Universidad Nacional Autónoma de México

Facultad de Ciencias

Inversión de Möbius: Generalización y aplicaciones

T E S I S

QUE PARA OBTENER EL TÍTULO DE:
MATEMÁTICO

PRESENTA:
EMILIANO GENEYRO SQUARZON

DIRECTOR DE TESIS:
OCTAVIO PÁEZ OSUNA

2012

Hoja de Datos del Jurado

1. Datos del alumno
Geneyro
Squarzon
Emiliano
56 51 10 28
Universidad Nacional Autónoma de México
Facultad de Ciencias
Matemáticas
406069850

2. Datos del tutor
Dr
Octavio
Páez
Osuna

3. Datos del sinodal 1
Dr
Rodolfo
San Agustín
Chi

4. Datos del sinodal 2
Mat
Julio César
Guevara
Bravo

5. Datos del sinodal 3
Mat
Anayanzi Delia
Martínez
Hernández

6. Datos del sinodal 4
Mat
Siddhartha
Estrella
Gutiérrez

7. Datos del trabajo escrito
Inversión de Möbius: Generalización y aplicaciones
65 p
2012

A mi madre, su existencia y cariño
son eternos en mi corazón.

A mi padre, por su cariño incondicional
y por permitirme aprender
de él cada día.

A Lorena, mi esposa, porque con su amor
y apoyo soy una mejor persona.

Agradecimientos

A la Universidad Nacional Autónoma de México y a la Facultad de Ciencias, por permitirme formar parte de esta gran comunidad y sobre todo por darme la oportunidad de tener una formación integral.

Al Dr. Octavio Páez Osuna, mi tutor de tesis, porque con su tiempo, consejos y apoyo hizo que todo este proceso fuera menos difícil y más placentero.

A los sinodales, Dr. Rodolfo San Agustín Chi, Mat. Julio César Guevara Bravo, Mat. Anayanzi Delia Martínez Hernández y Mat. Siddhartha Estrella Gutiérrez, por sus comentarios y correcciones que ayudaron a mejorar este trabajo.

A mi familia de sangre, a mi familia política y mis familiares por afecto. El cariño y el apoyo que me dan son fundamentales para seguir adelante.

A mis amigos, hermanos por elección, por permitirme compartir con ellos momentos de tristeza y alegría; pero sobre todo por estar siempre a mi lado.

A los integrantes del H. Comité de Amigos de la facultad, Zazil, Fernando, Manuel y Raybel porque con ellos, además de aprender, me he divertido y he compartido cada instante de esta experiencia inolvidable.

A los que están, los que estuvieron y los que estarán a mi lado disfrutando de esta aventura que llamamos “vida”.

Contenido

Introducción

La teoría de números es una rama de las matemáticas que se enfoca en el estudio de las propiedades de los números enteros. Si bien el interés por estos números es muy antiguo, la teoría relacionada con ellos sigue vigente y proporciona elementos para el desarrollo de nuevas ramas de las matemáticas.

La fórmula de inversión de Möbius es un ejemplo de esta relación entre la teoría de números y los distintos campos de estudio dentro de las matemáticas. Esta fórmula permite realizar inversiones de series, lo cual es de mucha utilidad y posee una gran variedad de aplicaciones a diversos problemas de las distintas ramas de las matemáticas.

La fórmula clásica de inversión fue introducida en la teoría de números por August Ferdinand Möbius (1790-1868). En ella se establece que si dos funciones aritméticas f y g poseen una relación entre ellas, dada por:

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

entonces, esta relación se puede invertir para todo entero $n > 1$, de la siguiente manera

$$g(n) = \sum_{d|n} \mu(\frac{n}{d}) f(d)$$

El alcance de esta fórmula pasaría sin desarrollarse hasta que Louis Weisner (1935) y Phillip Hall (1936), de manera separada, dieran una generalización de esta inversión, motivados por diversos problemas de la teoría de grupos; sin embargo, ninguno de estos autores profundizó en la teoría relacionada con la inversión de Möbius.

No fue hasta 1964, cuando Gian-Carlo Rota publicó un articulo (ref. [10]) dedicado a la función de Möbius, que comenzó a tomar importancia en el desarrollo de otra ramas de las matemáticas. Rota no sólo profundizó en la teoría relacionada a esta función, sino que generalizó dichos resultados a cualquier conjunto parcialmente ordenado; lo que le permitió encontrar diversas aplicaciones, principalmente en la combinatoria. A partir de entonces, la teoría de la fórmula de inversión de Möbius se ha convertido en un área sumamente activa de la combinatoria.

De esta manera, el trabajo de tesis busca presentar la teoría relacionada con esta fórmula de inversión. Para ello es necesario desarrollar diferentes conceptos y propiedades que serán de gran utilidad para desarrollar y entender dicha teoría.

Así, el Capítulo 1 de este trabajo se centra en introducir tres conceptos preliminares de suma importancia: divisibilidad, números primos y series. Iniciamos introduciendo el concepto de divisibilidad, el cual nos permite relacionar dos números enteros y definir, a partir del concepto de máximo común divisor, la primalidad de los números. A continuación exponemos algunas propiedades importantes de los números primos, donde destaca el Teorema Fundamental de la Aritmética. Este teorema es de gran utilidad, ya que nos permite descomponer a cualquier número entero positivo mayor que 1, como un producto único de números primos. Por último introduciremos el concepto de serie y presentaremos algunas propiedades importantes, relacionadas con la convergencia de las series, que facilitan su manipulación dentro del desarrollo de este trabajo.

El Capítulo 2 se centra en el planteamiento básico de la teoría de las funciones aritméticas. Dada la relevancia que poseen estas funciones en el desarrollo de la teoría de la inversión de Möbius, este capítulo se enfoca en presentar algunas propiedades y definiciones que nos permitirán entender mejor el comportamiento de dichas funciones, entre ellas la función μ de Möbius. Así pues, se definen operaciones entre estas funciones y se determina la estructura algebraica que forman. Con lo anterior plantearemos algunos resultados importantes de la inversa de una función aritmética y de las funciones aritméticas multiplicativas. Concluiremos este capítulo desarrollando el concepto de series de Dirichlet, las cuales aparecerán implícitamente en el desarrollo de los temas posteriores. Dentro de esta parte destacamos algunas

propiedades de convergencia de dichas series, así como una aplicación para determinar la infinitud de números primos.

El Capítulo 3 contiene los fundamentos teóricos de la inversión de Möbius, tema central de este trabajo. Iniciaremos deduciendo una definición de la función μ, parte fundamental de dicha teoría, y demostraremos el teorema de inversión de Möbius clásica. Lo anterior nos permitirá obtener una generalización para cualquier conjunto parcialmente ordenado localmente finito, para lo cual necesitaremos definir algunos conceptos generales como son el de orden, convolución y álgebra de incidencia. Una vez establecido el concepto de álgebra de incidencia, el cual es un conjunto de funciones que forman un álgebra asociativa, definiremos la inversa de la convolución y con ello daremos una caracterización alternativa de la función μ como inversa de la función zeta, denotada por ζ. Concluimos este capítulo con la generalización del teorema de inversión de Möbius, el cual nos permite aplicar dicha inversión a una mayor variedad de conjuntos cuyo orden no esté dado por la divisibilidad.

Por último, el Capítulo 4 ejemplifica algunas aplicaciones del teorema de inversión de Möbius. En la primera sección mostramos su uso para resolver problemas de conteo como son: el número de polinomios mónicos irreducibles de grado n en un campo de q elementos; las coloraciones propias con x colores de una gráfica de n vértices y la cantidad de vectores de dimensión r de la forma $(a_1, a_2, \ldots, a_r)$ tales que a_i sean números naturales menores que n y que cumplan que todas las entradas, junto con n, sean primos relativos entre sí. Concluimos este trabajo mostrando el uso de la inversión de Möbius para obtener identidades de las funciones de Von Mangoldt y de la phi de Euler (denotadas por Λ y φ respectivamente); así como una identidad de las sumas de Ramanujan.

Capítulo 1

Preliminares

En este capítulo se presentan algunas definiciones y resultados básicos, los cuales son de gran importancia para el desarrollo de los temas principales de esta tesis. Estos se engloban en tres secciones: divisibilidad, números primos y series infinitas. Dentro de las dos primeras destacan las propiedades de la divisibilidad y el Teorema Fundamental de la Aritmética, las cuales forman parte de la argumentación en varias de las principales demostraciones que se realizan en este trabajo. Las propiedades de series infinitas nos permiten su manipulación, dentro de las justificaciones de los resultados planteados, para poder alcanzar los objetivos buscados.

1.1. Divisibilidad

En el manejo de los números enteros es común encontrarnos algún tipo de relación entre sus elementos que nos permita manipularlos de forma coherente. La divisibilidad es una de estas relaciones, la cual nos permite comparar un número entero con respecto a otro y verificar si cumple la propiedad deseada. También puede ser entendida como una operación; sin embargo, nuestro mayor interés está en su uso como herramienta para relacionar dos números, además de que nos permitirá construir un elemento fundamental de nuestra teoría: La primalidad.

Así pues, decimos que un número entero a, distinto de cero, **divide a** b si existe otro número entero c tal que la multiplicación de a con c de como

resultado exactamente b, es decir cumple que

$$b = ac$$

Esta es la definición de divisibilidad y la denotamos $a|b$.

A continuación se presentan algunas propiedades básicas de la divisibilidad[1]. Entonces, dados a, b, c, d, m y n números enteros, la divisibilidad cumple que:

a) $a|a$

b) Si $d|n$ y $n|m$, entonces $d|m$

c) Si $d|n$ y $d|m$, entonces $d|(an + bm)$

d) Si $d|n$, entonces $ad|an$

e) Si $ad|an$ y $a \neq 0$, entonces $d|n$

f) $1|n$, para todo n entero.

g) $n|0$, para todo n entero.

h) Si $0|n$, entonces $n = 0$

i) Si $d|n$ y $n \neq 0$, entonces $|d| \leq |n|$

j) Si $d|n$ y $n|d$, entonces $|d| = |n|$

k) Si $d|n$ y $d \neq 0$, entonces $(n/d)|n$

l) Si $d|n$ y $c|m$, entonces $(dc)|nm$

Cuando un número entero d divide a dos números enteros distintos decimos que es un **común divisor** de ambos.

Como los números enteros positivos poseen un orden y dado que no es posible que un común divisor sea mayor que alguno de los números a los que divide, entonces la cantidad de divisores de ambos números queda acotada,

[1]Las demostraciones son omitidas ya que únicamente nos interesa enunciarlas para entender mejor el concepto, pero se pueden consultar en [8] y [9].

y además podemos pensar que dichos divisores forman un conjunto finito, el cual tiene un elemento máximo. Entonces, caracterizamos a dicho elemento máximo.

Definición 1.1.1. *El* ***máximo común divisor*** *de dos enteros a y b, denotado por (a, b), es el número entero d con las siguientes propiedades:*

a) d es un número entero no negativo.

b) d es común divisor de a y b.

c) Si e es un común divisor de a y b, entonces $e|d$

Dados a y b dos números enteros, construimos el conjunto de todas las combinaciones lineales de estos números.

$$P := \{sa + tb \mid s, t \in \mathbb{Z} \text{ y } sa + tb > 0\}$$

entonces el menor de los elementos de este conjunto es (a, b).

El máximo común divisor posee las siguientes propiedades.

a) $(a, b) = (b, a)$

b) $(a, (b, c)) = ((a, b), c)$

c) $(ca, cb) = |c|(a, b)$

d) $(1, a) = (a, 1) = 1$

e) $(0, a) = (a, 0) = |a|$

Un caso particular de gran importancia es cuando 1 es el máximo común divisor de dos enteros a y b. Entonces diremos que a y b son **primos relativos** si $(a, b) = 1$. Destacamos dos propiedades que nos permitirán realizar conclusiones importantes.

La primera de ellas afirma que dos números cualesquiera a y b pueden ser expresados, de forma separada, como el producto del máximo común divisor d y los enteros m y n respectivamente, entiéndase $a = md$ y $b = nd$, donde m y n son primos relativos entre sí.

La otra propiedad señala que si d divide al producto de dos números y es primo relativo con uno de ellos, entonces d debe dividir al otro. Esta propiedad es una generalización del Lema de Euclides, que plantea algo similar para números primos y que veremos más adelante.

1.2. Números Primos

Los números primos son de los elementos más intrigantes de las Matemáticas, ya que son parte fundamental en el desarrollo de diversas ramas de éstas.

Los números primos son números enteros con características muy específicas, lo cual nos podría llevar a la conclusión apresurada de que su estudio es sumamente simple. Nada más alejado de la realidad, ya que dentro del desarrollo de la teoría de los números primos se presentan dos grandes complicaciones: La verificación de que un número sea primo y la factorización de cualquier entero como producto de potencia de primos. Ambos problemas se relacionan con la eficiencia para obtener los resultados deseados.

Hasta ahora no se ha podido establecer una fórmula que determine exclusivamente a todos los números primos; entonces el problema en el análisis de éstos se centra en lograr tener métodos de comprobación eficientes. Por otro lado, si bien la factorización de cualquier entero en factores primos depende de saber qué número es primo, la factorización es un problema más difícil de resolver ya que no existen métodos eficientes (en términos prácticos) para lograrlo.

Sin embargo, a pesar de estas complicaciones, la teoría de los números primos es de gran importancia dentro del desarrollo de esta tesis; por lo tanto a continuación detallamos algunas definiciones y resultados importantes.

Definición 1.2.1. *Un entero positivo $p > 1$ es un* ***número primo*** *si sus únicos divisores positivos son 1 y p. Aquellos enteros $n > 1$ que no son primos se llaman* ***compuestos****.*

Proposición 1.2.1. Todo entero mayor que 1 puede expresarse como producto de números primos.

Demostración. Por inducción. Para $n = 2$ la hipótesis es cierta, ya que 2 es primo. Suponemos que todo $1 < k < n$ puede descomponerse en

factores primos. Debemos demostrar que n también se puede factorizar en números primos.

Suponemos que n es compuesto, ya que de no ser así n sería un primo y por lo tanto quedaría demostrada la hipótesis. Como n es un número compuesto, entonces posee un divisor d tal que $1 < d < n$ y por consiguiente $n = cd$ con $1 < c < n$. Por la hipótesis de inducción, como $1 < d < n$ y $1 < c < n$, tanto d como c se descomponen en factores primos y por ende, n permite una factorización en números primos. □

Teorema 1.2.2. *Sea n un número entero. Si un primo p no divide a n, entonces $(n, p) = 1$*

Demostración. Sea $d = (n, p)$. Tenemos que $d|p$, es decir, $d = 1$ o $d = p$. Por otro lado $d|n$, con lo cual $d \neq p$ ya que p no divide a n y por lo tanto $d = (n, p) = 1$ □

Proposición 1.2.3. Si un número primo p divide al producto de dos números enteros ab, entonces $p|a$ ó $p|b$.

Demostración. Suponemos que p no divide a b. Queremos demostrar que forzosamente $p|a$.

Ahora bien, como p no divide a b se tiene que $(p, b) = 1$. Por lo tanto como p divide al producto, entonces por las propiedades de la divisibilidad, se tiene que necesariamente que $p|a$. □

Teorema 1.2.4 (**Teorema Fundamental de la Aritmética**). *Todo entero $n > 1$ puede descomponerse en producto de números primos de manera única, salvo por un reordenamiento de sus factores.*

Demostración. Hacemos inducción sobre n. Para $n = 2$ el teorema es válido. Suponemos que el teorema es válido para todo número mayor que 1 y estrictamente menor que n. Si n es un primo, no hay nada que demostrar. Suponemos pues que n es un número compuesto que permite dos factorizaciones, entonces tenemos que:

$$n = p_1 p_2 \cdots p_m = q_1 q_2 \cdots q_k$$

Así pues, queremos demostrar que $m = k$ y que cada p_i con $1 \leq i \leq m$, es igual q_r para alguna $1 \leq r \leq k$. Como $p_1|n$, entonces $p_1|q_1 q_2 \cdots q_k$ y por

lo tanto p_1 divide por lo menos a uno de estos factores. Por comodidad, etiquetamos a los primos q_r de tal manera que $p_1|q_1$. Como p_1 y q_1 son primos se tiene que $p_1 = q_1$, ya que de lo contrario $q_1 = ap_1$ con $1 < a < q_1$, lo cual sería una contradicción al hecho de que q_1 es un número primo.

Cancelando p_1 en ambas factorizaciones obtenemos:

$$\frac{n}{p_1} = p_2 \cdots p_m = q_2 \cdots q_k$$

Dado que hemos supuesto que n es un número compuesto, tenemos que $m > 1$ ó $k > 1$ y por lo tanto $1 < n/p_1 < n$. Por hipótesis de inducción n/p_1 tiene una única factorización y por lo tanto las dos factorizaciones propuestas deben ser idénticas. Debido a que en la descomposición de n/p_1 solamente hemos cancelado a p_1, podemos concluir que $m = k$ y que ambas factorizaciones de n son la misma, excepto por la posible reordenación de términos que realizamos. □

Proposición 1.2.5. Existe una infinidad de números primos.

Demostración. Para demostrar este resultado procederemos por contradicción. Supongamos que existe una cantidad finita de números primos, $p_1, p_2, \ldots, p_r$.

Sea $n = 1 + p_1p_2 \cdots p_r$. Como n es un número entero mayor que 1, entonces el Teorema fundamental de la Aritmética nos permite asegurar que n es dividido por algún primo p. Por otro lado, p también divide a $p_1p_2 \cdots p_r$, ya que supusimos que la cantidad de números primos era finita y por lo tanto p forma parte de dicha multiplicación. Entonces tenemos que $p|n$ y $p|p_1p_2 \cdots p_r$, por lo que p debe dividir a la resta de ambos. Es decir, p divide a $(n - p_1p_2 \cdots p_r) = 1$, lo cual es imposible.

Concluimos que la suposición inicial resulta ser falsa, así que debe haber una infinidad de números primos. □

Cabe mencionar que en la descomposición en factores primos de un número n, puede ocurrir que un primo p aparezca más de una vez. En este caso podemos reescribir dicha factorización expresando únicamente los números primos

distintos entre sí. Es decir, sean $p_1, p_2, \ldots, p_m$ los factores primos distintos de n, tal que p_i aparezca a_i veces en la factorización original; entonces lo escribimos como:

$$n = p_1^{a_1} p_2^{a_2} \cdots p_m^{a_m}$$

o de la siguiente manera

$$n = \prod_{i=1}^{m} p_i^{a_i} \qquad \text{con } a_i > 0$$

A continuación presentamos dos resultados que permiten relacionar la divisibilidad y el máximo común divisor con la factorización en primos.

Teorema 1.2.6. *Sea n un entero con una factorización en primos distintos dada por:*

$$n = \prod_{i=1}^{r} p_i^{a_i} \qquad \textit{con } a_i > 0$$

Entonces cualquier d, divisor de n, posee una factorización en primos de la forma

$$d = \prod_{i=1}^{r} p_i^{c_i} \quad \textit{donde } 0 \leq c_i \leq a_i$$

Demostración. Buscamos demostrar que cualquier divisor de n posee la factorización en primos propuesta. Para esto suponemos que existe d que es un divisor de n que no cumple esa factorización y trataremos de obtener una contradicción.

Si d no cumple con la descomposición en primos dada, entonces existen dos posibilidades.

Una posibilidad es que en la factorización en primos de d aparezca un número primo q^b, con $1 < b$, distinto de aquellos que integran la descomposición de n. Entonces tendríamos que $q^b | d$ y $d | n$; por lo tanto $q^b | n$, lo cual es una contradicción, ya que en la factorización de n no existe q^b como factor de éste y por la unicidad no es posible tener otra factorización donde dicho

término sí aparezca.

Por otro lado, suponemos que al menos uno de los primos p_i aparecerá con una potencia b_i tal que $a_i < b_i$. Tomemos un primo p_i que posea esta característica. Entonces tendríamos que $p_i^{b_i}|d$ y $d|n$ y por transitividad obtendríamos que $p_i^{b_i}|n$. Es decir $p_i^{b_i-a_i}|(p_1p_2\cdots p_{i-1}p_{i+1}\cdots p_r^{a_r})$, lo que representa una contradicción al hecho de que todos los p_k $1 \leq k \leq r$ son números primos distintos entre sí.

Estas contradicciones surgieron de suponer que existe d un divisor de n que no posee la factorizacion propuesta y por lo tanto se concluye que todo divisor de n posee una factorización de la forma:

$$d = \prod_{i=1}^{r} p_i^{c_i} \quad \text{donde } 0 \leq c_i \leq a_i$$

□

Para demostrar el siguiente resultado necesitamos remarcar que es posible expresar cualquier número entero positivo como una factorización sobre todos los números primos. Para esto etiquetamos a los números primos de forma ascendente, es decir $p_1 = 2$, $p_2 = 3$, $p_3 = 5$, p_n =enésimo primo y así sucesivamente. Entonces n se puede expresar como:

$$n = \prod_{i=1}^{\infty} p_i^{a_i}$$

donde ahora cada exponente $a_i \geq 0$. Este producto es finito, ya que para $n > 1$ sólo existirán un número finito de a_i distintas de cero. Es decir, lo que hemos hecho es agregarle a la factorización en números primos aquellos primos que no aparecen, elevándolos a la potencia cero para no alterar la factorización. Ahora bien, si $n = 1$ entonces todos los $a_i = 0$ y el producto también será finito.

Teorema 1.2.7. *Si dos números positivos a y b tiene las siguientes factorizaciones*

$$a = \prod_{i=1}^{\infty} p_i^{a_i} \qquad b = \prod_{j=1}^{\infty} p_i^{b_i}$$

entonces la factorización del M.C.D de ambos será:

$$(a, b) = \prod_{i=1}^{\infty} p_i^{c_i}$$

donde $c_i = min\{a_i, b_i\}$.

Demostración. Sea d un número entero positivo con la siguiente factorización:

$$d = \prod_{i=1}^{\infty} p_i^{c_i} \text{ , donde } c_i = min\{a_i, b_i\}$$

Como $c_i \leq a_i$ y $c_i \leq b_i$, entonces $d|a$ y $d|b$ y por lo tanto d es un común divisor de a y b. Ahora sea e un común divisor de a y b, cuya factorización está dada por:

$$e = \prod_{i=1}^{\infty} p_i^{e_i}$$

Como e es un divisor de a y también lo es de b, entonces tenemos que $e_i \leq a_i$ y $e_i \leq b_i$. De lo anterior se deduce que $e_i \leq c_i = min\{a_i, b_i\}$ y por lo tanto $e|d$, es decir d es el M.C.D. □

1.3. Series

La suma aritmética es una de las operaciones más elementales de las matemáticas. Si bien el concepto es muy básico, se ha desarrollado una amplia teoría donde se generaliza su aplicación. Dicha generalización parte del hecho de que podemos realizar la suma de una gran cantidad de elementos de un conjunto de números, haciendo uso de sus propiedades, a pesar de que por definición sólo sea posible sumar dos elementos simultáneamente.

Para poder realizar la suma de varios elementos necesitamos establecerles un orden, lo cual nos permite obtener el resultado buscado realizando la operación de la siguiente forma: sumamos los dos primeros y a su resultado le sumamos el tercero, a este nuevo resultado le sumamos el cuarto y así consecutivamente hasta obtener la solución final. Este orden genera una secuencia

de los elementos, a la que denominaremos **sucesión**.

Cabe mencionar que dichas sucesiones pueden ser finitas o infinitas, dependiendo de la cantidad de elementos que utilicemos. Si tenemos n elementos y estos se repiten una cantidad finita de veces al ordenarlos, entonces denotamos su sucesión por:

$$(a_0, a_1, \ldots, a_n) \qquad \text{o} \qquad \{a_i\}_{i=1}^{n}$$

donde a_i es el i-ésimo elemento, una vez establecido el orden. Si la cantidad de elementos a ordenar es infinita, o bien si hay una cantidad finita de estos pero al menos uno de ellos se repite una infinidad de veces al ordenarlos, entonces diremos que la sucesión es infinita y la denotaremos por:

$$(a_0, a_1, a_2, \ldots) \qquad \text{o} \qquad \{a_i\}_{i\in\mathbb{N}}$$

Con esto ya podemos definir el objeto que nos interesa en esta sección. Llamaremos **serie** a la suma de todos los elementos de una sucesión, la cual realizamos en el orden en que aparecen los elementos dentro de dicha sucesión.

Si la sucesión es de la forma $(a_0, a_1, \ldots, a_n)$ diremos que es una **suma parcial** y la expresaremos como:

$$\sum_{i=1}^{n} a_i$$

De la misma forma si la sucesión es infinita, dada por $(a_0, a_1, a_2, \ldots)$, la llamaremos **serie infinita** y la denotaremos por:

$$\sum_{i=1}^{\infty} a_i$$

Ahora observemos que dichas series pueden tener como resultado un valor determinado, o bien nunca alcanzar un valor. Cuando la serie alcanza un valor $s < \infty$ diremos que la **serie es convergente** o que **converge a** s. Si no alcanza ningún valor determinado diremos que la serie **diverge**.

A continuación consideraremos series definidas en el conjunto de los números complejos y presentamos resultados importantes relacionados con la convergencia de éstas y algunas propiedades de gran utilidad. Dado que la teoría acerca de las series es muy extensa, sólo mencionaremos la mayoría de los resultados y únicamente demostraremos aquellos resultados que nos serán útiles para desarrollos posteriores. Estos resultados pueden ser expresados en términos de la sucesiones y análogamente los resultados aplicables a las sucesiones pueden ser expresados para sus series.

Primero necesitamos establecer criterios para saber si una serie converge. Uno de estos criterios afirma que para que una serie sea convergente se requiere verificar que para cada $\epsilon > 0$ exista un entero N, tal que

$$\left| \sum_{i=n}^{m} a_i \right| \leq \epsilon$$

si $N \leq n \leq m$. A este criterio se le conoce como el **criterio de Cauchy**. Su recíproco también es cierto y establece que lo anterior es una propiedad de las series convergentes. Por lo tanto lo usaremos como una definición de convergencia de series.

Otro método muy utilizado es el **criterio de comparación**. Este criterio es sumamente útil ya que nos permite concluir sobre la convergencia de una serie solamente sabiendo si otra serie que la acote converge o no.

Teorema 1.3.1. *Sean dos series $\sum_{i=1}^{\infty} a_i$ y $\sum_{i=1}^{\infty} c_i$. Si existe un número entero N_0 para el cual $|a_n| \leq c_n$ donde $N_0 \leq n$, y sabemos que $\sum_{i=1}^{\infty} c_i$ converge. Entonces la serie $\sum_{i=1}^{\infty} a_i$ también converge.*

Para demostrar lo anterior basta ver que como $\sum_{i=n}^{\infty} c_i$ converge, entonces para $\epsilon > 0$ existe $N \geq N_0$, tal que $m \geq n \geq N$, y esto implica que

$$\sum_{i=n}^{m} c_i \leq \epsilon$$

De lo anterior tenemos que

$$\left| \sum_{i=n}^{m} a_i \right| \leq \sum_{i=n}^{m} |a_i| \leq \sum_{i=n}^{m} c_i \leq \epsilon$$

y de aquí se deduce que $\sum_{i=1}^{\infty} a_i$ converge, por lo que queda demostrado el resultado.

Ahora si consideramos series donde cada uno de sus términos sean no negativos, podemos aplicar el resultado obtenido para afirmar que si tenemos dos series $\sum_{i=1}^{\infty} a_i$ y $\sum_{i=1}^{\infty} d_i$ tales que $d_n < a_n$ para $N_0 < n$ donde N_0 es algún entero, y además la serie de las d_i diverge. Entonces la serie de las a_i también diverge. Es decir, hemos encontrado un criterio de divergencia para este tipo particular de series.

Además de estos criterios de convergencia existen otros más, los cuales no presentamos aquí ya que no serán utilizados. Dentro de estos se encuentran: el **criterio de la razón** y el **de la raíz**.

Hasta aquí hemos utilizado exclusivamente el concepto de convergencia; sin embargo, a partir de éste podemos introducir la convergencia absoluta. Diremos que una serie $\sum_{i=1}^{\infty} a_i$ **converge absolutamente**, si la serie $\sum_{i=1}^{\infty} |a_i|$ converge.

De la definición anterior podemos afirmar que si una serie converge absolutamente, entonces ésta converge. Esto se sigue del criterio de Cauchy y de la desigualdad

$$\left| \sum_{i=n}^{m} a_i \right| \leq \sum_{i=n}^{m} |a_i|$$

De esta relación entre la convergencia y la convergencia absoluta, podemos deducir que cuando la serie es de términos no negativos, ambas definiciones son iguales. Además diremos que la serie $\sum_{i=1}^{\infty} a_i$ converge **no absolutamente** si ésta converge, pero $\sum_{i=1}^{\infty} |a_i|$ diverge.

Ya hemos dado las definiciones básicas de las series y de su convergencia. Ahora nos interesa hacer operaciones entre ellas, para lo cual las definimos de la siguiente manera.

Definición 1.3.1. *La suma de dos series* $\sum_{i=1}^{\infty} a_i$ *y* $\sum_{i=1}^{\infty} b_i$ *está dada por:*

$$\left(\sum_{i=1}^{\infty} a_i \right) + \left(\sum_{i=1}^{\infty} b_i \right) = \sum_{i=1}^{\infty} (a_i + b_i)$$

Cuando ambas series convergen, digamos $\sum_{i=1}^{\infty} a_i = A$ y $\sum_{i=1}^{\infty} b_i = B$. Entonces la suma de éstas converge a $A + B$.

Definición 1.3.2. *La multiplicación o producto de Cauchy de dos series* $\sum_{i=1}^{\infty} a_i$ *y* $\sum_{i=1}^{\infty} b_i$ *se define como:*

$$\left(\sum_{i=1}^{\infty} a_i\right)\left(\sum_{i=1}^{\infty} b_i\right) = \sum_{i=1}^{\infty} c_i, \qquad \textit{donde } c_i = \sum_{k=1}^{i} a_k \cdot b_{i-k+1}$$

Aquí cabe destacar que, a diferencia de la suma, el hecho de que ambas series converjan no garantiza que el producto sea convergente.

Para poder asegurar la convergencia del producto es necesario agregar la condición de que al menos una de ellas lo sea absolutamente. Más aún, con estas nuevas condiciones podremos afirmar que si las dos series convergen a A y B, respectivamente; entonces el producto convergerá a AB. Por otro lado, si sabemos que el producto de las dos series es convergente, entonces no será necesario agregar la condición de convergencia absoluta para garantizar que el producto converge a AB.

Por último buscamos saber bajo qué condiciones podemos intercambiar los índices de una serie reiterada de la forma:

$$\sum_{m=0}^{\infty}\sum_{n=0}^{\infty} c_{nm}$$

donde c_{nm} son valores que dependen de ambos índices.

Para ello diremos que esa serie reiterada $\sum_{m=0}^{\infty}\sum_{n=0}^{\infty} c_{nm}$ es absolutamente convergente si la serie $\sum_{m=0}^{\infty}\sum_{n=0}^{\infty} |c_{nm}|$ es convergente. Entonces el siguiente teorema muestra las condiciones que se requieren para poder realizar el cambio de índices.

Teorema 1.3.2. *Si la serie reiterada*

$$\sum_{m=0}^{\infty}\sum_{n=0}^{\infty} c_{nm}$$

converge absolutamente, entonces las siguientes series convergen absolutamente al mismo valor y por lo tanto

$$\sum_{m=0}^{\infty}\left(\sum_{n=0}^{\infty} c_{nm}\right) = \sum_{n=0}^{\infty}\left(\sum_{m=0}^{\infty} c_{nm}\right)$$

Demostración. Dado que se tiene que la serie reiterada converge absolutamente, entonces la serie

$$\sum_{m=0}^{\infty}\sum_{n=0}^{\infty} |c_{nm}|$$

converge. Ahora definimos $|z_n| = |\sum_{m=0}^{\infty} c_{nm}|$ para cada n, entonces

$$|z_n| = \left|\sum_{m=0}^{\infty} c_{nm}\right| \leq \sum_{m=0}^{\infty} |c_{nm}| < \infty$$

y por lo tanto

$$\sum_{n=0}^{\infty} |z_n| = \sum_{n=0}^{\infty}\left|\sum_{m=0}^{\infty} c_{nm}\right| \leq \sum_{n=0}^{\infty}\sum_{m=0}^{\infty} |c_{nm}| < \infty$$

Esto y un argumento similar para la otra serie, demuestra que ambas series convergen absolutamente.

La convergencia de ambas series se sigue de considerar aproximaciones por medio de las sumas parciales de éstas y estimar el valor de convergencia de cada una de ellas. □

Con este último resultado damos por terminado este capítulo. Ahora procederemos a desarrollar los distintos temas centrales que buscamos cubrir en este trabajo.

Capítulo 2

Funciones Aritméticas

2.1. Definición

Definición 2.1.1. *Llamamos* ***función aritmética*** *a aquella función con valores en los complejos y con dominio los números naturales, es decir*

$$f : \mathbb{N} \longrightarrow \mathbb{C}$$

Ahora, buscamos darle una estructura algebraica al conjunto de todas las funciones aritméticas (al cual denotaremos por $\mathcal{A}$); para ello definimos dos operaciones. La primera operación es la suma de dos funciones aritméticas $f, g \in \mathcal{A}$ y se define de manera natural como

$$(f + g)(n) = f(n) + g(n)$$

Para la segunda operación podríamos suponer, intuitivamente, que estaría definida como la multiplicación directa de las funciones; sin embargo, para poder obtener la estructura algebraica deseada la debemos definir de una forma distinta.

Definición 2.1.2 (Convolución de Dirichlet)**.** *Sean f, g dos funciones aritméticas, definimos*

$$(f * g)(r) = \sum_{t|r} f(t)g(\frac{r}{t})$$

Donde la suma del lado derecho corre sobre los divisores t de r.

Además de las operaciones, necesitamos obtener los neutros con respecto a la suma y la convolución. Proponemos pues las siguientes funciones

$$z(n) = 0 \quad \text{para toda } n \in \mathbb{N}$$

como el neutro aditivo, y

$$I(n) \;=\; \begin{cases} 1 & n = 1 \\ 0 & n > 1 \end{cases}$$

como el neutro de la convolución.

Proposición 2.1.1. La función z es el neutro aditivo

Demostración. Sean $f \in \mathcal{A}$ y $n \in \mathbb{N}$, se tiene que

$$(f + z)(n) = f(n) + z(n) = f(n) + 0 = f(n)$$

□

Proposición 2.1.2. La función I es el neutro con respecto a la convolución

Demostración. Sean $f \in \mathcal{A}$ y $n \in \mathbb{N}$, entonces

$$(f * I)(n) = \sum_{d|n} f(d)I(\frac{n}{d}) = f(n)$$

ya que $I(\frac{n}{d}) = 0$, para todo $d \neq n$.

Análogamente, como $I(d) = 0$ para todo $d \neq 1$ y $I(1) = 1$ entonces

$$(I * f)(n) = \sum_{d|n} I(d)f(\frac{n}{d}) = f(n)$$

□

El inverso aditivo de una función $f \in \mathcal{A}$, denotado por $(-f)$, está definido por

$$(-f)(n) = -f(n)$$

Definición 2.1.3. *La norma de una función aritmética f, denotada por $N(f)$, se define como el mínimo número natural a para el cual $f(a) \neq 0$ y $N(z) = 0$ donde z es función neutro aditivo. Es decir*

$$N(f) := \begin{cases} min\{a\colon f(a) \neq 0\} & Si\ f \neq z \\ 0 & Si\ f = z \end{cases}$$

Proposición 2.1.3. Sean dos funciones f, g distintas de la función cero. Entonces se cumple que

$$N(f * g) = N(f)N(g)$$

Demostración. Si $f = z$ y $g = z$, entonces $N(f) = 0$ y $N(g) = 0$. Sea a un natural, evaluando $f * g$ en dicho número obtenemos

$$(f * g)(a) = \sum_{t|a} f(t)g(\frac{a}{t}) = \sum_{t|a} 0 = 0$$

lo que significa que $(f * g) = z$ y de esta forma

$$N(f * g) = 0 = N(f)N(g)$$

Ahora supongamos que $N(f) = a$ y $N(g) = b$, con a y b distintos de 0. Observemos que para $r < ab$, la convolución de Dirichlet está dada por

$$(f * g)(r) = \sum_{t|r} f(t)g(\frac{r}{t})$$

Analicemos los posibles valores que puede tomar t y lo que sucede con la convolución.
1)Si $t < a$, entonces $f(t) = 0$ y por lo tanto en esos términos la convolución vale 0.
2) Si $t \geq a$, entonces $\frac{r}{t} \leq \frac{r}{a} < \frac{ab}{a} = b$ y por lo tanto $g(r/t) = 0$, anulando dichos términos.

Análogamente podemos ver que los términos cuando $t < b$ ó $t \geq b$ también se anulan. Por lo tanto, para $r < ab$ se tiene que $(f * g)(r) = 0$.

Ahora bien, por otro lado tenemos que

$$(f * g)(ab) = f(a)g(b) + f(b)g(a) = f(a)g(b)$$

ya que, tanto para $a < b$ como para $b < a$, el término $f(b)g(a)$ se anula. Por consiguiente

$$N(f * g) = ab = N(f)N(g)$$

□

Con lo anterior, podemos afirmar que el conjunto de todas las funciones aritméticas posee una estructura algebraica de **Dominio Entero**. En la siguiente proposición demostramos dicha afirmación, para lo cual basta probar que la convolución es asociativa, conmutativa y la no existencia de divisores de ceros.

Proposición 2.1.4. $(\mathcal{A}, +, *)$ es un dominio entero

Demostración. Sean $f, g \in \mathcal{A}$ y $n, d \in \mathbb{N}$.

1)*Asociatividad:*
Si tenemos que $d|n$, podemos afirmar que $n = d \cdot a$. Utilizando este hecho, se tiene que la definición de convolución se puede expresar de la siguiente forma:

$$(f * g)(n) = \sum_{a \cdot d = n} f(a)g(b)$$

Además, si tenemos que $d|n$ y $b|d$, es decir que $n = a \cdot d$ y $d = b \cdot c$. Entonces juntando ambas igualdades obtenemos que $n = a \cdot b \cdot c$.

Haciendo uso de las afirmaciones anteriores, se tiene que:

$$\begin{aligned}(f * (g * h))(n) &= \sum_{a \cdot d = n} f(a)(g * h)(d) = \sum_{a \cdot d = n} f(a) \left(\sum_{b \cdot c = d} g(b)h(c) \right) \\ &= \sum_{a \cdot b \cdot c = n} f(a)g(b)h(c)\end{aligned}$$

análogamente nos resulta que:

$$\begin{aligned}((f * g) * h)(n) &= \sum_{d \cdot c = n} (f * g)(d)h(c) = \sum_{d \cdot c = n} \left(\sum_{a \cdot b = d} f(a)(b) \right) h(c) \\ &= \sum_{a \cdot b \cdot c = n} f(a)g(b)h(c)\end{aligned}$$

Como en ambos resultados a, b y c corren sobre todos los divisores de n, entonces podemos renombrarlos adecuadamente y de esta manera obtener que

$$(f * (g * h))(n) = \sum_{x \cdot y \cdot w = n} f(x)g(y)h(w) = ((f * g) * h)(n)$$

2) *Conmutatividad:*

Notemos que el hecho de que $d|n$ quiere decir que $n = a \cdot d$ para una única $a \in \mathbb{N}$; entonces existe una correspondencia biyectiva entre los divisores d y los divisores $a = \frac{n}{d}$. De lo anterior se sigue que:

$$\begin{aligned}(f * g)(n) &= \sum_{d|n} f(d)g(\frac{n}{d}) = \sum_{a|n} f(\frac{n}{a})g(a) \\ &= \sum_{a|n} g(a)f(\frac{n}{a}) \\ &= (g * f)(n)\end{aligned}$$

3) *La no existencia de divisores de cero.*

Sea $f, g \in \mathcal{A}$ tales que ambas funciones sean distintas de z, la función neutro aditiva. Sabemos, por la definición de norma, que $N(f) \neq 0$ y $N(g) \neq 0$.

Por otro lado, hemos demostrado que

$$N(f * g) = N(f)N(g)$$

entonces, dado que $N(f) \neq 0$ y $N(g) \neq 0$, podemos concluir que

$$N(f * g) \neq 0$$

lo cual, únicamente sucede si $f * g \neq z$. Por lo tanto, no existe divisores de cero en $\mathcal{A}$. Con esto hemos demostrado que $(\mathcal{A}, +, *)$ es un dominio entero. □

Definición 2.1.4. *La inversa de una función no idénticamente cero ($f \not\equiv z$) está definida como la función f^{-1} para la cual*

$$f * f^{-1} = f^{-1} * f = I$$

Proposición 2.1.5. Una función aritmética f posee inversa si, y sólo si $f(1) \neq 0$.

Demostración.

$\Rightarrow$) Como f^{-1} existe, tenemos que:

$$f(1)f^{-1}(1) = (f * f^{-1})(1) = I(1) = 1, \text{ entonces } f(1) \neq 0$$

$\Leftarrow$)Para demostrar la existencia de la inversa de f, necesitamos que dicha función cumpla con:
a)$(f * f^{-1})(1) = I(1) = 1$

Por la definición de convolucion de Dirichlet, sabemos que

$$(f * f^{-1})(1) = f(1)f^{-1}(1)$$

con lo cual debe cumplir que

$$f(1)f^{-1}(1) = 1$$

y como $f(1) \neq 0$, entonces f^{-1} debe cumplir con:

$$f^{-1}(1) = \frac{1}{f(1)}$$

b)$(f * f^{-1})(n) = I(n) = 0$, para toda $n > 1$

Notemos que $(f * f^{-1})(n)$ está definida de la siguiente manera.

$$\begin{aligned}(f * f^{-1})(n) &= \sum_{d|n} f(d)f^{-1}(\frac{n}{d}) \\ &= f(1)f^{-1}(n) + \sum_{1<d,d|n} f(d)f^{-1}(\frac{n}{d})\end{aligned}$$

ya que buscamos que se cumpla la condición planteada, entonces

$$f(1)f^{-1}(n) + \sum_{1<d,d|n} f(d)f^{-1}(\frac{n}{d}) = 0$$

implica que

$$-f(1)f^{-1}(n) = \sum_{1<d,d|n} f(d)f^{-1}(\frac{n}{d})$$

Como $f(1) \neq 0$, entonces hemos obtenido la definición de f^{-1} para toda $n > 1$ dada por:

$$f^{-1}(n) = \frac{1}{f(1)} \sum_{1<d,d|n} f(d) f^{-1}(\frac{n}{d})$$

De esta forma hemos demostrado la existencia de la inversa de f. □

Proposición 2.1.6. Una función aritmética f es invertible si, y sólo si, $N(f) = 1$

Demostración. Por el resultado anterior sabemos que f es invertible si, y sólo si, $f(1) \neq 0$, lo que es equivalente con que $N(f) = 1$. □

Un subconjunto de las funciones aritméticas de gran importancia son las funciones multiplicativas, las cuales caracterizamos a continuación.

Definición 2.1.5. *Una función aritmética no idénticamente cero, f, es llamada* ***multiplicativa*** *si*

$$f(mn) = f(m)f(n) \quad si\ (m,n) = 1$$

y ***estrictamente multiplicativa*** *si*

$$f(mn) = f(m)f(n) \quad \forall\, m, n \in \mathbb{N}$$

Proposición 2.1.7. Si f es multiplicativa, entonces $f(1) = 1$

Demostración. Por definición sabemos que $f \not\equiv z$, por lo tanto existe $n \in \mathbb{N}$ tal que $f(n) \neq 0$. Además se tiene que $f(n) = f(1)f(n)$, ya que $M.C.D(n, 1) = 1$. Entonces, al dividir por $f(n)$ obtenemos que $f(1) = 1$ □

Proposición 2.1.8. Sea f tal que $f(1) = 1$, entonces:

1) f es multiplicativa si, y sólo si:

$$f(p_1^{a_1} \cdots p_r^{a_r}) = f(p_1^{a_1}) \cdots f(p_r^{a_r})$$

para todo primo p_i y todo entero $a_i \geq 1$.

2) Si f es multiplicativa, entonces es estrictamente multiplicativa si, y sólo si:

$$f(p^a) = f(p)^a$$

para todo primo p y todo entero $a \geq 1$

Demostración.
1) Suponemos que f es multiplicativa, entonces como los p_i son primos se tiene que $M.C.D\left((p_1^{a_1} \cdots p_{r-1}^{a_{r-1}}), p_r^{a_r}\right) = 1$ y por lo tanto cumple con

$$f\left(p_1^{a_1} \cdots p_r^{a_r}\right) = f\left(p_1^{a_1} \cdots p_{r-1}^{a_{r-1}}\right) f(p_r^{a_r})$$

Aplicando un argumento inductivo, obtenemos

$$f\left(p_1^{a_1} \cdots p_r^{a_r}\right) = f(p_1^{a_1}) \cdots f(p_r^{a_r})$$

Recíprocamente, suponemos que la igualdad se cumple y que f no es idénticamente cero. Sean $m, n \in \mathbb{N}$ tales que $M.C.D(m, n) = 1$, entonces la factorización en primos de m y n involucra conjuntos disjuntos de potencias de primos. Ahora bien, utilizando la igualdad para expresar a $f(nm)$, $f(n)$ y $f(m)$ podemos ver que f satisface que:

$$f(nm) = f(n)f(m)$$

y como $f \not\equiv z$, por lo tanto f es multiplicativa.

2) Si f es estrictamente multiplicativa, entonces tenemos que para cualquier primo p y número entero a se cumple que:

$$f(p^a) = f(p^{a-1}p) = f(p^{a-1})f(p) = f(p^{a-2})f(p)f(p) = \cdots = f(p)^a$$

De manera inversa, supongamos que f es multiplicativa y que para todo primo p y todo número entero a cumple $f(p^a) = f(p)^a$. Sean $m, n \in \mathbb{N}$, por el teorema de factorización única tenemos que:

$$n = \prod_{i=1}^{r} p_i$$

$$m = \prod_{j=1}^{k} s_i$$

donde p_i y s_j son números primos, no necesariamente distintos. Por lo tanto, ya que f es multiplicativa, por el resultado anterior se sigue que:

$$\begin{aligned} f(nm) =& f\left(\prod_{i=1}^{r} p_i \cdot \prod_{j=1}^{k} s_i\right) \\ =& f\left(\prod_{i=1}^{r} p_i\right) f\left(\prod_{j=1}^{k} s_i\right) \\ =& f(n)f(m) \end{aligned}$$

por lo tanto f es estrictamente multiplicativa. □

Proposición 2.1.9. Si f y g son multiplicativas, también lo es su convolución $f * g$.

Demostración. Sea $h = f * g$ y $m, n \in \mathbb{N}$ tales que $(m, n) = 1$. Observamos que:

$$h(mn) = \sum_{d|mn} f(d)g(\frac{mn}{d})$$

Ahora, cada divisor $d|mn$ puede ser factorizado de forma única como $d = ab$ donde $a|m$, $b|n$ y $(a, b) = 1$. Entonces

$$\begin{aligned} h(mn) &= \sum_{d|mn} f(d)g(\frac{mn}{d}) = \sum_{a|m,b|n} f(ab)g(\frac{mn}{ab}) \\ &= \sum_{a|m}\sum_{b|n} f(ab)g(\frac{mn}{ab}) \end{aligned}$$

Dado que $(a, b) = 1$, se tiene que $(\frac{m}{a}, \frac{n}{b}) = 1$. Aplicando a la doble suma la multiplicatividad de f y g, obtenemos:

$$\begin{aligned} h(mn) &= \sum_{a|m}\sum_{b|n} f(a)f(b)g(\frac{m}{a})g(\frac{n}{b}) \\ &= \left(\sum_{a|m} f(a)g(\frac{m}{a})\right)\left(\sum_{b|n} f(b)g(\frac{n}{b})\right) \\ &= (f * g)(a)(f * g)(b) \\ &= h(a)h(b) \end{aligned}$$

con lo anterior se demuestra el resultado □

Proposición 2.1.10. Si g y $(f * g)$ son multiplicativas, entonces f también lo es.

Demostración. Sea $h = f * g$. Suponemos que f no es multiplicativa. Entones existe $m, n \in \mathbb{N}$ tales que $(m, n) = 1$ para los cuales

$$f(mn) \neq f(m)f(n)$$

Escogemos el par de números m, n que cumplan con la condición anterior y cuyo producto sea el menor entero posible.
Si $mn = 1$, entonces $f(1) \neq f(1)f(1)$ y por lo tanto $f(1) \neq 1$. Sabemos que g es multiplicativa, por lo tanto se cumple que $g(1) = 1$. De lo anterior tenemos que:

$$h(1) = f(1)g(1) = f(1) \neq 1$$

Es decir que h no es multiplicativa, lo cual es una contradicción.
Si $mn > 1$, por como seleccionamos a m y n, tenemos que $f(ab) = f(a)f(b)$ para todo $a, b \in \mathbb{N}$ con $(a, b) = 1$ y $ab < mn$. Haciendo una argumentación similar a la proposición anterior se tiene que:

$$h(mn) = \sum_{\substack{a|m \\ b|n}} f(ab)g(\frac{mn}{ab})$$

Separando el término de la suma donde $a = m$ y $b = n$, podemos reescribir lo anterior como

$$h(mn) = \sum_{\substack{a|m \\ b|n \\ ab<mn}} f(ab)g(\frac{mn}{ab}) + f(mn)g(1)$$

Dado que g es multiplicativa y tenemos que $f(a, b) = f(a)f(b)$ si $ab < mn$, entonces:

$$\begin{aligned} h(mn) &= \sum_{\substack{a|m \\ b|n \\ ab<mn}} f(a)f(b)g(\frac{m}{a})\frac{n}{b} + f(mn) \\ &= \left(\sum_{a|m} f(a)g(\frac{m}{a})\right)\left(\sum_{b|n} f(b)g(\frac{n}{b})\right) - f(m)f(n) + f(mn) \\ &= h(m)h(n) - f(m)f(n) + f(mn) \end{aligned}$$

Como $f(mn) \neq f(m)f(n)$, entonces $h(mn) \neq h(m)h(n)$ y por lo tanto $f * g$ no es multiplicativa. Esto es una contradicción a la hipótesis de que $f * g$ era multiplicativa, demostrando así el resultado. □

Proposición 2.1.11. Si f es multiplicativa, entonces su inversa es multiplicativa.

Demostración. Dado que I y f son multiplicativas y $(f * f^{-1}) = I$, entonces por la proposición anterior se tiene el resultado □

2.2. Series de Dirichlet

Las series de Dirichlet pueden ser consideradas como series formales infinitas, es decir donde no se toma en consideración su convergencia; o bien, como funciones complejas de la variable s definidas en la región donde dicha serie converge.La variable s representa un número complejo de la forma:

$$s = u + iv, \text{ donde } u = Re(s) \text{ y } v = Im(s)$$

Entonces las definimos de la siguiente manera.

Definición 2.2.1. *Sea f una función aritmética y $s \in \mathbb{C}$. Definimos la* ***serie de Dirichlet de*** *f*

$$\sum_{n=1}^{\infty} \frac{f(n)}{n^s}$$

Proposición 2.2.1. Para toda serie de Dirichlet existe un número real u_a, llamado **abscisa de convergencia absoluta**, tal que para toda $s = u + iv$ la serie converge absolutamente si $u > u_a$ pero no converge absolutamente si $u < u_a$.

Demostración. Dada una serie de Dirichlet $F(s) = \sum_{n=1}^{\infty} \frac{f(n)}{n^s}$, sea A el conjunto de números complejos s para los cuales $F(s)$ converge absolutamente. Si el conjunto A es vacío basta tomar $u_a = \infty$ para que se cumpla el teorema. Ahora bien, si A no es vacío tomamos

$$u_a = inf\{Re(s) : s \in A\}$$

Por la definición de u_a, si $u < u_a$ entonces la serie $F(s)$ no converge absolutamente. Por otro lado, notamos que dados $s = u + iv$ y $s' = u' + iv'$ tales que $u' > u$ entonces $|n^s| = n^u < n^{u'} = |n^{s'}|$ y por lo tanto se tiene que:

$$\sum_{n=1}^{\infty} \left| \frac{f(n)}{n^{s'}} \right| = \sum_{n=1}^{\infty} \frac{|f(n)|}{n^{u'}} \leq \sum_{n=1}^{\infty} \frac{|f(n)|}{n^u} = \sum_{n=1}^{\infty} \left| \frac{f(n)}{n^s} \right|$$

Es decir que si $F(s)$ converge absolutamente para una s, por el criterio de comparación, entonces también converge absolutamente para las s' con $u < u'$.

Como, por definición de u_a, existe números complejos $s = u + iv$ con u arbitrariamente cercanos a u_a para los cuales la serie $F(s)$ converge absolutamente, entonces usando lo anterior se sigue que la serie converge absolutamente para todo s tal que $u_a < u$. □

A continuación demostramos que las funciones aritméticas están determinadas de manera única por su serie de Dirichlet.

Proposición 2.2.2. Supongamos que $F(s) = \sum_{n=1}^{\infty} \frac{f(n)}{n^s}$ y $G(s) = \sum_{n=1}^{\infty} \frac{g(n)}{n^s}$ son series de Dirichlet cuya abscisa de convergencia es finita y que satisface $F(s) = G(s)$ para toda s con u suficientemente grande. Entonces $f(n) = g(n)$ para toda n.

Demostración. Sea $h(n) = f(n) - g(n)$ y $H(s) = F(s) - G(s)$ su serie de Dirichlet. Por hipótesis existe u_a tal que $H(s)$ converge absolutamente cuando $u \geq u_a$, y es idénticamente 0 es esa región.
Para demostrar que $h(n) = 0$ para toda n, suponemos que h no es idénticamente 0 y así obtendremos una contradicción.
Sea n_0 el número entero más pequeño para el cual $h(n_0) \neq 0$. Entonces

$$H(s) = \frac{h(n_0)}{n_0^s} + \sum_{n=n_0+1}^{\infty} \frac{h(n)}{n^s}$$

Dado que $H(s) = 0$ para $u \geq u_a$, se sigue que par cualquier $u \geq u_a$

$$\frac{h(n_0)}{n_0^u} = -\sum_{n=n_0+1}^{\infty} \frac{h(n)}{n^u}$$

de donde se obtiene que:

$$|h(n_0)| \leq \left| \sum_{n=n_0+1}^{\infty} \frac{h(n)}{n^u} \right| n_0^u \leq \sum_{n=n_0+1}^{\infty} |h(n)| \frac{n_0^u}{n^u}$$

Ahora bien, reescribiendo a $u = u_a + \alpha$ con $\alpha \geq 0$, obtenemos que para $n \geq n_0 + 1$

$$\frac{n_0^u}{n^u} = \left(\frac{n_0}{n}\right)^{\alpha} \left(\frac{n_0^{u_a}}{n^{u_a}}\right) \leq \left(\frac{n_0}{n_0+1}\right)^{\alpha} \left(\frac{n_0^{u_a}}{n^{u_a}}\right)$$

con lo cual tenemos:

$$|h(n_0)| \leq n_0^{u_a} \left(\frac{n_0}{n_0+1}\right)^{\alpha} \sum_{n=n_0+1}^{\infty} \frac{|h(n)|}{n^{u_a}} = A \left(\frac{n_0}{n_0+1}\right)^{\alpha}$$

Donde $A = n_0^{u_a} \sum_{n=n_0+1}^{\infty} \frac{|h(n)|}{n^{u_a}}$ es una constante finita, independiente de α, debido a la convergencia absoluta de $H(u_a)$. Haciendo $\alpha \longrightarrow \infty$, el lado derecho tiende a 0; es decir $h(n_0) = 0$ lo cual contradice la hipótesis. □

Proposición 2.2.3. Sean $F(s), G(s)$ series de Dirichlet asociadas a dos funciones aritméticas f y g, respectivamente. Tomemos la convolución de ambas funciones, dada por $h = f * g$ y $H(s)$ como su correspondiente serie de Dirichlet. Si $F(s)$ y $G(s)$ convergen absolutamente para alguna s, entonces $H(s)$ converge absolutamente y además se tiene que:

$$H(s) = F(s)G(s)$$

Demostración. Para cualquier s para el cual ambas series convergen absolutamente tenemos que:

$$F(s)G(s) = \left(\sum_{n=1}^{\infty} \frac{f(n)}{n^s}\right)\left(\sum_{m=1}^{\infty} \frac{g(m)}{m^s}\right) = \sum_{n=1}^{\infty}\sum_{m=1}^{\infty} \frac{f(n)g(m)}{n^s m^s}$$

Dado que las series convergen absolutamente, podemos multiplicar las series y reordenar los términos sin alterar la suma. Agrupamos los términos para los cuales mn poseen el mismo valor y de ésta forma obtenemos:

$$F(s)G(s) = \sum_{k=1}^{\infty} \frac{1}{k^s} \sum_{mn=k} f(n)g(m) = \sum_{k=1}^{\infty} \frac{(f*g)(k)}{k^s}$$

Con esto se demuestra que $H(s) = F(s)G(s)$.

La convergencia absoluta de $H(s)$ se sigue de la convergencia absoluta de $F(s)$ y $G(s)$, junto con la siguiente desigualdad:

$$\begin{aligned} \sum_{n=1}^{\infty} \left|\frac{h(n)}{n^s}\right| = \sum_{n=1}^{\infty} \frac{1}{|n^s|} \left|\sum_{mk=n} f(k)g(m)\right| &\leq \sum_{n=1}^{\infty} \frac{1}{|n^s|} \sum_{mk=n} |f(k)| \cdot |g(m)| \\ &= \left(\sum_{k=1}^{\infty} \left|\frac{f(k)}{k^s}\right|\right)\left(\sum_{m=1}^{\infty} \left|\frac{g(m)}{m^s}\right|\right) \end{aligned}$$

□

Proposición 2.2.4. Sea f una función aritmética multiplicativa con F como la serie de Dirichlet asociada a ésta, y sea s un número complejo. Si $F(s)$ converge absolutamente en algún punto s, entonces $F(s)$ se puede expresar como un producto infinito absolutamente convergente extendido sobre todos los primos p, es decir:

$$\sum_{n=1}^{\infty} \frac{f(n)}{n^s} = \prod_{p} \left(1 + \sum_{m=1}^{\infty} \frac{f(p^m)}{p^{ms}}\right)$$

Si f es completamente multiplicativa, entonces se tiene que:

$$\sum_{n=1}^{\infty} \frac{f(n)}{n^s} = \prod_{p} \left(1 - \frac{f(p)}{p^s}\right)^{-1}$$

Demostración. Definimos el siguiente producto finito:

$$P_N(s) = \prod_{p<N} \left(1 + \sum_{m=1}^{\infty} \frac{f(p^m)}{p^{ms}}\right)$$

Para demostrar la igualdad, basta ver que $\lim_{N\to\infty} P_N(s) = F(s)$.
Sea $N \geq 2$ determinado, y sean $p_1, p_2, \ldots, p_k$ los números primos menores o iguales a N. Observamos que el término 1 en cada factor de P_N puede ser expresado como $f(p^m)/p^{ms}$ con $m = 0$, entonces desarrollando la multiplicación de P_N y utilizando el hecho de que f es multiplicativa, obtenemos:

$$\begin{aligned} P_N(s) &= \prod_{p<N} \left(\sum_{m=0}^{\infty} \frac{f(p^m)}{p^{ms}}\right) = \sum_{m_1=0}^{\infty} \cdots \sum_{m_k=0}^{\infty} \frac{f(p_1^{m_1}) \cdots f(p_k^{m_k})}{(p_1^{m_1 s} \cdots p_k^{m_k s})} \\ &= \sum_{m_1=0}^{\infty} \cdots \sum_{m_k=0}^{\infty} \frac{f(p_1^{m_1} \cdots p_k^{m_k})}{(p_1^{m_1} \cdots p_k^{m_k})^s} \end{aligned}$$

Los números de la forma $p_1^{m_1} \cdots p_k^{m_k}$ son enteros positivos cuyos factores primos p son menores o iguales a N. Es decir, son elementos del conjunto

$$A_N = \{n \in \mathbb{N} : p \text{ primo, tal que } p|n \Rightarrow p \leq N\}$$

Más aún, por el teorema fundamental de la Aritmética, cada elemento de A_N tiene una única factorización como $p_1^{m_1} \cdots p_k^{m_k}$ con $m_i \in \mathbb{N} \cup \{0\}$ y eso sucede una sola vez en la suma de P_N. Entonces tenemos que P_N se puede reescribir como

$$P_N = \sum_{n \in A_N} \frac{f(n)}{n^s}$$

Como A_N contiene todos los enteros cuyos factores primos son menores o iguales que N, tenemos que

$$\sum_{n=1}^{\infty} \frac{f(n)}{n^s} - P_N = \sum_{n \in B} \frac{f(n)}{n^s}$$

donde B es el conjunto de las n que poseen al menos un factor primo mayor que N. Por lo tanto

$$\left| \sum_{n=1}^{\infty} \frac{f(n)}{n^s} - P_N \right| = \left| \sum_{n \in B} \frac{f(n)}{n^s} \right| \leq \sum_{n \in B} \left| \frac{f(n)}{n^s} \right| \leq \sum_{n > N} \left| \frac{f(n)}{n^s} \right|$$

Observamos que como la serie $\sum\limits_{n=1}^{\infty} \frac{f(n)}{n^s}$ es absolutamente convergente, entonces la última suma de la derecha tiende a cero cuando $N \to \infty$. Es decir $\lim\limits_{N \to \infty} P_N(s) = F(s)$.

Sabemos que el producto infinito de la forma $\prod (1 + a_n)$ converge absolutamente cuando la serie $\sum a_n$ converge absolutamente. En nuestro caso tomamos:

$$a_p = \sum_{m=1}^{\infty} \frac{f(p^m)}{p^{ms}}$$

es decir, el producto se puede reescribir como:

$$\prod_p \left(1 + \sum_{m=1}^{\infty} \frac{f(p^m)}{p^{ms}} \right) = \prod_p (1 + a_p)$$

entonces basta ver que la serie $\sum_p a_p$ converge absolutamente. Para esto notemos que como $F(s)$ es absolutamente convergente cumple con:

$$F(s) = \sum_{n=1}^{\infty} \left| \frac{f(n)}{n^s} \right| < \infty$$

Por otro lado se cumple la siguiente desigualdad:

$$\sum_p |a_p| = \sum_p \left| \sum_{m=1}^{\infty} \frac{f(p^m)}{p^{ms}} \right| \leq \sum_p \sum_{m=1}^{\infty} \left| \frac{f(p^m)}{p^{ms}} \right| \leq \sum_{n=1}^{\infty} \left| \frac{f(n)}{n^s} \right| < \infty$$

de donde se concluye que $\sum_p a_p$ converge absolutamente y, por lo tanto el producto también converge absolutamente.

Por último, si f es completamente multiplicativa tenemos que $f(p^m) = f(p)^m$ y entonces

$$F(s) = \prod_p \left(1 + \sum_{m=1}^{\infty} \frac{f(p^m)}{p^{ms}} \right) = \prod_p \left(\sum_{m=0}^{\infty} \frac{f(p)^m}{p^{ms}} \right)$$

pero $\sum_{m=0}^{\infty} \frac{f(p)^m}{p^{ms}}$ es una serie geométrica convergente cuya suma es:

$$\sum_{m=0}^{\infty} \frac{f(p)^m}{p^{ms}} = \left(1 - \frac{f(p)}{p^s} \right)^{-1}$$

y por lo tanto podemos concluir que:

$$F(s) = \prod_p \left(1 - \frac{f(p)}{p^s} \right)^{-1}$$

Con esto queda demostrado el teorema. □

2.3. La función $\zeta(s)$ y los números primos

Una de las series de Dirichlet más importantes es la función zeta $\zeta(s)$, definida como la serie de Dirichlet asociada a la función aritmética idénticamente 1. Es decir, está dada por:

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s} \qquad (u > 1)$$

donde u es la parte real del complejo s.

Una de las razones por la cual esta función es sumamente importante es por su estrecha relación con los números primos. Como veremos más adelante, nos permite demostrar la infinitud de estos y además está sumamente relacionada con su distribución.

Primero demostraremos el siguiente resultado sobre la convergencia de la serie de $\zeta(s)$ para números reales.

Proposición 2.3.1. La serie de Dirichlet

$$\sum_{n=1}^{\infty} \frac{1}{n^s}$$

converge para todo $s > 1$ y diverge para $s \leq 1$, donde s es un número real.

Demostración. Suponemos primero que $s > 1$. Agrupando los términos de la serie en bloques de $2, 4, 8, \ldots$, obtenemos:

$$\sum_{n=1}^{\infty} \frac{1}{n^s} = 1 + \left(\frac{1}{2^s} + \frac{1}{3^s}\right) + \left(\frac{1}{4^s} + \cdots + \frac{1}{7^s}\right) + \left(\frac{1}{8^s} + \cdots + \frac{1}{15^s}\right) + \cdots$$

Observamos que

$$\begin{aligned} \frac{1}{2^s} + \frac{1}{3^s} &\leq \frac{1}{2^s} + \frac{1}{2^s} = \frac{2}{2^s} = 2^{1-s} \\ \frac{1}{4^s} + \cdots + \frac{1}{7^s} &\leq \frac{1}{4^s} + \cdots + \frac{1}{4^s} = \frac{4}{4^s} = \left(2^{1-s}\right)^2 \\ \frac{1}{8^s} + \cdots + \frac{1}{15^s} &\leq \frac{1}{8^s} + \cdots + \frac{1}{8^s} = \frac{8}{8^s} = \left(2^{1-s}\right)^3 \end{aligned}$$

así sucesivamente. Tomamos la serie geométrica $g(s)$, dada por:

$$g(s) = \sum_{n=0}^{\infty} \left(2^{1-s}\right)^n$$

la cual converge ya que $0 < (2^{1-s}) < 1$. Entonces por el criterio de comparación, $\zeta(s)$ también converge para $s > 1$; mas aún, dado que $1 \leq \zeta(s) \leq g(s)$ para todo real $s > 1$, donde

$$g(s) = \sum_{n=0}^{\infty} \left(2^{1-s}\right)^n = \frac{1}{1 - (2^{1-s})}$$

si s tiende a $+\infty$ entonces 2^{1-s} tiende a 0; es decir que $g(s) \to 1$ y por lo tanto

$$\lim_{s\to+\infty} \zeta(s) = 1$$

Ahora demostramos la divergencia de la serie para $s \leq 1$. Si $s \leq 0$ la divergencia es evidente, ya que $\frac{1}{n^s}$ no tiende a 0 cuando n tiende a infinito, entonces suponemos que $0 < s \leq 1$ .Agrupando los términos de la series en bloques de $1, 1, 2, 4, \ldots$, se tiene que:

$$\zeta(s) = 1 + \frac{1}{2^s} + \left(\frac{1}{3^s} + \frac{1}{4^s}\right) + \left(\frac{1}{5^s} + \cdots + \frac{1}{8^s}\right) + \cdots$$

Como $s \leq 1$, entonces

$$\begin{aligned} \frac{1}{2^s} &\geq \frac{1}{2} \\ \frac{1}{3^s} + \frac{1}{4^s} &\geq \frac{1}{4} + \frac{1}{4} = \frac{2}{4} = \frac{1}{2} \\ \frac{1}{5^s} + \cdots + \frac{1}{8^s} &\geq \frac{1}{8} + \cdots + \frac{1}{8} = \frac{4}{8} = \frac{1}{2} \end{aligned}$$

pero la serie $1 + \frac{1}{2} + \frac{1}{2} + \cdots$ diverge y por lo tanto, por comparación, $\zeta(s)$ también diverge. □

De aquí podemos darnos una idea sobre la infinitud de números primos, ya que si existieran sólo una cantidad finita de números primos $p_1, p_2, \cdots, p_k$, entonces $\zeta(s)$, cuando $s \to 1$, se aproximaría al producto finito

$$\prod_{i=1}^{k} \left(1 - \frac{1}{p_i^s}\right)^{-1}$$

Sin embargo $\zeta(s) \to +\infty$, lo cual sería una contradicción ya que el producto finito no puede ser divergente.

La idea anterior nos permite corroborar intuitivamente que existen una infinidad de primos; sin embargo, a continuación desarrollamos una demostración más rigurosa de este hecho.

Proposición 2.3.2. Existe una infinidad de números primos

Demostración. Suponemos que solamente existe una cantidad finita de primos, denotados por $p_1, p_2, \ldots, p_k$. Para cada p_i con $1 \leq i \leq k$ se tiene que $|1/p_i| < 1$, con lo cual existe una serie geométrica convergente tal que:

$$\sum_{n=0}^{\infty} \frac{1}{p_i^n} = \frac{1}{1 - p_i^{-1}}$$

Si multiplicamos estas k series distintas, su producto

$$\prod_{i=1}^{k} \left(\sum_{n=0}^{\infty} \frac{1}{p_i^n} \right) = \prod_{i=1}^{k} \frac{1}{1 - p_i^{-1}}$$

es finito.

Estas series convergentes tienen únicamente términos positivos, es decir que son absolutamente convergentes y entonces podemos multiplicarlas entre sí y reordenar los términos sin modificar el producto.
Seleccionamos un término general de cada serie, dado por $1/p_i^{a_i}$ con $1 \leq i \leq k$ y $a_i \geq 0$, entonces su producto es

$$\frac{1}{p_1^{a_1}} \cdot \frac{1}{p_2^{a_2}} \cdots \frac{1}{p_k^{a_k}} = \frac{1}{p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k}}$$

el cual representa un término típico de dicho producto. Por el Teorema Fundamental de la Aritmética, sabemos que cualquier entero $n \geq 1$ posee una única factorización en potencias de primos, los cuales supusimos ser una cantidad finita, entonces:

$$n = p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k} \qquad (a_i \geq 0)$$

La unicidad de dicha factorización implica que cada término del producto representa a un entero n distinto, es decir que:

$$\frac{1}{p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k}} = 1/n$$

Con lo cual al expandir el producto, este adquiere la siguiente forma:

$$\prod_{i=1}^{k} \left(\sum_{n=0}^{\infty} \frac{1}{p_i^n} \right) = \sum_{n=1}^{\infty} \frac{1}{n}$$

pero la suma del lado derecho representa la serie armónica, la cual es divergente. Esta es una contradicción, ya que habíamos demostrado que el producto del lado izquierdo de la igualdad era finito y por lo tanto no es posible que diverja. Entonces, se concluye que existen una infinidad de números primos. □

Capítulo 3

Möbius

Uno de los métodos de conteo más útiles en el análisis combinatorio es el Principio de inclusión y exclusión (P.I.E). En este capítulo usaremos esta herramienta para deducir, a través de la construcción de la función φ de euler, la función clásica de Möbius y la inversión de Möbius. Una vez obtenida ésta, desarrollaremos la relación existente entre los resultados obtenidos y la estructura de conjuntos parcialmente ordenados.

3.1. Möbius Clásica

Teorema 3.1.1 (**Principio de Inclusión y Exclusión**). *Sea C un conjunto con N elementos; $S_1,\dots S_r$ subconjuntos de C no necesariamente distintos. Definimos $N(M)$ como el número de elementos de C en $\bigcap_{i\in M} S_i$ con $M \subseteq \{1,\dots,r\}$. Además definimos*

$$N_j := \sum_{|M|=j} N(M)$$

con $0 \leq j \leq r$ es decir N_j es la suma de la cantidad de elementos de C que están en las distintas intersecciones de j de los subconjuntos $\{S_1,\dots,S_r\}$.

Entonces el número de elementos de C que **no está** *en ninguno de los S_i $1 \leq i \leq r$ es:*

$$N - N_1 + N_2 - N_3 + \ldots + (-1)^r N_r$$

DEMOSTRACIÓN. Necesitamos verificar que cualquier elemento $x \in S$ sea contado de forma correcta por la fórmula propuesta; para lo cual contemplaremos dos casos, dependiendo de la cantidad de S_i a los que pertenezca x.
Caso 1: $x \in S \backslash \{S_1 \cup S_2 \cup \cdots \cup S_r\}$.

En este caso como x no pertenece a ninguno de los S_i, entonces debería ser contado por la fórmula una única vez. Realizando el cálculo tenemos que

$$N - N_1 + N_2 - N_3 + \ldots + (-1)^r N_r = 1 - 0 + \cdots + (-1)^r \cdot 0 = 1$$

Caso 2: x está en exactamente k de los subconjuntos de S_i.

Como x está en algunos de los S_i, entonces no debería ser contado. Ahora bien como x está en exactamente k de los S_i, entonces aparece en la suma de N_1 k veces; en N_2 aporta $\binom{k}{2}$; en N_3 adiciona $\binom{k}{3}$ y así sucesivamente. Con lo cual,

$$N - N_1 + N_2 - N_3 + \ldots + (-1)^k N_k = 1 - \binom{k}{1} + \binom{k}{2} - \binom{k}{3} + \cdots + (-1)^k \binom{k}{k}$$

o lo que es lo mismo

$$N - N_1 + N_2 - N_3 + \ldots + (-1)^k N_k = \sum_{i=0}^{k} \binom{k}{i} (-1)^i$$

Por el teorema del Binomio de Newton sabemos que,

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

Es decir:

$$\begin{aligned} N - N_1 + N_2 - N_3 + \ldots + (-1)^k N_k &= \sum_{i=0}^{k} \binom{k}{i} (-1)^i \\ &= (1-1)^k = 0 \end{aligned}$$

□

Teorema 3.1.2. *Sea $n = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdots p_r^{\alpha_r}$ un entero positivo. Definimos la función $\varphi(n) := |\{x \in \{1, 2, \ldots, n\} : M.C.D(x, n) = 1\}|$, entonces*

$$\varphi(n) = n \prod_{i=1}^{r} (1 - \frac{1}{p_i})$$

DEMOSTRACIÓN. Sea $A = \{1, 2, 3, \ldots, n\}$ y $S_i = \{x \in \{1, 2, 3, \ldots, n\} : p_i \mid x\}$

Como buscamos primos relativos a n y éste se descompone en potencias de primos, es equivalente a buscar enteros menores que n que no sean divisibles por ninguno de los p_i $1 \leq i \leq r$

Aplicando el P.I.E. tenemos que:

$$\varphi(n) = n - N_1 + N_2 - N_3 + \cdots + (-1)^r N_r$$

donde:

$$\begin{aligned}
N_1 &= \sum_{i=1}^{r} |\{x \in \{1, 2, \ldots, n\} : p_i \mid x\}| \\
N_2 &= \sum_{1 \leq i < j \leq r} |\{x \in \{1, 2, \ldots, n\} : \quad p_i \cdot p_j \mid x\}| \\
N_3 &= \sum_{1 \leq i < j < k \leq r} |\{x \in \{1, 2, \ldots, n\} : \quad p_i \cdot p_j \cdot p_k \mid x\}| \\
&\vdots \\
N_r &= |\{x \in \{1, 2, \ldots, n\} : \quad p_1 \cdot p_2 \cdot p_3 \cdots p_r \mid x\}|
\end{aligned}$$

Los números enteros enteros menores que n que son divididos por p_i son de la forma βp_i donde $\beta \in \{1, 2, 3, \ldots, p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_i^{\alpha_i - 1} \cdots p_r^{\alpha_r}\}$. Con lo cual la cantidad de números enteros menores o iguales a n que son divididos por p_i es $\frac{n}{p_i}$. Análogamente obtenemos que la cantidad de números menores o iguales a n que son divididos por $p_i p_j$ es $\frac{n}{p_i p_j}$.

Usando los resultados obtenidos vemos que:

$$\begin{aligned}
\varphi(n) &= n - \sum_{i=1}^{r} \frac{n}{p_i} + \sum_{1\leq i<j\leq r} \frac{n}{p_i p_j} - \cdots + (-1)^r \frac{n}{p_1 p_2 \cdots p_r} \\
&= n\left[1 - \sum_{i=1}^{r} \frac{1}{p_i} + \sum_{1\leq i<j\leq r} \frac{1}{p_i p_j} - \cdots + (-1)^r \frac{1}{p_1 p_2 \cdots p_r}\right] \\
&= n\left[(1-\frac{1}{p_1})(1-\frac{1}{p_2})(1-\frac{1}{p_3})\ldots(1-\frac{1}{p_r})\right] \\
&= n\prod_{i=1}^{r}(1-\frac{1}{p_i})
\end{aligned}$$

□

Una deducción importante de la demostración anterior es que los términos de $\varphi(n)$ con productos impares de los primos p_i están multiplicados por (-1) (tienen signo negativo) y los términos que poseen un producto par de primos p_i se multiplican por 1, es decir son positivos. Ahora bien, los divisores de n que no están libres de raíces (aquellos que están formados por alguna potencia de los primos p_i) no aparecen en los términos de $\varphi(n)$. De las observaciones anteriores, podemos definir la siguiente función:

$$\mu(d) := \begin{cases} (-1) & \text{Si } d \text{ es producto impar de primos distintos} \\ 1 & \text{Si } d \text{ es producto par de primos distintos} \\ 0 & \text{Si } d \text{ no está libre de raíces} \end{cases}$$

Esta es la **función de Möbius clásica**.

Existe un relación estrecha entre la función φ y la función de Möbius, la cual queda de manifiesto en la siguiente propiedad.

Teorema 3.1.3. $\varphi(n) = n\sum_{d|n} \frac{\mu(d)}{d}$

Demostración. Si tomamos $d|n$ y reescribiendo a $\varphi(n)$, obtenemos

$$\begin{aligned}
\varphi(n) &= n\left[1 + \sum_{i=1}^{r} \frac{(-1)}{p_i} + \sum_{1\leq i<j\leq r} \frac{1}{p_i p_j} - \cdots + \frac{(-1)^r}{p_1 p_2 \cdots p_r}\right] \\
&= n\sum_{d|n} \frac{\mu(d)}{d}
\end{aligned}$$

□

Necesitamos demostrar la siguiente propiedad de la función μ que nos permitirá presentar el teorema central de estudio de esta tesis.

Teorema 3.1.4. $\sum_{d|n} \mu(d) = \begin{cases} 1 & n=1 \\ 0 & \textit{en otro caso} \end{cases}$

Demostración. La demostración es por inducción sobre n. Si $n = 1$ entonces posee un número par de factores primos (entendiéndose que tiene 0 factores) y por lo tanto tenemos que $\mu(1) = 1$.

Sea $n > 1$ de la forma $n = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdots p_r^{\alpha_r}$, donde p_i es un número primo y α_i es un entero positivo. Entonces considerando aquellos divisores de n que estén libres de raíces, obtenemos que:

$$\sum_{d|n} \mu(d) = \sum_{i=0}^{r} \binom{r}{i} (-1)^i = (1-1)^r = 0$$

□

Ya estamos en condiciones de demostrar el **Fórmula de Inversión de Möbius**, el cual es de suma importancia ya que nos permite dadas dos funciones, obtener los valores de éstas siempre y cuando una de ellas se pueda definir con respecto a la otra.

Teorema 3.1.5 (**Fórmula de Inversión de Möbius**). *Sea $f(n)$ y $g(n)$ funciones definidas para todo entero positivo n, tal que*

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

entonces g satisface

$$g(n) = \sum_{d|n} \mu(d) f(\frac{n}{d})$$

Demostración.

$$\sum_{d|n} \mu(d) f(\frac{n}{d}) = \sum_{d|n} \mu(\frac{n}{d}) f(d) = \sum_{d|n} \mu(\frac{n}{d}) \sum_{d'|d} g(d') = \sum_{d'|n} g(d') \sum_{m|(n/d')} \mu(m)$$

Por el Teorema 3.1.4 se tiene que $\sum_{m|(n/d')} \mu(m) = 0$ excepto cuando $n/d' = 1$; con lo cual la suma interior es 0 excepto en $d' = n$. Entonces, se tiene que:

$$\sum_{d'|n} g(d') \sum_{m|(n/d')} \mu(m) = 0 + 0 + \cdots + g(n) + 0 + 0 + \cdots = g(n)$$

y por lo tanto:

$$g(n) = \sum_{d|n} \mu(\frac{n}{d}) f(d) = \sum_{d|n} \mu(d) f(\frac{n}{d})$$

□

Así pues, hemos obtenido el teorema central de nuestro trabajo donde la divisibilidad nos permite realizar una comparación entre los números utilizados y de esta forma establecer, cuando sea posible, un orden entre dichos números. El concepto de orden, nos permitirá generalizar el Teorema de inversión de Möbius a otros conjuntos cuyo orden sea distinto de la divisibilidad.

3.2. Álgebra de Incidencia

Observemos que los resultados anteriores utilizan la divisibilidad como condición, lo cual implica verificar si un número divide a otro para poder utilizarlo. Por esto, es importante resaltar que realizar la verificación implica hacer uso de una relación binaria entre dichos elementos. Más aún, la divisibilidad es un orden parcial, ya que esta relación es reflexiva, antisimétrica y transitiva. Aunado a esto, se puede observar que la relación "divide a" no garantiza que cualesquiera dos elementos del conjunto puedan ser ordenados; es decir, no necesariamente dados a, b existentes en $\mathbb{Z}^+$ se puede afirmar que "a **divide a** b", o que "b **divide a** a".

Definición 3.2.1. *Un conjunto A es parcialmente ordenado (o Poset), si posee una relación binaria $\preceq$ que cumple con:*
1) $a \preceq a$, $\forall a \in A$
2) Si $a \preceq b$ y $b \preceq c$, entonces $a \preceq c$
3) Si $a \preceq b$ y $b \preceq a$, entonces $a = b$

Notamos que dicha definición no requiere que exista una relación entre cualesquiera dos elementos de A; es decir, que la condición de que $a \preceq b$ ó $b \preceq a$ puede no darse. Si ésta última se cumple para todos los elementos del conjunto, entonces dicho conjunto será totalmente ordenado. A continuación desarrollamos dicha teoría.

El siguiente ejemplo muestra como un mismo conjunto puede ser parcial o totalmente ordenado, dependiendo del tipo de relación que se utilice.

Ejemplo 3.2.1. Tomemos el conjunto $C = \{1, 2, 3, 4\}$.
Consideramos el orden "divide a" y lo denotamos por $\preceq$.

Notamos que:

$$1 \preceq 2,\ 1 \preceq 3,\ 1 \preceq 4 \text{ y } 2 \preceq 4$$

Ahora bien, como 1 divide a 2 y 2 divide a 4, tenemos que $1 \preceq 2 \preceq 4$.

¿ Es posible ordenar al 2 y al 3? La respuesta es no, ya que $2 \not\preceq 3$ (2 no divide a 3) y $3 \not\preceq 2$ (3 no divide a 2).

Entonces como no cualquier par de elementos se puede ordenar bajo la relación de divisibilidad, el orden dado por " divide a" es parcial.

Por otro lado, si consideramos la relación binaria " menor que", denotada por $\leq$, entonces estaríamos hablando de un orden total, ya que cualquier par de elementos de C se puede ordenar bajo esta relación. Es decir:

$$1 \leq 2 \leq 3 \leq 4$$

Cabe mencionar que la función de Möbius y las hipótesis de los resultados expuestos, solamente utilizan propiedades derivadas de la relación de divisibilidad; lo cual nos permite inferir que existe una generalización de estos resultados para cualquier tipo de conjunto parcialmente ordenado.

Definición 3.2.2. *Sean $a, b \in A$, donde A es un conjunto parcialmente ordenado. El segmento o intervalo cerrado $[a, b]$ es el conjunto*

$$[a, b] = \{z \in A \mid a \preceq z \preceq b\}$$

Diremos que A es localmente finito si todo segmento de A es finito y consideraremos para el desarrollo de este tema, salvo que se requiera de otra manera, únicamente este tipo de posets.

Teorema 3.2.1. *Sea A un poset localmente finito. Considérese la familia de funciones $\mathcal{I}(A)$, definida como:*

$$\mathcal{I}(A) := \{f : A \times A \to \mathbb{R} \mid f(a, b) = 0 \text{ si } a \not\preceq b\}$$

y para $f, g \in \mathcal{I}$ y $k \in \mathbb{R}$, definimos las siguientes operaciones:

1) $(f + g)(a, b) := f(a, b) + g(a, b)$ *(Suma)*
2) $(kf)(a, b) := k\,[f(a, b)]$ *(multiplicación escalar)*
3) $(f * g)(a, b) = \sum_{a \preceq z \preceq b} f(a, z)g(z, b)$ *(convolución)*

Bajo estas condiciones $\mathcal{I}(\mathcal{A})$ es un álgebra asociativa.

Demostración.
1) Sea $f, g, h \in \mathcal{I}(A)$ p.d $[(f * g) * h](a, b) = [f * (g * h)](a, b)$

$$\begin{aligned}
[(f * g) * h](a, b) &= \sum_{a \preceq z \preceq b} (f * g)(a, z) h(z, b) \\
&= \sum_{a \preceq z \preceq b} \left\{ \sum_{a \preceq y \preceq z} f(a, y) g(y, z) \right\} h(z, b) \\
&= \sum_{a \preceq y \preceq b} f(a, y) \left\{ \sum_{y \preceq z \preceq b} g(y, z) h(z, b) \right\} \\
&= \sum_{a \preceq y \preceq b} f(a, y)(g * h)(y, b) \\
&= [f * (g * h)](a, b)
\end{aligned}$$

□

Definición 3.2.3. *Al álgebra asociativa $\mathcal{I}(A)$ se le denomina* ***álgebra de incidencia*** *y a sus elementos* ***funciones de incidencia****.*

A continuación se definen algunas funciones que pertenecen a la familia $\mathcal{I}(A)$ que serán de gran utilidad en el desarrollo de los resultados buscados.

Definición 3.2.4. *La identidad o* ***delta de Kronecker****, denotada por $\delta(a, b)$*

$$\delta(a, b) = \begin{cases} 1 & a = b \\ 0 & a \neq b \end{cases}$$

La función ***zeta****, denotada por $\zeta(a, b)$, la definimos como:*

$$\zeta(a, b) = \begin{cases} 1 & a \preceq b \\ 0 & \textit{en otro caso} \end{cases}$$

En el siguiente resultado se caracterizan las unidades de $\mathcal{I}(A)$, a saber, aquellas funciones que poseen una inversa con respecto a la convolución. Con esto estaremos en condiciones de definir la función de Möbius para posets.

Proposición 3.2.2. $f \in \mathcal{I}(A)$ es una unidad $\Leftrightarrow \forall a \in A$, $f(a, a) \neq 0$.

Además la inversa de f, denotada por f^{-1}, es única.

Demostración.
⇒)
Sean $f \in \mathcal{I}(A)$ una unidad y $g \in \mathcal{I}(A)$, tal que $f * g = \delta$. Entonces, $\forall a \in A$ se tiene que:

$$1 = \delta(a,a) = (f * g)(a,a) = f(a,a)g(a,a)$$

Con lo cual $f(a,a) \neq 0$.

⇐)
Sea $f \in \mathcal{I}(A)$, tal que $\forall a \in A$ $f(a,a) \neq 0$. Dado que buscamos una función $g \in \mathcal{I}(A)$ que sea la inversa derecha de f, ésta debe de cumplir que para toda a suceda que:

$$(f * g)(a,a) = \delta(a,a) = 1 \Rightarrow f(a,a)g(a,a) = 1$$

y como $f(a,a) \neq 0$ entonces se tiene que $g(a,a) = \dfrac{1}{f(a,a)}$.

Para definir $g(a,b)$ cuando $a \prec b$ lo haremos de manera inductiva. Es decir, suponemos que hemos encontrado el valor de $g(a,z)$ para cada z que satisface $a \prec z \preceq b$. Ahora bien, buscamos que g cumpla con

$$(f * g)(a,b) = \delta(a,b) = 0$$

entonces

$$\begin{aligned} 0 &= (f * g)(a,b) = \sum_{a \preceq z \preceq b} f(a,z)g(z,b) \\ &= f(a,a)g(a,b) + \sum_{a \prec z \preceq b} f(a,z)g(z,b) \end{aligned}$$

con lo cual

$$-f(a,a)g(a,b) = \sum_{a \prec z \preceq b} f(a,z)g(z,b)$$

como $f(a,a) \neq 0$ y todos los términos de la suma son conocidos, entonces hemos obtenido el valor de $g(a,b)$. Así pues, hemos demostrado la existencia

de la inversa derecha de la función f, denotada por f^{-1}, y a la cual definimos como sigue:

$$f^{-1}(a,a) = \frac{1}{f(a,a)}$$

$$f^{-1}(a,b) = \frac{1}{f(a,a)} \left(- \sum_{a \prec z \preceq b} f(a,z) g(z,b) \right)$$

De la misma manera, aplicando inducción a los términos de la forma $a \preceq z \prec b$ se demuestra la existencia de la inversa izquierda de f.

Por último, para demostrar la unicidad suponemos que para $f \in \mathcal{I}(A)$, existen $g, h \in \mathcal{I}(A)$ que son inversa izquierda y derecha, respectivamente. Entonces tenemos que

$$g = g * \delta = g * (f * h) = (g * f) * h = \delta * h = h$$

□

Es importante destacar que hemos obtenido de manera explícita, las inversas de cualquier unidad del álgebra de incidencia. Esto nos permite dar dos definiciones equivalentes de la función de Möbius. Por un lado, dado que para toda $a \in A$ se tiene que $\zeta(a,a) \neq 0$, entonces ζ es una unidad de $\mathcal{I}(A)$ y por lo tanto existe su inversa. A dicha función se le denomina **función de Möbius** y se le denota por μ. Es decir que μ queda definida como:

$$\mu := \zeta^{-1}$$

Sin embargo, utilizando la expresión explícita conseguida de las funciones inversas y considerando a μ como inversa derecha de ζ, se tiene que:

1) Para toda $a \in A$
Como $\zeta(a,a) = 1$, entonces

$$\mu(a,a) = \frac{1}{\zeta(a,a)} = 1$$

2)Sean $a, b \in A$, tales que $a \prec b$
Sabemos que $\zeta(a,a) = 1$ y $\zeta(a,b) = 1$, entonces

$$\mu(a,b) = -\frac{\sum_{a \prec z \preceq b} \zeta(a,z)\mu(z,b)}{\zeta(a,a)} = -\sum_{a \prec z \preceq b} \mu(z,b)$$

Análogamente, podemos obtener una definición similar si consideramos a μ como la inversa izquierda de la función zeta.

Es decir, μ está definida inductivamente de la siguiente manera:

$$\mu(a,b) := \begin{cases} 1 & \text{Si } a = b \\ 0 & \text{Si } a \not\preceq b \\ -\sum_{a \prec z \preceq b} \mu(z,b) & \text{Si } a \prec b \end{cases}$$

o bien

$$\mu(a,b) := \begin{cases} 1 & \text{Si } a = b \\ 0 & \text{Si } a \not\preceq b \\ -\sum_{a \preceq z \prec b} \mu(a,z) & \text{Si } a \prec b \end{cases}$$

A continuación presentamos el teorema de inversión de Möbius para poset.

Teorema 3.2.3. *Sea A un poset localmente finito y sean $f, g \in \mathcal{I}(A)$. Entonces*

$$g(a,b) = \sum_{a \preceq z \preceq b} f(a,z) \iff f(a,b) = \sum_{a \preceq z \preceq b} g(a,z)\mu(z,b)$$

Demostración. $\Rightarrow$) Dado que $\zeta(z,b) = 1$ para toda z que cumple con $a \preceq z \preceq b$, entonces se tiene que:

$$g(a,b) = \sum_{a \preceq z \preceq b} f(a,z) = \sum_{a \preceq z \preceq b} f(a,z)\zeta(z,b)$$

lo cual, por la definición de convolución, es equivalente a

$$g(a,b) = (f * \zeta)(a,b)$$

Aplicando μ como inversa derecha de ζ y como $\mathcal{I}(A)$ es asociativa, obtenemos que

$$\begin{aligned}(g * \mu)(a,b) &= [(f * \zeta) * \mu](a,b) = [f * (\zeta * \mu)](a,b) \\ &= (f * \delta)(a,b) = f(a,b)\end{aligned}$$

Es decir

$$f(a,b) = (g * \mu)(a,b) = \sum_{a \preceq z \preceq b} g(a,z)\mu(z,b)$$

$\Leftarrow$) Se tiene que

$$f(a,b) = \sum_{a \preceq z \preceq b} g(a,z)\mu(z,b) = (g * \mu)(a,b)$$

Si aplicamos la convolución con ζ a la igualdad y utilizando la asociatividad de $\mathcal{I}(A)$, tenemos

$$\begin{aligned}(f * \zeta)(a,b) &= [(g * \mu) * \zeta](a,b) = [g * (\mu * \zeta)](a,b) \\ &= (g * \delta)(a,b) = g(a,b)\end{aligned}$$

entonces

$$g(a,b) = (f * \zeta)(a,b) = \sum_{a \preceq z \preceq b} f(a,z)\zeta(z,b)$$

pero $\zeta(z,b) = 1$ para toda z que cumple con $a \preceq z \preceq b$, por lo tanto

$$g(a,b) = \sum_{a \preceq z \preceq b} f(a,z)$$

□

Corolario. Sea A un poset localmente finito y sean $f, g \in \mathcal{I}(A)$. Entonces

$$g(a,b) = \sum_{a \preceq z \preceq b} f(z,b) \Longleftrightarrow f(a,b) = \sum_{a \preceq z \preceq b} \mu(a,z)g(z,b)$$

La demostración es análoga a la anterior.

La fórmula de inversión de Möbius definida por Gian-Carlo Rota [10] es un caso particular de la que aquí proponemos. Utilizando las hipótesis de Rota; es decir, sea A un poset localmente finito, $f, g : A \longrightarrow \mathbb{R}$ y p tal que $f(x) = 0$ salvo para $p \preceq x$. Basta definir $F(p, x) = f(x)$ y $G(p, x) = g(x)$; aplicando nuestro resultado a las nuevas funciones definidas obtenemos el resultado propuesto por G. Rota.

Capítulo 4

Aplicaciones

Dadas dos funciones definidas en un conjunto parcialmente ordenado, donde una de ellas se expresa como la suma infinita de la otra, entonces la fórmula de inversión de Möbius nos permite invertir dicha relación. Esta propiedad de la inversión de Möbius es de gran importancia, ya que muchas veces puede ser muy complicado obtener de forma directa un resultado deseado. Entonces la inversión de Möbius nos permite tener otra forma para lograr el objetivo que uno se platea. Esto es, basta encontrar un resultado secundario definido como una suma infinita donde nuestro objetivo forme parte de ella para después invertir la relación y así reescribir nuestro resultado como una suma de otros, probablemente más sencillos de encontrar. A continuación mostramos algunos ejemplos de las aplicaciones de la inversión de Möbius.

4.1. Problemas de Conteo

Ejemplo 4.1.1. Conteo de polinomios mónicos irreducibles de grado n sobre un campo de q elementos

Conocer el número de polinomios mónicos irreducibles de grado n en un campo con q elementos, se obtiene al realizar el conteo de polinomios mónicos de grado n en dicho campo.

Sean $f_1(x), f_2(x), f_3(x), \ldots$ todos los polinomios mónicos irreducibles de grado al menos 1; cuyos grados son $d_1, d_2, d_3, \ldots$ respectivamente.

Ahora sea N_d el número de polinomios mónicos irreducibles de grado d, con $d = 1, 2, 3, \ldots$

Si tomamos $i_1, i_2, i_3, \ldots$ números enteros no negativos (donde casi todos estos son iguales a cero, salvo una cantidad finita), entonces:

$$f(x) = (f_1(x))^{i_1}(f_2(x))^{i_2}(f_3(x))^{i_3}\cdots$$

es un polinomio mónico cuyo grado es $n = i_1d_1 + i_2d_2 + i_3d_3 + \cdots$.

Ahora bien, cada polinomio mónico de grado n se puede escribir solamente una vez de esta forma. Es decir, existe una correspondencia 1 a 1 entre estos y las sucesiones $(i_1, i_2, i_3, \ldots)$ que cumplen con la condición $n = i_1d_1 + i_2d_2 + i_3d_3 + \cdots$

Observemos que el número de polinomios mónicos de grado n es q^n. Esta cantidad aparece en la siguiente serie como el coeficiente correspondiente a x^n:

$$\frac{1}{1-qx} = 1 + qx + (qx)^2 + (qx)^3 + \cdots$$

Por otro lado, el número de sucesiones $i_1, i_2, i_3, \ldots$ que cumplen con la condición $n = i_1d_1 + i_2d_2 + i_3d_3 + \cdots$ se puede obtener como el coeficiente de x^n en la multiplicación de las siguientes series:

$$(1 + x^{d_1} + x^{2d_1} + x^{3d_1} + \cdots)(1 + x^{d_2} + x^{2d_2} + x^{3d_2} + \cdots)\cdots$$

Ahora, juntando ambos resultados tenemos que:

$$\begin{aligned}
&\frac{1}{1-qx} = \prod_{i=1}^{\infty}\frac{1}{1-x^{d_1}} = \prod_{d=1}^{\infty}(\frac{1}{1-x^d})^{N_d}\\
\Rightarrow\quad &log(\frac{1}{1-qx}) = log(\prod_{d=1}^{\infty}(\frac{1}{1-x^d})^{N_d})\\
\Rightarrow\quad &\sum_{n=1}^{\infty}\frac{(qx)^n}{n} = \sum_{n=1}^{\infty}N_d\cdot log(\frac{1}{1-x^d}) = \sum_{d=1}^{\infty}N_d\sum_{j=1}^{\infty}\frac{(x^d)^j}{j}
\end{aligned}$$

El coeficiente de x^n en la serie del lado izquierdo es $\frac{q^n}{n}$. Para obtener dicho coeficiente en la serie de la derecha nos tenemos que fijar, únicamente, en los elementos de $\sum_{j=1}^{\infty} \frac{(x^d)^j}{j}$ que cumplen la condición $n = jd$, lo cual ocurre cuando $j = \frac{n}{d}$, es decir cuando $d|n$. De donde tenemos que el coeficiente de x^n es:

$$\sum_{d|n} N_d \cdot \frac{1}{n/d}$$

Juntando ambos resultados, se tiene que:

$$\frac{q^n}{n} = \sum_{d|n} N_d \cdot \frac{1}{n/d} \Rightarrow q^n = \sum_{d|n} N_d \cdot (\frac{1}{n/d})n = \sum_{d|n} N_d \cdot d$$

Aplicando la inversión de Möbius, donde $f(n) = q^n$ y $g(d) = N_d \cdot d$, se obtiene:

$$n \cdot N_n = \sum_{d|n} \mu(\frac{n}{d})q^d \Rightarrow N_n = \frac{1}{n}\sum_{d|n} \mu(\frac{n}{d})q^d$$

De esta forma hemos obtenido que el número de polinomios mónicos irreducibles de grado n, en un campo con q elementos es

$$\frac{1}{n}\sum_{d|n} \mu(\frac{n}{d})q^d$$

Otra de sus aplicaciones se relaciona con la coloración de una Gráfica. Una Gráfica G consiste de un conjunto de vértices $V(G)$, un conjunto de aristas $E(G)$ y un mapeo que le asocia a cada arista $e \in E(G)$ un par no ordenado de vértices a y b, a los que llamamos puntos extremos de e. Dada una gráfica G podemos colorear, usando un número finito de colores, sus aristas o bien los vértices. Para nuestro ejemplo consideremos una coloración de los vértices.

Diremos que una coloración de vértices es propia, si los puntos extremos de las aristas poseen colores diferentes entre sí. Entonces nos interesa saber cuántas de estas coloraciones podemos realizar en una gráfica dada.

Ejemplo 4.1.2. Número de coloraciones propias con x colores, $X_G(x)$, de una gráfica G con n vértices.

Notemos que colorear los vértices es equivalente a aplicar una función que envía los vértices de la gráfica a los distintos colores. Es decir, esta función envía particiones del conjunto de los vértices al conjunto de los colores, donde entendemos por partición a una descomposición del conjunto original en subconjuntos no vacíos disjuntos entre sí, cuya unión es exactamente el conjunto original.

Ahora tomemos una partición A de los vértices, de tal manera que cada bloque de ésta posea una conexión entre todos sus elementos. Dicha conexión puede ser de una sola arista, o bien de una unión dos o más de éstas.
Si denotamos por $g(A)$ al número de coloraciones de los vértices de G tal que cada bloque de A reciba el mismo color, entonces tenemos que

$$g(A) = x^{|A|}$$

Definamos $f(A)$ como el número de coloraciones para los cuales cada bloque posee el mismo color, pero que los puntos extremos de las aristas que conectan bloques distintos sean diferentes. Entonces podemos dar una partición B mas gruesa que A juntando aquellos bloques con el mismo color que posean una arista que los una, de tal manera que si una coloración es contada en $g(A)$ también sea contada $f(B)$. Entonces,

$$g(A) = \sum_{B \geq A} f(B)$$

y por la fórmula de inversión de Möbius obtenemos

$$f(A) = \sum_{B \geq A} \mu(A, B) g(B)$$

El número de coloraciones propias se obtiene evaluando f en la partición donde cada bloque está compuesto por un solo vértice. Es decir, si denotamos por U a dicha partición obtenemos

$$X_G(x) = \sum_{B} \mu(U, B) x^{|B|}$$

Ejemplo 4.1.3. Número de $r - tuplas$

Las $r-tupla$ son secuencia ordenada de r elementos, las cuales puede ser interpretadas como vectores de dimensión r. Ahora bien, tomando el conjunto de los números naturales, nos interesa poder dar una expresión para el número de $r-tuplas$ de la forma $(a_1, a_2, \ldots, a_r)$ tales que $a_i \leq n$ y que satisfagan $M.C.D(a_1, a_2, \ldots, a_r, n) = 1$.

Para ello denotamos por $J_r(n)$ a la cantidad de $r-tuplas$ que satisfacen dichas condiciones. Realizamos una partición del total de $r-tuplas$ de acuerdo a su máximo común divisor, es decir $d = M.C.D(a_1, a_2, \ldots, a_r, n)$. Entonces $1 = M.C.D(\frac{a_1}{d}, \frac{a_2}{d}, \ldots, \frac{a_r}{d}, \frac{n}{d})$ con cada $a_i \leq n$, de donde se obtiene que:

$$n^r = \sum_{d|n} J_r(n/d)$$

y aplicando la inversión de Möbius, donde tomamos $f(n) = n^r$ y $g(n/d) = J_r(n/d)$, resulta

$$J_r(n) = \sum_{d|n} \mu(d)(\frac{n}{d})^r$$

pero ya hemos probado que

$$\sum_{d|n} \mu(d)(\frac{n}{d}) = \varphi(n) = n \prod_{d|n} (1 - \frac{1}{p})$$

entonces tenemos que

$$J_r(n) = n^r \prod_{d|n} (1 - \frac{1}{p^r})$$

De esta forma, hemos obtenido de manera explicita una fórmula para calcular el número de las $r-tuplas$ que cumplan con las condiciones que establecimos.

4.2. Identidades de funciones

Ejemplo 4.2.1. La función de Von Mangoldt Λ

Esta función posee una estrecha relación con la función zeta de Riemman y tiene un papel central en el estudio de la distribución de los primos. Si bien estos temas son sumamente interesantes, requieren un amplio desarrollo y nuestro interés se centra solamente en mostrar una aplicación de la inversión de Möbius.

Definimos la función de Von Mangoldt, denotada por Λ, como:

$$\Lambda(n) \quad = \quad \begin{cases} log\,(p) & \text{si } n = p^a \text{ para algún } p \text{ primo y entero } a \geq 1 \\ 0 & \text{en otro caso} \end{cases}$$

Ahora tomemos un entero $n > 1$. Por el teorema fundamental de la aritmética n se puede factorizar como

$$n = \prod_{i=1}^{r} p_i^{m_i}$$

donde p_i son números primos distintos.

Ahora aplicando el logaritmo tenemos que

$$\log n = \log \left(\prod_{i=1}^{r} p_i^{m_i} \right) = \sum_{i=1}^{r} m_i \log p_i$$

Ahora analizamos la suma de los valores $\Lambda(d)$ cuando esta corre sobre todos los divisores de n. Es decir,

$$\sum_{d|n} \Lambda(d)$$

En esta suma los únicos términos distintos de cero son aquellos para los cuales los divisores son de la forma $d = p_i^m$ para $m = 1, 2, \ldots, m_i$ e $i = 1, 2, \ldots, r$. Entonces

$$\sum_{d|n} \Lambda(d) = \sum_{i=1}^{r} \sum_{m=1}^{m_i} \Lambda(p_k^m) = \sum_{i=1}^{r} \sum_{m=1}^{m_i} \log p_i = \sum_{i=1}^{r} m_i \log p_i$$

pero como ya hemos visto que $\sum_{i=1}^{r} m_i \log p_i = \log n$, entonces podemos concluir que

$$\sum_{d|n} \Lambda(d) = \log n$$

Por último, si hacemos $f(n) = n$, $g(d) = \Lambda(d)$ y aplicamos la fórmula de inversión de Möbius obtenemos:

$$\Lambda(n) = g(n) = \sum_{d|n} \mu(d) f(\frac{n}{d}) = \sum_{d|n} \mu(d) \log \frac{n}{d}$$

notemos lo siguiente:

$$\begin{aligned} \sum_{d|n} \mu(d) \log \frac{n}{d} &= \log n \sum_{d|n} \mu(d) - \sum_{d|n} \mu(d) \log d \\ &= -\sum_{d|n} \mu(d) \log d \end{aligned}$$

esto debido a que, como ya hemos visto, para $n > 1$ tenemos $\sum_{d|n} \mu(d) = 0$.

En resumen, haciendo uso de la inversión hemos obtenido una expresión para la función de Von Mangoldt dada por:

$$\Lambda(n) = \sum_{d|n} \mu(d) \log \frac{n}{d} = -\sum_{d|n} \mu(d) \log d$$

Como ya hemos visto, existe una identidad que relaciona φ de Euler con la función de μ de Möbius; sin embargo podemos utilizar la inversión de Möbius para dar una demostración alternativa de dicha identidad.

Ejemplo 4.2.2. $\varphi(n) = n \sum_{d|n} \frac{\mu(d)}{d}$

Antes de enfocarnos en la demostración de la identidad propuesta observemos que

$$\sum_{d|n} \varphi(d) = n$$

Para esto, tomemos el conjunto $S = \{1, 2, \ldots, n\}$. Distribuyamos estos enteros en conjuntos disjuntos $A(d)$, cuyos elementos son aquellos números k de S para los cuales el máximo común divisor entre k y n sea el entero d, es decir $(k, n) = 1$. Como $A(d)$ son disjuntos, entonces la unión de todos ellos es el conjunto S.

Ahora si denotamos por $C(d)$ al número de elementos de $A(d)$, entonces tenemos que

$$\sum_{d|n} C(d) = n$$

Pero sabemos que $(k, n) = d$ si y sólo si $(k/d, n/d) = 1$; de la misma manera $0 < k \leq n$ si y sólo si $0 < k/d \leq n/d$. Entonces si tomamos $q = k/d$ existe una correspondencia biyectiva entre los elementos de $A(d)$ y los números enteros q que cumple que $0 < q \leq n/k$ y $(q, n/k) = 1$. Pero el número de tales enteros q está dado por $\varphi(n/d)$. Por lo tanto $C(d) = \varphi(n/d)$ y sustituyendo esto en la igualdad que habíamos obtenido, resulta que

$$\sum_{d|n} \varphi(n/d) = n$$

Pero ésta es equivalente a $\sum_{d|n} \varphi(d) = n$, ya que cuando d corre sobre todos los divisores de n también lo hace d/n. Con esto hemos completado la demostración de esta igualdad.

Retomando nuestro problema inicial de este ejemplo, ahora sabemos que

$$\sum_{d|n} \varphi(d) = n$$

entonces tomando $f(n) = n$, $g(d) = \varphi(d)$ y aplicando la inversión de Möbius se concluye

$$\varphi(n) = g(n) = \sum_{d|n} \mu(d) f(\frac{n}{d}) = \sum_{d|n} \mu(d)(\frac{n}{d})$$

y por lo tanto queda demostrado que

$$\varphi(n) = n \sum_{d|n} \frac{\mu(d)}{d}$$

Ejemplo 4.2.3. Suma de Ramanujan

La suma de Ramanujan $c_n(m)$ está definida por:

$$c_n(m) = \sum_{\substack{1\leq h\leq n \\ (h,n)=1}} e(\frac{hm}{n})$$

donde $e(t) = e^{2\pi it}$

Comencemos haciendo que

$$g(n) = \sum_{1\leq h\leq n} e(\frac{hm}{n})$$

como esta es una suma de una progresión geométrica, podemos ver que

$$g(n) \quad = \quad \begin{cases} n & \text{si } n|m \\ 0 & \text{en otro caso} \end{cases}$$

pero podemos escribir a $g(n)$ como

$$\begin{aligned} g(n) &= \sum_{d|n} \sum_{\substack{1\leq h\leq n \\ (h,n)=d}} e(\frac{hm}{n}) \\ &= \sum_{d|n} \sum_{\substack{1\leq h_1\leq n_1 \\ (h_1,n_1)=1}} e(\frac{h_1 m}{n_1}) \end{aligned}$$

donde hemos reescrito $h = dh_1$ y $n = dn_1$. Entonces

$$g(n) = \sum_{d|n} c_{n/d}(m)$$

Aquí hacemos uso de la inversión de Möbius, utilizando $f(n/d) = c_{n/d}(m)$ y $g(n)$, y obtenemos

$$c_n(m) = \sum_{d|n} \mu(d) g(\frac{n}{d}) = \sum_{d|n} \mu(\frac{n}{d}) g(d)$$

pero $g(d)$ se anula excepto cuando $d|m$. Por lo tanto, como también sucede que $d|n$, podemos concluir

$$c_n(m) = \sum_{d|(n,m)} \mu(\frac{n}{d})d$$

Esta es la expresión de $c_n(m)$ que buscábamos. Notemos que si hacemos $m = 1$ en la identidad que encontramos, obtenemos una forma distinta de representar a $\mu(n)$

$$\mu(n) = \sum_{\substack{1\leq h\leq n \\ (h,n)=1}} e(\frac{h}{n})$$

ya que como $(n, 1) = 1$ entonces $d = 1$.

De esta manera hemos ejemplificado algunas de las distintas formas de aplicación de la fórmula de inversión de Möbius. Dicha aplicaciones muestran la gran utilidad que tiene la inversión de Möbius para resolver problemas de conteo, así como su uso como herramienta para obtener identidades alternativas de distintas funciones importantes.

Bibliografía

[1] Aigner, M., *Combinatorial Theory,* Springer-Verlag, 1997.

[2] Apostol, T. M., *Introduction to Analityc Number Theory,* Springer-Verlag, 1976.

[3] Bender, E. A.; Goldman,J.R *On the Applications of Mobius Inversion in Combinatorial Analysis,* The American Mathematical Monthly, Vol. 82, No. 8., pp. 789-803 (1975).

[4] Godsil, C. D., *An Introduction to the Moebius Function,* Combinatorics and Optimization, University of Waterloo, Waterloo Ontario.

[5] Hall, M. *Combinatorial Theory,* John Wiley and Sons, 1998.

[6] Hardy, G. H. *The general theory of Dirichlet's series,* Cornell University Library, 1915.

[7] Jastrzebska, M.; Grabowski, A., *On the properties of the Möbius function*, Formalized Mathematics, 14(1),pp. 29–36 (2006).

[8] Jones, G. A.; Jones, J. M. *Elementary Number Theory,* Springer, 1998.

[9] Rosen, K. H., *Elementary number theory and its applications,* Addison Wesley, 2005.

[10] Rota, G.-C. *On the Foundations of Combinatorial Theory: I. Theory of Möbius Inversion,* Z. Wahrscheinlichkeitstheorie 2,pp. 340-368 (1964).

[11] Sándor, J.; Crstici, B. *Handbook of number theory II,* Springer, 2004.

[12] Sándor, J.; Bege, A. *The Möbius function: generalizations and extensions,* Contemporary Mathematics, 6 (2003), 77–128.

[13] Sivaramakrishnan,R., *Classical Theory of Arithmetic Functions,* Marcell Dekker,1989.

[14] Sivaramakrishnan,R. *Certain number-theoretic episodes in algebra,* Chapman & Hall, 2007.

[15] Stanley,R.P., *Enumerative Combinatorics,* Cambridge University Press, 2002.

[16] titchmarsh,E. C. *The theory of functions,* Oxford University Press, 1952.

[17] van Lint, A. F.; Wilson, R.M. *A course in combinatorics,* Cambridge University Press, 2001.

[18] van Lint, J. *Combinatorial theory seminar, Eindhoven University of Technology,* Springer-Verlag, 1974.