan el desafío de completar este documento a cabalidad; la experiencia se complementa con la oportunidad de leer su trabajo en el idioma original, es decir, en francés.

Finalmente, debido a la evidente extensión del documento, se decidió presentarlo en formato de libro, esto en combinación con un sueño propio de escribir uno. Sin nada más que añadir, reciba una cordial bienvenida a esta disertación.

1.1. Introducción

La teoría de números es una de las primeras ramas estudiadas de la matemática, la cual se remota desde la época helénica. A lo largo de los años, varias escuelas europeas han sido referentes en la materia, dentro de las cuales destacan la inglesa, francesa y germánica. Este documento se concentra en el trabajo de uno de los miembros de l'Acádemie des Sciences, el matemático francés Joseph Liouville.

Joseph Liouville vivió en el siglo XIX y destacó en las ramas de análisis complejo, ecuaciones diferenciales y teoría de números, cuyas ideas se encuentran plasmadas en su revista científica "Journal de Mathématiques Pures et Appliquées" en forma de artículos o tratados matemáticos tras ser influenciado por Dirichlet a introducirse en la teoría analítica de números; en particular, se trabajará con tres identidades. Sin embargo, la problemática surge debido a que estos resultados fueron enunciados por el propio Liouville, pero muchas veces no incluyó las demostraciones ni las ideas de desarrollo.

Las identidades se sustentan en las funciones aritméticas, la congruencia modular y las ecuaciones diofánticas, y cada una de ellas tiene aplicación dentro de problemas clásicos de la teoría de números. En efecto, la primera permite abordar las condiciones necesarias para que un número pueda ser expresado como la suma de dos cuadrados, la segunda expresa la cantidad de formas que un número puede expresarse como la suma de dos cuadrados y la tercera es útil para calcular sumas de convolución en las que intervienen funciones aritméticas. Como se verá a posteriori, el trabajo de varios matemáticos como Girard, Fermat, Euler, Dirichlet y Jacobi están involucrados en el desarrollo y aplicación de estas identidades. Adicionalmente, permite explorar distintas ramas de la matemática durante las demostraciones; en concreto, se esclarecen ciertas conexiones con la combinatoria, la teoría de conjuntos y el álgebra abstracta.

De esta manera, se partirá desde una descripción del tiempo que vivió Liouville, a modo de una biografía para poder ubicar el contexto histórico en el que surgen identidades. Además, se busca analizar el trabajo original de Liouville publicado en su revista; en específico, varios artículos publicados entre 1850 y 1860. Para empezar con el desarrollo de las ideas de Liouville, se

pretende introducir conceptos y teoremas de la teoría de números que permitan interpretar el trabajo de Liouville; en particular, se enfatiza las funciones aritméticas que intervienen en las identidades. Finalmente, se establecen los objetivos de demostrarlas, para lo cual se emplean argumentos lógicos directos, inducción, contraposición y contradicción; y de presentar algunas de sus aplicaciones dentro de problemas clásicos de la propia matemática.

CAPÍTULO 2

Contexto Histórico

«It's not an idea until you write it down.»

No es una idea hasta que la escribes.

Ivan Sutherland

El principal eje de esta disertación está focalizado en el trabajo del matemático francés Joseph Liouville dentro del ámbito de la teoría de números analítica publicado en su revista "Journal de Mathématiques Pures et Appliquées". Por tal motivo, se considera oportuno dedicar un capítulo para abordar su obra en el quehacer matemático, y de igual forma, comprender el panorama histórico en el que vivió.

2.1. Joseph Liouville

Joseph Liouville nació el 24 de marzo de 1809 en Saint-Omer, Francia. Fue uno de los matemáticos más influyentes del siglo XIX; en efecto, Lützen [1], lo cataloga como el matemático principal entre Cauchy y Hermite. Fue criado en el seno de una familia cercana al régimen napoleónico dado que su padre era capitán de la Armada. Liouville inició su formación en el campo de la matemática en el Collège Saint Louis en París y a los 16 años ingresó a l'École Polytechnique donde estudió análisis, geometría, física, química, geodesia, entre otros. Posteriormente, se formó como ingeniero en l'École des Ponts et Chaussées hasta 1830, cuando inició su carrera como matemático y obtuvo su doctorado en 1836. En dicho año, fundó la revista "Journal de Mathématiques Pures et Appliquées", considerada también como "Journal de Liouville". Adicionalmente, contrajo nupcias con Marie Louise Balland con quien tuvo 4 hijos, 3 mujeres y 1 varón.

Mantuvo contacto con varios matemáticos de la época, entre ellos Charles François Sturm, con quien desarrolló la teoría Sturm-Liouville inspirado en la conducción de calor y manejo de operadores diferenciales. Como manifiesta Lützen [1], su principal contribución en esta rama fue la demostración de que una función arbitraria tiene una expansión convergente mediante series de Fourier, en términos de autofunciones.

En 1837, Liouville obtuvo un puesto en el Collège de France, en reemplazo de Jean Baptiste Biot. Al año siguiente, fue nombrado profesor de análisis y mecánica en l'École Polytechnique; y posteriormente, consiguió un puesto en l'Académie des Sciences tras el fallecimiento de Michel Lalande. Para 1840, fue elegido miembro de Bureau des Longitudes, sociedad a la que aportó con sus investigaciones en astronomía y geodesia.

Otra de sus principales contribuciones a la matemática fue la primera demostración de la existencia de los números trascendentales, dada en 1844. En efecto, construyó un número compuesto por 0s y 1s tal que no sea solución de alguna ecuación polinómica. De acuerdo con Conway y Guy [2], el número

descrito por Liouville viene dado por

$$l = \sum_{n=1}^{\infty} 10^{-n!} = 0{,}110001000000000000000001\ldots \tag{2.1}$$

donde los únicos dígitos no nulos están en la $1^{\underline{a}}$, $2^{\underline{a}}$, $6^{\underline{a}}$, $24^{\underline{a}}$, $\ldots, (n!)^{\underline{a}}$, $\ldots$ posición decimal y su demostración se fundamenta en una contradicción del Teorema Fundamental del Álgebra. Este número se lo conoce como la constante de Liouville.

Según Lützen [1], Liouville también fue pionero en probar la existencia de funciones elementales cuyas integrales no pueden ser expresadas en términos de antiderivadas elementales. En este mismo año, desarrolló una primera aproximación a las funciones elípticas bajo funciones complejas con doble periodicidad y la observación de que tales funciones deben presentar singularidades si no son constantes, las cuales surgen como funciones inversas de las integrales elípticas; este resultado se lo conoce en la actualidad como el teorema de Liouville dentro de la variable compleja.

En cuanto al ámbito como profesor, tuvo como alumnos a Hervé Faye, Joseph Serret, Charles Hermite, Joseph Bertrand, Lord Kelvin, Jacob Steiner, Paul Laurent y Eugène Catalan. Con base en lo mencionado por Williams [3], Liouville también fue el primer matemático en reconocer el trabajo realizado por Évariste Galois dentro de la teoría de resolución de ecuaciones; en efecto, incluyó varios de los trabajos de Galois en su revista.

En 1856, bajo la influencia de su amigo Dirichlet, se introdujo en la rama de la teoría de números analítica, a la cual se dedicaría por el resto de su vida. Liouville dedicaría varias notas a esta rama en su revista y en los siguientes veinte años escogería 11 cursos sobre la misma en los próximos veinte años. No obstante, únicamente publicó sus ideas dentro de esta rama sin colocar su origen ni sus demostraciones, como lo señala Williams [3].

Con una carta de recomendación de Karl Weierstraß, fue elegido miembro de la Academia de Berlín en 1876. Adicionalmente, también fue nombrado miembro de la British Royal Society, y de igual manera, en otras 14 academias. En Francia, fue promovido a comandante de la Legión de Honor.

En sus últimos años de vida padeció artritis y depresión, problemas que se agudizarían en 1880 tras la muerte de su esposa y de su hijo. Cinco días antes de su muerte, asistió por última vez a la reunión de Bureau des Longitudes. Finalmente, falleció a los 73 años, el 8 de septiembre de 1882 en París, Francia.

2.2. Journal de Mathématiques Pures et Appliquées

El “Journal de Mathématiques Pures et Appliquées.[es] la segunda revista científica más antigua a nivel mundial, la cual fue creada en 1836 por el matemático Joseph Liouville. En efecto, buscó retornar la idea de la revista matemática “Annales de Mathématiques Pures et Appliquées", también denominada como “Annales de Gergonne", extinta en 1832. Liouville, en conjunto con otros matemáticos de la época como Cauchy, Poisson, Poncelet, Ampère, entre otros, enviaron sus trabajos a la revista para su publicación. Como lo menciona Verdier, Gergonne y Lavernède fundaron la primera revista matemática francesa en París, en 1810; en reacción a la cantidad de revistas dedicadas a otras ramas, en las cuales no podía divulgarse el trabajo matemático. De esta manera, Liouville estuvo a cargo de la edición de la revista entre los años de 1836 y 1874. En la actualidad, publica artículos de distintas ramas de la matemática en francés e inglés, elaborados por matemáticos de todo el mundo y los presenta en un tomo, una vez por año.

CAPÍTULO 3

Fundamentos de la Aritmética

«Die Mathematik ist die Königin der Wissenschaften, und die Arithmetik ist die Königin der Mathematik.»

La matemática es la reina de las ciencias y la aritmética es la reina de las matemáticas.

Carl Gauß

Antes de abordar los tópicos correspondientes a la teoría analítica de números, es de vital importancia tener claro ciertas definiciones y resultados que son elementales dentro de la aritmética. Por tal motivo, se decidió dedicar un capítulo netamente a estos fundamentos para que los siguientes tópicos abordados en esta disertación sean más fáciles de desarrollar, y en especial, evitar ambigüedades por notación o conceptos erróneos. Para esto, se parte desde la divisibilidad y la descomposición en factores primos hasta la congruencia modular.

Con base en lo mencionado por Dudley [4], la aritmética estudia los números enteros sobre los cuales se definen las operaciones habituales de adición, sustracción, multiplicación y división, y se establece un orden.

3.1. Algoritmo de la división

Al analizar las operaciones entre números enteros, todas excepto la división, dan como resultado siempre otro entero. A rasgo más profundo, $\mathbb{Z}$ forma un anillo dado que verifica las propiedades distributiva, asociatividad, elemento neutro y clausura bajo adición y multiplicación; además, la adición satisface las propiedades de conmutatividad y elemento identidad.

De esta forma, el estudio de la operación de división toma un rol crucial cuando se trabajó con enteros, puesto que se pretende hallar condiciones bajo las cuales la operación también retorne un entero. Con base en esto se obtuvo uno de los resultados más elementales de la teoría de números, el algoritmo de la división.

Teorema 3.1.1. ***Algoritmo de la división***
Dados $a \in \mathbb{Z}$ y $b \in \mathbb{N}$, entonces $\exists! q, r \in \mathbb{Z}$ tal que $a = bq + r$ para $0 \leq r < b$.

Demostración: Defínase el conjunto $S = \{a - sb : s \in \mathbb{Z}, a - sb \geq 0\}$. Obsérvese que $S \neq \emptyset$ puesto que si $a \geq 0$, entonces $a \in S$ debido a que $a = a - 0 \cdot b \geq 0$. Por el contrario, considérese $a < 0$. Obsérvese que en este caso, se verifica que $a - ab = a(1 - b) \in S$ dado que $1 \leq b \Longrightarrow 1 - b \leq 0$. Por lo tanto, $(-(1 - b) \geq 0 \wedge -a > 0) \Longrightarrow -(1 - b)(-a) = a(1 - b) \geq 0$.

Ahora, por el principio del buen ordenamiento, S tiene un elemento mínimo y tómese a dicho elemento como $a - qb = r \geq 0$. Nótese que $r - b = (a - qb) - b = a - (q + 1)b < 0$, de lo contrario, r no fuese elemento mínimo. Por consiguiente, $r - b < 0 \Longrightarrow r < b$. De esta forma, se prueba la existencia de q y r.

Para demostrar unicidad, supóngase que $\exists q_1, r_1, q_2, r_2 \in \mathbb{Z}$ tales que $a = bq_1 + r_1 = bq_2 + r_2$ para $0 \leq r_1, r_2 < b$. Entonces

$$bq_1 + r_1 = bq_2 + r_2,$$

$$bq_1 + r_1 - bq_2 - r_2 = 0,$$
$$b(q_1 - q_2) + r_1 - r_2 = 0.$$

Obsérvese que $b|0$, lo que implica que $b|b(q_1-q_2)+r_1-r_2$. Claramente $b|b(q_1-q_2)$ por lo tanto, $b|r_1 - r_2$. Además, dado que $0 \leq r_1, r_2 < b$, se tiene que $-b < r_1-r_2 < b$. No obstante, el único múltiplo de b en $(-b, b)$ es 0. En consecuencia, $r_1 - r_2 = 0 \iff r_1 = r_2$. Esto indica que $b(q_1 - q_2) = 0$ y dado que $b \neq 0$, entonces $q_1 - q_2 = 0 \iff q_1 = q_2$. Por consiguiente, q, r son únicos. □

3.2. Algoritmo de Euclides

En un contexto similar al de los números primos, es posible dar con una definición de primalidad relativa entre dos naturales, no necesariamente en primos, en virtud de su divisibilidad. No obstante, se precisa del concepto de máximo común divisor.

Definición 3.2.1. Máximo común divisor gcd

Sean $a, b \in \mathbb{N}$. Si $c \in \mathbb{Z}$ tal que $c|a$ y $c|b$, entonces c se dice ser un divisor común de a y b. En particular, se denomina como máximo común divisor de a y b al mayor divisor común de a y b; dicho número se denota por $gcd(a, b)$.

Definición 3.2.2. Números coprimos

Sean $x, y \in \mathbb{N}$. Se dice que x, y son coprimos o relativamente primos entre sí, cuando $gcd(x, y) = 1$.

Por simple inspección, resulta sumamente sencillo encontrar el máximo común divisor entre dos enteros pequeños; sin embargo, el cálculo puede volverse engorroso para números mayores. El siguiente teorema constituye una herramienta fundamental para obtener el gcd entre cualesquiera dos números enteros.

Teorema 3.2.1. ***Algoritmo de Euclides***

Dados $a, b \in \mathbb{N}$ tal que $b \nmid a$ y $a > b$, sean $r_0 = a$, $r_1 = b$ y obténgase los restos $r_2, \ldots, r_n, r_{n+1}$ al aplicar el algoritmo de la división iteradamente, de forma que para $k \in \{0, 1, \ldots n-1\}$, se verifica que $r_k = r_{k+1}q_{k+1} + r_{k+2}$ tal que $0 \leq r_{k+2} < r_{k+1}$, y $r_{n+1} = 0$. Entonces, $r_n = gcd(a, b)$.

Demostración: En primer lugar, nótese que el algoritmo es finito dado que el conjunto de restos r_k es estrictamente decreciente y eventualmente se llega al resto $r_{n+1} = 0$. Al considerar la última iteración, $r_{n-1} = r_n q_n + r_{n+1}$, se tiene que $r_n | r_{n-1}$ puesto que $r_{n+1} = 0$.

Ahora, analícese la penúltima iteración, $r_{n-2} = r_{n-1}q_{n-1} + r_n$. Dado que $(r_n|r_n \wedge r_n|r_{n-1}) \implies r_n|r_{n-2}$. Sea $k \in \mathbb{N}$ tal que $k < n-1$ y supóngase validez para toda iteración posterior a la k-ésima, es decir, $r_n|r_m$ para $m \in \mathbb{N}$ y $k < m < n-1$. Finalmente, evalúese r_k; por el algoritmo de la división, se tiene que $r_k = r_{k+1}q_{k+1} + r_{k+2}$. Dado que $r_n|r_{k+2}$ y $r_n|r_{k+1}$ por el paso inductivo, entonces $r_n|r_k$. De esta forma, por el principio de inducción matemática, $r_n|r_k$ para $k \in \{0, 1, \ldots, n-1\}$. En particular, $r_n|r_0$ y $r_n|r_1$, es decir, $r_n|a$ y $r_n|b$.

Por último, considérese c un divisor común cualquiera de a y b distinto de r_n. Por la primera iteración del algoritmo de la división, se verifica que $r_0 = r_1q_1 + r_2 \iff r_2 = r_0 - r_1q_1$. Dado que $(c|r_0 \wedge c|r_1) \implies c|r_2$. Sea $k \in \mathbb{N}$ tal que $k > 1$ y supóngase validez para toda iteración anterior a la k-ésima, es decir, $r_n|r_m$ para $m \in \mathbb{N}$ y $1 < m < k$. Finalmente, evalúese r_k; por el algoritmo de la división, se tiene que $r_{k-2} = r_{k-1}q_{k-1} + r_k \iff r_k = r_{k-2} - r_{k-1}q_{k-1}$. Dado que $c|r_{k-2}$ y $c|r_{k-1}$ por el paso inductivo, entonces $c|r_k$. De esta forma, por inducción se sigue que $c|r_k$ para todo $k \in \mathbb{N}$. En particular, $c|r_n$.

Por propiedad de la división, $(c|r_n \wedge c \neq r_n) \implies c < r_n$. Como c es un divisor común arbitrario de a y b, entonces r_n es mayor que cualquier otro divisor común de a y b. Por consiguiente, r_n es el máximo común divisor de a y b. □

Una de las aplicaciones del gcd radica en la resolución de ecuaciones diofánticas, sobre las cuales se construyen las tres identidades de Liouville; en consecuencia, serán tratadas en un capítulo posterior. Ante esta premisa, se presenta uno de los resultados más importantes basados en el máximo común divisor, nombrado en honor del matemático francés Étienne Bézout.

Teorema 3.2.2. ***Lema de Bézout***

Dados $a, b \in \mathbb{N}$, existen $x, y \in \mathbb{Z}$ tales que

$$gcd(a, b) = ax + by. \tag{3.1}$$

Demostración: Sea $d = \gcd(a, b)$. Por la última iteración del algoritmo de Euclides, se verifica que $r_{n-2} = r_{n-1}q_{n-1} + d \iff d = r_{n-2} - r_{n-1}q_{n-1}$. Adicionalmente, dicho algoritmo establece de forma general que $r_k = r_{k+1}q_{k+1} + r_{k+2} \iff r_{k+2} = r_k - r_{k+1}q_{k+1}$ para $k \in \{0, 1, \ldots, n-2\}$.

Como sustento para la demostración, conjetúrese que es posible expresar d como $d = c_k r_k + c_{k+1} r_{k+1}$, $c_k, c_{k+1} \in \mathbb{Z}$ para $k \in \{0, 1, \ldots, n-2\}$. Para probar este enunciado, procédase con inducción. Primero, considérese la penúltima iteración, $r_{n-1} = r_{n-3} - r_{n-2}q_{n-2}$, de forma que al sustituir en la expresión para d, se obtiene que

$$d = r_{n-2} - (r_{n-3} - r_{n-2}q_{n-2})q_{n-1} = r_{n-3}(-q_{n-1}) + r_{n-2}(q_{n-1}q_{n-2} + 1).$$

Sea $k \in \mathbb{N}$ tal que $k < n-2$ y supóngase validez para toda iteración posterior a la k-ésima, es decir, $d = c_m r_m + b_{m+1} c_{m+1}$ para $m \in \mathbb{N}$ y $k < m < n-2$. Finalmente, evalúese para $k-1$ y k. Por el paso inductivo, $\exists c_{k+1}, c_{k+2} \in \mathbb{Z}$ tales que $d = c_{k+1} r_{k+1} + c_{k+2} r_{k+2}$. De acuerdo con el algoritmo de Euclides, se verifica que $r_{k+2} = r_k - r_{k+1} q_{k+1}$. Al sustituir en la expresión para d,

$$d = c_{k+1} r_{k+1} + c_{k+2}(r_k - r_{k+1} q_{k+1}) = r_k c_{k+2} + r_{k+1}(c_{k+1} - c_{k+2} q_{k+1}).$$

Nuevamente, por el algoritmo de Euclides, $r_{k+1} = r_{k-1} - r_k q_k$. Al sustituir en la expresión para d,

$$d = c_{k+2} r_k + (c_{k+1} - c_{k+2} q_{k+1})(r_{k-1} - r_k q_k),$$

$$d = r_{k-1}(c_{k+1} - c_{k+2} q_{k+1}) + r_k(c_{k+2} - c_{k+1} q_k + c_{k+2} q_{k+1} q_k).$$

Sea $c_{k-1} = c_{k+1} - c_{k+2} q_{k+1}$ y $c_k = c_{k+2} - c_{k+1} q_k + c_{k+2} q_{k+1} q_k$. Dado que $\mathbb{Z}$ es un anillo, entonces $c_{k-1}, c_k \in \mathbb{Z}$. En consecuencia, se sigue por inducción que $\exists c_k, c_{k+1} \in \mathbb{Z}$ tales que $d = c_k r_k + c_{k+1} r_{k+1}$, $k \in \{0, 1, \ldots, n-2\}$ con lo que se demuestra la conjetura. En particular, $\exists c_0, c_1 \in \mathbb{Z}$ tales que $d = r_0 c_0 + r_1 c_1$. Como $r_0 = a$ y $r_1 = b$, la demostración se completa. □

3.3. Descomposición canónica

Los números primos han sido uno de los temas más estudiados por los matemáticos a lo largo de los años y sirven de base para la teoría de números analítica. Uno de los resultados más importantes que involucran los números primos es el Teorema Fundamental de la Aritmética, que describe que todo número natural puede descomponerse en potencias de factores primos.

Teorema 3.3.1. ***Teorema Fundamental de la Aritmética***

Todo número natural n distinto de la unidad puede representarse de forma única, salvo el orden, como el producto de potencias de primos distintos,

$$n = \prod_{i \in \mathbb{N}} p_i^{\alpha_i}, \alpha_i \in \mathbb{N}, p_i \text{ primo.} \tag{3.2}$$

Demostración: Obsérvese que todo número natural n distinto de 1 tiene un factor primo. Considérese el conjunto de divisores de n mayores a 1 y menores que n. Si el conjunto es vacío, por definición, n es un número primo. Ahora, si dicho conjunto es no vacío, por el principio del buen ordenamiento, existe un elemento mínimo p entre esos divisores. Nótese que no puede existir un divisor de p mayor a 1 y menor a p, de lo contrario, n tendría un divisor menor que p

y resulta en una contradicción. En consecuencia, p es primo y por lo tanto, n tiene a p como factor primo.

A continuación, nótese que todo número natural n distinto de 1 puede expresarse como el producto de factores primos. Este resultado se sigue del principio de inducción matemática. Considérese el caso base con $n = 2$ y véase que 2 es un número primo. Ahora, supóngase validez para todo $k \in \mathbb{N}$, tal que $2 \leq k < n$. Finalmente, resta analizar el caso n. Obsérvese que existen dos posibilidades para n. Si n es un número primo, entonces la demostración es directa. Tómese n como número compuesto. Por definición, $\exists a, b \in \mathbb{N}$ con $2 \leq a, b < n$, tales que $n = ab$. Por el paso inductivo, se tiene que a, b pueden descomponerse en factores primos y, por consiguiente, n también puede hacerlo.

De esta manera, solo hace falta probar unicidad para completar la demostración del teorema. Primero, nótese que para todo primo p, se satisface que $p|ab \implies (p|a \vee p|b)$. Dado que p es primo, $\gcd(a, p) = 1 \vee \gcd(a, p) = p$. Véase que $\gcd(a, p) = p \implies p|a$, entonces considérese que $\gcd(a, p) = 1$. Por definición, se verifica que $\exists x, y \in \mathbb{Z}$ tales que $ax + py = 1$; al multiplicar por b, se obtiene $abx + pby = b$. Claramente se verifica que $p|pby$ y obsérvese que $p|aby$, dado que $p|ab$. En consecuencia, $p|abx + pby$, es decir, $p|b$.

Véase que al considerar factor primo p tal que $p|q_1 \dots q_k$, entonces $p|q_i$ para algún $i \in \{1, \dots, k\}$ y en particular, $p = q_i$. La primera parte se sigue del principio de inducción matemático; para el caso $k = 1$, $p|q_1$ trivialmente. El siguiente caso para $k = 2$ también es válido; por lo demostrado previamente, se satisface que $p|q_1q_2 \implies (p|q_1 \vee p|q_2)$. Ahora, supóngase validez para $k = l$ y analícese el caso $k = l + 1$. Sea $x = q_1 \dots q_l$. Por lo demostrado previamente, $p|xq_{l+1} \implies (p|x \vee p|q_{l+1})$. Obsérvese que si $p|q_{l+1}$, la verificación es directa; entonces, considérese que $p|x$. No obstante, $x = q_1 \dots q_l$, y por el paso inductivo, existe un $i \in \{1, \dots, l\}$ tal que $p|q_i$. En consecuencia, se verifica para todo $k \in \mathbb{N}$ por inducción. Por último, dado que p y $q_i, i \in \{1, \dots, k\}$ son primos, y $p|q_i$, por definición de número primo, se concluye que $p = q_i$.

Para concluir con la demostración del Teorema Fundamental de la Aritmética, procédase por inducción. El caso base con $n = 2$, se satisface trivialmente. Ahora, supóngase que se cumple para todo $x \in \mathbb{N}$, tal que $2 \leq x < n$. De esta forma, evalúese el caso n. Para demostrar unicidad, supóngase que existen dos formas de expresar la descomposición canónica de n. Sin pérdida de generalidad, considérese factores primos $q_1, \dots, q_k$ y $r_1, \dots, r_m$ tales que $n = q_1 \dots q_k$ y $n = r_1 \dots r_m$, es decir, $q_1 \dots q_k = r_1 \dots r_m$. Según lo demostrado previamente, al considerar q_1, existe un $r_i, i \in \{1, \dots, k\}$ tal que $q_1 = r_i$. En consecuencia, al dividir la expresión para q_1 en ambos lados, se obtiene que

$$q_2 \dots q_k = r_1 \dots r_{i-1} r_{i+1} \dots r_m.$$

Obsérvese que el número resultante es inferior a x, y por el paso inductivo, este puede descomponerse en factores primos de forma única. Como resultado, los factores $r_1 \dots r_{i-1} r_{i+1} \dots r_m$ constituyen un reordenamiento de $q_2 \dots q_k$ y dado que $p_1 = q_i$, se completa la demostración del Teorema Fundamental de la Aritmética. □

3.4. Aritmética modular

Al considerar el algoritmo de la división, uno de los términos involucrados en él corresponde al resto o residuo. En consecuencia, a partir de la división euclídea entre enteros y el conjunto de restos, surge una nueva rama dentro de la teoría de números denominada como aritmética modular o congruencia modular. De acuerdo con lo establecido por Santos [5], las congruencias fueron introducidas por Carl Gauß en su libro "Disquisitiones Arithmeticae" en 1801.

La teoría de congruencias sirve de base para la resolución de ecuaciones diofánticas que como se mencionó anteriormente, serán discutidas en un capítulo posterior. Para empezar, se presenta una definición formal de congruencia.

Definición 3.4.1. Congruencia

Sean $a, b \in \mathbb{Z}$ y $m \in \mathbb{N}$. Se dice que a es congruente a b módulo m si $m|a-b$ y se denota por $a \equiv b \pmod{m}$. El número m se denomina módulo de congruencia.

Definición 3.4.2. Resto

Sean $k, r \in \mathbb{Z}$ y $m \in \mathbb{N}$ tales que $k \equiv r \pmod{m}$. Se dice que r es un resto o residuo de k módulo r.

Recuérdese que una relación de equivalencia verifica las propiedades reflexiva, simétrica y transitiva y se la puede tratar como una bicondicionalidad, es decir, presenta analogías con respecto a la relación de igualdad. Al considerar la congruencia, se tiene el siguiente resultado.

Proposición 3.4.1. La congruencia aritmética define una relación de equivalencia.

Demostración: Sean $a, b, c \in \mathbb{Z}$ y $m \in \mathbb{N}$. Obsérvese que para demostrar equivalencia, la congruencia debe satisfacer las siguientes propiedades:

1. $a \equiv a \pmod{m}$

   Obsérvese que $0 = a - a$ y trivialmente $m|0$. Por definición de congruencia, $m|a-a \Longrightarrow a \equiv a \pmod{m}$.

2. $a \equiv b \pmod{m} \Longrightarrow b \equiv a \pmod{m}$

   Supóngase que $m|a-b$, lo que implica que $a \equiv b \pmod{m}$. Por propiedad de la división, $\exists k \in \mathbb{Z}$ tal que $a - b = mk \Longleftrightarrow b - a = m(-k)$. Dado que $-k \in \mathbb{Z}$, por propiedad de la división, $m|b - a$. Por lo tanto, $b \equiv a \pmod{m}$.

3. $(a \equiv b \pmod{m} \wedge b \equiv c \pmod{m}) \Longrightarrow a \equiv c \pmod{m}$

   Supóngase que $m|a - b$ y $m|b - c$, lo que implica que $a \equiv b \pmod{m}$ y $b \equiv c \pmod{m}$, respectivamente. Por propiedad de la división, $\exists x, y \in \mathbb{Z}$ tales que $a - b = xm \Longleftrightarrow b = a - xm$ y $b - c = ym \Longleftrightarrow b = c + ym$. En consecuencia,

   $$a - xm = c + ym \Longleftrightarrow a - c = (x + y)m \Longleftrightarrow m|a - c.$$

   Por lo tanto, $a \equiv c \pmod{m}$.

□

Ahora, se incluyen enunciados que se basan exclusivamente en las definiciones de congruencia y división euclídea, que como se apreció, están estrechamente relacionadas.

Proposición 3.4.2. Sean $a, b \in \mathbb{Z}$ y $m \in \mathbb{N}$ tales que $a \equiv b \pmod{m}$. Si $0 \leq |a - b| < m$, entonces $a = b$.

Demostración: Supóngase que $0 \leq |a - b| < m$. Por definición de congruencia, $m|a - b$, lo que implica que $m \leq |a - b|$ salvo si $|a - b| = 0$. No obstante, $|a - b| < m$, por lo cual $|a - b| = 0 \Longleftrightarrow a - b = 0 \Longleftrightarrow a = b$. □

Proposición 3.4.3. Sean $a, b \in \mathbb{Z}$ y $m \in \mathbb{N}$. Entonces, $a \equiv b \pmod{m}$ si y solo si a y b dejan el mismo resto cuando se dividen para m.

Demostración: Primero, pártase de que a y b dejan el mismo resto al dividirlos para m. Por el algoritmo de la división, $a = mq_1 + r \Longleftrightarrow r = a - mq_1$ y $b = mq_2 + r \Longleftrightarrow r = b - mq_2$ para $q_1, q_2 \in \mathbb{N}$ y $0 \leq r < m$. En consecuencia,

$$a - mq_1 = b - mq_2 \Longleftrightarrow a - b = m(q_1 - q_2) \Longleftrightarrow m|a - b.$$

Por lo tanto, $a \equiv b \pmod{m}$. Ahora, considérese el recíproco, pártase de que $a \equiv b \pmod{m}$. Por definición, $m|a - b$ y nótese que $a - b = a - b - 0$, de esta manera $a - b \equiv 0 \pmod{m}$. Por el algoritmo de la división, $a = mq_1 + r_1$ y $b = mq_2 + r_2$ para $q_1, q_2 \in \mathbb{N}$ y $0 \leq r_1, r_2 < m$. De esta forma, al restar ambas

expresiones, se obtiene que $0 \leq |r_1 - r_2| < m$ y

$$a-b = mq_1+r_1-(mq_2+r_2) \iff a-b-(r_1-r_2) = m(q_1-q_2) \iff m|a-b-(r_1-r_2).$$

Por consiguiente, $a - b \equiv r_1 - r_2 \pmod{m}$. Dado que la congruencia describe una relación de equivalencia, como $a-b \equiv 0 \pmod{m}$, se tiene que $0 \equiv r_1 - r_2 \pmod{m}$. Según la proposición 3.4.2, como $0 \leq |r_1 - r_2| < m$, entonces $0 = r_1 - r_2 \iff r_1 = r_2$. □

Nótese que de forma natural, se pueden aplicar operaciones aritméticas dentro de las congruencias. A continuación, se detallan algunos de los resultados.

Teorema 3.4.1. *Sean $a, b, c, d \in \mathbb{Z}$ y $m \in \mathbb{N}$ tales que $a \equiv b \pmod{m}$ y $c \equiv d \pmod{m}$, entonces:*

$$a \pm c \equiv b \pm d \pmod{m}, \tag{3.3}$$

y también

$$ac \equiv bd \pmod{m}. \tag{3.4}$$

Demostración: Por definición de congruencia, $m|a - b$ y $m|c - d$. Según las propiedades de la división, $\exists x, y \in \mathbb{Z}$ tales que $a - b = xm$ y $c - d = ym$.

Para probar 3.3, súmese o réstese ambas expresiones, entonces

$$a-b\pm(c-d) = xm+ym \iff a\pm c-(b\pm d) = (x+y)m \iff m|a\pm c-(b\pm d).$$

Por lo tanto, $a \pm c \equiv b \pm d \pmod{m}$.

Ahora para 3.4, multiplíquese la primera expresión por c y la segunda por b, entonces $ac-bc = cxm \iff bc = ac-cxm$ y $bc-bd = bym \iff bc = bd+bym$. En consecuencia,

$$ac - cxm = bd + bym \iff ac - bd = (cx + by)m \iff m|ac - bd.$$

Por lo tanto, $ac \equiv bd \pmod{m}$. □

Teorema 3.4.2. *Sean $a, b \in \mathbb{Z}$ y $m, n \in \mathbb{N}$ tales que $a \equiv b \pmod{m}$, entonces*

$$a^n \equiv b^n \pmod{m}. \tag{3.5}$$

Demostración: Obsérvese que para $n = 1$, la prueba es directa; para el resto de casos, procédase por inducción. Considérese el caso base con $n = 2$. Con base en 3,4 al tomar $c = a$ y $b = d$, se obtiene que $a^2 \equiv b^2 \pmod{m}$. Ahora, supóngase validez para algún $k \in \mathbb{N}$ y analícese el caso $n = k + 1$. Nótese

que $a \equiv b \pmod{m}$ por definición, y según el paso inductivo, se verifica que $a^k \equiv b^k \pmod{m}$. Nuevamente, al aplicar 3.4, se concluye que $a^{k+1} \equiv b^{k+1} \pmod{m}$. Por el principio de inducción matemática, la expresión es válida para todo $n \in \mathbb{N}$ con lo que se completa la demostración. □

Los siguientes resultados involucran al máximo común divisor dentro de la congruencia.

Teorema 3.4.3. ***Ley de cancelación***
Sean $a, b, c, d, m \in \mathbb{N}$. Si $ac \equiv bc \pmod{m}$ y $d = gcd(m, c)$, entonces

$$a \equiv b \left(\mod \frac{m}{d}\right). \tag{3.6}$$

Demostración: Supóngase que $ac \equiv bc \pmod{m}$, de esta manera, por definición se verifica que $m|ac - bc \iff c(a - b) = km, k \in \mathbb{Z}$. Sea $d = \gcd(m, c)$, de forma que $d|m$ y $d|c$, lo cual implica que $\frac{m}{d}, \frac{c}{d} \in \mathbb{Z}$. Por lo tanto, al dividir la expresión para d,

$$\frac{c}{d}(a - b) = k\left(\frac{m}{d}\right) \iff \frac{m}{d}\Big| a - b.$$

Por consiguiente, $a \equiv b \left(\mod \frac{m}{d}\right)$. □

Teorema 3.4.4. *Sean $a, b \in \mathbb{Z}$ y $m, c \in \mathbb{N}$ tales que $a \equiv b \pmod{m}$. Si $c|m$ y $c|a$, entonces $c|b$.*

Demostración: Por definición, se verifica que $m|a - b$; por lo cual, $\exists k \in \mathbb{Z}$ tal que $a - b = mk \iff a - mk = b$. De esta forma, $c|m \wedge c|a \implies c|a - mk$, es decir, $c|b$. □

Teorema 3.4.5. *Sean $a, b, m \in \mathbb{N}$. Si $a \equiv b \pmod{m}$, entonces $gcd(a, m) = gcd(b, m)$.*

Demostración: Sean $c = \gcd(a, m)$ y $d = \gcd(b, m)$ y supóngase que $a \equiv b \pmod{m}$. Por definición de máximo común divisor y con base en el teorema 3.4.4, $c|a \wedge c|m \implies c|b$ y $d|b \wedge d|m \implies d|a$; lo cual a su vez implica que $c|d$ y $d|c$, respectivamente. En consecuencia, $c = d$, por propiedad de la división. □

Por último, se presentan dos teoremas fundamentales de la teoría de números que involucran la aritmética modular, los cuales serán de vital importancia en capítulos posteriores; estos son el pequeño teorema de Fermat y el teorema de Wilson. Como manifiesta Dudley [4], el primero fue enunciado por Pierre de Fermat en 1640 y su alcance es de vital importancia para el estudio de congruencias cuadráticas.

Teorema 3.4.6. ***Pequeño teorema de Fermat***
Sea p un primo y $a \in \mathbb{N}$ tal que $\gcd(a, p) = 1$. *Entonces,*

$$a^{p-1} \equiv 1 \pmod{p}. \tag{3.7}$$

Demostración: Para empezar, considérese la siguiente la congruencia

$$a^p \equiv a \pmod{p}. \tag{3.8}$$

Por el teorema 3.4.1, la congruencia 3.7 implica 3.8. Además, dado que $\gcd(a, p) = 1$, por la ley de cancelación, la congruencia 3.8 conlleva 3.7. En consecuencia, ambas expresiones son equivalentes.

A continuación, fíjese un primo p y procédase por inducción. De esta forma, considérese el caso base con $a = 1$ puesto que $\gcd(1, p) = 1$. Evidentemente, $1^p \equiv 1 \pmod{p}$. Supóngase validez para $a = k$ tal que $\gcd(k, p) = 1$, es decir, $k^p \equiv k \pmod{p}$. Ahora analícese el caso $a = k + 1$ tal que $\gcd(k + 1, p) = 1$. Por la fórmula del binomio de Newton,

$$(k+1)^p = \sum_{i=0}^{p} \binom{p}{i} k^{p-i} = k^p + \sum_{i=1}^{p-1} \binom{p}{i} k^{p-i} + 1.$$

Por definición, los coeficientes binomiales vienen dados por

$$\binom{p}{i} = \frac{p!}{i!(p-i)!}.$$

En consecuencia, $p \mid \binom{p}{i}$ para $1 \leq i \leq p - 1$. De esta manera, al considerar la congruencia módulo p, se tiene

$$(k+1)^p \equiv k^p + \sum_{i=1}^{p-1} (0) k^{p-i} + 1 \equiv k^p + 1 \pmod{p}.$$

Por el paso inductivo, se satisface que $k^p \equiv k \pmod{p}$, lo cual a su vez implica que $(k + 1)^p \equiv k + 1 \pmod{p}$. Por el principio de inducción matemática, la congruencia se verifica para todo $n \in \mathbb{N}$ y, dado que la elección del factor primo p es arbitraria, se finaliza la demostración. □

Finalmente, se introduce el teorema de Wilson que otorga una condición suficiente y necesaria para evaluar la primalidad de un número.

Teorema 3.4.7. ***Teorema de Wilson***
Sea $p \in \mathbb{N}$, entonces p es primo si y solo si

$$(p-1)! \equiv -1 \pmod{p}. \tag{3.9}$$

Demostración: Primero, pártase de que $(p-1)! \equiv -1 \pmod{p}$ y procédase por contradicción. Supóngase que p es compuesto. En consecuencia, existe un $d \in \mathbb{N}$ con $1 < d < p$ tal que $d|p$ y por ende, $d|(p-1)!$. Ahora, como $d > 1$, se tiene que $d \nmid (p-1)!+1$, lo cual a su vez implica que $p|(p-1)!+1$. No obstante, esto es imposible, puesto que $(p-1)! \equiv -1 \pmod{p} \iff p|(p-1)!+1$. Por consiguiente, se tiene una contradicción y la suposición inicial es errónea. De manera que p es primo.

A continuación, pártase de que p es primo. Si $p = 2$, trivialmente se cumple que $1! \equiv 1 \equiv -1 \pmod{2}$. Entonces, trabájese con un primo impar p. Sea $a \in \{1, \ldots, p-1\}$ y obsérvese que a tiene un inverso x módulo p. Dado que p es primo, $p \nmid a$, es decir, $\gcd(a, p) = 1$. Por el lema de Bézout, $\exists x, y \in \mathbb{Z}$ tal que $ax + py = 1$. De esta manera, al analizar la congruencia módulo p, se tiene que

$$ax + py \equiv ax \equiv 1 \pmod{p}.$$

Nótese que dicho inverso es único; para ver esto, supóngase que x y x' son ambos inversos de a. Por definición, $ax \equiv ax' \equiv 1 \pmod{p}$. Por la ley de cancelación, dado que $\gcd(a, p) = 1$, se concluye que $x \equiv x' \pmod{p}$.

Ahora, considérese el caso en que a es inverso consigo mismo, por definición, $a^2 \equiv 1 \pmod{p} \iff a^2 - 1 \equiv 0 \pmod{p} \iff (a+1)(a-1) \equiv 0 \pmod{p}$. Por lo tanto, $a + 1 \equiv 0 \pmod{p}$ o $a - 1 \equiv 0 \pmod{p}$, es decir, $a \equiv -1 \pmod{p}$ o $a \equiv 1 \pmod{p}$. Nótese que $p - 1 \equiv -1 \pmod{p}$, de manera que se concluye que 1 y $p - 1$ son los únicos elementos que son inversos módulo p consigo mismos. Por lo tanto, como p es impar y se descartan 1 y $p - 1$, entonces es posible agrupar los demás restos en $\frac{p-3}{2}$ pares (h, k), de tal forma que estos sean inversos módulo p, es decir, $hk \equiv 1 \pmod{p}$ para $h, k \in \{2, \ldots, p-2\}$ y $h \neq k$. En consecuencia,

$$(p-1)! \equiv (p-1)(1) \prod_{i=2}^{p-2} i \equiv (-1) \prod_{i=1}^{\frac{p-3}{2}} h_i k_i \equiv - \prod_{i=1}^{\frac{p-3}{2}} 1 \equiv -1 \pmod{p}.$$

Luego, se satisface la bicondicionalidad y la demostración se completa. □

CAPÍTULO 4

Funciones Aritméticas

«C'est avec la logique que nous prouvons
et avec l'intuition que nous trouvons.»

Probamos por medio de la lógica, pero descubrimos por medio de la intuición.

Henri Poincaré

A rasgo general, las funciones son una parte muy estudiada dentro de la matemática, principalmente en análisis, combinatoria y teoría de números. Recuérdese que una función se interpreta como una asociación de elementos entre dos conjuntos, tales que a cada elemento del conjunto de salida o dominio se le asigna un único elemento del conjunto de llegada o codominio. Según lo establecido por Santos [5], una función aritmética es aquella función compleja o real valuada que se define para todos los enteros. Este tipo de funciones constituyen un eje fundamental en la teoría de números analítica, y en particular, son el pilar de las identidades de Liouville. En este capítulo, se abordarán varias de ellas.

4.1. Funciones multiplicativas

La propiedad de multiplicidad es una herramienta muy útil al momento de definir una fórmula cerrada para las funciones aritméticas. A continuación, se dará una definición para esta propiedad.

Definición 4.1.1. Funciones multiplicativas
Sea f una función aritmética. Se dice que f es multiplicativa si para todo $m, n \in \mathbb{N}$ tal que m y n son coprimos, se verifica que $f(mn) = f(m)f(n)$.

Al suprimir la condición de primalidad relativa, se puede dar con otro tipo de funciones.

Definición 4.1.2. Funciones completamente multiplicativas
Sea f una función aritmética. Se dice que f es una función completamente multiplicativa, si $f(mn) = f(m)f(n), \forall m, n \in \mathbb{N}$.

Obsérvese que dos números primos distintos trivialmente son coprimos entre sí. En consecuencia, resulta factible aprovechar la descomposición canónica y trabajar con factores primos para calcular el valor numérico de las funciones multiplicativas. En consecuencia, la dificultad que se presenta es hallar algún método que permita probar dicha propiedad en las funciones aritméticas. A continuación, se tiene el siguiente resultado.

Teorema 4.1.1. *Sea f una función multiplicativa. En consecuencia, la función*

$$G(n) = \sum_{d|n} f(d)$$

es también multiplicativa.

Demostración: Con base en la definición de función multiplicativa, considérese m, n coprimos y evalúese la función $G(mn) = \sum_{d|mn} f(d)$.

Dado que m y n son coprimos, entonces $\gcd(m, n) = 1$. Por el Teorema Fundamental de la Aritmética, m y n pueden descomponerse en factores primos de forma única. Sin pérdida de generalidad, tómese $m = p_1^{\alpha_1} \dots p_k^{\alpha_k}$ y $n = q_1^{\beta_1} \dots q_r^{\beta_r}$. Como m y n son coprimos, la intersección entre los factores primos de m y n es vacía. En consecuencia, $mn = p_1^{\alpha_1} \dots p_k^{\alpha_k} q_1^{\beta_1} \dots q_r^{\beta_r}$. Ahora, al considerar un divisor d de mn, este viene dado por $d = p_1^{a_1} \dots p_k^{a_k} q_1^{b_1} \dots q_r^{b_r}$, con $0 \leq a_i < \alpha_i$ para $i \in \{1, \dots, k\}$ y $0 \leq b_j < \beta_j$ para $j = \{1, \dots r\}$. De esta manera, sea $x = p_1^{a_1} \dots p_k^{a_k}$ y $y = q_1^{b_1} \dots q_r^{b_r}$. Evidentemente, se verifica que $\gcd(x, y) = 1$, $x|m$, $y|n$ y $d = xy$. Nuevamente, el Teorema Fundamental de la Aritmética garantiza la unicidad de x y y.

Por lo demostrado previamente y dado que f es multiplicativa, G puede expresarse de la siguiente manera

$$G(mn) = \sum_{d|mn} f(d) = \sum_{\substack{x|m \\ y|n}} f(xy) = \sum_{\substack{x|m \\ y|n}} f(x)f(y).$$

Obsérvese que la doble condición puede separarse como doble sumatoria. Por consiguiente,

$$G(mn) = \sum_{x|m} \sum_{y|n} f(x)f(y) = \sum_{x|m} f(x) \sum_{y|n} f(y) = G(m)G(n).$$

□

4.2. Algunas funciones aritméticas

Los divisores de un número natural n desempeñan un papel importante; de esta manera, se definen las siguientes funciones aritméticas.

Definición 4.2.1. Función τ

La función τ devuelve el número de divisores positivos de un número natural n, es decir,

$$\tau(n) = \sum_{d|n} 1. \tag{4.1}$$

Proposición 4.2.1. Dada la descomposición canónica de un número natural

n, la función τ viene dada por

$$\tau(n) = \prod_{i \in \mathbb{N}} (\alpha_i + 1). \tag{4.2}$$

Demostración: Obsérvese que τ es una función multiplicativa. Dado que $\tau(n) = \prod_{d|n} 1$ y $f(n) = 1$ es multiplicativa de forma trivial, por el teorema 4.1.1, τ es multiplicativa.

Ahora, es posible hacer uso de la descomposición canónica para aprovechar la propiedad multiplicativa al considerar los factores primos. De esta forma, evalúese $\tau(p^k)$ cuando p es primo y $k \in \mathbb{N}$. Nótese que como p es primo, entonces los únicos divisores de p^k son las potencias p^i con $i \in \mathbb{N}$ tal que $0 \leq i \leq k$. Mediante un conteo simple, se concluye que p^k tiene exactamente $k + 1$ divisores positivos. Por consiguiente, $\tau(p^k) = k + 1$.

Finalmente, recúrrase al hecho de que τ es multiplicativa y aplíquese el Teorema Fundamental de la Aritmética. De esta manera,

$$\tau(n) = \tau\left(\prod_{i \in \mathbb{N}} p_i^{\alpha_i}\right) = \prod_{i \in \mathbb{N}} \tau(p_i^{\alpha_i}) = \prod_{i \in \mathbb{N}} (a_i + 1).$$

□

Definición 4.2.2. Función σ

La función σ devuelve la suma de todos los divisores positivos de un número natural n, es decir,

$$\sigma(n) = \sum_{d|n} d. \tag{4.3}$$

Proposición 4.2.2. Dada la descomposición canónica de un número natural n, la función σ viene dada por

$$\sigma(n) = \prod_{i \in \mathbb{N}} \frac{p_i^{\alpha_i + 1} - 1}{p_i - 1}. \tag{4.4}$$

Demostración: Obsérvese que σ es una función multiplicativa. Dado que $\sigma(n) = \prod_{d|n} d$ y $f(n) = n$ es multiplicativa, por el teorema 4.1.1, σ es multiplicativa.

En consecuencia, considérese la descomposición canónica de n y analícese $\sigma(p^k)$ cuando p es primo y $k \in \mathbb{N}$. Previamente, se observó que los divisores

de p^k son las potencias p^i con $i \in \mathbb{N}$ tal que $0 \leq i \leq k$. En consecuencia, los divisores de p^k se hallan en una progresión geométrica con razón p y cuyo término inicial es $p^0 = 1$. De esta manera, como $\tau(p^k) = k + 1$, se verifica que $\sigma(p^k)$ es igual a la suma de los primeros $k + 1$ términos de la progresión geométrica. Por lo tanto,

$$\sigma(p^k) = \sum_{i=0}^{k} p^i = \frac{p^{k+1} - 1}{p - 1}.$$

Finalmente, por el Teorema Fundamental de la Aritmética y dado que σ es multiplicativa,

$$\sigma(n) = \sigma\left(\prod_{i\in\mathbb{N}} p_i^{\alpha_i}\right) = \prod_{i\in\mathbb{N}} \sigma(p_i^{\alpha_i}) = \prod_{i\in\mathbb{N}} \frac{p_i^{\alpha_i+1} - 1}{p_i - 1}.$$

□

Para estas dos funciones aritméticas que trabajan con los divisores de un natural, se puede definir una tercera que sirva de generalización, tal como se muestra a continuación.

Definición 4.2.3. Función σ_k

Para todo $k \in \mathbb{C}$, la función σ_k se define como la suma de las k-ésimas potencias de los divisores de n, es decir,

$$\sigma_k(n) = \sum_{d|n} d^k. \tag{4.5}$$

Obsérvese que τ y σ son un caso particular de σ_k. En efecto, se tiene que

$$\sigma_0(n) = \sum_{d|n} d^0 = \sum_{d|n} 1 = \tau(n),$$

$$\sigma_1(n) = \sum_{d|n} d^1 = \sum_{d|n} d = \sigma(n).$$

Proposición 4.2.3. Dada la descomposición canónica de un número natural n, la función σ_k con $k \neq 0$ viene dada por

$$\sigma_k(n) = \prod_{i\in\mathbb{N}} \frac{p_i^{k(\alpha_i+1)} - 1}{p_i - 1}. \tag{4.6}$$

Demostración: En primer lugar, nótese que $f(n) = n^k, k \in \mathbb{C}$ es multiplicativa. Por propiedad de los exponentes, se verifica que

$$f(mn) = (mn)^k = (m^k)(n^k) = f(m)f(n).$$

Por el teorema 4,1,1 y dado que $\sigma_k(n) = \prod_{d|n} d^k$, σ_k es multiplicativa.

Ahora, considérese la descomposición canónica de n y analícese $\sigma_k(p^r)$ cuando p es primo y $r \in \mathbb{N}$. En la demostración de la proposición 4.2 se observó que los divisores de p^r se hallan en una progresión geométrica, cuyo término inicial es $p^0 = 1$. En este caso, como se deben considerar las k-ésimas potencias, la progresión tiene razón p^k. Por consiguiente, como $\tau(p^r) = k + 1$, se verifica que $\sigma_k(p^r)$ es igual a la suma de los primeros $k + 1$ términos de la progresión. Entonces,

$$\sigma_k(p^r) = \sum_{i=0}^{r} (p^k)^i = \frac{p^{k(r+1)} - 1}{p - 1}.$$

Finalmente, por el Teorema Fundamental de la Aritmética y dado que σ_k es multiplicativa,

$$\sigma_k(n) = \sigma_k\left(\prod_{i\in\mathbb{N}} p_i^{\alpha_i}\right) = \prod_{i\in\mathbb{N}} \sigma_k(p_i^{\alpha_i}) = \prod_{i\in\mathbb{N}} \frac{p_i^{k(r+1)} - 1}{p - 1}.$$

Para el caso $k = 0$, véase la ecuación 4.1 obtenida para τ. □

Por su parte, Williams [3], realiza una distinción de esta última función en virtud de la paridad. En este caso, se trabajará con σ_k al considerar divisores que generan un número impar y se define la siguiente función aritmética.

Definición 4.2.4. Función σ_k^*

Para todo $k \in \mathbb{C}$, se define la función σ_k^* como la suma de las k-ésimas potencias de los divisores de n tal que su cociente es impar, es decir,

$$\sigma_k^*(n) = \sum_{\substack{d|n \\ 2\nmid \frac{n}{d}}} d^k. \tag{4.7}$$

En particular, para $k = 1$ simplemente se denota $\sigma_1^* = \sigma^*$.

Para dar con una fórmula para σ_k^*, se trabajará con las funciones aritméticas previamente definidas.

Proposición 4.2.4. La función σ_k^* es multiplicativa y para todo $n \in \mathbb{N}$, se satisface que

$$\sigma_k^*(n) = \sigma_k(n) - \sigma_k\left(\frac{n}{2}\right). \tag{4.8}$$

Demostración: Considérese m, n coprimos y evalúese la función $\sigma_k^*(mn)$. Bajo las mismas consideraciones detalladas en la demostración del teorema 4.1.1, se verifica que:

$$\sigma_k^*(mn) = \sum_{\substack{d|mn \\ 2\nmid \frac{mn}{d}}} d^k = \sum_{\substack{x|m \\ y|n \\ 2\nmid \frac{mn}{xy}}} (xy)^k = \sum_{\substack{x|m \\ 2\nmid \frac{m}{x}}} x^k \sum_{\substack{y|n \\ 2\nmid \frac{n}{y}}} y^k = \sigma_k^*(m)\sigma_k^*(n).$$

En consecuencia, σ_k^* es multiplicativa.

Nota: La condición $2 \nmid \frac{mn}{xy}$ implica que $2 \nmid \frac{mn}{x}$ y $2 \nmid \frac{mn}{y}$. En particular, dado que $x|m$ y $y|n$, puede simplificarse como $2 \nmid \frac{m}{x}$ y $2 \nmid \frac{n}{y}$.

Ahora, procédase a analizar los el conjunto de los divisores de n tal que $\frac{n}{d}$ es par.

$$\left\{d \in \mathbb{N} : d|n, 2 \;\middle|\; \frac{n}{d}\right\} = \left\{d \in \mathbb{N} : d|n, d \;\middle|\; \frac{n}{2}\right\} = \left\{d \in \mathbb{N} : d \;\middle|\; \frac{n}{2}\right\}.$$

Como consecuencia del algoritmo de la división, todos los enteros son de la forma $2k$ o $2k-1$ para $k \in \mathbb{Z}$, es decir, el conjunto de los números pares e impares es disjunto. Por lo tanto, el conjunto de divisores de n puede expresarse como:

$$\{d \in \mathbb{N} : d|n\} = \left\{d \in \mathbb{N} : d|n, 2 \;\middle|\; \frac{n}{d}\right\} \cup \left\{d \in \mathbb{N} : d|n, 2 \nmid \frac{n}{d}\right\}.$$

Con base en lo demostrado previamente, se concluye que

$$\left\{d \in \mathbb{N} : d|n, 2 \nmid \frac{n}{d}\right\} = \{d \in \mathbb{N} : d|n\} \setminus \left\{d \in \mathbb{N} : d \;\middle|\; \frac{n}{2}\right\}.$$

De esta manera, se deduce que

$$\sigma_k^*(n) = \sum_{\substack{d|n \\ 2\nmid \frac{n}{d}}} d^k = \sum_{d|n} d^k - \sum_{d|\frac{n}{2}} d^k = \sigma_k(n) - \sigma_k\left(\frac{n}{2}\right).$$

□

Los siguientes teoremas, que se tratarán a continuación, constituyen una herramienta fundamental para las aplicaciones de la primera identidad de Liouville, como se podrá apreciar en un capítulo posterior. Cada uno de estos resultados guarda una conexión intrínseca con la aritmética modular.

Teorema 4.2.1. *Sea $n \in \mathbb{N}$. Si $n \equiv 0 \pmod 2$, entonces $\sigma^*(n) \equiv 0 \pmod 2$.*

Demostración: Sea $n \equiv 0 \pmod 2$; de esta manera, la descomposición canónica viene dada por $n = 2^\alpha k$ con $\alpha, k \in \mathbb{N}$ y $k \equiv 1 \pmod 2$. Por teorema, σ^* es multiplicativa y con base en la proposición 4.2.4, se concluye que

$$\sigma^*(n) = \sigma^*(2^\alpha k) = \sigma^*(2^\alpha)\sigma^*(k) = \left(\sigma(2^\alpha) - \sigma\left(2^{\alpha-1}\right)\right)\sigma^*(k).$$

Por la proposición 4.2.2,

$$\sigma(2^\alpha) - \sigma\left(2^{\alpha-1}\right) = 2^{\alpha+1} - 1 - (2^\alpha - 1) = 2^\alpha.$$

En consecuencia,

$$\sigma^*(n) = 2^\alpha \sigma^*(k) \equiv 0 \pmod 2.$$

□

Teorema 4.2.2. *Sean $n, N \in \mathbb{N}$ tal que N es el mayor divisor impar de n. Entonces, $\sigma(n) \equiv 1 \pmod 2$ si y solo si N es un cuadrado perfecto.*

Demostración: Por teorema, la función σ es multiplicativa; entonces, es posible trabajar con la descomposición canónica de n. Sin pérdida de generalidad, tómese

$$n = 2^\alpha \prod_{i \in \mathbb{N}} p_i^{\beta_i}, \alpha \in \mathbb{N}, \beta_i \in \mathbb{N}, p_i \text{ primo impar.}$$

En este caso, el mayor divisor impar de n viene dado por $N = \prod_{i \in \mathbb{N}} p_i^{\beta_i}$. Por la proposición 4.2.2,

$$\sigma(n) = (2^{\alpha+1} - 1) \prod_{i \in \mathbb{N}} \frac{p_i^{\beta_i+1} - 1}{p_i - 1} = (2^{\alpha+1} - 1) \prod_{i \in \mathbb{N}} \left(\sum_{k=0}^{\beta_i} p_i^k \right).$$

Obsérvese que por el teorema 3.4.2, como $p_i \equiv 1 \pmod 2$, entonces $p_i^k \equiv 1 \pmod 2$ para todo $k \in \mathbb{N}$. Por lo tanto,

$$\sum_{k=0}^{\beta_i} p_i^k \equiv \begin{cases} 1 \pmod 2, & \beta_i \equiv 0 \pmod 2 \\ 0 \pmod 2, & \beta_i \equiv 1 \pmod 2 \end{cases}.$$

Nótese que $2^{\alpha+1} - 1 \equiv 1 \pmod 2$, lo que implica que

$$\sigma(n) \equiv \begin{cases} 1 \pmod 2, & \beta_i \equiv 0 \pmod 2 \\ 0 \pmod 2, & \beta_i \equiv 1 \pmod 2 \end{cases}.$$

Finalmente, interprétese cada caso; $\beta_i \equiv 0$ significa que N es un cuadrado perfecto y $\beta_i \equiv 1 \pmod 2$, lo contrario. Dado que la congruencia modular verifica una relación de equivalencia, la bicondicionalidad se satisface y se concluye la demostración. □

Teorema 4.2.3. *Sea $n \in \mathbb{N}$. Entonces, $\sigma^*(n) \equiv 1 \pmod 2$ si y solo si n un cuadrado perfecto impar.*

Demostración: Primero, sea $\sigma^*(n) \equiv 1 \pmod 2$. Por la contrapositiva del teorema 4.2.1, $n \equiv 1 \pmod 2$. Con base en la proposición 4.2.4, se verifica que

$$\sigma^*(n) = \sigma(n) - \sigma\left(\frac{n}{2}\right) = \sigma(n).$$

En consecuencia, $\sigma \equiv 1 \pmod 2$. Dado que n es impar, entonces n no tiene divisores pares. Por el teorema 4.2.2, n es un cuadrado perfecto impar.

Ahora, sea n un cuadrado perfecto impar. Por el teorema 4.2.2 y lo obtenido previamente, $\sigma(n) = \sigma^*(n) \equiv 1 \pmod 2$. □

Recuérdese que el algoritmo de Euclides, permite clasificar a los enteros según su clase equivalente en virtud del resto que dejan al dividirlos para algún entero k. De esta forma, es posible definir una nueva función aritmética al realizar esta modificación a la función τ como se indica a continuación.

Definición 4.2.5. Función $\tau_{k,m}$

Para $k \in \mathbb{Z}$ y $m \in \mathbb{N}$, la función $\tau_{k,m}$ se define como el número de divisores positivos de n tales que $d \equiv k \pmod m$, es decir,

$$\tau_{k,m}(n) = \sum_{\substack{d|n \\ d \equiv k \pmod m}} 1. \tag{4.9}$$

Teorema 4.2.4. *Sean $m, n \in \mathbb{N}$ tal que $m|n$ y $k \in [m]$, entonces*

$$\tau_{0,m}(n) = \tau\left(\frac{n}{m}\right), \tag{4.10}$$

$$\sum_{i=0}^{n-1} \tau_{i,m}(n) = \tau(n). \tag{4.11}$$

Sea $r \in \mathbb{N}$. Si $r|k$ y $r|m$, entonces

$$\tau_{k,m}(n) = \tau_{\frac{k}{r},\frac{m}{r}}\left(\frac{n}{r}\right). \tag{4.12}$$

Demostración: Por propiedad de la congruencia modular, se verifica que $d \equiv 0 \pmod{m} \iff m|d \iff d = am, a \in \mathbb{Z}$. En consecuencia,

$$\tau_{0,m}(n) = \sum_{\substack{d|n \\ d\equiv 0 \pmod{m}}} 1 = \sum_{am|n} 1 = \sum_{a|\frac{n}{m}} 1 = \tau\left(\frac{n}{m}\right).$$

Ahora, trabájese para demostrar la segunda identidad. Según la definición 4.2.5

$$\sum_{i=0}^{n-1} \tau_{i,m}(n) = \sum_{i=0}^{n-1} \sum_{\substack{d|n \\ d\equiv i \pmod{m}}} 1.$$

Por el Algoritmo de Euclides, todos los enteros pueden clasificarse según su clase equivalente módulo m y dichas clases son disjuntas. Nótese que existen m posibles restos módulo m, estos son $\{0, 1, \ldots, m-1\}$. Por lo tanto, si se considera la suma del número de divisores de n de todas las clases equivalentes módulo m, se obtiene el número total de divisores de n. De esta forma,

$$\sum_{i=0}^{n-1} \tau_{i,m}(n) = \sum_{d|n} 1 = \tau(n).$$

Finalmente, obsérvese que

$$\tau_{k,m}(n) = \sum_{\substack{d|n \\ d\equiv k \pmod{m}}} 1 = \sum_{\substack{d|n \\ d\equiv \frac{rk}{r} \pmod{\frac{rm}{r}}}} 1.$$

Dado que $r|k$ y $r|m$, entonces $\frac{k}{r}, \frac{m}{r} \in \mathbb{Z}$. Sin pérdida de generalidad, tómese $x = \frac{k}{r}$ y $y = \frac{m}{r}$. Por propiedad de la congruencia modular se satisface que $d \equiv rx \pmod{ry} \iff ry|d - rx \iff d - rx = ary, a \in \mathbb{Z}$.

En consecuencia, $d = ary + rx = r(ay + x) \iff r|d \iff d \equiv 0 \pmod{r}$. De esta manera, $b = \frac{d}{r} \in \mathbb{N}$ y

$$\tau_{k,m}(n) = \sum_{\substack{b|\frac{n}{r} \\ b\equiv \frac{k}{r} \pmod{\frac{m}{r}}}} 1 = \tau_{\frac{k}{r},\frac{m}{r}}\left(\frac{n}{r}\right).$$

□

Como señala Williams [3], es posible definir una nueva función aritmética fundamentada puramente en la divisibilidad de dos enteros.

Definición 4.2.6. Función F_k
Dados $k, n \in \mathbb{N}$, se define la función $F_k(n)$ como

$$F_k(n) = \begin{cases} 1, & k \mid n \\ 0, & k \nmid n \end{cases} . \tag{4.13}$$

Teorema 4.2.5. *Sean $k, n \in \mathbb{N}$, entonces*

$$\sum_{d|n} F_k(d) = \tau\left(\frac{n}{k}\right). \tag{4.14}$$

Demostración: Por definición de la función F_k, se verifica que

$$\sum_{d|n} F_k(d) = \sum_{\substack{d|n \\ k|d}} 1.$$

Obsérvese que $k|d \iff d = ak, a \in \mathbb{Z}$. En consecuencia,

$$\sum_{d|n} F_k(d) = \sum_{ak|n} 1 = \sum_{a|\frac{n}{k}} 1 = \tau\left(\frac{n}{k}\right).$$

□

Otra de importante utilidad corresponde a la función máximo entero, la cual será relevante para el siguiente el capítulo.

Definición 4.2.7. Función máximo entero $[\![\ ]\!]$
Para todo $x \in \mathbb{R}$, la función máximo entero, también denominada función piso o parte entera, devuelve el único entero $[\![x]\!]$ tal que $[\![x]\!] \leq x < [\![x]\!] + 1$. Matemáticamente, viene dada por

$$[\![x]\!] = \max_{n \in \mathbb{Z}} \{n : n \leq x\}. \tag{4.15}$$

Teorema 4.2.6. *Sean $n \in \mathbb{Z}$ y $x \in \mathbb{R}$. Entonces,*

$$[\![x + n]\!] = [\![x]\!] + n. \tag{4.16}$$

Demostración: Por definición de máximo entero,

$$[\![x]\!] \leq x < [\![x]\!] + 1,$$

$$[\![x]\!] + n \leq x + n < [\![x]\!] + n + 1.$$

Obsérvese que $[\![x]\!] \in \mathbb{Z}$ y recuérdese que $n \in \mathbb{Z}$, por definición. Dado que $\mathbb{Z}$ forma un anillo, se verifica clausura bajo adición, y, por lo tanto, $[\![x]\!] + n$ y $[\![x]\!] + n + 1$ son enteros consecutivos. En consecuencia,

$$[\![x + n]\!] = \max_{m \in \mathbb{Z}} \{m : m \leq x + n\} = [\![x]\!] + n.$$

□

Finalmente, Apostol [6], incluye una función aritmética definida por Joseph Liouville que cobrará importancia a posteriori. No obstante, se precisa definir otra función antes de abordarla.

Definición 4.2.8. Función Ω

La función Ω devuelve el número de factores primos de todo número natural n al contar multiplicidades. Si $n = p_1^{\alpha_1} \dots p_k^{\alpha_k}$ con $p_1, \dots, p_k$ primos distintos, entonces

$$\Omega(n) = \sum_{i=1}^{k} \alpha_i. \tag{4.17}$$

Por convención, $\Omega(1) = 1$.

Teorema 4.2.7. *La función Ω es completamente aditiva, es decir,*

$$\Omega(mn) = \Omega(m) + \Omega(n), \forall m, n \in \mathbb{N}. \tag{4.18}$$

Demostración: Sean $m, n \in \mathbb{N}$ y considérese su descomposición canónica. Sin pérdida de generalidad, tómese $n = p_1^{\alpha_1} \dots p_k^{\alpha_k}$ y $m = q_1^{\beta_1} \dots q_r^{\beta_r}$, por lo cual $mn = q_1^{\beta_1} \dots q_r^{\beta_r} p_1^{\alpha_1} \dots p_k^{\alpha_k}$.

Por definición de la función Ω,

$$\Omega(mn) = \beta_1 + \ldots + \beta_r + \alpha_1 + \ldots + \alpha_k = \sum_{i=1}^{r} \beta_i + \sum_{i=1}^{k} \alpha_i = \Omega(m) + \Omega(n).$$

□

Definición 4.2.9. Función de Liouville λ

Para todo número natural n, la función de Liouville viene definida por

$$\lambda(n) = (-1)^{\Omega(n)}. \tag{4.19}$$

Teorema 4.2.8. *La función λ es completamente multiplicativa y para todo $n \in \mathbb{N}$,*

$$\sum_{d|n} \lambda(d) = \begin{cases} 1, & n \text{ cuadrado perfecto} \\ 0, & \text{de lo contrario} \end{cases} . \tag{4.20}$$

Demostración: Sean $m, n \in \mathbb{N}$ y analícese $\lambda(mn)$. Dado que Ω es completamente aditiva y por propiedad de los exponentes, se verifica que

$$\lambda(mn) = (-1)^{\Omega(mn)} = (-1)^{\Omega(m)+\Omega(n)} = (-1)^{\Omega(m)}(-1)^{\Omega(n)} = \lambda(m)\lambda(n).$$

Sea $s(n) = \sum_{d|n} \lambda(d)$. Por el teorema 4.1.1 se verifica que $s(n)$ es multiplicativa, dado que λ es multiplicativa. De esta manera, considérese descomposición en factores primos para hacer uso de la propiedad multiplicativa. Entonces, evalúese $s(p^k)$ cuando p es primo y $k \in \mathbb{N}$. Recuérdese que los únicos divisores de p^k son las potencias p^i con $0 \leq i \leq k$. Por lo tanto,

$$s(p^k) = \sum_{i=0}^{k} \lambda(p^i) = \sum_{i=0}^{k} (-1)^{\Omega(p^i)} = \lambda(1) + \sum_{i=1}^{k} (-1)^{\Omega(p^i)}.$$

Nótese que $\Omega(p^i) = i, \forall i \in \mathbb{N}$ y $\lambda(1) = 1$. En consecuencia,

$$s(p^k) = 1 + \sum_{i=1}^{k} (-1)^i.$$

Véase que $(-1)^i = 1$ si $2|i$ y $(-1)^i = -1$ si $2 \nmid i$. Entonces, analícese la sumatoria según la paridad de k. Por el Algoritmo de Euclides, los enteros puede ser de la forma $2r, r \in \mathbb{N}$ y $2r-1, r \in \mathbb{N}$; evalúese cada caso de manera independiente y sepárese la sumatoria.

1. $k = 2r \iff r = \frac{k}{2}$

$$s(p^k) = 1 + \sum_{r=1}^{\frac{k}{2}} (-1)^{2r-1} + \sum_{r=1}^{\frac{k}{2}} (-1)^{2r} = 1 - \sum_{r=1}^{\frac{k}{2}} 1 + \sum_{r=1}^{\frac{k}{2}} 1 = 1.$$

2. $k = 2r - 1 \iff r = \frac{k+1}{2}$

$$s(p^k) = 1 + \sum_{r=1}^{\frac{k+1}{2}} (-1)^{2r-1} + \sum_{r=1}^{\frac{k+1}{2}-1} (-1)^{2r} = 1 - 1 - \sum_{r=1}^{\frac{k+1}{2}-1} 1 + \sum_{r=1}^{\frac{k+1}{2}-1} 1 = 0.$$

Por consiguiente,

$$s(p^k) = \begin{cases} 1, & 2 \mid k \\ 0, & 2 \nmid k \end{cases} .$$

Al aplicar el Teorema Fundamental de la Aritmética y como la función es multiplicativa, se obtiene que

$$s(n) = s\left(\prod_{i\in\mathbb{N}} p_i^{\alpha_i}\right) = \prod_{i\in\mathbb{N}} s(p_i^{\alpha_i}).$$

Obsérvese que si existe algún $j \in \mathbb{N}$ tal que α_j es impar, entonces $s(n) = 0$ puesto que $s(p_j^{\alpha_j}) = 0$. Por lo tanto, $s(n) = 1$ únicamente cuando todos los exponentes α_i son pares, lo cual implica que n es un cuadrado perfecto.

Luego,

$$s(n) = \begin{cases} 1, & n \text{ cuadrado perfecto} \\ 0, & \text{de lo contrario} \end{cases} .$$

□

CAPÍTULO 5

Ecuaciones Diofánticas

«Chaque problème que je résolvais devenait une règle, qui servait ensuite à résoudre d'autres problèmes.»

Cada problema que resolví, se volvió una regla que sirvió más tarde para resolver otros problemas.

René Descartes

Las ecuaciones diofánticas constituyen por sí solas una rama de estudio propia dentro de la teoría de números. En este caso, se destinará un capítulo a esta clase de ecuaciones, dado que son cruciales para establecer las tres identidades de Liouville. En efecto, se precisa definir de una sumatoria para un conjunto de enteros que sean soluciones de una ecuación diofántica.

5.1. Nociones básicas

La teoría de números se desarrolla sobre el anillo de los números enteros $\mathbb{Z}$ y sus propiedades; por lo tanto, varias de sus ramas se centran en los enteros. En particular, las ecuaciones diofánticas son un tipo de ecuación algebraica en las cuales se buscan soluciones enteras. A continuación, se dará una breve introducción a los conceptos básicos y principales resultados que involucran ecuaciones diofánticas.

Definición 5.1.1. Ecuación diofántica
Una ecuación polinómica con coeficientes enteros en la que se buscan soluciones enteras se denomina diofántica.

Estas ecuaciones reciben el nombre de diofánticas en honor del matemático helénico Diofanto de Alejandría. De acuerdo con lo establecido por Alaca y Williams [7], Diofanto fue el pionero en introducir la notación algebraica y planteó una serie de problemas que deben resolverse en el conjunto de los enteros o racionales en su obra "Arithmetica".

Obsérvese que las ecuaciones diofánticas pueden ser de distinto grado y pueden tener infinitas soluciones en los enteros o ninguna. De acuerdo con lo postulado por Alaca y Williams [7], las ecuaciones diofánticas han sido objeto de estudio a lo largo de los años de varios matemáticos, como Pitágoras, Bachet, Fermat, Euler, Bézout, Hilbert, entre otros.

5.2. Ecuación diofántica lineal

Uno de los pioneros en abordar el análisis diofántico durante la Edad Moderna fue el matemático francés Claude Bachet. Como señala Rashed [8], la primera crítica de la obra de Diofanto se debe a Bachet, la cual serviría de base para el estudio de la teoría de números durante dos siglos y medio; adicionalmente, contribuyó con el estudio de las ecuaciones diofánticas indeterminadas de primer grado. De esta manera, se introduce la ecuación diofántica más sencilla.

Definición 5.2.1. Ecuación diofántica lineal

Una ecuación del tipo $ax + by = c$ con $a, b, c \in \mathbb{Z}$ se denomina ecuación diofántica lineal.

Evidentemente, este tipo de ecuaciones tiene infinitas soluciones en los racionales, simplemente despéjese una variable en función de la otra; sin embargo, no necesariamente es resoluble para los enteros. Obsérvese que lo establecido en la definición 5.2.1, mantiene una conexión con la aritmética modular, como se verá más adelante. En efecto, el siguiente teorema relacionado con la existencia de soluciones para congruencias lineales se le atribuye a Bachet.

Teorema 5.2.1. ***Teorema de Bachet***

Sean $a, b \in \mathbb{Z}$ y $c \in \mathbb{N}$ y considérese la congruencia lineal $ax \equiv b \pmod{c}$. Si $\gcd(a, c) = 1$, entonces la congruencia tiene una única solución. Si $\gcd(a, c) = d$ y $d|b$, entonces existen d soluciones incongruentes; si $d \nmid b$, entonces no existe solución para la congruencia.

Demostración: Sea $\gcd(a, c) = 1$. De esta manera, $\exists m, n \in \mathbb{Z}$ tales que $am + cn = 1$. Por lo tanto,

$$b = b(am + cn) = a(bm) + c(bn),$$

$$c(bn) = b - a(bm) \Longleftrightarrow c|b - a(bm).$$

Por definición de congruencia, $a(bm) \equiv b \pmod{c}$, lo cual implica que bm es solución para $ax \equiv b \pmod{c}$. Para probar unicidad, supóngase que x_1 y x_2 son ambas soluciones para la congruencia lineal tales que $0 \leq x_1, x_2 < c$, es decir, $ax_1 \equiv ax_2 \equiv b \pmod{c}$. Por la ley de cancelación, $x_1 \equiv x_2 \pmod{c}$. Dado que $-c < x_1 - x_2 < c$, se verifica que $0 \leq |x_1 - x_2| < c$; por la proposición 3.4.2, $x_1 = x_2$, con lo que se verifica que la congruencia tiene solución única.

Ahora, sea $d = \gcd(a, c)$ tal que $d|b$. Por propiedad de máximo común divisor, $d|a$; con base en el algoritmo de la división, $\exists r, s \in \mathbb{Z}$ tal que $a = rd$ y $b = sd$. En consecuencia, se tiene la congruencia $(rd)x \equiv sd \pmod{c}$. Nuevamente por la ley de cancelación, $rx \equiv s \pmod{\frac{c}{d}}$. Obsérvese que $r = \frac{a}{d}$ y $\gcd(r, \frac{c}{d}) = 1$. Por lo demostrado previamente, la congruencia tiene solución única. Denótese por x_1 a la solución de la congruencia. Trivialmente, x_1 es también solución para $ax \equiv b \pmod{c}$. Sea x_2 otra solución para esta congruencia, de forma que $ax_1 \equiv ax_2 \equiv b \pmod{c}$. Por la ley de cancelación, $x_1 \equiv x_2 \pmod{\frac{c}{d}} \Longleftrightarrow \frac{c}{d}|x_2 - x_1$. Según el algoritmo de la división, $\exists k \in \mathbb{Z}$ tal que $k(\frac{c}{d}) = x_2 - x_1 \Longleftrightarrow x_2 = x_1 + k(\frac{c}{d})$. Recuérdese que x_1 es solución de $rx \equiv s \pmod{\frac{c}{d}}$, por lo cual $0 \leq x_1 < \frac{c}{d}$, y tómese $k \leq d - 1$. Por lo tanto,

$$0 \leq x_1 + k\left(\frac{c}{d}\right) < \frac{c}{d} + (d - 1)\left(\frac{c}{d}\right) = d\left(\frac{c}{d}\right) = c.$$

Con lo cual $0 \leq x_2 < c$ y x_2 es un residuo mínimo. Dado que para $0 \leq k \leq d-1$, existen d enteros, se concluye que la congruencia $ax \equiv b \pmod{c}$ tiene exactamente d soluciones incongruentes.

Finalmente, considérese el enunciado: si $ax \equiv b \pmod{c}$ tiene solución, entonces $d|b$. Sin pérdida de generalidad, tómese x_1 como solución. Por definición de congruencia, $ax_1 \equiv b \pmod{c} \iff c|b-ax_1$. Por el algoritmo de la división, $\exists y \in \mathbb{Z}, cy = b - ax_1 \iff b = ax_1 + cy$. Dado que $d = \gcd(a,c)$, se verifica que $d|ax_1$ y $d|cy$; por consiguiente, $d|b$. En consecuencia, por la contrapositiva, si $d \nmid b$, entonces $ax \equiv b \pmod{c}$ no tiene solución. □

A continuación, se establece la conexión entre congruencias lineales y ecuaciones diofánticas lineales mediante el siguiente resultado.

Teorema 5.2.2. *La ecuación diofántica lineal $ax + by = c$ es resoluble si y solo si $d|c$, $d = \gcd(a,b)$. Adicionalmente, si (x_0, y_0) es una solución particular, entonces las soluciones generales vienen dadas por:*

$$\begin{cases} x = x_0 + k\left(\dfrac{b}{d}\right) \\ \\ y = y_0 - k\left(\dfrac{a}{d}\right) \end{cases}, \ k \in \mathbb{Z}. \tag{5.1}$$

Demostración: Obsérvese que $ax + by = c \iff by = c - ax \iff b|c - ax$.

Por la definición de congruencia, la ecuación diofántica es equivalente a la congruencia lineal $ax \equiv c \pmod{b}$. Con base en el teorema de Bachet, la congruencia tiene solución si y solo si $d|c$, $d = \gcd(a,b)$. Adicionalmente, si x_0 es solución de la congruencia, entonces la solución general corresponde a $x = x_0 + k(\frac{b}{d}), k \in \mathbb{Z}$.

De esta manera,

$$y = \frac{c}{b} - \frac{ax}{b} = \frac{c}{b} - \frac{a}{b}\left(x_0 + k\left(\frac{b}{d}\right)\right) = \frac{c - ax_0}{b} - k\left(\frac{a}{d}\right).$$

Sea $y_0 = \frac{c-ax_0}{b}$, lo cual implica que $y = y_0 - k(\frac{a}{d})$. □

5.3. Ecuación de Pell-Fermat

Al considerar ecuaciones diofánticas de segundo grado, se encuentran las ecuaciones de Pell, estudiadas desde la antigüedad. Este tipo de ecuaciones servirá como preámbulo a la ecuación de Liouville. De acuerdo con Tattersall

[9], el estudio de sus soluciones fue atribuido a Pell erróneamente por Leonhard Euler, mientras que Pierre de Fermat fue el pionero en la investigación de soluciones no triviales.

Definición 5.3.1. Ecuación de Pell-Fermat
Una ecuación del tipo $x^2 - Ny^2 = 1$ donde $x, y \in \mathbb{Z}$ y N no es un cuadrado perfecto, se denomina ecuación de Pell-Fermat.

Es importante recalcar la importancia de considerar que N no sea un cuadrado perfecto cuando se trabaja con soluciones en $\mathbb{Z}$, tal y como se evidencia a continuación.

Proposición 5.3.1. La ecuación $x^2 - Ny^2 = 1$ con $x, y \in \mathbb{Z}$ y N un cuadrado perfecto, solo admite las soluciones triviales $(x, y) = (\pm 1, 0)$.

Demostración: Obsérvese que $x^2 - Ny^2 = (x + \sqrt{N}y)(x - \sqrt{N}y) = 1$. Dado que N es un cuadrado perfecto, $x + \sqrt{N}y, x - \sqrt{N}y \in \mathbb{Z}$. Por lo tanto,

$$\begin{cases} x + \sqrt{N}y = \pm 1 \\ x - \sqrt{N}y = \pm 1 \end{cases}.$$

De esta forma, al sumar ambas expresiones, se obtiene que

$$2x = 2(\pm 1) \iff x = \pm 1.$$

Dado que $N \in \mathbb{N}$, se verifica que $N \neq 0$. En consecuencia,

$$\pm 1 + \sqrt{N}y = \pm 1,$$
$$\sqrt{N}y = 0,$$
$$y = 0.$$

□

La demostración de la proposición 5.3.1 permite identificar una clara relación entre el anillo $\mathbb{Z}[\sqrt{N}] = \{x + y\sqrt{N} : x, y \in \mathbb{Z}\}$ y la solución de las ecuaciones de Pell-Fermat. Efectivamente, los elementos $x + y\sqrt{N} \in \mathbb{Z}[\sqrt{N}]$ tales que $x^2 - Ny^2 = 1$ otorgan las soluciones enteras (x, y) de la ecuación.

Una de las primeras aproximaciones a la resolución de estas ecuaciones se debió a Brahmagupta mediante la identidad que lleva su nombre.

Teorema 5.3.1. ***Identidad de Brahmagupta***
Para $a, b, c, d, N \in \mathbb{Z}$,

$$(a^2 - Nb^2)(c^2 - Nd^2) = (ac \pm Nbd)^2 - N(ad \pm bc)^2. \tag{5.2}$$

Demostración: Obsérvese que

$$\begin{aligned}(a^2 - Nb^2)(c^2 - Nd^2) &= a^2c^2 - Na^2d^2 - Nb^2c^2 + N^2b^2d^2 \\ &= (a^2c^2 + N^2b^2d^2) - N(a^2d^2 + b^2c^2) + (2Nabcd - 2Nabcd) \\ &= (a^2c^2 \pm 2Nabcd + N^2b^2d^2) - N(a^2d^2 \pm 2abcd + b^2c^2) \\ &= (ac \pm Nbd)^2 - N(ad \pm bc)^2.\end{aligned}$$

□

A continuación, se procede a la construcción de la solución general a partir de la solución fundamental (r, s), es decir, con base en los menores $r, s \in \mathbb{N}$ tales que $r^2 - Ns^2 = 1$.

Teorema 5.3.2. ***Teorema de Lagrange***

Sea (r, s) la solución fundamental de una ecuación de Pell-Fermat. Entonces, todas las soluciones de la ecuación de Pell-Fermat vienen dadas por (x_n, y_n) donde $x_n + y_n\sqrt{N} = (r + s\sqrt{N})^n, n \in \mathbb{N}$.

Demostración: Sea $\theta \in \mathbb{Z}[\sqrt{N}]$ tal que θ genera una solución de una ecuación Pell-Fermat, es decir, $a^2 - Nb^2 = 1$; y nótese que $\theta^n, n \in \mathbb{Z}$ también genera una solución. Sin pérdida de generalidad, tómese $\theta = a + b\sqrt{N}$ con $a, b \in \mathbb{N}$ y procédase a analizar para $n = 0$. En este caso, se verifica $\theta^0 = 1$; de esta manera, $(x, y) = (1, 0)$ que corresponde a la solución trivial.

Ahora, tómese $n \in \mathbb{N}$ y considérese el caso base para $n = 2$. Véase que

$$\theta^2 = (a + b\sqrt{N})^2 = a^2 + 2ab\sqrt{N} + Nb^2 = (a^2 + Nb^2) + 2ab\sqrt{N}.$$

Por la identidad de Brahmagupta con $a = c$ y $b = d$, se verifica que

$$(a^2 + Nb^2)^2 - N(2ab)^2 = (a^2 - Nb^2)^2 = 1^2 = 1.$$

Por consiguiente, θ^2 genera una solución de la ecuación de Pell-Fermat. A continuación, supóngase validez para $n = k$ y analícese el caso $n = k + 1$. Por el paso inductivo, θ^k es solución de la ecuación; entonces, sin pérdida de generalidad, sea $\theta^k = c + d\sqrt{N}$ con $c, d \in \mathbb{N}$ tal que $c^2 - Nd^2 = 1$. Obsérvese que

$$\theta^{k+1} = \theta^k \cdot \theta = (c + d\sqrt{N})(a + b\sqrt{N}) = (ac + Nbd) + (ad + bc)\sqrt{N}.$$

Por la identidad de Brahmagupta,

$$(ac + Nbd)^2 - N(ad + bc)^2 = (a^2 - Nb^2)(c^2 - Nd^2) = (1)(1) = 1.$$

Por lo tanto, θ^{k+1} genera una solución de la ecuación de Pell-Fermat. Esto implica que $\theta^n, \forall n \in \mathbb{N}$ también genera una solución con base en el principio de inducción matemática.

Finalmente, sobra verificar la validez para $n \leq -1$. Pártase de $\theta^k, k \in \mathbb{N}$ y analícese θ^{-k}. Como se probó previamente, θ^k genera una solución de la ecuación, es decir, $\theta^k = u + v\sqrt{N}$ tal que $u^2 - Nv^2 = 1$. Entonces,

$$\theta^{-k} = \frac{1}{\theta^k} = \frac{1}{u + v\sqrt{N}} \left(\frac{u - v\sqrt{N}}{u - v\sqrt{N}} \right) = \frac{u - v\sqrt{N}}{u^2 - Nv^2} = u - v\sqrt{N}.$$

Nótese que $u^2 - N(-v)^2 = u^2 - Nv^2 = 1$, por lo cual, θ^{-k} es también solución. Dado que la elección de k es arbitraria, esto se cumple para todo $n \in \mathbb{N}$ y a su vez para $n \leq -1$.

Ahora, considérese la solución fundamental. Sea $\alpha = r + s\sqrt{N}$ y (a, b) otra solución en $\mathbb{N}^2$, sin pérdida de generalidad, tómese $\theta = a + b\sqrt{N}$ con $a, b \in \mathbb{N}$. Por definición de solución fundamental, $r \leq a$ y $s \leq b$. Por lo tanto,

$$\begin{gathered} s\sqrt{N} \leq b\sqrt{N}, \\ r + s\sqrt{N} \leq a + b\sqrt{N}, \\ \alpha \leq \theta. \end{gathered}$$

Si $\theta = \alpha^n$ con $n \in \mathbb{N}$, la demostración es directa. Entonces, supóngase que este no es el caso, de manera que $\exists k \in \mathbb{N}$ tal que $\alpha^k < \theta < \alpha^{k+1}$. En consecuencia,

$$\alpha^k \alpha^{-k} < \theta \alpha^{-k} < \alpha^{k+1} \alpha^{-k},$$

$$0 < \theta \alpha^{-k} < \alpha.$$

Con base en lo demostrado anteriormente, α^{-k} es solución a la ecuación de Pell-Fermat dado que α es solución, por lo cual, tómese $\alpha^{-k} = c + d\sqrt{N}$ con $c, d \in \mathbb{N}$. Análogamente a lo hallado previamente, es posible concluir que $\theta\alpha^{-k} = (ac + Nbd) + (ac + bc)\sqrt{N}$ y por la identidad de Brahmagupta, se deduce que $(ac + Nbd)^2 - N(ad + bc)^2 = 1$; por consiguiente, $\theta\alpha^{-k}$ es también solución de la ecuación. No obstante, esto es imposible, puesto que α es la solución fundamental. En consecuencia, se tiene una contradicción y la suposición hecha es falsa, con lo que se culmina la demostración. □

Es importante recalcar que pese a que se trabajó con la forma general de las soluciones a la ecuación de Pell-Fermat, el teorema de Lagrange no garantiza la existencia de la solución fundamental. En consecuencia, no se concibe que soluciones enteras no triviales existan para esta ecuación. Con base en lo

indicado por Martinez et al.[10], las soluciones se interpretan geométricamente como los látices que definen una hipérbola y para demostrar la existencia de dichos látices, es necesario considerar una aproximación diofántica. De esta forma, se apela al siguiente resultado atribuido a Dirichlet. No obstante, se debe introducir una función ligada a la función máximo entero definida en el capítulo anterior, para su demostración.

Definición 5.3.2. Función mantisa $\{\ \}$

La función mantisa, también denominada función parte fraccionaria, devuelve la parte decimal de un número real y se define mediante la expresión

$$\{x\} = x - [\![x]\!]. \tag{5.3}$$

Teorema 5.3.3. ***Teorema de aproximación de Dirichlet***

Sean $\alpha \in \mathbb{R}$ y $N \in \mathbb{N}$. Entonces, existen $p, q \in \mathbb{Z}$ tales que $1 \leq q \leq N$ y

$$|q\alpha - p| \leq \frac{1}{N}. \tag{5.4}$$

Demostración: Considérese la colección de reales $0, \{\alpha\}, \{2\alpha\}, \ldots, \{N\alpha\}$. Por definición de las funciones máximo entero y mantisa,

$$[\![x]\!] \leq x < [\![x]\!] + 1,$$

$$0 \leq x - [\![x]\!] < 1,$$

$$0 \leq \{x\} < 1.$$

De esta manera, la colección de $N+1$ reales se halla en el intervalo $[0, 1]$. Ahora, tómese una partición de $[0, 1]$ en intervalos de amplitud $\frac{1}{N}$, en cuyo caso, se obtienen N intervalos disjuntos. Por el principio del palomar, existe al menos un intervalo que contiene dos de los números reales. Sin pérdida de generalidad, denótese a estos números por $\{k\alpha\}$ y $\{m\alpha\}$, tal que $0 \leq k < m \leq N$. Ahora, obsérvese que la diferencia entre estos dos números viene dada por

$$|\{m\alpha\} - \{k\alpha\}| = |(m\alpha - [\![m\alpha]\!]) - (k\alpha - [\![k\alpha]\!])| = |(m-k)\alpha - ([\![m\alpha]\!] - [\![k\alpha]\!])|.$$

Sean $p = [\![m\alpha]\!] - [\![k\alpha]\!]$ y $q = m - k$, y nótese que $p, q \in \mathbb{Z}$. Evidentemente, $1 \leq m - k \leq N$ dado que $k < m$. Finalmente, como $\{k\alpha\}$ y $\{m\alpha\}$ pertenecen a un intervalo de amplitud $\frac{1}{N}$, se concluye que

$$|\{m\alpha\} - \{k\alpha\}| = |q\alpha - p| \leq \frac{1}{N}.$$

□

Una consecuencia directa de la aproximación de Dirichlet es la pieza clave para demostrar la existencia de soluciones de la ecuación de Pell-Fermat.

Corolario 5.3.1. Sea $\alpha \in \mathbb{R}\backslash\mathbb{Q}$. Entonces, existen infinitos pares $p \in \mathbb{Z}$ y $q \in \mathbb{N}$ que satisfacen la desigualdad

$$\left|\alpha - \frac{p}{q}\right| \leq \frac{1}{q^2}.$$

Demostración: Considérese un $N \in \mathbb{N}$. Por el teorema de aproximación de Dirichlet, existen $p, q \in \mathbb{Z}$ tales que $1 \leq q \leq N$ y

$$|q\alpha - p| \leq \frac{1}{N},$$

$$q\left|\alpha - \frac{p}{q}\right| \leq \frac{1}{N},$$

$$\left|\alpha - \frac{p}{q}\right| \leq \frac{1}{qN}.$$

Además, como $q \leq N$, se verifica que $\frac{1}{N} \leq \frac{1}{q}$. Por lo tanto,

$$\left|\alpha - \frac{p}{q}\right| \leq \frac{1}{q^2}.$$

Sea $N' \in \mathbb{N}$ tal que

$$\frac{1}{\left|\alpha - \frac{p}{q}\right|} < N'.$$

Nótese que dicho N' siempre existe, dado que $\alpha \notin \mathbb{Q}$, $q \in \mathbb{N}$ y

$$q^2 \leq \frac{1}{\left|\alpha - \frac{p}{q}\right|}.$$

Bajo el mismo razonamiento, al aplicar el teorema de aproximación de Dirichlet por segunda vez, se tiene que existen $p', q' \in \mathbb{Z}$ tales que $1 \leq q' \leq N'$ y

$$\left|\alpha - \frac{p'}{q'}\right| \leq \frac{1}{q'N'} < \frac{\left|\alpha - \frac{p}{q}\right|}{q'} \leq \left|\alpha - \frac{p}{q}\right| \leq \frac{1}{q^2}.$$

Dado que se tiene una desigualdad estricta, necesariamente se verifica que $\frac{p'}{q'} \neq \frac{p}{q}$. Como α es irracional, entonces es posible obtener una sucesión de racionales $\{\frac{p_n}{q_n} : p_n \in \mathbb{Z}, q_n \in \mathbb{N}\}$ al emplear el teorema de aproximación de Dirichlet indefinidamente, tal que

$$\left|\alpha - \frac{p_n}{q_n}\right| \leq \frac{1}{q_n^2}, n \in \mathbb{N}.$$

En consecuencia, la desigualdad se satisface para infinitos racionales. □

Por último, con base en los resultados formulados por Dirichlet, se culmina el estudio de las ecuaciones de Pell-Fermat con el siguiente teorema.

Teorema 5.3.4. *Una ecuación de Pell-Fermat posee solución no trivial, es decir,* $(x, y) \neq (\pm 1, 0)$.

Demostración: Recuérdese que las soluciones de la ecuación de Pell-Fermat (x, y) se obtienen mediante elementos del anillo $\mathbb{Z}[\sqrt{N}]$. Por el corolario 5.3.1, existen infinitos pares $x \in \mathbb{Z}$ y $y \in \mathbb{N}$, tales que $|\sqrt{N} - \frac{x}{y}| < \frac{1}{y^2}$. De esta manera, obsérvese que

$$|x^2 - Ny^2| = y^2 \left|N - \frac{x^2}{y^2}\right| = y^2 \left|\sqrt{N} - \frac{x}{y}\right| \left|\sqrt{N} + \frac{x}{y}\right|$$

$$< y^2 \left(\frac{1}{y^2}\right) \left|\sqrt{N} + \frac{x}{y}\right| = \left|\sqrt{N} + \frac{x}{y}\right|.$$

Por la desigualdad triangular, se satisface que

$$\left|\sqrt{N} + \frac{x}{y} + (\sqrt{N} - \sqrt{N})\right| = \left|2\sqrt{N} - \left(\sqrt{N} - \frac{x}{y}\right)\right| \leq 2\sqrt{N} + \left|\sqrt{N} - \frac{x}{y}\right|.$$

En particular, por el teorema de aproximación de Dirichlet, existen $x \in \mathbb{Z}$ y $y \in \mathbb{N}$ tales que $|\sqrt{N} - \frac{x}{y}| \leq 1$. En consecuencia,

$$|x^2 - Ny^2| < 2\sqrt{N} + 1.$$

Sea $S = \{j \in \mathbb{Z} : x^2 - Nd^2 = j, |j| < 2\sqrt{N} + 1\}$ y nótese que existen infinitos pares (x, y) que verifican la desigualdad. Sin embargo, existen finitos $j \in \mathbb{Z}$ tales que $|j| < 2\sqrt{N} + 1$, lo cual implica que S es finito. Por el principio del palomar, existe al menos un $k \in S$ tal que $x^2 - Ny^2 = k$ para infinitos pares (x, y). Obsérvese que únicamente existen $|k|$ restos módulo k, por lo tanto, solo hay

$|k|^2$ posibilidades incongruentes para ($x \pmod{k}, y \pmod{k}$). En particular, siempre es posible tomar dos pares de soluciones enteras distintas (x_1, y_1) y (x_2, y_2), tales que $x_1 \equiv x_2 \pmod{k}$ y $y_1 \equiv y_2 \pmod{k}$. Por definición,

$$\begin{cases} x_1^2 - Ny_1^2 = k \\ \\ x_2^2 - Ny_2^2 = k \end{cases}.$$

Al multiplicar ambas expresiones y mediante la identidad de Brahmagupta, se verifica que

$$\begin{aligned} (x_1^2 - Ny_1^2)(x_2^2 - Ny_2^2) &= k^2, \\ (x_1x_2 - Ny_1y_2)^2 - N(x_1y_2 - x_2y_1)^2 &= k^2, \\ \left(\frac{x_1x_2 - Ny_1y_2}{k}\right)^2 - N\left(\frac{x_1y_2 - x_2y_1}{k}\right)^2 &= 1. \end{aligned}$$

Como $x_1 \equiv x_2 \pmod{k}$ y $y_1 \equiv y_2 \pmod{k}$, por el teorema 3.4.1

$$\begin{aligned} x_1x_2 - Ny_1y_2 \equiv x_1^2 - Ny_1^2 = k \equiv 0 \pmod{k}, \\ x_1y_2 - x_2y_1 \equiv x_1y_1 - x_1y_1 = 0 \pmod{k}. \end{aligned}$$

Por consiguiente, $(x_0, y_0) = \left(\frac{x_1x_2 - Ny_1y_2}{k}, \frac{x_1y_2 - x_2y_1}{k}\right) \in \mathbb{Z}^2$ y por ende, solución a la ecuación de Pell-Fermat. Ahora, sola falta probar que no es una solución trivial, es decir, $y_0 \neq 0$. Supóngase que $y_0 = 0$, lo que implica que $x_0 = \pm 1$. En consecuencia,

$$\begin{cases} \dfrac{x_1x_2 - Ny_1y_2}{k} = \pm 1 \iff x_1x_2 - Ny_1y_2 = \pm k \\ \\ \dfrac{x_1y_2 - x_2y_1}{k} = 0 \iff x_1y_2 = x_2y_1 \end{cases}.$$

Por consiguiente,

$$\pm kx_1 = \pm(x_1x_2 - Ny_1y_2)x_1 = \pm(x_1^2x_2 - Nx_2y_1^2) = \pm(x_1^2 - Ny_1^2)x_2 = \pm kx_2.$$

Como resultado, se obtiene que

$$\begin{aligned} \pm kx_1 = \pm kx_2 \iff x_1 = x_2, \\ (x_1y_2 = x_2y_1 \wedge x_1 = x_2) \iff y_1 = y_2. \end{aligned}$$

Esto indica que $(x_1, y_1) = (x_2, y_2)$; no obstante, esto es imposible, puesto que son soluciones enteras distintas, por definición. Por lo tanto, se tiene una contradicción y la suposición hecha es falsa. Luego, la ecuación de Pell-Fermat tiene una solución no trivial. □

5.4. Ecuación de Liouville

Los siguientes resultados corresponden al eje de la aritmética desarrollada por Joseph Liouville y su considerable alcance en otros ámbitos. Con base en lo establecido por Uspensky y Heaslet [11], la teoría de números proporciona importantes artilugios de investigación en distintas ramas de la matemática, en especial, se destacan los métodos geométricos y analíticos, estrechamente relacionados con ecuaciones elípticas; particularmente, sobresale el trabajo de Liouville que permiten obtener resultados sofisticados sin la necesidad de requerir una profunda experticia en curvas elípticas. En efecto, las tres identidades de Liouville se definen sobre el conjunto de soluciones de una ecuación diofántica de segundo orden, la ecuación de Liouville.

Definición 5.4.1. Ecuación de Liouville
Una ecuación del tipo $i^2 + jk = n$ *donde* $i, j, k \in \mathbb{Z}$ *y* $n \in \mathbb{N}$*, se denomina ecuación de Liouville.*

Evidentemente, si no se restringe el conjunto de soluciones, la ecuación de Liouville tiene infinitas soluciones. En efecto, obsérvese que al fijar $k = 1$ y tomar $i = r, r \in \mathbb{Z}$, implica que $j = n - r^2$; como $\mathbb{Z}$ tiene una cardinalidad infinita, el conjunto de soluciones también es infinito.

Como se precisan sumatorias para establecer las identidades de Liouville, como se verá a posteriori, representa un desafío constante maniobrar sobre un conjunto infinito por los posibles inconvenientes de divergencia de las series. De esta manera, resulta oportuno restringir el dominio de las variables para garantizar finitud.

Proposición 5.4.1. Si $j, k \in \mathbb{N}$, la ecuación de Liouville tiene a lo mucho $n^2(1 + 2[\![\sqrt{n}]\!])$ soluciones.

Demostración: Obsérvese que $i \in \mathbb{Z} \Longrightarrow i^2 \geq 0$ y $j, k \in \mathbb{N} \Longrightarrow jk > 0$. De esta forma, como se requiere que $i^2 + jk = n$, es posible establecer las siguientes cotas

$$\begin{cases} 0 \leq i^2 \leq n \\ 1 \leq j \leq n \\ 1 \leq k \leq n \end{cases}.$$

Para los dos últimos casos, trivialmente se aprecia que existen a lo sumo n posibilidades para j y k. Entonces, trabájese con la primera desigualdad, dado que $i \in \mathbb{Z}$, se verifica que

$$0 \leq i^2 \leq n,$$

$$0 \leq |i| \leq [\![\sqrt{n}]\!].$$

Nótese que la desigualdad implica que hay a lo mucho $[\![\sqrt{n}]\!]$ posibilidades para $i > 0$ y para $i < 0$; además, debe contabilizarse el caso en el que $i = 0$. Por lo tanto, i puede tomar como máximo $1 + 2[\![\sqrt{n}]\!]$ valores.

Por el principio multiplicativo, existen a lo sumo $n^2(1 + 2[\![\sqrt{n}]\!])$ soluciones para la ecuación de Liouville restringida. □

Para definir el dominio de las identidades de Liouville, hace falta incluir una condición más, tal como se muestra a continuación.

Definición 5.4.2. Conjunto A

El conjunto A corresponde al conjunto de ternas (i, j, k) tal que

$$A(n) = \{(i, j, k) \in \mathbb{Z} \times \mathbb{N} \times \mathbb{N} : i^2 + jk = n, 2 \nmid k\}. \tag{5.5}$$

Proposición 5.4.2. El conjunto A es finito y no vacío. Además,

$$(i, j, k) \in A(n) \iff (-i, j, k) \in A(n). \tag{5.6}$$

Demostración: Sea S el conjunto de ternas que son soluciones a la ecuación de Liouville restringida definida en la proposición 5.4.1 y nótese que $A \subset S$. Dado que S es finito, A también lo es.

Por simple inspección, se aprecia que $(0, n, 1) \in A(n), \forall n \in \mathbb{N}$ puesto que $0^2 + n(1) = n$ y $2 \nmid 1$. Por lo tanto, A es no vacío.

Finalmente, la biyección se satisface debido a que $i^2 = (-i)^2, \forall i \in \mathbb{Z}$. En consecuencia, $i^2 + jk = n \iff (-i^2) + jk = n$. □

Las proposiciones 5.4.1 y 5.4.2 son conclusiones bastante elementales con demostración sencilla, pero serán útiles al momento de operar con los componentes de las ternas de A. De esta forma, se presentan los siguientes teoremas que servirán como soporte (lemas) para las tres identidades de Liouville.

Teorema 5.4.1. *Sea $n \in \mathbb{N}$, entonces*

$$\sum_{(i,j,k) \in A(n)} (-1)^i i = 0. \tag{5.7}$$

Demostración: Obsérvese que $\{(i, j, k) \in A(n) : i = 0\}$ y $\{(i, j, k) \in A(n) : i \neq 0\}$ son conjuntos disjuntos. Por lo tanto,

$$\sum_{(i,j,k) \in A(n)} (-1)^i i = \sum_{\substack{(i,j,k) \in A(n) \\ i=0}} (-1)^i i + \sum_{\substack{(i,j,k) \in A(n) \\ i \neq 0}} (-1)^i i = \sum_{\substack{(i,j,k) \in A(n) \\ i \neq 0}} (-1)^i i.$$

Adicionalmente, dado es $i \neq 0$, entonces es posible considerar dos nuevos grupos disjuntos con base en el signo de i. De esta manera,

$$\sum_{(i,j,k)\in A(n)} (-1)^i i = \sum_{\substack{(i,j,k)\in A(n)\\ i<0}} (-1)^i i + \sum_{\substack{(i,j,k)\in A(n)\\ i>0}} (-1)^i i.$$

Como $i \neq 0$, por la proposición 5.4.2, cada terna $(i,j,k) \in A(n)$ tiene su homóloga $(-i,j,k) \in A(n)$. Por consiguiente, en cada sumatoria intervienen exactamente los mismos enteros i, pero con signo opuesto. Adicionalmente, nótese que para cualquier $i \in \mathbb{Z}\backslash\{0\}$,

$$(-1)^{-i}(-i) + (-1)^i i = (-1)^{-i}(-i)(1-(-1)^{2i}) = (-1)^{-i}(-i)(1-1) = 0.$$

En consecuencia, se concluye que

$$\sum_{(i,j,k)\in A(n)} (-1)^i i = 0.$$

□

Teorema 5.4.2. *Sea $n \in \mathbb{N}$, entonces*

$$\sum_{(i,j,k)\in A(n)} (-1)^i j = \sigma^*(n) + 2 \sum_{\substack{i\in\mathbb{N}\\ 1\leq i<\sqrt{n}}} (-1)^i \sigma^*(n-i^2). \tag{5.8}$$

Demostración: Análogamente a la demostración del teorema 5.4.1, se verifica que

$$\sum_{(i,j,k)\in A(n)} (-1)^i j = \sum_{\substack{(i,j,k)\in A(n)\\ i=0}} (-1)^i j + \sum_{\substack{(i,j,k)\in A(n)\\ i\neq 0}} (-1)^i j.$$

De esta forma, trabájese con cada sumatoria por separado. Por definición del conjunto A, se verifica que

$$\sum_{\substack{(i,j,k)\in A(n)\\ i=0}} (-1)^i j = \sum_{\substack{j,k\in\mathbb{N}\\ 2\nmid k\\ jk=n}} j.$$

Por el algoritmo de la división, como $jk = n$ y $2 \nmid k$, entonces $j|n$ y $2 \nmid \frac{n}{j}$. Por definición de la función σ^*, se concluye que

$$\sum_{\substack{(i,j,k)\in A(n)\\ i=0}} (-1)^i j = \sum_{\substack{j|n\\ 2\nmid \frac{n}{j}}} j = \sigma^*(n).$$

Similarmente, procédase para el caso $i \neq 0$.

$$\sum_{\substack{(i,j,k)\in A(n)\\ i\neq 0}} (-1)^i j = \sum_{\substack{i\in\mathbb{Z}\setminus\{0\}\\ j,k\in\mathbb{N}\\ 2\nmid k\\ i^2+jk=n}} (-1)^i j.$$

Por la proposición 5.4.1, se tiene que $0 < i^2 < n$. La desigualdad es estricta, puesto que $i \neq 0$ y $j, k \in \mathbb{N}$, lo que implica que $jk \neq 0$. Adicionalmente, nótese que $(-1)^i = (-1)^{-i}, \forall i \in \mathbb{N}$. De esta manera, expándase en una doble sumatoria

$$\begin{aligned}
\sum_{\substack{(i,j,k)\in A(n)\\ i\neq 0}} (-1)^i j &= \sum_{\substack{i\in\mathbb{Z}\\ 0<i^2<n}} (-1)^i \sum_{\substack{j,k\in\mathbb{N}\\ 2\nmid k\\ jk=n-i^2}} j \\
&= \sum_{\substack{i\in\mathbb{Z}\\ -\sqrt{n}<i<0}} (-1)^i \sum_{\substack{j,k\in\mathbb{N}\\ 2\nmid k\\ jk=n-i^2}} j + \sum_{\substack{i\in\mathbb{Z}\\ 0<i<\sqrt{n}}} (-1)^i \sum_{\substack{j,k\in\mathbb{N}\\ 2\nmid k\\ jk=n-i^2}} j \\
&= 2 \sum_{\substack{i\in\mathbb{N}\\ 0<i<\sqrt{n}}} (-1)^i \sum_{\substack{j,k\in\mathbb{N}\\ 2\nmid k\\ jk=n-i^2}} j.
\end{aligned}$$

Análogamente, por el algoritmo de la división, $j|n-i^2$ y $2 \nmid \frac{n-i^2}{j}$. Entonces,

$$\sum_{\substack{(i,j,k)\in A(n)\\ i\neq 0}} (-1)^i j = 2 \sum_{\substack{i\in\mathbb{N}\\ 1\leq i<\sqrt{n}}} (-1)^i \sum_{\substack{j|n-i^2\\ 2\nmid \frac{n-i^2}{j}}} j = 2 \sum_{\substack{i\in\mathbb{N}\\ 1\leq i<\sqrt{n}}} (-1)^i \sigma^*(n-i^2).$$

Por último, al superponer ambas sumatorias, se concluye que

$$\sum_{(i,j,k)\in A(n)} (-1)^i j = \sigma^*(n) + 2 \sum_{\substack{i\in\mathbb{N}\\ 1\leq i<\sqrt{n}}} (-1)^i \sigma^*(n-i^2).$$

□

Teorema 5.4.3. *Sea $n \in \mathbb{N}$, entonces*

$$\sum_{(i,j,k)\in A(n)} (-1)^i k = \sigma(n) - 2\sigma\left(\frac{n}{2}\right) + 2 \sum_{\substack{i\in\mathbb{N}\\ 1\leq i<\sqrt{n}}} (-1)^i \left(\sigma(n-i^2) - 2\sigma\left(\frac{n-i^2}{2}\right)\right). \tag{5.9}$$

Demostración: Análogamente a la demostración del teorema 5.4.1, se verifica que

$$\sum_{(i,j,k)\in A(n)} (-1)^i k = \sum_{\substack{(i,j,k)\in A(n)\\ i=0}} (-1)^i k + \sum_{\substack{(i,j,k)\in A(n)\\ i\neq 0}} (-1)^i k.$$

Similarmente, considérese cada sumatoria por separado bajo el mismo criterio empleado previamente. Obsérvese que

$$\sum_{\substack{(i,j,k)\in A(n)\\ i=0}} (-1)^i k = \sum_{\substack{j,k\in\mathbb{N}\\ 2\nmid k\\ jk=n}} k = \sum_{\substack{k|n\\ 2\nmid k}} k.$$

Obsérvese que los conjuntos $\{k \in \mathbb{N} : k|n, 2|n\}$ y $\{k \in \mathbb{N} : k|n, 2 \nmid n\}$ son disjuntos, y su unión resulta en $\{k \in \mathbb{N} : k|n\}$. Por consiguiente,

$$\sum_{\substack{(i,j,k)\in A(n)\\ i=0}} (-1)^i k = \sum_{\substack{k|n\\ 2\nmid k}} k + \left(\sum_{\substack{k|n\\ 2|k}} k - \sum_{\substack{k|n\\ 2|k}} k \right) = \sum_{k|n} k - \sum_{\substack{k|n\\ 2|k}} k.$$

Dado que $2|k$, por el algoritmo de la división, $k = 2m, m \in \mathbb{N}$. En conjunto con la definición de la función σ, se establece que

$$\sum_{\substack{(i,j,k)\in A(n)\\ i=0}} (-1)^i k = \sigma(n) - \sum_{2m|n} 2m = \sigma(n) - 2\sum_{m|\frac{n}{2}} m = \sigma(n) - 2\sigma\left(\frac{n}{2}\right).$$

Ahora, repítase el mismo razonamiento para $k \neq 0$ con base en la demostración

del teorema 5.4.2 y lo obtenido previamente. En este caso,

$$\begin{aligned}
\sum_{\substack{(i,j,k)\in A(n)\\ i\neq 0}} (-1)^i k &= 2 \sum_{\substack{i\in\mathbb{N}\\ 0<i<\sqrt{n}}} (-1)^i \sum_{\substack{j,k\in\mathbb{N}\\ 2\nmid k\\ jk=n-i^2}} k \\
&= 2 \sum_{\substack{i\in\mathbb{N}\\ 1\leq i<\sqrt{n}}} (-1)^i \left(\sum_{\substack{k|n-i^2\\ 2\nmid k}} k + \left(\sum_{\substack{k|n-i^2\\ 2|k}} k - \sum_{\substack{k|n-i^2\\ 2|k}} k \right) \right) \\
&= 2 \sum_{\substack{i\in\mathbb{N}\\ 1\leq i<\sqrt{n}}} (-1)^i \left(\sum_{k|n-i^2} k - \sum_{2m|n-i^2} 2m \right) \\
&= 2 \sum_{\substack{i\in\mathbb{N}\\ 1\leq i<\sqrt{n}}} (-1)^i \left(\sum_{k|n-i^2} k - 2 \sum_{m|\frac{n-i^2}{2}} m \right).
\end{aligned}$$

Por definición de la función σ,

$$\sum_{\substack{(i,j,k)\in A(n)\\ i\neq 0}} (-1)^i k = 2 \sum_{\substack{i\in\mathbb{N}\\ 1\leq i<\sqrt{n}}} (-1)^i \left(\sigma(n-i^2) - 2\left(\frac{n-i^2}{2}\right)\right).$$

En consecuencia, al superponer ambas sumatorias, se concluye que

$$\sum_{(i,j,k)\in A(n)} (-1)^i k = \sigma(n) - 2\sigma\left(\frac{n}{2}\right) + 2 \sum_{\substack{i\in\mathbb{N}\\ 1\leq i<\sqrt{n}}} (-1)^i \left(\sigma(n-i^2) - 2\sigma\left(\frac{n-i^2}{2}\right)\right).$$

□

Para finalizar, se recurre al siguiente resultado que relaciona a los elementos de A mediante congruencia aritmética. La proposición enunciada a continuación cobrará importancia en la demostración de la segunda identidad de Liouville.

Proposición 5.4.3. Sea $n \in \mathbb{N}$. Si $(i,j,k) \in A(n)$, entonces $i+j \equiv n \pmod 2$.

Demostración: Sea $(i,j,k) \in A(n)$. Con base en la definición del conjunto A, $k \equiv 1 \pmod 2$ dado que $2 \nmid k$. Además, se satisface que $i^2 + jk = n$. Ahora, analícese la congruencia módulo 2 en la ecuación de Liouville.

$$i^2 + jk \equiv n \pmod 2,$$

$$i^2 + j \equiv n \pmod 2.$$

A continuación, obsérvese que $i \equiv i^2 \pmod 2, i \in \mathbb{Z}$. Para ver esto, considérese $i \equiv a \pmod 2$ donde $a \in \{0, 1\}$. Por el teorema 3.4.2, $i^2 \equiv a^2 \equiv a \pmod 2$. Dado que la congruencia modular define una relación de equivalencia, se concluye que $i \equiv i^2 \pmod 2$. En consecuencia,

$$i + j \equiv n \pmod 2.$$

□

CAPÍTULO 6

Primera Identidad de Liouville

«Strong reasons make strong actions.»

Fuertes razones hacen fuertes acciones.

William Shakespeare

Joseph Liouville incluyó varias de sus ideas de teoría de números en su revista "Journal des Mathématiques Pures et Apliquées", entre ellas destacan tres identidades para esta área. En este punto, se pretende establecer y demostrar cada una de ellas, lo que corresponde a la esencia de esta disertación, en los próximos tres capítulos. Es importante notar que estos resultados propuestos por Liouville requieren otras herramientas matemáticas para su deducción y demostración, las cuales también se adjuntarán en cada capítulo.

La primera identidad relaciona aquellas funciones aritméticas que presentan como codominio a los números complejos y se exigen condiciones de paridad para la función. Esta identidad permite encontrar una relación de recurrencia para la función σ^* cuya utilidad radica en una demostración alternativa del teorema de Girard-Fermat.

6.1. Identidad de Liouville

Como menciona Liouville en su séptimo artículo "Sur quelques formules générales qui peuvent être utiles dans la théorie des nombres"[12], las fórmulas derivadas al descomponer un número en partes enteros presentan una gran utilidad en el estudio de series, puesto que no son más que una dependencia de funciones aritméticas. A continuación, se presenta la primera identidad establecida por Liouville que se define sobre el conjunto A, abordado en el capítulo anterior. Para su demostración, se recurre al uso de mapas biyectivos sugeridos por Williams [3]. Si bien el autor, no justifica la propiedad de biyectividad de cada función, la demostración presentada incluirá dicho detalle en conjunto con la validación adecuada de definición de dominios y codominios.

Teorema 6.1.1. ***Primera Identidad de Liouville***

Sean $F : \mathbb{Z} \to \mathbb{C}$ una función impar, es decir, $F(-x) = -F(x)$ y $n \in \mathbb{N}$. Entonces,

$$\sum_{(i,j,k)\in A(n)} (-1)^i F(i+j) = \begin{cases} (-1)^{\sqrt{n}+1}\sqrt{n}F(\sqrt{n}), & n \in \mathbb{N}^2 \\ 0, & n \notin \mathbb{N}^2 \end{cases}. \tag{6.1}$$

Demostración: Obsérvese que los subconjuntos de $A(n)$ definidos como $\{(i,j,k) \in A(n) : 2i + j - k < 0\}$, $\{(i,j,k) \in A(n) : 2i + j - k = 0\}$ y $\{(i,j,k) \in A(n) : 2i + j - k > 0\}$ son disjuntos por pares y su unión corresponde a $A(n)$, con

base en la ley de la tricotomía. En consecuencia,

$$\sum_{(i,j,k)\in A(n)} (-1)^i F(i+j) = \sum_{\substack{(i,j,k)\in A(n)\\ 2i+j-k<0}} (-1)^i F(i+j) + \sum_{\substack{(i,j,k)\in A(n)\\ 2i+j-k=0}} (-1)^i F(i+j) + \sum_{\substack{(i,j,k)\in A(n)\\ 2i+j-k>0}} (-1)^i F(i+j).$$

De esta forma, trabájese con cada sumatoria por separado. Primero, sea $B(n) = \{(i,j,k) \in A(n) : 2i+j-k > 0\}$ y defínase la función $\phi : B \to B$ como $\phi(i,j,k) = (-i+k, 2i+j-k, k)$. Nótese que ϕ está bien definido dado que $2 \nmid k$ y

$$(-i+k)^2 + (2i+j-k)k = i^2 - 2ik + k^2 + 2ik + jk - k^2 = i^2 + jk = n,$$

$$2(-i+k) + 2i + j - k - k = -2i + 2k + 2i + j - 2k = j > 0.$$

Adicionalmente, ϕ es una involución, puesto que

$$\begin{aligned}\phi(\phi(i,j,k)) &= \phi(-i+k, 2i+j-k, k)\\ &= (-(-i+k)+k, 2(-i+k)+(2i+j-k)-k, k)\\ &= (i-k+k, -2i+2k+2i+j-k-k, k)\\ &= (i,j,k).\end{aligned}$$

Por definición, una función es biyectiva si y solo si es invertible. Trivialmente, se verifica que ϕ es una biyección dado que su inversa existe y esta corresponde a la propia función, con base en la definición de involución.

Considérese $G(i,j,k) = (-1)^i F(i+j)$. En consecuencia, como B es un conjunto finito y ϕ es una biyección, se satisface

$$\sum_{(i,j,k)\in B(n)} G(i,j,k) = \sum_{(i,j,k)\in B(n)} G(\phi(i,j,k)).$$

Por lo tanto,

$$\begin{aligned}\sum_{(i,j,k)\in B(n)} (-1)^i F(i+j) &= \sum_{(i,j,k)\in B(n)} (-1)^{-i+k} F(-i+k+2i+j-k)\\ &= \sum_{(i,j,k)\in B(n)} (-1)^{-i}(-1)^k F(i+j).\end{aligned}$$

Dada la definición del conjunto A, se verifica que $2 \nmid k$, y recuérdese también que $(-1)^i = (-1)^{-i}, \forall i \in \mathbb{Z}$. Como resultado,

$$\sum_{(i,j,k)\in B(n)} (-1)^i F(i+j) = -\sum_{(i,j,k)\in B(n)} (-1)^i F(i+j) = 0.$$

Ahora, defínase el conjunto $C(n) = \{(i,j,k) \in A(n) : 2i + j - k = 0\}$. Evidentemente, $2|2i$ y como $2i + j - k = 0$, entonces $2|j - k$, por el algoritmo de la división. Adicionalmente, como $2 \nmid k$, esto implica que $2 \nmid j$ para satisfacer la igualdad. De igual forma, se obtiene que $i = \frac{-j+k}{2}$. Por lo tanto,

$$\begin{aligned} i^2 + jk &= n, \\ \left(\frac{-j+k}{2}\right)^2 + jk &= n, \\ \frac{j^2}{4} + \frac{jk}{2} + \frac{k^2}{4} &= n, \\ \left(\frac{j+k}{2}\right)^2 &= n. \end{aligned}$$

De esta manera,

$$\sum_{(i,j,k)\in C(n)} (-1)^i F(i+j) = \sum_{\substack{j,k\in\mathbb{N} \\ 2\nmid j,k \\ (\frac{j+k}{2})^2 = n}} (-1)^{\frac{-j+k}{2}} F\left(\frac{j+k}{2}\right).$$

Evidentemente, si n no es un cuadrado perfecto, la sumatoria se vuelve nula, puesto que implica que no existen pares $(j,k) \in \mathbb{N} \times \mathbb{N}$ tales que $(\frac{j+k}{2})^2 = n$, es decir, sus límites se definen sobre un conjunto vacío. Por lo tanto, analícese el caso cuando $n \in \mathbb{N}^2$. Sin pérdida de generalidad, asúmase que $n = m^2, m \in \mathbb{N}$.

En consecuencia,

$$\begin{aligned}\sum_{\substack{(i,j,k)\in C(n)\\ n\in\mathbb{N}^2}}(-1)^i F(i+j) &= \sum_{\substack{j,k\in\mathbb{N}\\ 2\nmid j,k\\ (\frac{j+k}{2})^2=m^2}}(-1)^{\frac{(j-j)-j+k}{2}}F\left(\frac{j+k}{2}\right)\\ &= \sum_{\substack{j,k\in\mathbb{N}\\ 2\nmid j,k\\ \frac{j+k}{2}=m}}(-1)^{\frac{j+k}{2}}(-1)^{-j}F\left(\frac{j+k}{2}\right)\\ &= \sum_{\substack{j,k\in\mathbb{N}\\ 2\nmid j,k\\ j+k=2m}}(-1)^m(-1)F(m)\\ &= (-1)^{m+1}F(m)\sum_{\substack{j,k\in\mathbb{N}\\ 2\nmid j,k\\ j+k=2m}}1.\end{aligned}$$

Nótese que existen $2m-1$ posibles pares $(j,k)\in\mathbb{N}\times\mathbb{N}$ tales que $j+k=2m$. Ahora, al descartar los casos pares dado que $2\nmid j,k$, se obtiene un total de m posibilidades. Por consiguiente,

$$\sum_{\substack{(i,j,k)\in C(n)\\ n\in\mathbb{N}^2}}(-1)^i F(i+j) = (-1)^{m+1}mF(m) = (-1)^{\sqrt{n}+1}\sqrt{n}F(\sqrt{n}).$$

Al unir ambos resultados, se concluye que

$$\sum_{(i,j,k)\in C(n)}(-1)^i F(i+j) = \begin{cases}(-1)^{\sqrt{n}+1}\sqrt{n}F(\sqrt{n}), & n\in\mathbb{N}^2\\ 0, & n\notin\mathbb{N}^2\end{cases}.$$

Finalmente, sea $D(n)=\{(i,j,k)\in A(n): 2i+j-k<0\}$ y considérese los conjuntos disjuntos $P(n)=\{(i,j,k)\in D(n): 2\nmid j\}$ y $Q(n)\{(i,j,k)\in D(n): 2|j\}$. De manera que,

$$\sum_{(i,j,k)\in D(n)}(-1)^i F(i+j) = \sum_{(i,j,k)\in P(n)}(-1)^i F(i+j) + \sum_{(i,j,k)\in Q(n)}(-1)^i F(i+j).$$

Defínase la función $\psi: Q\to Q$ como $\psi(i,j,k)=(-i-j,j,-2i-j+k)$ y nótese que ψ está bien definida dado que $(2|j\wedge 2\nmid k)\Longrightarrow 2\nmid -2i-j+k$ y

$$(-i-j)^2+j(-2i-j+k)=i^2+2ij+j^2-2ij-j^2+jk=i^2+jk=n,$$

$$2(-i-j)+j-(-2i-j+k) = -2i-2j+j+2i+j-k = -k < 0.$$

Además, se satisface que ψ es involución.

$$\begin{aligned}\psi(\psi(i,j,k)) &= \psi(-i-j,j,-2i-j+k)\\ &= (-(-i-j)-j,j,-2(-i-j)-j+(-2i-j+k))\\ &= (i+j-j,j,2i+2j-j-2i-j+k)\\ &= (i,j,k).\end{aligned}$$

Como se observó previamente, ψ es una biyección, $(-1)^j = (-1)^{-j}, \forall j \in \mathbb{Z}$ y $2|j$, por ende,

$$\begin{aligned}\sum_{(i,j,k)\in Q(n)} (-1)^i F(i+j) &= \sum_{(i,j,k)\in Q(n)} (-1)^{-i-j} F(-i-j+j)\\ &= \sum_{(i,j,k)\in Q(n)} (-1)^{-i}(-1)^{-j} F(-i)\\ &= \sum_{(i,j,k)\in Q(n)} (-1)^i F(-i).\end{aligned}$$

Ahora, dado que F es una función impar, por definición, $F(-x) = -F(x)$, consecuentemente

$$\sum_{(i,j,k)\in Q(n)} (-1)^i F(i+j) = -\sum_{(i,j,k)\in Q(n)} (-1)^i F(i).$$

Sea $R(n) = \{(i,j,k) \in B(n) : 2|j\}$ y defínase la función $\eta : P \to R$ como $\eta(i,j,k) = (i+j, -2i-j+k, j)$. Obsérvese que η está bien definido dado que $2 \nmid j,k \Longrightarrow 2|-2i-j+k$ y

$$(i+j)^2 + (-2i-j+k)j = i^2+2ij+j^2-2ij-j^2+jk = i^2+jk = n,$$

$$2(i+j)+(-2i-j+k)-j = 2i+2j-2i-j+k-j = k > 0.$$

Adicionalmente, defínase la función $\alpha : R \to P$ como $\alpha(i,j,k) = (i-k, k, 2i+j-k)$ y nótese que la función está bien definida, puesto que $(2|j \wedge 2 \nmid k) \Longrightarrow 2 \nmid 2i+j-k)$ y

$$(i-k)^2 + k(2i+j-k) = i^2-2ik+k^2+2ik+jk-k^2 = i^2+jk = n,$$

$$2(i-k)+k-(2i+j-k) = 2i-2k+k-2i-j+k = -j < 0.$$

Obsérvese que $\alpha = \eta^{-1}$

$$\begin{aligned}\eta(\alpha(i,j,k)) &= \eta(i-k,k,2i+j-k)\\ &= (i-k+k,-2(i-k)-k+2i+j-k,k)\\ &= (i,-2i+2k-k+2i+j-k,k)\\ &= (i,j,k).\end{aligned}$$

En consecuencia, se concluye que η es una biyección y como P es un conjunto finito

$$\sum_{(i,j,k)\in P(n)} G(i,j,k) = \sum_{(i,j,k)\in R(n)} G(\eta^{-1}(i,j,k)).$$

Por consiguiente,

$$\begin{aligned}\sum_{(i,j,k)\in P(n)} (-1)^i F(i+j) &= \sum_{(i,j,k)\in R(n)} (-1)^{i-k} F(i-k+k)\\ &= -\sum_{(i,j,k)\in R(n)} (-1)F(i).\end{aligned}$$

En consecuencia, al superponer ambas sumatorias

$$\begin{aligned}\sum_{(i,j,k)\in D(n)} (-1)^i F(i+j) &= -\sum_{(i,j,k)\in Q(n)} (-1)^i F(i) - \sum_{(i,j,k)\in R(n)} (-1)^i F(i)\\ &= -\sum_{(i,j,k)\in Q(n)\cup R(n)} (-1)^i F(i).\end{aligned}$$

De esta forma, basta analizar la unión de conjuntos resultante.

$$Q(n)\cup R(n) = \{(i,j,k)\in A(n) : 2|j, 2\nmid k, 2i+j-k\neq 0\}.$$

Obsérvese que $(2|j \wedge 2\nmid k) \Longrightarrow 2\nmid 2i+j-k$. De esta manera, $2i+j-k \equiv 1$ (mód 2) lo que implica que $2i+j-k \neq 0$. Por tal motivo, la unión puede reducirse a

$$Q(n)\cup R(n) = \{(i,j,k)\in A(n) : 2|j, 2\nmid k\}.$$

Similarmente a la demostración de la proposición 5.4.2, se puede concluir que $(i,j,k)\in Q(n)\cup R(n) \Longleftrightarrow (-i,j,k)\in Q(n)\cup R(n)$. Dado que F es una función

impar, se tiene como resultado que

$$\begin{aligned}\sum_{(i,j,k)\in D(n)}(-1)^i F(i+j) &= -\sum_{\substack{(i,j,k)\in Q(n)\cup R(n)\\ i<0}}(-1)^i F(i) - \sum_{\substack{(i,j,k)\in Q(n)\cup R(n)\\ i>0}}(-1)^i F(i)\\ &= -\sum_{\substack{(i,j,k)\in Q(n)\cup R(n)\\ i>0}}(-1)^{-i} F(-i) - \sum_{\substack{(i,j,k)\in Q(n)\cup R(n)\\ i>0}}(-1)^i F(i)\\ &= \sum_{\substack{(i,j,k)\in Q(n)\cup R(n)\\ i>0}}(-1)^i F(i) - \sum_{\substack{(i,j,k)\in Q(n)\cup R(n)\\ i>0}}(-1)^i F(i)\\ &= 0.\end{aligned}$$

La demostración concluye al superponer las tres sumatorias obtenidas por la partición original del conjunto A con base en la ley de tricotomía, así se sigue que

$$\sum_{(i,j,k)\in A(n)}(-1)^i F(i+j) = \begin{cases}(-1)^{\sqrt{n}+1}\sqrt{n}F(\sqrt{n}), & n\in\mathbb{N}^2\\ 0, & n\notin\mathbb{N}^2\end{cases}.$$

□

6.2. Aplicaciones

Uno de los principales usos de la primera identidad de Liouville radica en que constituye una herramienta para obtener una demostración alterna y más sencilla del teorema de Girard-Fermat que la utilizada originalmente por Pierre de Fermat mediante su método de descenso infinito. Evidentemente, esta denotación de simpleza debe asumirse tras la prueba de dicha identidad. Antes de introducir formalmente el teorema, se precisa obtener una fórmula recursiva para σ^*, la cual servirá como lema en la posteridad.

Teorema 6.2.1. *Sea $n\in\mathbb{N}$ y defínase la función $s:\mathbb{N}\to\{0,1\}$ tal que*

$$s(n) = \sum_{d|n}\lambda(d).$$

Entonces,

$$\sigma^*(n) = 2\sum_{\substack{i\in\mathbb{N}\\ 1\le i<\sqrt{n}}}(-1)^{i+1}\sigma^*(n-i^2) + (-1)^{n+1}ns(n). \tag{6.2}$$

Demostración: Sea $F(x) = x$ y nótese que F verifica imparidad. Por la primera identidad de Liouville,

$$\sum_{(i,j,k)\in A(n)} (-1)^i(i+j) = \begin{cases} (-1)^{\sqrt{n}+1}n, & n \in \mathbb{N}^2 \\ 0, & n \notin \mathbb{N}^2 \end{cases}.$$

Según la demostración de la proposición 5.4.3, $\sqrt{n} \equiv n \pmod 2$, lo cual implica que $(-1)^{\sqrt{n}} = (-1)^n, n \in \mathbb{N}^2$. Con base en el teorema 4.2.8, se concluye que

$$\sum_{(i,j,k)\in A(n)} (-1)^i(i+j) = (-1)^{n+1}ns(n).$$

Ahora, por los teoremas 5.4.1 y 5.4.2, se verifica que

$$\begin{aligned} \sum_{(i,j,k)\in A(n)} (-1)^i(i+j) &= \sum_{(i,j,k)\in A(n)} (-1)^i i + \sum_{(i,j,k)\in A(n)} (-1)^i j \\ &= \sigma^*(n) + 2 \sum_{\substack{i\in\mathbb{N} \\ 1\le i<\sqrt{n}}} (-1)^i \sigma^*(n-i^2). \end{aligned}$$

Por consiguiente,

$$(-1)^{n+1}ns(n) = \sigma^*(n) + 2 \sum_{\substack{i\in\mathbb{N} \\ 1\le i<\sqrt{n}}} (-1)^i \sigma^*(n-i^2),$$

$$\begin{aligned} \sigma^*(n) &= (-1)^{n+1}ns(n) - 2 \sum_{\substack{i\in\mathbb{N} \\ 1\le i<\sqrt{n}}} (-1)^i \sigma^*(n-i^2) \\ &= 2 \sum_{\substack{i\in\mathbb{N} \\ 1\le i<\sqrt{n}}} (-1)^{i+1} \sigma^*(n-i^2) + (-1)^{n+1}ns(n). \end{aligned}$$

□

Con base en este resultado, es posible abordar la representación de enteros mediante fórmulas cuadráticas, un problema clásico dentro de la teoría de números que en la actualidad se lo conoce como el teorema de Girard-Fermat. Como señala Williams [3], el matemático francés Albert Girard fue el primero en enunciarlo mediante observación numérica; sin embargo, su demostración fue desarrollada por Fermat en 1654. A lo largo de los años, varios matemáticos como Lagrange, Euler y Dedekind probaron este resultado bajo distintas aproximaciones. A continuación, incluye una demostración basada en la primera identidad de Liouville.

Teorema 6.2.2. ***Teorema de Girard-Fermat***

Un número primo impar p puede representarse como la suma de dos cuadrados si y solo si $p \equiv 1 \pmod 4$.

Demostración: Sea p un número primo impar y considérese $a, b \in \mathbb{N}$ tales que $p = a^2 + b^2$. Supóngase que a, b tienen la misma paridad. Por el teorema 3.4.2, si $a \equiv b \pmod 2$, entonces se verifica que $a^2 \equiv b^2 \pmod 2$. Por el teorema 3.4.1, $a^2 + b^2 \equiv 2b^2 \equiv 0 \pmod 2$. En consecuencia, $a^2 + b^2$ es par; sin embargo, esto es imposible, puesto que $a^2 + b^2 = p$ y p es impar, por definición. Por lo tanto, se tiene una contradicción y la suposición es errónea. De esta manera, a, b tienen distinta paridad. Sin pérdida de generalidad, tómese $a = 2m$ y $b = 2n - 1$ con $m, n \in \mathbb{N}$. Por consiguiente,

$$p = a^2 + b^2 = (2m)^2 + (2n-1)^2 = 4m^2 + 4n^2 - 4n + 1 = 4(m^2 + n^2 - n) + 1.$$

Como resultado, se concluye que $p \equiv 1 \pmod 4$.

Ahora, sea p un número primo tal que $p \equiv 1 \pmod 4$. Por las proposiciones 4.2.2 y 4.2.4, se verifica que

$$\sigma^*(p) = \sigma(p) - \sigma\left(\frac{p}{2}\right) = \frac{p^2 - 1}{p - 1} = p + 1 \equiv 2 \pmod 4.$$

Con base en el teorema 6.2.1 y dado que $s(p) = 0$ puesto que p no es un cuadrado perfecto, se satisface que

$$\sigma^*(p) = 2 \sum_{\substack{i \in \mathbb{N} \\ 1 \leq i < \sqrt{p}}} (-1)^{i+1} \sigma^*(p - i^2).$$

Por lo obtenido previamente y la ley de cancelación, se tiene que

$$\sum_{\substack{i \in \mathbb{N} \\ 1 \leq i < \sqrt{p}}} (-1)^{i+1} \sigma^*(p - i^2) \equiv 1 \pmod 2.$$

Obsérvese que $(-1)^{i+1} \equiv 1 \pmod 2$ puesto que $(-1)^{i+1} = \pm 1, i \in \mathbb{N}$. En consecuencia,

$$\sum_{\substack{i \in \mathbb{N} \\ 1 \leq i < \sqrt{p}}} \sigma^*(p - i^2) \equiv 1 \pmod 2.$$

Por propiedad de congruencia modular, se verifica que $\exists b \in \mathbb{N}$ y $1 \leq b < \sqrt{p}$ tal que $\sigma^*(p - b^2) \equiv 1 \pmod 2$. Con base en el teorema 4.2.3, $p - b^2$ es un cuadrado perfecto impar. En otras palabras, $\exists a \in \mathbb{N}$ con $a \equiv 1 \pmod 2$ tal que $p - b^2 = a^2$. Por consiguiente, $p = a^2 + b^2$. □

CAPÍTULO 7

Segunda Identidad de Liouville

«Lo studio senza desiderio rovina la memoria e non trattiene nulla di ciò che accoglie.»

El estudio sin deseo estropea la memoria y no retiene nada de lo que toma.

Leonardo da Vinci

La segunda identidad de Liouville comparte características con la anterior; no obstante, precisa tomar una función con dominio en $\mathbb{Z}^2$ en lugar de una función aritmética en el sentido convencional y adicionalmente se requiere definir una condición análoga a la paridad que funcione en dicho dominio. En consecuencia, puede entenderse como una extensión en dos dimensiones de la primera identidad establecida en el capítulo anterior.

El uso de esta segunda identidad se encuentra en la fórmula de Jacobi, mediante la cual se puede establecer el resultado de la suma de un número par de cuadrados perfectos.

7.1. Identidad de Liouville

Liouville establece una conexión con la identidad anterior, tal como lo presenta en su octavo artículo "Sur quelques formules générales qui peuvent être utiles dans la theórie des nombres"[12], la partición sobre la cual se trabaja el conjunto de soluciones de la ecuación diofántica, se conserva. En efecto, se mantiene el conjunto A como el intervalo sobre el cual se define la identidad aritmética. Similarmente a lo tratado a priori, para su demostración se emplearán los mapas biyectivos sugeridos por Williams [3]. Dado que concibe un resultado en dos dimensiones, se precisa de un tratamiento especial que emule la condición de paridad en el sentido unidimensional, como se verá a continuación.

Teorema 7.1.1. ***Segunda Identidad de Liouville***

Sean $F : \mathbb{Z} \times \mathbb{Z} \to \mathbb{C}$ *tal que* $f(x,-y) = f(-x,y) = -f(x,y), \forall x,y \in \mathbb{Z}$ *y* $m,n \in \mathbb{N}$. *Entonces,*

$$\sum_{(i,j,k)\in A(n)} (-1)^{\frac{k-1}{2}} f(-2i+k, i+j) = \begin{cases} \sum_{r=1}^{m} (-1)^{m+r} f(2r-1,m), & n = m^2 \\ 0, & n \neq m^2 \end{cases}. \tag{7.1}$$

Demostración: Considérese la partición del conjunto A en los conjuntos B, C, D realizada en la demostración de la primera identidad de Liouville.

De esta forma,

$$\sum_{(i,j,k)\in A(n)} (-1)^{\frac{k-1}{2}} f(-2i+k, i+j) = \sum_{(i,j,k)\in B(n)} (-1)^{\frac{k-1}{2}} f(-2i+k, i+j) + \sum_{(i,j,k)\in C(n)} (-1)^{\frac{k-1}{2}} f(-2i+k, i+j) + \sum_{(i,j,k)\in D(n)} (-1)^{\frac{k-1}{2}} f(-2i+k, i+j).$$

Procédase a trabajar con cada suma por separado. Recuérdese las biyecciones empleadas en el capítulo anterior para la demostración de la primera identidad de Liouville. Considérese la función $\phi(i,j,k) = (-i+k, 2i+j-k, k)$ y el conjunto B, por lo tanto,

$$\begin{aligned} S_1 &= \sum_{(i,j,k)\in B(n)} (-1)^{\frac{k-1}{2}} f(-2i+k, i+j) \\ &= \sum_{(i,j,k)\in B(n)} (-1)^{\frac{k-1}{2}} f(-2(-i+k)+k, -i+k+2i+j-k) \\ &= \sum_{(i,j,k)\in B(n)} (-1)^{\frac{k-1}{2}} f(-(-2i+k), i+j). \end{aligned}$$

Con base en la definición de f, se verifica que $f(-x,y) = -f(x,y)$. Entonces,

$$\sum_{(i,j,k)\in B(n)} (-1)^{\frac{k-1}{2}} f(-2i+k, i+j) = -\sum_{(i,j,k)\in B(n)} (-1)^{\frac{k-1}{2}} f(-2i+k, i+j) = 0.$$

Ahora, trabájese con el conjunto C. Como se demostró previamente, $j \equiv k \equiv 1$ (mód 2), $i = \frac{-j+k}{2}$ y $n = (\frac{j+k}{2})^2$. De esta manera,

$$\begin{aligned} S_2 &= \sum_{(i,j,k)\in C(n)} (-1)^{\frac{k-1}{2}} f(-2i+k, i+j) \\ &= \sum_{\substack{j,k\in\mathbb{N} \\ 2\nmid j,k \\ (\frac{j+k}{2})^2 = n}} (-1)^{\frac{k-1}{2}} f\left(-2\left(\frac{-j+k}{2}\right)+k, \frac{-j+k}{2}+j\right) \\ &= \sum_{\substack{j,k\in\mathbb{N} \\ 2\nmid j,k \\ (\frac{j+k}{2})^2 = n}} (-1)^{\frac{k-1}{2}} f\left(j, \frac{j+k}{2}\right). \end{aligned}$$

De acuerdo con la demostración anterior, $S_2 = 0$ cuando n no es un cuadrado perfecto. Entonces, considérese $n = m^2, m \in \mathbb{N}$. En este caso, dado que $2 \nmid j, k$, tómese $j = 2r - 1, r \in \mathbb{N}$, lo que implica que

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

Además, como $r \equiv -r \pmod 2$, se tiene que $(-1)^r = (-1)^{-r}$. Por lo tanto,

$$\begin{aligned}\sum_{\substack{j,k\in\mathbb{N}\\ 2\nmid j,k\\ (\frac{j+k}{2})^2=n}} (-1)^{\frac{k-1}{2}} f\left(j, \frac{j+k}{2}\right) &= \sum_{r=1}^{m} (-1)^{\frac{2m-2r+1-1}{2}} f(2r-1, m)\\ &= \sum_{r=1}^{m} (-1)^{m-r} f(2r-1, m)\\ &= \sum_{r=1}^{m} (-1)^{m+r} f(2r-1, m).\end{aligned}$$

Como resultado, se concluye que

$$S_2 = \begin{cases} \displaystyle\sum_{r=1}^{m} (-1)^{m+r} f(2r-1, m), & n = m^2 \\ 0, & n \neq m^2 \end{cases}.$$

Finalmente, considérese el conjunto D con su respectiva partición en los conjuntos P y Q. De esta manera,

$$\begin{aligned}S_3 &= \sum_{(i,j,k)\in D(n)} (-1)^{\frac{k-1}{2}} f(-2i+k, i+j)\\ &= \sum_{(i,j,k)\in P(n)} (-1)^{\frac{k-1}{2}} f(-2i+k, i+j) + \sum_{(i,j,k)\in Q(n)} (-1)^{\frac{k-1}{2}} f(-2i+k, i+j).\end{aligned}$$

Adicionalmente, recuérdese la biyección $\psi(i, j, k) = (-i - j, j, -2i - j + k)$. Entonces,

$$\begin{aligned}S_A &= \sum_{(i,j,k)\in Q(n)} (-1)^{\frac{k-1}{2}} f(-2i+k, i+j)\\ &= \sum_{(i,j,k)\in Q(n)} (-1)^{\frac{-2i-j+k-1}{2}} f(-2(-i-j)-2i-j+k, -i-j+j)\\ &= \sum_{(i,j,k)\in Q(n)} (-1)^{-i+\frac{k-j-1}{2}} f(j+k, -i).\end{aligned}$$

Por la proposición 5.4.3, dado que $2|j \iff j \equiv 0 \pmod 2$, se deduce que $i \equiv n \pmod 2$. Además, $-i \equiv i \pmod 2$, lo cual implica que $(-1)^{-j} = (-1)^n$ y por definición, $f(x,-y) = -f(x,y)$. Por consiguiente,

$$\begin{aligned} S_A &= \sum_{(i,j,k)\in Q(n)} -(-1)^{n+\frac{k-j-1}{2}} f(j+k,i) \\ &= (-1)^n \sum_{(i,j,k)\in Q(n)} (-1)^{\frac{k-j+1}{2}} f(j+k,i) \\ &= (-1)^n \sum_{(i,j,k)\in Q(n)} (-1)^{\frac{j-k-1}{2}} f(j+k,i). \end{aligned}$$

Ahora, considérese el conjunto R y la biyección $\eta((i,j,k)) = (i+j, -2i-j+k, j)$ junto a su inversa $\eta^{-1}((i,j,k)) = (i-k, k, 2i+j-k)$. Adicionalmente, por definición de R, $2|j$. Nuevamente por la proposición 5.4.3, $(-1)^{-j} = (-1)^n$. Por lo tanto,

$$\begin{aligned} S_B &= \sum_{(i,j,k)\in P(n)} (-1)^{\frac{k-1}{2}} f(-2i+k, i+j) \\ &= \sum_{(i,j,k)\in R(n)} (-1)^{i+\frac{j-k-1}{2}} f(-2(i-k)+2i+j-k, i-k+k) \\ &= (-1)^n \sum_{(i,j,k)\in R(n)} (-1)^{\frac{j-k-1}{2}} f(j+k,i). \end{aligned}$$

En consecuencia, al superponer ambas sumatorias y por la proposición 5.4.1, se tiene que

$$\begin{aligned}
S_3 &= S_A + S_B \\
&= (-1)^n \sum_{(i,j,k)\in Q(n)\cup R(n)} (-1)^{\frac{j-k-1}{2}} f(j+k,i) \\
&= (-1)^n \sum_{\substack{(i,j,k)\in Q(n)\cup R(n) \\ i<0}} (-1)^{\frac{j-k-1}{2}} f(j+k,i) \\
&+ (-1)^n \sum_{\substack{(i,j,k)\in Q(n)\cup R(n) \\ i>0}} (-1)^{\frac{j-k-1}{2}} f(j+k,i) \\
&= (-1)^n \sum_{\substack{(i,j,k)\in Q(n)\cup R(n) \\ i>0}} (-1)^{\frac{j-k-1}{2}} f(j+k,-i) \\
&+ (-1)^n \sum_{\substack{(i,j,k)\in Q(n)\cup R(n) \\ i>0}} (-1)^{\frac{j-k-1}{2}} f(j+k,i).
\end{aligned}$$

Recuérdese que $Q(n) \cup R(n) = \{(i,j,k) \in A(n) : 2|j, 2 \nmid k\}$, como se demostró previamente. Según la definición de f, se verifica que $f(x,-y) = -f(x,y)$, lo cual implica que

$$\begin{aligned}
S_3 &= (-1)^n \sum_{\substack{(i,j,k)\in Q(n)\cup R(n) \\ i>0}} (-1)^{\frac{j-k-1}{2}} f(j+k,i) \\
&- (-1)^n \sum_{\substack{(i,j,k)\in Q(n)\cup R(n) \\ i>0}} (-1)^{\frac{j-k-1}{2}} f(j+k,i) \\
&= 0.
\end{aligned}$$

Se concluye la demostración al superponer S_1, S_2 y S_3. Luego,

$$\sum_{(i,j,k)\in A(n)} (-1)^{\frac{k-1}{2}} f(-2i+k,i+j) = \begin{cases} \sum_{r=1}^{m} (-1)^{m+r} f(2r-1,m), & n = m^2 \\ 0, & n \neq m^2 \end{cases}.$$

□

7.2. Aplicaciones

Como se ha podido evidenciar, la segunda identidad de Liouville se puede entender como una generalización de la identidad abordada en el capítulo anterior para un entorno de dos dimensiones. Como resultado, es sugerente pensar una aplicación análoga dentro de la representación de enteros como suma de cuadrados. En este apartado, la intuición es correcta, pero amerita introducir varios teoremas que se deducen a partir de esta identidad y una nueva definición dentro de teoría de números, el símbolo de Jacobi. A priori, se presenta el siguiente preámbulo con algunos resultados importantes.

Teorema 7.2.1. *Sean $n, m, \lambda_1, \lambda_2 \in \mathbb{N}$ tal que $2 \nmid \lambda_1, \lambda_2$. Entonces,*

$$\sum_{(i,j,k)\in A(n)} (-1)^{\frac{k-1}{2}} (-2i+k)^{\lambda_1} (i+j)^{\lambda_2} = \begin{cases} \sum_{r=1}^{m} (-1)^{m+r} (2r-1)^{\lambda_1} m^{\lambda_2}, & n = m^2 \\ 0, & n \neq m^2 \end{cases}. \tag{7.2}$$

Demostración: Sea $F(x,y) = x^{\lambda_1} y^{\lambda_2}$, dado que $2 \nmid \lambda_1, \lambda_2$ se verifica que

$$-F(x,y) = -(x^{\lambda_1} y^{\lambda_2}) = (-x)^{\lambda_1} y^{\lambda_2} = x^{\lambda_1} (-y)^{\lambda_2}.$$

Por consiguiente, $F(-x,y) = F(x,-y) = -F(x,y)$. Por la segunda identidad de Liouville,

$$\sum_{(i,j,k)\in A(n)} (-1)^{\frac{k-1}{2}} (-2i+k)^{\lambda_1} (i+j)^{\lambda_2} = \begin{cases} \sum_{r=1}^{m} (-1)^{m+r} (2r-1)^{\lambda_1} m^{\lambda_2}, & n = m^2 \\ 0, & n \neq m^2 \end{cases}.$$

□

Teorema 7.2.2. *Sean $g : \mathbb{Z}^3 \to \mathbb{C}$ una función tal que $g(-i,j,k) = -g(i,j,k)$ con $(i,j,k) \in \mathbb{Z}^3$ y $n \in \mathbb{N}$. Entonces,*

$$\sum_{(i,j,k)\in A(n)} g(i,j,k) = 0. \tag{7.3}$$

Demostración: Por la proposición 5.4.1, se satisface que $(i,j,k) \in A(n) \iff (-i,j,k) \in A(n)$. Dado que $g(-i,j,k) = -g(i,j,k)$, se concluye que

$$\sum_{(i,j,k)\in A(n)} g(i,j,k) = \sum_{(-i,j,k)\in A(n)} g(-i,j,k) = -\sum_{(i,j,k)\in A(n)} g(i,j,k) = 0.$$

□

A continuación, se introduce una función intrínseca dentro de la teoría de representación de enteros como suma de cuadrados.

Definición 7.2.1. Función r_k

Para todo $n \in N \cup \{0\}$, se define la función $r_k(n), k \in \mathbb{N}$, como el número de formas en las que es posible representar n como la suma de k cuadrados, es decir,

$$r_k(n) = |\{(x_1, \ldots, x_k) \in \mathbb{Z}^k : n = x_1^2 + \ldots + x_k^2\}|. \tag{7.4}$$

Nótese que $r_k(0) = 1, \forall k \in \mathbb{N}$ puesto que la única representación posible como suma de cuadrados de 0 es $x_i = 0, i \in \{1, \ldots, k\}$; esto se debe a que $x^2 \geq 0, \forall x \in \mathbb{Z}$. Ahora, se establece una fórmula de recursión para la función r_k.

Teorema 7.2.3. *Sean $n, k \in \mathbb{N}$, entonces*

$$\sum_{\substack{i \in \mathbb{Z} \\ |i| \leq \sqrt{n}}} (n - (k+1)i^2) r_k(n - i^2) = 0. \tag{7.5}$$

Demostración: Obsérvese que si $n = x_1^2 + \ldots + x_k^2 + x_{k+1}^2$ con $(x_1, \ldots, x_k, x_{k+1}) \in \mathbb{Z}^{k+1}$, se verifica que $x_m^2 \leq n \Longrightarrow |x_m| \leq \sqrt{n}, \forall m \in \{1, \ldots, k, k+1\}$. De esta forma, con base en la definición de r_k,

$$r_{k+1}(n) = \sum_{\substack{(x_1,\ldots,x_k,x_{k+1}) \in \mathbb{Z}^{k+1} \\ n = x_1^2 + \ldots + x_k^2 + x_{k+1}^2}} 1 = \sum_{\substack{x_{k+1} \in \mathbb{Z} \\ |x_{k+1}| \leq \sqrt{n}}} \sum_{\substack{(x_1,\ldots,x_k) \in \mathbb{Z}^k \\ n - x_{k+1}^2 = x_1^2 + \ldots + x_k^2}} 1 = \sum_{\substack{i \in \mathbb{Z} \\ |i| \leq \sqrt{n}}} r_k(n - i^2)$$

Ahora, considérese una permutación ϕ_j de los $x_m \in \mathbb{Z}, m \in \{1, \ldots, k, k+1\}$ para $j \in \{1, \ldots, k\}$, la cual se define por

$$\phi_j(x_1, \ldots\ x_{j-1}, x_j, x_{j+1}, \ldots, x_k, x_{k+1}) = (x_1, \ldots\ x_{j-1}, x_{k+1}, x_{j+1}, \ldots, x_k, x_j).$$

Evidentemente, ϕ_j es una involución al tratarse de una permutación. Como resultado, se verifica que

$$\sum_{\substack{(x_1,\ldots,x_k,x_{k+1}) \in \mathbb{Z}^{k+1} \\ n = x_1^2 + \ldots + x_k^2 + x_{k+1}^2}} x_{k+1}^2 = \sum_{\substack{(x_1,\ldots,x_k,x_{k+1}) \in \mathbb{Z}^{k+1} \\ n = x_1^2 + \ldots + x_k^2 + x_{k+1}^2}} x_j^2, j \in \{1, \ldots, k\}.$$

Por lo tanto,

$$n r_{k+1}(n) = \sum_{\substack{(x_1,\ldots,x_k,x_{k+1}) \in \mathbb{Z}^{k+1} \\ n = x_1^2 + \ldots + x_k^2 + x_{k+1}^2}} n = \sum_{\substack{(x_1,\ldots,x_k,x_{k+1}) \in \mathbb{Z}^{k+1} \\ n = x_1^2 + \ldots + x_k^2 + x_{k+1}^2}} \sum_{m=1}^{k+1} x_m^2.$$

Obsérvese que como ambas sumatorias son finitas, puesto que r_{k+1} es finito, es posible intercambiar su orden. En consecuencia,

$$nr_{k+1}(n) = \sum_{m=1}^{k+1} \sum_{\substack{(x_1,\ldots,x_k,x_{k+1})\in\mathbb{Z}^{k+1} \\ n=x_1^2+\ldots+x_k^2+x_{k+1}^2}} x_m^2 = (k+1) \sum_{\substack{(x_1,\ldots,x_k,x_{k+1})\in\mathbb{Z}^{k+1} \\ n=x_1^2+\ldots+x_k^2+x_{k+1}^2}} x_{k+1}^2.$$

Adicionalmente, se satisface que

$$\sum_{\substack{(x_1,\ldots,x_k,x_{k+1})\in\mathbb{Z}^{k+1} \\ n=x_1^2+\ldots+x_k^2+x_{k+1}^2}} x_{k+1}^2 = \sum_{\substack{x_{k+1}\in\mathbb{Z} \\ |x_{k+1}|\leq\sqrt{n}}} x_{k+1}^2 \sum_{\substack{(x_1,\ldots,x_k)\in\mathbb{Z}^k \\ n-x_{k+1}^2=x_1^2+\ldots+x_k^2}} 1 = \sum_{\substack{i\in\mathbb{Z} \\ |i|\leq\sqrt{n}}} i^2 r_k(n-i^2).$$

Por consiguiente,

$$nr_{k+1}(n) = (k+1) \sum_{\substack{i\in\mathbb{Z} \\ |i|\leq\sqrt{n}}} i^2 r_k(n-i^2),$$

$$n \sum_{\substack{i\in\mathbb{Z} \\ |i|\leq\sqrt{n}}} r_k(n-i^2) = (k+1) \sum_{\substack{i\in\mathbb{Z} \\ |i|\leq\sqrt{n}}} i^2 r_k(n-i^2),$$

$$\sum_{\substack{i\in\mathbb{Z} \\ |i|\leq\sqrt{n}}} (n-(k+1)i^2) r_k(n-i^2) = 0.$$

□

La importancia de esta recursión se ve reflejada en el siguiente teorema de unicidad.

Teorema 7.2.4. *r_k es la única función que satisface la recurrencia 7.5.*

Demostración: Supóngase que existe otra función $F : \mathbb{N}\cup\{0\} \to \mathbb{Z}$ tal que $G(0) = 1$ y

$$\sum_{\substack{i\in\mathbb{Z} \\ |i|\leq\sqrt{n}}} (n-(k+1)i^2) f(n-i^2) = 0, n \in \mathbb{N}.$$

Ahora, defínase $G : \mathbb{N}\cup\{0\} \to \mathbb{Z}$ por $G(n) = F(n) - r_k(n), n \in \mathbb{N}\cup\{0\}$. Obsérvese que $G(0) = F(0) - r_k(0) = 1 - 1 = 0$. Por el teorema 7.2.3 y la definición de F, se verifica que

$$\sum_{\substack{i\in\mathbb{Z} \\ |i|\leq\sqrt{n}}} (n-(k+1)i^2) G(n-i^2) = \sum_{\substack{i\in\mathbb{Z} \\ |i|\leq\sqrt{n}}} (n-(k+1)i^2)[F(n-i^2) - r_k(n-i^2)] = 0.$$

Por lo tanto,

$$\sum_{\substack{i\in\mathbb{Z}\\ |i|\leq\sqrt{n}}} (n-(k+1)i^2)G(n-i^2)=0,$$

$$nG(n)+\sum_{\substack{i\in\mathbb{Z}\\ 0<|i|\leq\sqrt{n}}} (n-(k+1)i^2)G(n-i^2)=0,$$

$$G(n)=\frac{-1}{n}\sum_{\substack{i\in\mathbb{Z}\\ 0<|i|\leq\sqrt{n}}} (n-(k+1)i^2)G(n-i^2).$$

Se requiere demostrar que $G(n)=0, \forall n\in\mathbb{N}$, para esto, procédase por inducción fuerte. Considérese el caso base con $n=1$ en la fórmula de recursión y recuérdese que $G(0)=0$, de esta manera,

$$G(1)=\sum_{\substack{i\in\mathbb{Z}\\ 0<|i|\leq 1}} (1-(k+1)i^2)G(1-i^2)=(1-(k+1))G(0)=0.$$

A continuación, supóngase validez para $n<m, m\in\mathbb{N}$, es decir, $G(n)=0, n<m$ y analícese el caso $n=m$.

$$G(m)=\frac{-1}{m}\sum_{\substack{i\in\mathbb{Z}\\ 0<|i|\leq\sqrt{m}}} (m-(k+1)i^2)G(m-i^2).$$

Nótese que $0<|i|\leq\sqrt{m}$, se verifica que

$$0<i^2\leq m,$$

$$-m\leq -i^2<0,$$

$$0\leq m-i^2<m.$$

En consecuencia, por el paso inductivo, se concluye que $G(m)=0$. Dado que se verifica para $n=m$, entonces también lo hace para todo $n\in\mathbb{N}$. Por consiguiente, $G(n)=0 \iff F(n)-r_k(n)=0 \iff F(n)=r_k(n), n\in\mathbb{N}$. Luego, r_k es la única función que satisface la recursión 7.5. □

De acuerdo a Williams [3], se precisa introducir los símbolos de Legendre

y de Jacobi para poder enunciar formalmente la fórmula de Jacobi para el número de representaciones de un entero como suma de dos cuadrados. Primero, se define el símbolo de Legendre, una función aritmética estrechamente relacionada con las congruencias cuadráticas. Como menciona Tattersall [9], este símbolo fue introducido por Adrien-Marie Legendre en su trabajo "Essai sur la Théorie des Nombres" en 1798.

Definición 7.2.2. Símbolo de Legendre

Sean p un número primo y $m \in \mathbb{Z}$. Entonces, el símbolo de Legendre se define por

$$\left(\frac{m}{p}\right) = \begin{cases} 0, & p|m \\ 1, & p \nmid m \text{ y } x^2 \equiv m \pmod{p} \text{ para algún } x \in \mathbb{Z}\,. \\ -1, & x^2 \not\equiv m \pmod{p} \text{ para todo } x \in \mathbb{Z} \end{cases} \tag{7.6}$$

Como se apreció en la definición, el símbolo de Legendre permite conocer el comportamiento de las congruencias cuadráticas para distintos módulos y en sustento con este eje, se relaciona con el criterio formulado por Leonhard Euler para determinar cuáles enteros son restos cuadráticos de un determinado número primo impar.

Teorema 7.2.5. ***Criterio de Euler***

Sean p un número primo impar y $m \in \mathbb{Z}$ tal que $\gcd(m, p) = 1$. *Entonces,*

$$\left(\frac{m}{p}\right) \equiv m^{\frac{p-1}{2}} \pmod{p}. \tag{7.7}$$

Demostración: Para empezar, se requiere clasificar la naturaleza de m con base en la congruencia módulo p y trabajar cada caso por separado.

Considérese que m es un resto cuadrático módulo p, es decir, $\exists n \in N$ tal que $n^2 \equiv m \pmod{p}$. Nótese que $\frac{p-1}{2} \in \mathbb{N}$ puesto que p es un primo impar, y con base en el teorema 3.4.2, se tiene que $n^{(p-1)} \equiv m^{\frac{p-1}{2}} \pmod{p}$. Ahora, como $p \nmid m$, evidentemente, $p \nmid n$; de lo contrario, $m \equiv 0 \pmod{p}$. Por el pequeño teorema de Fermat, se tiene que $n^{p-1} \equiv 1 \pmod{p}$. En consecuencia, $m^{\frac{p-1}{2}} \equiv 1 \pmod{p}$; como $(\frac{m}{p}) = 1$, por definición del símbolo de Legendre, se concluye que $(\frac{m}{p}) \equiv m^{\frac{p-1}{2}} \pmod{p}$.

A continuación, considérese que m no es un resto cuadrático módulo p. Sea $a \in \{1, \ldots, p-1\}$ y analícese la congruencia lineal $ax \equiv m \pmod{p}$; dado que p es primo, se verifica que $\gcd(a, p) = 1$. Por el teorema de Bachet, la congruencia tiene una única solución b módulo p. Como m no es un resto

cuadrático módulo p, se verifica que $a \not\equiv b \pmod{p}$. Por consiguiente, cada resto $1, \ldots, p-1$ puede agruparse en $\frac{p-1}{2}$ pares (a, b) tal que $ab \equiv m \pmod{p}$. De esta manera,

$$(p-1)! \equiv \prod_{i=1}^{\frac{p-1}{2}} a_i b_i \equiv \prod_{i=1}^{\frac{p-1}{2}} m \equiv m^{\frac{p-1}{2}} \pmod{p}.$$

Por el teorema de Wilson, $(p-1)! \equiv -1 \pmod{p}$ con lo que se concluye que $m^{\frac{p-1}{2}} \equiv -1 \pmod{p}$. Según la definición del símbolo de Legendre, $(\frac{m}{p}) = -1$ y por ende, $(\frac{m}{p}) \equiv m^{\frac{p-1}{2}} \pmod{p}$. □

Recuérdese la definición de funciones multiplicativas y completamente multiplicativas, con base en esto se concibe el siguiente teorema como herramienta fundamental para computar símbolos de Legendre.

Teorema 7.2.6. *El símbolo de Legendre es completamente multiplicativo, es decir, para todo primo p y $m, n \in \mathbb{Z}$ se verifica que*

$$\left(\frac{mn}{p}\right) = \left(\frac{n}{p}\right)\left(\frac{n}{p}\right) \tag{7.8}$$

Demostración: Primero, al tomar $p|mn$, se tiene que $p|m$ o $p|n$. De esta forma, trivialmente se verifica que

$$\left(\frac{mn}{p}\right) = \left(\frac{m}{p}\right)\left(\frac{n}{p}\right) = 0.$$

Ahora, considérese que $p \nmid mn$. Nótese que si $p = 2$, entonces $mn \equiv 1 \pmod{2}$ dado que $2 \nmid mn$, y por ende, $m \equiv n \equiv 1 \pmod{2}$. Evidentemente, 1 es un residuo cuadrático módulo 2, por lo cual,

$$\left(\frac{mn}{2}\right) = \left(\frac{m}{2}\right)\left(\frac{n}{2}\right) = 1.$$

De esta manera, basta analizar el caso cuando p es un primo impar y $p \nmid mn$, lo cual implica que $p \nmid m$ y $p \nmid n$. Por el criterio de Euler,

$$\left(\frac{mn}{p}\right) \equiv (mn)^{\frac{p-1}{2}} \equiv m^{\frac{p-1}{2}} n^{\frac{p-1}{2}} \equiv \left(\frac{m}{p}\right)\left(\frac{n}{p}\right) \pmod{p}.$$

Con base en la definición del símbolo de Legendre, este únicamente toma valores de 1 y -1 cuando el numerador no es divisible para p. Esto, en conjunto con que p es un primo impar, lleva a la igualdad

$$\left(\frac{mn}{p}\right) = \left(\frac{m}{p}\right)\left(\frac{n}{p}\right).$$

Luego, se deduce que el símbolo de Legendre es completamente multiplicativo. □

Al percatarse de que la definición del símbolo de Legendre precisa que el denominador sea primo, resulta lógico pensar en la existencia de una posible generalización. En efecto, este cometido se consigue con el símbolo de Jacobi que fundamenta en la descomposición canónica de un número.

Definición 7.2.3. Símbolo de Jacobi

Sean $m \in Z$ y $n \in \mathbb{N}$. Entonces, dada la descomposición canónica de n, el símbolo de Jacobi se define por

$$\left(\frac{m}{n}\right) = \prod_{i \in \mathbb{N}} \left(\frac{m}{p_i}\right)^{\alpha_i}. \tag{7.9}$$

En particular, resulta crucial analizar el comportamiento del símbolo de Jacobi cuando $m = -4$ puesto que interviene en la fórmula de Jacobi, tal como se verá más adelante.

Proposición 7.2.1. Sea $n \in \mathbb{N}$, entonces

$$\left(\frac{-4}{n}\right) = \begin{cases} 0, & n \equiv 0 \pmod 2 \\ 1, & n \equiv 1 \pmod 4 \\ -1, & n \equiv 3 \pmod 4 \end{cases} \tag{7.10}$$

.

Demostración: Considérese las clases congruentes módulo 4 y analícese el símbolo de Jacobi por separado.

1. $n \equiv 0 \pmod 2$

   Obsérvese que este caso abarca $n \equiv 0 \pmod 4$ y $n \equiv 2 \pmod 4$, lo cual implica que $2|n$. En consecuencia, por definición del símbolo de Jacobi, se verifica que

   $$\left(\frac{-4}{n}\right) = \left(\frac{-4}{2}\right)^{\alpha_1} \prod_{\substack{i \in \mathbb{N} \\ i \geq 2}} \left(\frac{-4}{p_i}\right)^{\alpha_i}.$$

   Ahora, obsérvese que $2| -4$. Por definición del símbolo de Legendre,

   $$\left(\frac{-4}{2}\right) = 0.$$

   Por consiguiente,

   $$\left(\frac{-4}{n}\right) = 0.$$

2. $n \equiv 1 \pmod 4$

   En este caso, $2 \nmid n$, es decir, 2 no aparece en la descomposición canónica de n. Por lo tanto, ningún símbolo de Legendre que aparece en la productoria del símbolo de Jacobi es nulo, debido a que 2 es el único factor primo que divide a -4.

   Ahora, procédase a evaluar la descomposición canónica de n. Obsérvese que como $2 \nmid n$, los factores primos p_i de n verifican que $p_i \equiv 1 \pmod 4$ o $p_i \equiv -1 \pmod 4$ con $i \in \mathbb{N}$. Por el teorema 7.2.6, los símbolos de Legendre son multiplicativos y, como $p_i \nmid 4$ para todos los factores primos p_i, se satisface que

   $$\left(\frac{-4}{p_i}\right) = \left(\frac{-1}{p_i}\right)\left(\frac{2}{p_i}\right)^2 = \left(\frac{-1}{p_i}\right)(\pm 1)^2 = \left(\frac{-1}{p_i}\right).$$

   Por definición del símbolo de Jacobi,

   $$\left(\frac{-4}{n}\right) = \prod_{i\in\mathbb{N}} \left(\frac{-4}{p_i}\right)^{\alpha_i} = \prod_{i\in\mathbb{N}} \left(\frac{-1}{p_i}\right)^{\alpha_i}$$

   A continuación, nótese que con base en la congruencia módulo 4, es posible separar la descomposición canónica de n en dos productorios, de manera que

   $$n = \left(\prod_{i\in\mathbb{N}} q_i^{\beta_i}\right)\left(\prod_{i\in\mathbb{N}} r_i^{\gamma_i}\right),$$

   donde cada $q_i \equiv 1 \pmod 4$ y cada $r_i \equiv -1 \pmod 4$.

   Obsérvese que

   $$\prod_{i\in\mathbb{N}} q_i^{\beta_i} \equiv \prod_{i\in\mathbb{N}} 1^{\beta_i} \equiv \prod_{i\in\mathbb{N}} 1 \equiv 1 \pmod 4.$$

   Dado que $n \equiv 1 \pmod 4$, por la ley de cancelación, se concluye que

   $$\prod_{i\in\mathbb{N}} r_i^{\gamma_i} \equiv \prod_{i\in\mathbb{N}} (-1)^{\gamma_i} \equiv 1 \pmod 4.$$

   Como $q_i \equiv 1 \pmod 4$ para todo factor primo q_i, se verifica que $q_i = 4k+1, k \in \mathbb{Z}$. Por el criterio de Euler,

   $$\left(\frac{-1}{q_i}\right) \equiv (-1)^{\frac{q_i-1}{2}} \equiv (-1)^{\frac{4k+1-1}{2}} \equiv (-1)^{2k} \equiv 1 \pmod{q_i}.$$

Análogamente, como $r_i \equiv -1 \pmod 4$ para todo factor primo r_i, se verifica que $r_i = 4k-1, k \in \mathbb{Z}$. Por el criterio de Euler,

$$\left(\frac{-1}{r_i}\right) \equiv (-1)^{\frac{r_i-1}{2}} \equiv (-1)^{\frac{4k-1-1}{2}} \equiv (-1)^{2k-1} \equiv -1 \pmod{r_i}.$$

Por definición, el símbolo de Legendre solo toma valores de 1 y -1 y como los factores primos son impares, se verifica la igualdad. Por consiguiente,

$$\left(\frac{-1}{q_i}\right) = 1,$$

$$\left(\frac{-1}{r_i}\right) = -1.$$

En consecuencia, el símbolo de Jacobi viene dado por

$$\begin{aligned}\left(\frac{-1}{n}\right) &= \left(\prod_{i\in\mathbb{N}} \left(\frac{-1}{q_i}\right)^{\beta_i}\right)\left(\prod_{i\in\mathbb{N}} \left(\frac{-1}{r_i}\right)^{\gamma_i}\right) \\ &= \left(\prod_{i\in\mathbb{N}} 1^{\beta_i}\right)\left(\prod_{i\in\mathbb{N}} (-1)^{\gamma_i}\right) \\ &= \left(\prod_{i\in\mathbb{N}} 1\right)\left(\prod_{i\in\mathbb{N}} (-1)^{\gamma_i}\right) \\ &= \prod_{i\in\mathbb{N}} (-1)^{\gamma_i}.\end{aligned}$$

Nótese que la última productoria únicamente puede tomar valores de 1 y -1. De esta manera,

$$\prod_{i\in\mathbb{N}} (-1)^{\gamma_i} \equiv 1 \pmod 4 \Longrightarrow \prod_{i\in\mathbb{N}} (-1)^{\gamma_i} = 1.$$

Por consiguiente,

$$\left(\frac{-4}{n}\right) = 1.$$

3. $n \equiv 3 \pmod 4$

   La demostración de este caso es análoga al anterior. Primero, nótese que el símbolo de Jacobi no es nulo, puesto que $2 \nmid n$ y los factores primos dejan resto 1 y -1 módulo 4. De esta forma, es posible separar

n en dos sumatorias, como se especificó previamente. Recuérdese que la productoria con los q_i es congruente con 1 (mód 4) y obsérvese que $n \equiv 3 \equiv -1 \pmod 4$.

Por la ley de cancelación,

$$\prod_{i\in\mathbb{N}} r_i^{\gamma_i} \equiv \prod_{i\in\mathbb{N}} (-1)^{\gamma_i} \equiv -1 \pmod 4.$$

Como la última productoria solo toma valores de 1 y -1, se concluye que

$$\prod_{i\in\mathbb{N}} (-1)^{\gamma_i} = -1.$$

Por definición del símbolo y según lo calculado previamente, se satisface que

$$\left(\frac{-4}{n}\right) = \prod_{i\in\mathbb{N}} (-1)^{\gamma_i} = -1.$$

Luego,

$$\left(\frac{-4}{n}\right) = \begin{cases} 0, & n \equiv 0 \pmod 2 \\ 1, & n \equiv 1 \pmod 4 \\ -1, & n \equiv 3 \pmod 4 \end{cases}.$$

□

Finalmente, se han desarrollado todas las herramientas requeridas para llegar a la aplicación última de la segunda identidad de Liouville prevista para este capítulo, la denominada fórmula de Jacobi.

Teorema 7.2.7. ***Fórmula de Jacobi***
Sea $n \in \mathbb{N}$, entonces

$$r_2(n) = 4 \sum_{d|n} \left(\frac{-4}{d}\right).$$

Demostración: Sean $\lambda_1 = \lambda_2 = 1$ y como $2 \nmid 1$, por el teorema 7.2.1 se verifica que

$$\sum_{(i,j,k)\in A(n)} (-1)^{\frac{k-1}{2}} (-2i+k)(i+j) = \begin{cases} (-1)^m \sum_{r=1}^{m} (-1)^r (2r-1)m, & n = m^2 \\ 0, & n \neq m^2 \end{cases}.$$

Ahora, nótese que

$$\begin{aligned}\sum_{r=1}^{m}(-1)^r(2r-1) &= \sum_{r=1}^{m}(-1)^r(r+r-1)\\ &= \sum_{r=1}^{m}(-1)^r r + (-1)^r(r-1)\\ &= \sum_{r=1}^{m}(-1)^r r - (-1)^{r-1}(r-1).\end{aligned}$$

Obsérvese que la última sumatoria es una suma telescópica, de forma que únicamente se toma en consideración el primer y el último término. Por lo tanto,

$$\sum_{r=1}^{m}(-1)^r(2r-1) = (-1)^m m - (-1)^{1-1}(1-1) = (-1)^m m.$$

Recuérdese la función s definida en el teorema 4.2.8, de forma que

$$\sum_{(i,j,k)\in A(n)} (-1)^{\frac{k-1}{2}}(-2i+k)(i+j) = \begin{cases}(-1)^{2m}m^2, & n = m^2\\ 0, & n \neq m^2\end{cases},$$

$$\sum_{(i,j,k)\in A(n)} (-1)^{\frac{k-1}{2}}(-2i^2-2ij+ik+jk) = ns(n).$$

Es importante recalcar que la sumatoria se trabaja sobre soluciones de la ecuación de Liouville, por lo cual $i^2+jk = n \iff jk = n-i^2$. Entonces,

$$\sum_{(i,j,k)\in A(n)} (-1)^{\frac{k-1}{2}}(-2i^2-2ij+ik+n-i^2) = ns(n),$$

$$\sum_{(i,j,k)\in A(n)} (-1)^{\frac{k-1}{2}}(-2ij+ik+n-3i^2) = ns(n).$$

Sea $g(i,j,k) = (-1)^{\frac{k-1}{2}}(-2ij+ik)$ y véase que $g(-i,j,k) = -g(i,j,k) = (-1)^{\frac{k-1}{2}}(2ij-ik)$. Por el teorema 7.2.2,

$$\sum_{(i,j,k)\in A(n)} (-1)^{\frac{k-1}{2}}(-2ij+ik) = 0.$$

De esta manera, la expresión se reduce a

$$\sum_{(i,j,k)\in A(n)} (-1)^{\frac{k-1}{2}}(n-3i^2) = ns(n).$$

Sepárese la sumatoria en dos, al considerar que como $(i,j,k) \in A(n)$, se tiene que $|i| < \sqrt{n}, i \in \mathbb{Z}$ y $jk = n - i^2$ tal que $2 \nmid k$; y el algoritmo de la división, $k|n-i^2$. Por consiguiente,

$$\sum_{\substack{i\in\mathbb{Z}\\ |i|<\sqrt{n}}} (n-3i^2) \sum_{\substack{k\in\mathbb{N}\\ k|n-i^2\\ 2\nmid k}} (-1)^{\frac{k-1}{2}} = ns(n),$$

$$\sum_{\substack{i\in\mathbb{Z}\\ |i|<\sqrt{n}}} (n-3i^2)\cdot 4 \sum_{\substack{k\in\mathbb{N}\\ k|n-i^2\\ 2\nmid k}} (-1)^{\frac{k-1}{2}} = 4ns(n).$$

Sea $d \in \mathbb{N}$ y considérese la sumatoria

$$\sum_{\substack{d|n\\ 2\nmid d}} (-1)^{\frac{d-1}{2}},$$

y obsérvese que si $d \equiv 0 \pmod 2$, entonces la sumatoria es nula. Esto se debe a que $d \nmid 2$ y por el algoritmo de la división, un entero no deja dos restos distintos módulo 2. Como se apreció previamente,

$$(-1)^{\frac{d-1}{2}} = \begin{cases} 1, & d \equiv 1 \pmod 4 \\ -1, & d \equiv 3 \pmod 4 \end{cases}.$$

Por la proposición 7.2.1, se concluye que

$$\sum_{\substack{d|n\\ 2\nmid d}} (-1)^{\frac{d-1}{2}} = \sum_{d|n} \left(\frac{-4}{d}\right).$$

Ahora, defínase la función G por $G(0) = 1$ y

$$G(n) = 4\sum_{d|n} \left(\frac{-4}{d}\right), \forall n \in \mathbb{N}.$$

En consecuencia,

$$\sum_{\substack{i\in\mathbb{Z}\\ |i|<\sqrt{n}}} (n-3i^2)G(n-i^2) = 4ns(n).$$

Finalmente, evalúese la naturaleza de la sumatoria al incluir $|i| = \sqrt{n}$ según si n es un cuadrado perfecto o no. Para esto, analícese cada caso por separado.

1. $n = m^2, m \in \mathbb{N}$

   Por definición de la función s, se verifica que $s(n) = 1$. Por lo tanto, al separar la sumatoria en el caso en el que se satisface la igualdad, se concluye que

$$\begin{aligned}\sum_{\substack{i\in\mathbb{Z}\\ |i|\leq\sqrt{n}}} (n-3i^2)G(n-i^2) &= \sum_{\substack{i\in\mathbb{Z}\\ |i|<\sqrt{n}}} (n-3i^2)G(n-i^2)\\ &\quad + (n-3(-\sqrt{n})^2)G(n-(-\sqrt{n})^2)\\ &\quad + (n-3(\sqrt{n})^2)G(n-(\sqrt{n})^2)\\ &= \sum_{\substack{i\in\mathbb{Z}\\ |i|<\sqrt{n}}} (n-3i^2)G(n-i^2) + 2(-2n)G(0)\\ &= 4n-4n\\ &= 0.\end{aligned}$$

2. $n \neq m^2, \forall m \in \mathbb{N}$

   Por definición de la función s, se verifica que $s(n) = 0$. Por lo tanto, la sumatoria con $\leq$ es igual a la sumatoria con $<$. De esta manera, se concluye que

$$\begin{aligned}\sum_{\substack{i\in\mathbb{Z}\\ |i|\leq\sqrt{n}}} (n-3i^2)G(n-i^2) &= \sum_{\substack{i\in\mathbb{Z}\\ |i|<\sqrt{n}}} (n-3i^2)G(n-i^2)\\ &= 0.\end{aligned}$$

Como resultado, se obtiene que

$$\sum_{\substack{i\in\mathbb{Z}\\ |i|\leq\sqrt{n}}} (n-3i^2)G(n-i^2) = 0, \forall n \in \mathbb{N}.$$

De esta forma, en relación con el teorema 7.2.4 con $k = 2$, se tiene que la única función que satisface la última expresión es r_2.

Por consiguiente, se deduce que $r_2(n) = G(n), \forall n \in \mathbb{N}$.
Luego,

$$r_2(n) = 4 \sum_{d|n} \left(\frac{-4}{d} \right).$$

□

CAPÍTULO 8

Tercera Identidad de Liouville

«La science est l'oeuvre de l'esprit humain, qui est plutôt destiné à étudier qu'à connaître, à chercher qu'à trouver la vérité.»

La ciencia es el trabajo del espíritu humano que está destinado a estudiar como a concocer, tanto a buscar la verdad como a encontrarla.

Évariste Galois

La tercera identidad de Liouville mantiene una conexión intrínseca y, en cierta forma, más pura con las funciones aritméticas abordadas previamente. En efecto, este impresionante resultado hace posible evaluar una sumatoria de una función aritmética par en términos del número y suma de divisores. Esta identidad difiere de las anteriores en el conjunto de soluciones sobre el cual se trabaja, el cual está formada por las tétradas de naturales correspondientes a la solución de una ecuación diofántica lineal.

Esta poderosa herramienta se relaciona con la congruencia aritmética y es un resultado muy conveniente al momento de calcular sumatorias de convolución. Un resultado particular que se abordará en este capítulo es la fórmula de Besge, donde la función σ se hace presente.

8.1. Identidad de Liouville

La alucinante fórmula aritmética fue deducida gracias al brillante ingenio de Liouville, evidencia que se encuentra en su cuarto artículo "Sur quelques formules générales qui peuvent être utiles dans la theórie des nombres" [13], donde concibe la expansión de la sumatoria de una función par evaluada para un arbitrario entero n en virtud del número de sus divisores y su respectiva suma, por medio de la descomposición de n como la adición de dos enteros.

Tal como se mencionó en la presentación del capítulo, es menester definir el nuevo conjunto de soluciones que constituye la piedra angular de la tercera identidad de Liouville.

Definición 8.1.1. Conjunto B

El conjunto B corresponde al conjunto de tétradas (a, b, x, y) tal que

$$B(n) = \{(a, b, x, y) \in \mathbb{N}^4 : ax + by = n\}. \tag{8.1}$$

Una vez llegado a este punto, se recordará que para las dos primeras identidades se dedicó una sección dentro de capítulo netamente al estudio del comportamiento del conjunto A. Si bien el conjunto B no es excepción, no se contempló necesario proceder de igual manera, puesto que solo se precisa de un único teorema, el cual se introduce a continuación, para poder abordar formalmente a la identidad. Para su demostración, se contempla calcular una sumatoria mediante dos particiones distintas, como lo señala Williams [3].

Teorema 8.1.1. *Sean $n, k \in \mathbb{N}$. Entonces,*

$$2 \sum_{\substack{(a,b,x,y)\in B(n)\\ a-b=k}} 1 - \sum_{\substack{(a,b,x,y)\in B(n)\\ a+b=k}} 1 = \left(1 - k + \frac{2n}{k}\right) F_k(n) - 2\sum_{\substack{v|n\\ v\geq k}} 1. \tag{8.2}$$

Demostración: En primer lugar, considérese la sumatoria

$$\sum_{\substack{(b,x,y)\in N^3\\ kx+by=n}} 1,$$

y tómese dos particiones del conjunto de ternas en tres subconjuntos disjuntos por pares según la ley de la tricotomía para x y b. De esta manera, defínase las siguientes sumas

$$A_1 = \sum_{\substack{(b,x,y)\in\mathbb{N}^3\\ kx+by=n\\ x<y}} 1, \quad A_2 = \sum_{\substack{(b,x,y)\in\mathbb{N}^3\\ kx+by=n\\ x=y}} 1, \quad A_3 = \sum_{\substack{(b,x,y)\in\mathbb{N}^3\\ kx+by=n\\ x>y}} 1.$$

Por consiguiente, se tiene una suma directa y se satisface que

$$A_1 + A_2 + A_3 = \sum_{\substack{(b,x,y)\in N^3\\ kx+by=n}} 1.$$

Similarmente, defínase las sumas

$$B_1 = \sum_{\substack{(b,x,y)\in\mathbb{N}^3\\ kx+by=n\\ b<k}} 1, \quad B_2 = \sum_{\substack{(b,x,y)\in\mathbb{N}^3\\ kx+by=n\\ b=k}} 1, \quad B_3 = \sum_{\substack{(b,x,y)\in\mathbb{N}^3\\ kx+by=n\\ b>k}} 1.$$

Nuevamente se obtiene una suma directa, por lo cual se verifica que

$$B_1 + B_2 + B_3 = \sum_{\substack{(b,x,y)\in N^3\\ kx+by=n}} 1.$$

En consecuencia, $A_1 + A_2 + A_3 = B_1 + B_2 + B_3$. A continuación, analícese las sumatorias definidas por A_3 y B_3. Obsérvese que $y > 0$ puesto que $y \in \mathbb{N}$, de manera que al sustituir x por $x + y$, implícitamente se cumple la condición $x > y$. Por lo tanto,

$$A_3 = \sum_{\substack{(b,x,y)\in\mathbb{N}^3\\ kx+by=n\\ x>y}} 1 = \sum_{\substack{(b,x,y)\in\mathbb{N}^3\\ k(x+y)+by=n}} 1 = \sum_{\substack{(b,x,y)\in\mathbb{N}^3\\ kx+ky+by=n}} 1.$$

Análogamente, $k > 0$ puesto que $k \in \mathbb{N}$, de manera que b puede sustituirse por $b + k$ para que se cumpla la condición $b > k$. Por consiguiente,

$$B_3 = \sum_{\substack{(b,x,y)\in\mathbb{N}^3\\ kx+by=n\\ b>k}} 1 = \sum_{\substack{(b,x,y)\in\mathbb{N}^3\\ kx+(b+k)y=n}} 1 = \sum_{\substack{(b,x,y)\in\mathbb{N}^3\\ kx+ky+by=n}} 1.$$

De esta forma, se concluye que $A_3 = B_3$ y por ende, $A_1 + A_2 = B_1 + B_2$. Procédase a evaluar la suma A_2, por el algoritmo de la división, se tiene que

$$A_2 = \sum_{\substack{(b,x,y)\in\mathbb{N}^3 \\ kx+by=n \\ x=y}} 1 = \sum_{\substack{(b,x)\in\mathbb{N}^2 \\ kx+bx=n}} 1 = \sum_{\substack{(b,x)\in\mathbb{N}^2 \\ (k+b)x=n}} 1 = \sum_{k+b|n} 1.$$

Denótese $k+b$ por v y dado que $b, k \in \mathbb{N}$, nótese que $v > k$. Por consiguiente,

$$A_2 = \sum_{\substack{v|n \\ v>k}} 1 = \sum_{\substack{v|n \\ v\geq k}} 1 - \sum_{\substack{v|n \\ v=k}} 1 = \sum_{\substack{v|n \\ v\geq k}} 1 - \sum_{k|n} 1.$$

Obsérvese que como k es fijo, la segunda sumatoria puede tomar solo el valor de 0 a 1, el cual depende de la divisibilidad de n entre k. Por la definición de la función F_k, se satisface que

$$A_2 = \sum_{\substack{v|n \\ v\geq k}} 1 - F_k(n).$$

A continuación, analícese la suma B_2.

$$B_2 = \sum_{\substack{(b,x,y)\in\mathbb{N}^3 \\ kx+by=n \\ b=k}} 1 = \sum_{\substack{(x,y)\in\mathbb{N}^2 \\ kx+ky=n}} 1 = \sum_{\substack{(x,y)\in\mathbb{N}^2 \\ k(x+y)=n}} 1 = \sum_{\substack{(x,y)\in\mathbb{N}^2 \\ x+y=\frac{n}{k}}} 1.$$

En relación con el algoritmo de división, si $k \nmid n$, entonces $\nexists x, y \in \mathbb{N}$ tales que $x + y = \frac{n}{k}$ y por ende, $B_2 = 0$. De esta forma, B_2 solo tiene un valor no nulo cuando $k|n$, en cuyo caso, $\frac{k}{n} \in \mathbb{N}$. Obsérvese que el valor B_2 cuando $k|n$ corresponde al número de soluciones naturales de la ecuación $x + y = \frac{n}{k}$. Sean N_1 el número de soluciones enteras no negativas de $x + y = \frac{n}{k}$ y N_2 el número de soluciones enteras tales que $x = 0$ o $y = 0$. Por el principio de inclusión-exclusión, se satisface que $B_2 = S_1 - S_2$. Evidentemente, $S_2 = 2$ puesto que las únicas soluciones son $(\frac{n}{k}, 0)$ y $(0, \frac{n}{k})$. Ahora, mediante análisis combinatorio, se tiene que S_1 viene dado por la fórmula de Bose-Einstein

$$S_1 = \binom{2 + \frac{n}{k} - 1}{\frac{n}{k}} = \binom{\frac{n}{k} + 1}{\frac{n}{k}} = \frac{(\frac{n}{k} + 1)(\frac{n}{k})!}{(\frac{n}{k})!} = \frac{n}{k} + 1.$$

Por consiguiente, cuando $k|n$, se obtiene que

$$B_2 = \frac{n}{k} + 1 - 2 = \frac{n}{k} - 1.$$

En consecuencia, como B_2 depende de la divisibilidad de n entre k, al emplear la función F_k, se concluye que

$$B_2 = \left(\frac{n}{k} - 1\right) F_k(n) = \frac{n}{k} F_k(n) - F_k(n).$$

Como resultado, se tiene que

$$A_1 + \sum_{\substack{v|n \\ v \geq k}} 1 - F_k(n) = B_1 + \frac{n}{k} F_k(n) - F_k(n),$$

$$A_1 - B_1 = \frac{n}{k} F_k(n) - \sum_{\substack{v|n \\ v \geq k}} 1.$$

Acto seguido, procédase a analizar las sumatorias que aparecen en el lado izquierdo de la ecuación 8.2. Véase que

$$\sum_{\substack{(a,b,x,y) \in B(n) \\ a-b=k}} 1 = \sum_{\substack{(a,b,x,y) \in \mathbb{N}^4 \\ ax+by=n \\ a=b+k}} 1 = \sum_{\substack{(b,x,y) \in \mathbb{N}^3 \\ (b+k)x+by=n}} 1 = \sum_{\substack{(b,x,y) \in \mathbb{N}^3 \\ kx+b(x+y)=n}} 1.$$

Obsérvese que $y > 0$ dado que $y \in \mathbb{N}$, por lo cual al sustituir $x + y$ por y, implica que $x < y$. Por lo tanto,

$$\sum_{\substack{(a,b,x,y) \in B(n) \\ a-b=k}} 1 = \sum_{\substack{(b,x,y) \in \mathbb{N}^3 \\ kx+by=n \\ x<y}} 1 = A_1.$$

Sepárese la segunda sumatoria al considerar la ley de la tricotomía.

$$\sum_{\substack{(a,b,x,y) \in B(n) \\ a+b=k}} 1 = \sum_{\substack{(a,b,x,y) \in \mathbb{N}^4 \\ ax+by=n \\ a+b=k}} 1 = \sum_{\substack{(a,b,x,y) \in \mathbb{N}^4 \\ ax+by=n \\ a+b=k \\ x<y}} 1 + \sum_{\substack{(a,b,x,y) \in \mathbb{N}^4 \\ ax+by=n \\ a+b=k \\ x=y}} 1 + \sum_{\substack{(a,b,x,y) \in \mathbb{N}^4 \\ ax+by=n \\ a+b=k \\ x>y}} 1.$$

Trabájese las sumatorias por separado.

$$\sum_{\substack{(a,b,x,y) \in \mathbb{N}^4 \\ ax+by=n \\ a+b=k \\ x=y}} 1 = \sum_{\substack{(a,b,x) \in \mathbb{N}^3 \\ ax+bx=n \\ a+b=k}} 1 = \sum_{\substack{(a,b,x) \in \mathbb{N}^3 \\ (a+b)x=n \\ a+b=k}} 1 = \sum_{\substack{(a,b,x) \in \mathbb{N}^3 \\ kx=n \\ a+b=k}} 1.$$

Por el algoritmo de la división, la sumatoria es nula si $k \nmid n$, puesto que $\nexists x \in \mathbb{Z}$ tal que $kx = n$. Ahora, la sumatoria cuando $k|n$ es equivalente al número de

soluciones naturales de la ecuación $a+b=k$. Obsérvese que el cálculo de esta sumatoria es análogo al de B_2, por lo cual empléese el mismo análisis combinatorio. Por la fórmula de Bose-Einstein y el principio de inclusión-exclusión, se tiene que

$$\sum_{\substack{(a,b)\in\mathbb{N}^2\\ a+b=k}} 1 = \binom{2+k-1}{k} - 2 = \binom{k+1}{k} - 2 = \frac{(k+1)k!}{k!} - 2 = k+1-2 = k-1.$$

Como la sumatoria depende de la divisibilidad de n entre k, al emplear la función F_k, se concluye que

$$\sum_{\substack{(a,b,x)\in\mathbb{N}^3\\ kx=n\\ a+b=k}} 1 = (k-1)F_k(n).$$

Por último, obsérvese que las dos sumatorias restantes son iguales, puesto que se trata de una permutación de x y de y. Por lo tanto,

$$\sum_{\substack{(a,b,x,y)\in\mathbb{N}^4\\ ax+by=n\\ a+b=k\\ x<y}} 1 + \sum_{\substack{(a,b,x,y)\in\mathbb{N}^4\\ ax+by=n\\ a+b=k\\ x>y}} 1 = 2 \sum_{\substack{(a,b,x,y)\in\mathbb{N}^4\\ ax+by=n\\ a+b=k\\ x<y}} 1.$$

Con base en lo obtenido previamente, la condición $x<y$ se halla implícita al reemplazar y por $x+y$. De esta manera,

$$\sum_{\substack{(a,b,x,y)\in\mathbb{N}^4\\ ax+by=n\\ a+b=k\\ x<y}} 1 + \sum_{\substack{(a,b,x,y)\in\mathbb{N}^4\\ ax+by=n\\ a+b=k\\ x>y}} 1 = 2 \sum_{\substack{(a,b,x,y)\in\mathbb{N}^4\\ ax+b(x+y)=n\\ a+b=k}} 1 = 2 \sum_{\substack{(a,b,x,y)\in\mathbb{N}^4\\ (a+b)x+by=n\\ a+b=k}} 1 = 2 \sum_{\substack{(b,x,y)\in\mathbb{N}^3\\ kx+by=n}} 1.$$

Además, como $k=a+b$ y $a,b\in\mathbb{N}$, entonces $b<k$, con lo cual se deduce que

$$\sum_{\substack{(a,b,x,y)\in\mathbb{N}^4\\ ax+by=n\\ a+b=k\\ x<y}} 1 + \sum_{\substack{(a,b,x,y)\in\mathbb{N}^4\\ ax+by=n\\ a+b=k\\ x>y}} 1 = 2 \sum_{\substack{(b,x,y)\in\mathbb{N}^3\\ kx+by=n\\ b<k}} 1 = 2B_1.$$

En consecuencia, al superponer las sumatorias se obtiene que

$$\sum_{\substack{(a,b,x,y)\in B(n)\\ a+b=k}} 1 = 2B_1 + (k-1)F_k(n).$$

Por consiguiente,

$$\begin{aligned}
2\sum_{\substack{(a,b,x,y)\in B(n)\\ a-b=k}} 1 - \sum_{\substack{(a,b,x,y)\in B(n)\\ a+b=k}} 1 &= 2A_1 - (2B_1 + (k-1)F_k(n)) \\
&= 2(A_1 - B_1) - (k-1)F_k(n) \\
&= 2\left(\frac{n}{k}F_k(n) - \sum_{\substack{v|n\\ v\geq k}} 1\right) + (1-k)F_k(n) \\
&= \left(1 - k + \frac{2n}{k}\right)F_k(n) - 2\sum_{\substack{v|n\\ v\geq k}} 1.
\end{aligned}$$

□

Finalmente, se disponen de todas las definiciones imprescindibles para introducir formalmente la tercera y última identidad de Liouville a tratarse, así como las herramientas matemáticas requeridas para su demostración, tal como se especifica a continuación.

Teorema 8.1.2. ***Tercera Identidad de Liouville***

Sean $f : \mathbb{Z} \longrightarrow C$ una función par y $n \in \mathbb{N}$. Entonces,

$$\sum_{\substack{(a,b,x,y)\in\mathbb{N}^4\\ ax+by=n}} (f(a-b) - f(a+b)) =$$

$$f(0)(\sigma(n) - \tau(n)) + \sum_{d|n}\left(1 + \frac{2n}{d} - d\right)f(d) - 2\sum_{d|n}\sum_{k=1}^{d} f(k). \quad (8.3)$$

Demostración: Procédase a trabajar con el lado izquierdo de la identidad.

Como $a, b \in \mathbb{N}$, se verifica que $a+b \in \mathbb{N}$ y $a-b \in \mathbb{Z}$. Por lo tanto,

$$\begin{aligned}\sum_{\substack{(a,b,x,y)\in\mathbb{N}^4\\ ax+by=n}} (f(a-b)-f(a+b)) &= \sum_{\substack{(a,b,x,y)\in\mathbb{N}^4\\ ax+by=n}} f(a-b) - \sum_{\substack{(a,b,x,y)\in\mathbb{N}^4\\ ax+by=n}} f(a+b)\\ &= \sum_{\substack{(a,b,x,y)\in\mathbb{N}^4\\ k\in\mathbb{Z}\\ ax+by=n\\ a-b=k}} f(k) - \sum_{\substack{(a,b,x,y)\in\mathbb{N}^4\\ k\in\mathbb{N}\\ ax+by=n\\ a+b=k}} f(k)\\ &= \sum_{k\in\mathbb{Z}} f(k) \sum_{\substack{(a,b,x,y)\in\mathbb{N}^4\\ ax+by=n\\ a-b=k}} 1 - \sum_{k\in\mathbb{N}} f(k) \sum_{\substack{(a,b,x,y)\in\mathbb{N}^4\\ ax+by=n\\ a+b=k}} 1.\end{aligned}$$

Obsérvese que la primera doble sumatoria puede separarse a base de la ley de la tricotomía. En efecto, como $k \in \mathbb{Z}$, se tiene $k<0$, $k=0$ y $k>0$, en cuyo caso, $-k \in \mathbb{N}$, $a-b=0$ y $k \in \mathbb{N}$, respectivamente. De esta forma,

$$\begin{aligned}\sum_{\substack{(a,b,x,y)\in\mathbb{N}^4\\ ax+by=n}} (f(a-b)-f(a+b)) &= \sum_{-k\in\mathbb{N}} f(k) \sum_{\substack{(a,b,x,y)\in\mathbb{N}^4\\ ax+by=n\\ a-b=k}} 1 + f(0) \sum_{\substack{(a,b,x,y)\in\mathbb{N}^4\\ ax+by=n\\ a-b=0}} 1\\ &\quad + \sum_{k\in\mathbb{N}} f(k) \sum_{\substack{(a,b,x,y)\in\mathbb{N}^4\\ ax+by=n\\ a-b=k}} 1 - \sum_{k\in\mathbb{N}} f(k) \sum_{\substack{(a,b,x,y)\in\mathbb{N}^4\\ ax+by=n\\ a+b=k}} 1\\ &= \sum_{k\in\mathbb{N}} f(-k) \sum_{\substack{(a,b,x,y)\in\mathbb{N}^4\\ ax+by=n\\ a-b=-k}} 1 + f(0) \sum_{\substack{(a,b,x,y)\in\mathbb{N}^4\\ ax+by=n\\ a=b}} 1\\ &\quad + \sum_{k\in\mathbb{N}} f(k) \sum_{\substack{(a,b,x,y)\in\mathbb{N}^4\\ ax+by=n\\ a-b=k}} 1 - \sum_{k\in\mathbb{N}} f(k) \sum_{\substack{(a,b,x,y)\in\mathbb{N}^4\\ ax+by=n\\ a+b=k}} 1.\end{aligned}$$

Por el algoritmo de la división,

$$\sum_{\substack{(a,b,x,y)\in\mathbb{N}^4\\ ax+by=n\\ a=b}} 1 = \sum_{\substack{(a,x,y)\in\mathbb{N}^3\\ ax+ay=n}} 1 = \sum_{\substack{(a,x,y)\in\mathbb{N}^3\\ a(x+y)=n}} 1 = \sum_{\substack{(a,x,y)\in\mathbb{N}^3\\ x+y=\frac{n}{a}\\ a|n}} 1 = \sum_{a|n} \sum_{\substack{(x,y)\in\mathbb{N}^2\\ x+y=\frac{n}{a}}} 1.$$

Por lo hallado en la demostración del teorema 8.1.1, la segunda sumatoria corresponde al número de soluciones naturales de la ecuación $x+y=\frac{n}{a}$. Por la

fórmula de Bose-Einstein y el principio de inclusión-exclusión, se deduce que

$$\sum_{\substack{(x,y)\in\mathbb{N}^2\\ x+y=\frac{n}{a}}} 1 = \binom{2+\frac{n}{a}-1}{\frac{n}{a}} - 2 = \frac{n}{a} - 1.$$

De esta forma, al considerar las definiciones de las funciones σ y τ y como $a|n \iff \frac{n}{a}|n$, se satisface que

$$\sum_{\substack{(a,b,x,y)\in\mathbb{N}^4\\ ax+by=n\\ a=b}} 1 = \sum_{a|n}\left(\frac{n}{a}-1\right) = \sum_{a|n} a - \sum_{a|n} 1 = \sigma(n) - \tau(n).$$

Además, como f es una función par, se verifica que $f(x) = f(-x), \forall x \in \mathbb{Z}$. Por consiguiente,

$$\sum_{k\in\mathbb{N}} f(-k) \sum_{\substack{(a,b,x,y)\in\mathbb{N}^4\\ ax+by=n\\ a-b=-k}} 1 = \sum_{k\in\mathbb{N}} f(k) \sum_{\substack{(a,b,x,y)\in\mathbb{N}^4\\ ax+by=n\\ b-a=k}} 1.$$

Obsérvese que la última sumatoria no es más que una permutación de a con b y x con y, entonces

$$\sum_{k\in\mathbb{N}} f(-k) \sum_{\substack{(a,b,x,y)\in\mathbb{N}^4\\ ax+by=n\\ a-b=-k}} 1 = \sum_{k\in\mathbb{N}} f(k) \sum_{\substack{(a,b,x,y)\in\mathbb{N}^4\\ ax+by=n\\ a-b=k}} 1.$$

En consecuencia,

$$\begin{aligned}\sum_{\substack{(a,b,x,y)\in\mathbb{N}^4\\ ax+by=n}} (f(a-b)-f(a+b)) &= \sum_{k\in\mathbb{N}} f(k) \sum_{\substack{(a,b,x,y)\in\mathbb{N}^4\\ ax+by=n\\ a-b=k}} 1 + f(0)(\sigma(n)-\tau(n))\\ &\quad + \sum_{k\in\mathbb{N}} f(k) \sum_{\substack{(a,b,x,y)\in\mathbb{N}^4\\ ax+by=n\\ a-b=k}} 1 - \sum_{k\in\mathbb{N}} f(k) \sum_{\substack{(a,b,x,y)\in\mathbb{N}^4\\ ax+by=n\\ a+b=k}} 1\\ &= \sum_{k\in\mathbb{N}} f(k) \left(2 \sum_{\substack{(a,b,x,y)\in\mathbb{N}^4\\ ax+by=n\\ a-b=k}} 1 - \sum_{\substack{(a,b,x,y)\in\mathbb{N}^4\\ ax+by=n\\ a+b=k}} 1 \right)\\ &\quad + f(0)(\sigma(n)-\tau(n)).\end{aligned}$$

Con base en la definición del conjunto B y por el teorema 8.1.1, se puede concluir que

$$2\sum_{\substack{(a,b,x,y)\in\mathbb{N}^4\\ ax+by=n\\ a-b=k}} 1-\sum_{\substack{(a,b,x,y)\in\mathbb{N}^4\\ ax+by=n\\ a+b=k}} 1=2\sum_{\substack{(a,b,x,y)\in B(n)\\ a-b=k}} 1-\sum_{\substack{(a,b,x,y)\in B(n)\\ a+b=k}} 1$$

$$=\left(1-k+\frac{2n}{k}\right)F_k(n)-2\sum_{\substack{v|n\\ v\geq k}}1.$$

De esta forma, se verifica que

$$\sum_{k\in\mathbb{N}} f(k)\left(2\sum_{\substack{(a,b,x,y)\in\mathbb{N}^4\\ ax+by=n\\ a-b=k}} 1-\sum_{\substack{(a,b,x,y)\in\mathbb{N}^4\\ ax+by=n\\ a+b=k}} 1\right)=\sum_{k\in\mathbb{N}} f(k)\left(\left(1-k+\frac{2n}{k}\right)F_k(n)-2\sum_{\substack{v|n\\ v\geq k}}1\right)$$

$$=\sum_{k|n}\left(1-k+\frac{2n}{k}\right)f(k)-2\sum_{v|n}\left(\sum_{k=1}^{v} f(k)\right).$$

Luego, al denotar a los divisores de n como d, se obtiene la expresión

$$\sum_{\substack{(a,b,x,y)\in\mathbb{N}^4\\ ax+by=n}} (f(a-b)-f(a+b))=$$

$$f(0)(\sigma(n)-\tau(n))+\sum_{d|n}\left(1+\frac{2n}{d}-d\right)f(d)-2\sum_{d|n}\left(\sum_{k=1}^{d} f(k)\right).$$

□

8.2. Aplicaciones

La tercera identidad de Liouville puede aplicarse para computar sumas de convolución en las que intervienen funciones aritméticas relacionadas con los divisores de un número. Resulta apropiado hacer una breve remembranza de la definición de convolución. En efecto, esta puede interpretarse como un operador matemático que describe la superposición de dos funciones combinadas. En concreto, esta sección está destinada únicamente a abordar una única convolución, la cual se halla establecida en la denominada fórmula de Besge. A

diferencia de los capítulos anteriores, todos los elementos que participan en su demostración han sido desarrollados a completitud, por lo cual, la fórmula de Besge constituirá el único y, por consiguiente, último teorema de la disertación.

En lo referente al contexto histórica de la fórmula, Williams [3] postula que fue tratada formalmente por primera vez en una carta de Besge a Joseph Liouville en 1862; sin embargo, menciona que la identidad de Besge no está descifrada a cabalidad, a tal punto que se alude como un pseudónimo empleado por el propio Liouville.

Teorema 8.2.1. ***Fórmula de Besge***
Sea $n \in \mathbb{N}$, entonces

$$\sum_{m=1}^{n-1} \sigma(n)\sigma(n-m) = \frac{5}{12}\sigma_3(n) + \left(\frac{1}{12} - \frac{n}{2}\right)\sigma(n). \tag{8.4}$$

Demostración: Sea $f(x) = x^2$ y obsérvese que f es una función par, puesto que $x^2 = (-x)^2$ De esta manera,

$$\begin{aligned}
\sum_{\substack{(a,b,x,y)\in\mathbb{N}^4 \\ ax+by=n}} (f(a-b) - f(a+b)) &= \sum_{\substack{(a,b,x,y)\in\mathbb{N}^4 \\ ax+by=n}} ((a-b)^2 - (a+b)^2) \\
&= \sum_{\substack{(a,b,x,y)\in\mathbb{N}^4 \\ ax+by=n}} (a-b+a+b)(a-b-a-b) \\
&= \sum_{\substack{(a,b,x,y)\in\mathbb{N}^4 \\ ax+by=n}} (2a)(-2b) \\
&= -4 \sum_{\substack{(a,b,x,y)\in\mathbb{N}^4 \\ ax+by=n}} ab.
\end{aligned}$$

Nótese que como $(a,b,x,y) \in B(n)$, $0 < ax < n \implies n > n - ax > 0$. Sea $ax = m$, por lo cual, $by = n - ax = n - m$. Ahora, por el algoritmo de la división, se satisface que $a|m$ y $b|n-m$. Por la definición de la función σ_k,

$$\begin{aligned}
\sum_{\substack{(a,b,x,y)\in\mathbb{N}^4 \\ ax+by=n}} (f(a-b) - f(a+b)) &= -4 \sum_{m=1}^{n-1} \left(\sum_{a|m} a\right)\left(\sum_{b|n-m} b\right) \\
&= -4 \sum_{m=1}^{n-1} \sigma(m)\sigma(n-m).
\end{aligned}$$

No obstante, la sumatoria original puede evaluarse directamente al aplicar la tercera identidad de Liouville. De esta forma, como $f(0) = 0$ y según la definición de la función σ_k, se deduce que

$$\begin{aligned}\sum_{\substack{(a,b,x,y)\in\mathbb{N}^4\\ ax+by=n}} (f(a-b)-f(a+b)) &= \sum_{d|n}\left(1+\frac{2n}{d}-d\right)f(d) - 2\sum_{d|n}\left(\sum_{k=1}^{d} f(k)\right)\\ &= \sum_{d|n}\left(1+\frac{2n}{d}-d\right)d^2 - 2\sum_{d|n}\left(\sum_{k=1}^{d} k^2\right)\\ &= \sum_{d|n} d^2 + 2n\sum_{d|n} d - \sum_{d|n} d^3 - 2\sum_{d|n}\left(\sum_{k=1}^{d} k^2\right)\\ &= \sigma_2(n) + 2n\sigma(n) - \sigma_3(n) - 2\sum_{d|n}\left(\sum_{k=1}^{d} k^2\right).\end{aligned}$$

A continuación, obsérvese que la última sumatoria puede calcularse a base de la fórmula de los primeros d cuadrados consecutivos. Por lo tanto,

$$-2\sum_{d|n}\left(\sum_{k=1}^{d} k^2\right) = -2\sum_{d|n}\frac{d(d+1)(2d+1)}{6} = -\sum_{d|n}\left(\frac{2d^3+3d^2+d}{3}\right) =$$

$$-\frac{2}{3}\sum_{d|n} d^3 - \sum_{d|n} d^2 - \frac{1}{3}\sum_{d|n} d = -\frac{2}{3}\sigma_3(n) - \sigma_2(n) - \frac{1}{3}\sigma(n).$$

Por consiguiente,

$$\begin{aligned}-4\sum_{m=1}^{n-1}\sigma(m)\sigma(n-m) &= \sigma_2(n) + 2n\sigma(n) - \sigma_3(n) - \frac{2}{3}\sigma_3(n) - \sigma_2(n) - \frac{1}{3}\sigma(n)\\ &= -\frac{5}{3}\sigma_3(n) - \left(\frac{1}{3}-2n\right)\sigma(n).\end{aligned}$$

Luego,

$$\sum_{m=1}^{n-1}\sigma(m)\sigma(n-m) = \frac{5}{12}\sigma_3(n) + \left(\frac{1}{12}-\frac{n}{2}\right)\sigma(n).$$

□

CAPÍTULO 9

Epílogo

«Non quia difficilia sunt non audemus, sed quia non audemus, difficilia sunt.»

No nos atrevemos a muchas cosas porque son difíciles, pero son difíciles porque no nos atrevemos a hacerlas.

Seneca

A lo largo de estos capítulos, se ha podido adentrar en extensiones de la matemática pura y explorar parte del territorio vasto de la teoría de números. Por supuesto, los tópicos tratados en estas hojas no son más que áreas concretas de esta rama, y este margen no delimita el alcance completo de la aritmética que como se observó, se ha desarrollado a lo largo de siglos de la humanidad gracias al trabajo de numerosos matemáticos, como se apreció durante todas estas páginas.

A estas instancias, se debería tener una nueva noción del quehacer de un matemático que rompe con el paradigma inicial, donde se evidencia el estudio de esta rama del saber in se y per se. En efecto, se puede observar un enfoque más analítico y abstracto de las ideas que sustentan dentro de la misma matemática y que dan apertura a la investigación y en especial, despierta la creatividad para que las ideas fluyan y se expandan a distintos horizontes por medio de una cadena de razonamientos lógicos.

Como experiencia personal, se puso en manifiesto el reto de enfrentarse a estas tres identidades con el conocimiento adquirido durante varios años de estudios. Donde se extrae como enseñanza que el simple hecho de poseer una aspiración, establecer un objetivo, tener la valentía de aventurarse a lo desconocido para no rendirse antes de intentarlo y creer en las capacidades de uno mismo son primordiales al momento de hacer una disertación; pero sobre todo ser apasionado con lo que se hace porque eso brinda una motivación más que suficiente para apreciar con detalle y paciencia toda la evolución y progreso del trabajo para no desfallecer en el camino.

En definitiva, realizar una disertación no se reduce únicamente a colocar en un conglomerado el conocimiento adquirido, sino que es una oportunidad única de autoconocimiento y superación personal, puesto que uno mismo se fija los límites y las metas a desarrollar. De esta manera, se obtiene una propuesta propia y, al final, la satisfacción gratificante de haberla completado tras un arduo esfuerzo y varias horas de trabajo. En especial, se suscita un enorgullecimiento a partida doble, puesto que en toda su extensión, el documento presentado está libre de inteligencia artificial; esta última premisa no representa una crítica, sino un recordatorio de que aún existen personas capaces de pensar en autonomía.

Las palabras son ecos del alma y las ideas deben brotar en completa libertad, las anécdotas son la conciencia de la memoria y las historias son el legado, mas un libro es un portal a otra dimensión. Precisamente de esta forma se culmina esta obra, como una invitación a nunca dejar de intentar y perseguir las metas propuestas. Y a usted, un profundo agradecimiento por llegar hasta este punto y una sincera muestra de gratitud por dar apertura al apasionante

mundo de la teoría de números, en nombre de un servidor y futuro matemático.

9.1. Conclusión

Tras analizar el trabajo de Joseph Liouville de 1858 y 1859, publicado regularmente en su revista "Journal de Mathématiques Pures et Appliquées", se identificaron tres identidades clave dentro de la teoría de números analítica. Para un contraste con ideas modernas, se precisaron conceptos relacionados con la divisibilidad, en los cuales se incluyen el algoritmo de la división, el algoritmo de Euclides, el Teorema Fundamental de la Aritmética y la congruencia aritmética. Además, se requirió un trasfondo de funciones aritméticas y ecuaciones diofánticas.

El alcance de estos teoremas está directamente asociado con la resolución de problemas clásicos de la teoría de números. Por tal motivo, se consideró apropiado destinar un capítulo entero para cada identidad, donde se incluyó su demostración y su respectiva aplicación dentro de la propia matemática.

Efectivamente, la primera identidad relacionada con funciones impares unidimensionales y el conjunto A, permitió resolver el problema de la representación de un entero como la suma de dos cuadrados, una interrogante presente desde el siglo XVII y tratada por primera vez por los matemáticos Pierre de Fermat y Albert Girard.

La segunda identidad pudo interpretarse como una generalización a la primera, pero al tomar una función bidimensional y su aplicación, se mantuvo ligada al problema de la representación, salvo que en esta ocasión, se enfocó en determinar el número de soluciones; un enigma que data de los siglos XVIII y XIX, gracias al trabajo de Adrien-Marie Legendre y Carl Gustav Jacobi.

Por último, la tercera identidad conectó funciones pares con funciones aritméticas convencionales mediante el conjunto B y constituyó una herramienta importante para computar sumas de convolución; en particular, se trató la convolución de la suma de divisores o función σ, una fórmula deducida en el siglo XIX.

Si bien se abordan problemas clásicos, la parte innovadora se localiza precisamente en su demostración al ampliar el horizonte a las ideas modernas de la teoría de números para reemplazar las comprobaciones originales y en muchos de los casos, reducir su complejidad al ser tratadas como corolarios de las identidades de Liouville. En este mismo aspecto, se pudo evidenciar una nueva faceta como matemático de Joseph Liouville, diferente a su rol en el margen de las ecuaciones diferenciales y variable compleja.

En síntesis, se completó el objetivo primordial de esta disertación corres-

pondiente a la exploración e interpretación de las principales ideas de Liouville mediante un análisis exhaustivo y la inclusión detallada de su respectiva demostración. Además, se logró la concepción de una obra o un libro con un enfoque más purista de la investigación, que se centra en profundidad en la investigación y desencadena en un producto tangible del quehacer matemático.

El alcance de este trabajo permite sincronizar varias ramas de la matemática para un resultado afín, como lo suscitado con combinatoria, álgebra abstracta y teoría de conjuntos. Finalmente, se cierra con la apertura hacia nuevas vías de investigación a partir de todo lo desarrollado en este documento; por ejemplo, una aproximación generalizada de la teoría de representación de enteros como la suma de un número par de cuadrados, una expansión hacia otro tipo de números poligonales y la inserción de otras convoluciones.

Bibliografía

[1] Jesper Lützen. *Part VI: Mathematicians - 39. Joseph Liouville.* Princeton University Press, Princeton, 2008.

[2] John Conway and Richard Guy. *The Book of Numbers.* Copernicus, 1996.

[3] Kenneth Williams. *Number Theory in the Spirit of Liouville.* London Mathematical Society Student Texts. Cambridge University Press, 2011.

[4] Underwood Dudley. *Elementary Number Theory.* Dover, 2008.

[5] José Plíneo de Oliveira Santos. *Introdução à Teoria dos Números.* Coleção Matemática Universitária. Instituto Nacional de Matemática Pura e Aplicada, 2020.

[6] Tom Apostol. *Introduction to Analytic Number Theory.* Undergraduate Texts in Mathematics. Springer, 1976.

[7] Şaban Alaca and Kenneth Williams. *Introductory Algebraic Number Theory.* Cambridge University Press, 2004.

[8] Roshdi Rashed. *Historie de l'Analyse Diophantienne Classique: D'Abu Kamil à Fermat.* De Gruyter, Inc, 2013.

[9] James Tattersall. *Elementary Number Theory in Nine Chapters.* Cambridge, 1999.

[10] Fabio Martinez, Gustavo Moreira, Nicolau Saldanha, and Eduardo Tengan. *Teoria dos números: Un passeio com primos e outros números familiares pelo mundo inteiro.* Projeto Euclides. Instituto Nacional de Matemática Pura e Aplicada, 2015.

[11] James Victor Uspensky and Maxwell Heaslet. *Elementary Number Theory.* McGraw-Hill, 1939.

[12] Joseph Liouville. *Recueil Mensuel de Mémoires sur les Diverses Parties des Mathématiques.* Journal de Mathématiques Pures et Appliquées, 1859.

[13] Joseph Liouville. *Recueil Mensuel de Mémoires sur les Diverses Parties des Mathématiques.* Journal de Mathématiques Pures et Appliquées, 1858.