UNIVERSITAT JAUME I

Grado en Matemática Computacional

Trabajo Final de Grado

Transformadas discretas de Fourier y el teorema de Dirichlet

Autor:
Daniel Soler Littleales

Tutor académico:
Jorge Galindo Pastor

Fecha de lectura: 10 de Julio de 2022
Curso académico 2021/2022

Resumen

En este trabajo vamos a recoger la información adquirida a lo largo del Grado en Matemática Computacional para realizar un estudio sobre el uso de la transformada de Fourier discreta en la demostración de la existencia de progresiones aritméticas formadas por números primos Necesitamos para ello introducir la dualidad entre un grupo abeliano finito y su grupo de caracteres.

En primer lugar abordaremos brevemente el desarrollo histórico de las diferentes aproximaciones de los números primos, terminando con la demostración de Euler. Este será el pilar que nos permitirá explicar el teorema de Dirichlet. Terminamos el trabajo identificando los res problemas principales que presenta la demostración de Dirichlet.

Palabras clave

Grupos abelianos, caracteres, función zeta, caracteres de Dirichlet, funciones L de Dirichlet

Keywords

Abelian Groups, characters, zeta function, Dirichlet Character's, Dirichlet L-functions

Índice general

Capítulo 1

Introducción

1.1. Contexto y motivación del proyecto

Este proyecto representa el Trabajo de Final de Grado en el Grado en Matemática Computacional. Cuyo objetivo es poner en práctica los conocimientos adquiridos a lo largo del grado e introducir al estudiante al área de la investigación matemática a un nivel académico.

El trabajo está basado en el libro escrito por los coautores E.M. Stein y R.Shakarchi [6] sobre el análisis de Fourier y sus varias aplicaciones a otras ramas de las matemáticas. Nos centraremos en profundizar los resultados obtenidos por P.G Lejeune Dirichlet en la aplicación de series de Fourier sobre progresiones aritméticas.

1.2. Estructura del TFG

Primero, para estudiar la series de Fourier finitas, necesitaremos una introducción a los grupos abelianos finitos, especialmente el grupo $\mathbb{Z}(N)$. Luego, necesitaremos entender el concepto de carácter, centrándonos en los caracteres sobre el grupo $\mathbb{Z}(N)$ que nos proporcionará una base ortonormal para el espacio vectorial V de funciones complejas sobre $\mathbb{Z}(N)$. Estos caracteres, serán fundamentales a la hora de definir la serie de Fourier sobre una función $f \in V$.

En el siguiente capítulo, introduciremos el estudio de la infinitud de los primos. Para ello, primero, necesitamos conocer unos conceptos básicos sobre la teoría elemental de números, en específico queremos llegar al teorema fundamental de la aritmética. Seguidamente, estudiaremos los resultados obtenidos por Euler remarcando la importancia de la función ζ y el producto de

Euler. Para finalizar, estudiaremos los caracteres y las funciones L de Dirichlet y nos centraremos en los tres aspectos más complicados de tratar a la hora de demostrar el teorema de Euler.

Capítulo 2

Análisis de Fourier finito

En este apartado vamos a estudiar la transformada de Fourier para el grupo de N raíces de unidad. Es uno de los grupos más fáciles de estudiar ya que parte la circunferencia de unidad en N partes iguales, lo que nos interesa para aplicar la teoría de Fourier más adelante. Cabe remarcar que a medida que N tiende a infinito la partición del circulo es menor, de manera que esperamos que la teoría discreta de Fourier tiende a la teoría continua de las series de Fourier en la circunferencia.

2.1. El grupo $\mathbb{Z}$(N)

Sea N un entero positivo y z un número complejo. Decimos que z es una N-ésima raíz de unidad si $z^N = 1$. El conjunto de las raíces N-ésimas de las unidades:

$$\{1, e^{2\pi i/N}, e^{2\pi i 2/N}, ..., e^{2\pi i(N-1)/N}\}$$

Definimos $\zeta = e^{2\pi i/N}$ y nos encontramos con que ζ^k nos proporciona todas las N raíces de unidad.

Proposición 1. *$\zeta^n = \zeta^m$ si y solo si $n - m$ es divisible por N*

Demostración. Suponemos que $\zeta^n = \zeta^m$. Eso significa que

$$\frac{\zeta^m}{\zeta^n} = 1$$

o sea

$$\zeta^{(m-n)} = 1$$

Pero esta igualdad solo se cumple si $m - n$ es múltiplo de N, $m - n = aN$, ya que $\zeta^{aN} = 1$ con $a \in \mathbb{Z}$.
Ahora suponemos que $m - n$ es divisible por N, por lo tanto $m - n = aN$ con $a \in \mathbb{Z}$. Podemos reescribir $n = aN + m$. Y tenemos que:

$$\zeta^n = \zeta^{aN+m}$$

por la propiedad de los exponentes

$$\zeta^n = \zeta^{aN}\zeta^m = 1\zeta^m = \zeta^m$$

□

Corolario 1.1. *Las raíces N-ésimas de 1 son*

$$\{1, \zeta, \ldots, \zeta^{N-1}\}$$

Demostración. Aplicando la proposición 1 vemos que para todo $k > N$ $\zeta^k = \zeta^{K-N}$y por lo tanto solo hay N raíces de unidad que corresponden a ζ^k con $0 \leq k \leq N - 1$. □

Definición 1.1. *Denotamos al conjunto de N raíces de unidad como $\mathbb{Z}(N)$. Este conjunto cumple las siguientes propiedades:*

(i) *Si $z, w \in \mathbb{Z}(N)$, entonces $zw \in \mathbb{Z}(N)$ y $zw = wz$*

(ii) $1 \in \mathbb{Z}(N)$

(iii) *Si $z \in \mathbb{Z}(N)$, entonces $z^{-1} = 1/z \in \mathbb{Z}(N)$ y $zz^{-1} = 1$*

Demostración. Demostramos cada propiedad individualmente

(i) Sean $z, w \in \mathbb{Z}(N)$ son de la forma ζ^k con $k \in \mathbb{Z}$. Escribimos $z = \zeta^a$ y $w = \zeta^b$ y tenemos que $\zeta^a\zeta^b = \zeta^{a+b} \in \mathbb{Z}(N)$ ya que $a + b \in \mathbb{Z}$ y $\zeta^a\zeta^b = \zeta^{a+b} = \zeta^{b+a} = \zeta^b\zeta^a$.

(ii) Si escogemos $k = 0$, $\zeta^0 = e^{2\pi i 0/N} = e^0 = 1$

(iii) Dado $z \in \mathbb{Z}(N)$ escribimos $z = \zeta^a$ y definimos $z^{-1} = 1/z = \zeta^{-a} \in \mathbb{Z}(N)$. Multiplicando ambos nos encontramos con que $zz^{-1} = \zeta^a\zeta^{-a} = \zeta^0 = 1$

□

Por las 3 propiedades de arriba concluimos que el grupo $\mathbb{Z}(N)$ dotado de la multiplicación de complejos tiene estructura de grupo abeliano.

Dado dos enteros x e y, decimos que son congruentes módulo N, si la diferencia $x - y$ es múltiplo de N y lo escribimos como $x \equiv y \mod (N)$ si se cumplen las siguientes 3 propiedades:

1. $x \equiv x \mod N$ para todos los enteros x
2. si $x \equiv y \mod N$ entonces $y \equiv x \mod N$
3. Si $x \equiv x \mod N$ y $y \equiv z \mod N$ entonces $x \equiv z \mod N$

Como se puede observar, las propiedades de arriba representan las relaciones reflexiva, simétrica y transitiva respectivamente. Por lo tanto la clase módulo es una relación de equivalencia en $\mathbb{Z}$. Definiremos la clase de equivalencia o grupo cociente del entero x como $R(x)$. Es decir, un elemento perteneciente a $R(x)$ si es de la forma $x + kN$ con $k \in \mathbb{Z}$. En total tendremos N clases de equivalencia uno por cada entero entre 0 y $N - 1$. Ahora pasaremos a definir la suma de clases de equivalencia como:

$$R(x) + R(y) = R(x + y)$$

Cabe indicar que esta definición es independiente de las representates que escojamos, ya que si cogemos $x' \in R(x)$ e $y' \in R(y)$ tenemos que

$$x' + kN + y' + kN = x' + y' + 2kN = x' + y' + kN \in R(x + y)$$

Esto convierte la clase de relaciones de equivalencia en un grupo abeliano llamado grupo de enteros módulo N, que a veces se escribe como $\mathbb{Z}/N\mathbb{Z}$. Ahora, podremos hacer la correspondencia entre los dos grupos abelianos que hemos descrito hasta ahora $\mathbb{Z}(N)$ y $\mathbb{Z}/N\mathbb{Z}$. Las operaciones se traducen entre los grupos ya que la suma de enteros modulo N se convierte en la multiplicación de números complejos.

Lema 1.1. *El grupo cociente $\mathbb{Z}/N\mathbb{Z}$ es isomorfo a $\mathbb{Z}(N)$.*

Demostración. Tenemos que encontrar un homomorfismo biyectivo entre los dos grupos. Sea $f : \mathbb{Z}(N) \to \mathbb{Z}/N\mathbb{Z}$ tal que $f(\zeta^n) = n$

$$f(\zeta^n \zeta^m) = f(\zeta^{n+m}) = n + m = f(n) + f(m)$$

Definimos $f' : \mathbb{Z}/N\mathbb{Z} \to \mathbb{Z}(N)$ tal que $f'(n) = \zeta^n$

$$f'(n + m) = \zeta^{n+m} = \zeta^n \zeta^m = f'(n) f'(m)$$

Hemos encontrado un homomorfismo biyectivo entre los dos grupos, por lo tanto $\mathbb{Z}(N) \approx \mathbb{Z}/N\mathbb{Z}$. □

Ahora, pasaremos a entender la correspondencia anterior como funciones de espacios vectoriales, es decir, si tenemos V y W los espacios vectoriales de funciones complejas en los grupos de enteros modulo N y de las N raíces de unidad, respectivamente. Tenemos que:

$$F(k) \leftrightarrow f(e^{2\pi ik/N})$$

Para resumir, de ahora en adelante cuando escribimos $\mathbb{Z}(N)$ se puede entender como el grupo de enteros modulo N o como el grupo de N raíces de unidad.

2.2. El teorema de la inversión de Fourier y la identidad de Plancherel en $\mathbb{Z}(N)$

Antes de comenzar con esta sección, tenemos que describir el conjunto de funciones complejas sobre el grupo $\mathbb{Z}(N)$ que lo denotaremos como $F(\mathbb{Z}(N), \mathbb{C})$ es decir, son las funciones que actúan sobre $\mathbb{Z}(N)$ y la imagen está en $\mathbb{C}$.

2.2.1. Estructura geométrica de $F(\mathbb{Z}(N), \mathbb{C})$

En este apartado, queremos ver el conjunto de funciones complejas $F(\mathbb{Z}(N), \mathbb{C})$ es de hecho un espacio vectorial sobre $\mathbb{Z}(N)$. Esto se puede ver claramente, si vemos una función $f \in \mathbb{C}^N$ como un vector de dimensión N. Es decir, dado una función $f \in \mathbb{C}^n$ sobre $\mathbb{Z}(N)$ la función puede tomar N valores distintos, $(f(1), f(\zeta^1), f(\zeta^2), \ldots, f(\zeta^{N-1}))$. Por lo tanto, decimos que $F(\mathbb{Z}(N), \mathbb{C})$ es un espacio vectorial con operación interna $\langle F, G\rangle \in F(\mathbb{Z}(N), \mathbb{C})$, y operación externa multiplicación de vectores por escalares, $\mathbb{Z}(N)$, $a \cdot F \in F(\mathbb{Z}(N), \mathbb{C})$, con $a \in \mathbb{C}$.

Definimos la operación interna, producto Hermitiano interior, del espacio vectorial como:

$$\langle F, G\rangle = \sum_{k=0}^{N-1} F(k)\overline{G(k)}$$

y con la norma asociada

$$\|F\|^2 = \sum_{k=0}^{N-1} |F(k)|^2$$

Una vez hemos introducido el espacio vectorial, podemos pasar a desarrollar el análisis de Fourier en $\mathbb{Z}(N)$ vamos a tener que trabajar con los exponentes $e_n = e^{2\pi inx}$ ya que estos harán de coeficientes en las series de Fourier más en adelante. Por lo tanto, nuestro objetivo es encontrar las funciones que correspondan a dichos exponentes. Las propiedad más importante de las funciones $e_n : [0, 1] \to \Pi$ es

$$e_n(x + y) = e_n(x)e_n(y)$$

Lema 1.2. *El conjunto* $\{e_0, ..., e_{N-1}\}$ *es ortogonal. De hecho:*

$$\langle e_m, e_l \rangle = \begin{cases} N & si \quad m = l \\ 0 & si \quad m \neq l \end{cases}$$

Demostración. Tenemos que

$$\langle e_m, e_l \rangle = \sum_{k=0}^{N-1} \zeta^{mk} \zeta^{-lk} = \sum_{k=0}^{N-1} \zeta^{(m-l)k}$$

Si $m = l$ todos los términos serán igual a $\zeta^0 = 1$ y como es la suma de N términos, el resultado será N. En cambio, si $m \neq l$ entonces poniendo $q = \zeta^{(m-l)k}$ es distinto a 1 y la suma será:

$$1 + q + q^2 + ... + q^{N-1} = \frac{1 - q^N}{1 - q}$$

Como $q^N = 1$ obtenemos que el resultado es 0. □

Lema 1.3. *El conjunto* $e_0, \ldots, e_{N-1}$ *son linealmente independientes.*

Demostración. Definimos $v \in V$ como

$$v = \sum_{i=0}^{N-1} \alpha_i e_i = 0$$

Escogemos j con $0 \leq j < N$ y hacemos el producto interior $\langle v, e_j \rangle$ que será igual a 0 ya que $v = 0$. Por otro lado, utilizando el producto interior descrito tenemos que

$$\langle v, e_j \rangle = \sum_{i=0}^{N-1} \alpha_i \langle e_i, e_j \rangle$$

Como $\{e_0, \ldots, e_{N-1}\}$ forman una base ortonormal, el resultado de $\langle e_i, e_j \rangle = 0$ excepto cuando $i = j$ que el resultado será distinto de 0 eso implica que $\alpha_j = 0$. Repetimos este argumento para todo valor posible de j y llegamos a la conclusión que $\alpha_j = 0$ para todo $0 \leq j < N$ y por lo tanto los elementos de la base $\{e_0, \ldots, e_{N-1}\}$ son linealmente independientes □

Lema 1.4. *La dimensión del espacio vectorial* $F(\mathbb{Z}(N), \mathbb{C})$ *es* N.

Demostración. Si tomamos las funciones como vectores de números complejos, es decir, dada $f \in F(\mathbb{Z}(N), \mathbb{C})$ tenemos que $f : \mathbb{Z}(N) \to \mathbb{C}$ donde a cada elemento $\zeta \in \mathbb{Z}(N)$ le asigna un valor $f(\zeta) \in \mathbb{C}$, f solo podrá tomar N valores distintos. Ahora definimos el conjunto, $\{\alpha_0, \alpha_1, \ldots, \alpha_{N-1}\}$ de funciones en el espacio vectorial, $\alpha_i : \mathbb{Z}(N) \to \mathbb{C}$ tal que

$$\alpha_i(n) = \begin{cases} 1 & \text{si } n = \zeta^i \\ 0 & \text{resto de valores de } \mathbb{Z}(N) \end{cases}$$

es fácil comprobar que son linealmente independientes. Dada $f \in F(\mathbb{Z}(N), \mathbb{C})$ una función cualquiera podemos escribirla como $f(n) = a_0\alpha_1(n) + a_1\alpha_1(n) + \cdots + a_{N-1}\alpha_{N-1}(n)$ con $a_i \in \mathbb{C}$. El conjunto $\{\alpha_0, \alpha_1, \ldots, \alpha_{N-1}\}$ es un sistema generador de $F(\mathbb{Z}(N), \mathbb{C})$ y linealmente independiente por lo tanto es una base del espacio vectorial $F(\mathbb{Z}(N), \mathbb{C})$ de dimensión N. □

Como el conjunto $\{e_0, ..., e_{N-1}\}$ es linealmente independiente y de dimensión N forma una base ortogonal del espacio vectorial $F(\mathbb{Z}(N), \mathbb{C})$. Además, por el lema 1.2 se deduce que cada vector de dicho espacio tendrá norma igual a $\sqrt{N}$, definimos:

$$e_l^* = \frac{1}{\sqrt{N}} e_l$$

así tenemos el nuevo conjunto $\{e_0^*, ..., e_{N-1}^*\}$ que forma una base ortonormal de $F(\mathbb{Z}(N), \mathbb{C})$. Por lo tanto, cualquier $F \in F(\mathbb{Z}(N), \mathbb{C})$ será combinación lineal de nuestra base ortonormal

$$F = \sum_{n=0}^{N-1} \langle F, e_n^* \rangle e_n^* \quad y \quad ||F||^2 = \sum_{n=0}^{N-1} |\langle F, e_n^* \rangle|^2 \tag{2.1}$$

Definición 1.2. *Definimos el n-ésimo* ***coeficiente de Fourier*** *de F como:*

$$\hat{f}(n) = \langle f, e_n \rangle$$

Entonces, tenemos que la ***serie de Fourier*** *de F es*

$$F = \sum_{n=0}^{N-1} \hat{f}(n) e_n$$

Ahora pasamos a estudiar los dos teoremas más importantes de esta sección

Teorema 1.1 (**Teorema de inversión de Fourier**). *Si $F \in F(\mathbb{Z}(N), \mathbb{C})$ es una función en $\mathbb{Z}(N)$, entonces*

$$F(k) = \sum_{n=0}^{N-1} f(n) e^{2\pi i n k/N}$$

con

$$\hat{f}(n) = \frac{1}{N} \sum_{k=0}^{N-1} F(k)\overline{e_n}$$

Demostración. Primero de todo tenemos que

$$\hat{f}(n) = \langle F, e_n \rangle = \frac{1}{N} \sum_{k=0}^{N-1} F(K)\overline{e_n}$$

esto se cumple gracias al producto interior definido. Esta igualdad se conoce como la **transformada inversa de Fourier discreta**. Podemos reescribir la serie de Fourier como

$$F = \sum_{n=0}^{N-1} \hat{f}(n)e_n = \sum_{n=0}^{N-1} \langle f, e_n \rangle e_n$$

que como podemos observar es igual a la ecuación 2.1 y por lo tanto la serie evaluada en k es igual a

$$F(k) = \sum_{n=0}^{N-1} \hat{f}(n)e_n(k) = \sum_{n=0}^{N-1} \hat{f}(n)e^{2\pi ink/N}$$

Resumiendo, lo que acabamos de ver es que la función F es igual a su serie de Fourier y por lo tanto podemos encontrar los valores de F para un cierto punto k gracias la la transformada inversa de Fourier. □

Teorema 1.2 (**Teorema de Plancherel**). *El cuadrado de una función $F \in F(\mathbb{Z}(N), \mathbb{C})$ es igual a la suma del cuadrado de su transformada.*

$$\sum_{n=0}^{N-1} |a_n|^2 = \frac{1}{N} \sum_{k=0}^{N-1} |F(k)|^2$$

Demostración. Tenemos que $\sum_{n=0}^{N-1} |a_n|^2 = ||a_n||^2 = \langle a_n, a_n \rangle$ vamos a desarrollar el producto

$$\begin{aligned}
\langle a_n, a_n \rangle &= \frac{1}{N} \langle \sum_{k=0}^{N-1} F(K)\overline{e_n}, \sum_{k=0}^{N-1} F(K)\overline{e_n} \rangle \\
&= \frac{1}{N} \langle \langle F(k), e_0 \rangle e_0, \langle F(k), e_0 \rangle e_0 \rangle + \cdots + \frac{1}{N} \langle \langle F(k), e_{N-1} \rangle e_{N-1}, \langle F(k), e_{N-1} \rangle e_{N-1} \rangle \\
&= \frac{1}{N} |\langle F(k), e_1 \rangle|^2 + \cdots + \frac{1}{N} |\langle F(k), e_{N-1} \rangle|^2 \\
&= \frac{1}{N} \sum_{k=0}^{N-1} |F(k)|^2
\end{aligned}$$

□

2.3. Análisis de Fourier en grupos finitos

Una vez hemos estudiado el análisis de Fourier y hemos definido el grupo finito $\mathbb{Z}(N)$. Ahora nos toca describir el análisis de Fourier para grupos abelianos finitos. Estudiáremos los caracteres, que juegan el mismo papel que los exponenciales $e_0, ..., e_{N-1}$ en el grupo $\mathbb{Z}(N)$ y nos

darán paso a desarrollar el teorema de grupos abelianos arbitrarios finitos. Si logramos demostrar que de hecho hay un número finito de caracteres, N caracteres, podremos relativamente fácil encontrar el teorema finito de Fourier deseado. Para empezar a definir los caracteres necesitamos una breve introducción sobre la teoría de grupos finitos abelianos.

2.3.1. Homomorfismo

Un **homomorfismo** es un mapa entre dos grupos abelianos $(G, \cdot)$ y $(H, *)$, $f : G \to H$ que cumple la siguiente propiedad:

$$f(a \cdot b) = f(a) * f(b)$$

Como se puede observar en el lado izquierdo de la igualdad tenemos la operación interna del grupo G y en el derecho la del grupo H. Los homomorfismos son funciones que preservan las operaciones de grupo. Además, decimos que dos grupos G y H son **isomorfos** si existe otro homomorfismo $f' : H \to G$, de manera que para todo$a \in G$ y $b \in H$

$$(f' \circ f)(a) = a$$

y

$$(f \circ f')(b) = b$$

Es decir, existe un homomorfismo biyectivo entre G y H, y se expreso como $G \approx H$. Cabe destacar que los grupos isomorfos describen el mismo objeto ya que como hemos mencionado antes, los homomorfismos preservan la estructura interna del grupo aunque la representación particular de cada uno sea distinta.

Nosotros nos centrarnos en grupos finitos abelianos. Denotamos el **orden del grupo** como $|G|$ que indica el número de elementos de G. Ahora pasaremos a estudiar los grupos que más nos interesan para la demostración del teorema de Dirichlet.

2.3.2. El grupo $\mathbb{Z}^*(q)$

Dado q un entero positivo $\mathbb{Z}(q)$ tiene dos operaciones que le dota con estructura de anillo, $(\mathbb{Z}(q), +, \cdot)$. Llamamos **unidad** a los elementos que tienen inversa respecto multiplicación en el anillo. Es decir, $n \in \mathbb{Z}(q)$ es una **unidad** si existe $m \in \mathbb{Z}(q)$ tal que:

$$nm \equiv 1 \quad \text{mód } q$$

Denotamos el conjunto de unidades de $\mathbb{Z}(q)$ como $\mathbb{Z}^*(q)$. Otra manera de ver el grupo de unidades, es como los elementos de $\mathbb{Z}(q)$ que son primos respecto de q, es decir, $m.c.d(a, q) = 1$ para todo $a \in \mathbb{Z}^*(q)$. Esto es debido a que dos números enteros a y q son coprimos si a tiene

inverso para el producto módulo q. Es decir, existe $b \in \mathbb{Z}$ tal que $ab \equiv 1 \mod q$ que es justamente la definición de unidad. Un ejemplo de grupo de unidad:
Dado el grupo $\mathbb{Z}(5) = \{0, 1, 2, 3, 4\}$ el grupo de unidad correspondiente sería

$$\mathbb{Z}^*(5) = \{1, 2, 3, 4\}$$

Como podemos ver, tenemos que $1 \equiv 1 \mod 5$, $2 \cdot 3 \equiv 1 \mod 5$ y $4 \cdot 4 \equiv 1 \mod 5$

2.3.3. Caracteres

Finalmente, una vez introducido algunos conceptos básicos de teoría de grupos finitos, podemos introducir los **caracteres**.

Sea G un grupo finito abeliano con multiplicación y sea S^1 la circunferencia unidad en el plano de los complejos. Decimos que un carácter de G es una función compleja $e : G \to S^1$ que satisface la siguiente condición:

$$e(a \cdot b) = e(a) \cdot e(b)$$

Como se puede observar, el carácter cumple la condición de homomorfismo. Por lo tanto, podemos decir que un carácter es un homomorfismo entre G y S^1. Gracias a que los caracteres cumplen la propiedad multiplicativa, generalizan la identidad entre las funciones exponenciales en S^1, $e_l : \mathbb{Z}(\mathbb{N}) \to \mathbb{C}$, y la propiedad:

$$e_l(k + m) = e_l(k)e_l(m)$$

que se cumplían para las funciones exponenciales $e_0, ..., e_{N-1}$ en la teoría de Fourier en $\mathbb{Z}(N)$. De hecho, las funciones $e_0, ..., e_{N-1}$ son todos los caracteres del grupo $\mathbb{Z}(N)$ no hay más.

Teorema 1.3. *Solo existen N caracteres sobre el grupo $\mathbb{Z}(N)$ que son exactamente las funciones exponenciales e_j para $0 \leq j \leq N - 1$.*

Demostración. Tenemos

$$\mathbb{Z}(N) = \{1, \zeta, ..., \zeta^{N-1}\}$$

es decir esta generado por

$$\zeta = e^{2\pi i/N}$$

Si existen dos caracteres e y χ tal que $e(\zeta) = \chi(\zeta)$ entonces $e = \chi$. Esto es debido a que por la propiedad multiplicativa

$$e(\zeta^k) = e(\zeta)e(\zeta)...e(\zeta) = e(\zeta)^k = \chi(\zeta)^k$$

para $k \in \mathbb{Z}$ entonces tenemos que $e(\zeta^k) = \chi(\zeta^k)$ esto implica que $e = \chi$. Es más, como $e(\zeta) = \zeta^j = e_j$ para algún j con $0 \leq j \leq N-1$ y como acabamos de ver no se pueden repetir caracteres, solo existen $N - 1$ de ellos que son justamente $\{e_0, e_1, \ldots, e_{N-1}\}$. □

Definición 1.3. *Sea G un grupo finito abeliano, denotamos por $\widehat{G}$ el conjunto de todos los caracteres de G, que hereda la estructura de un grupo abeliano.*

Lema 1.5. *El conjunto $\widehat{G}$ es un grupo abeliano bajo multiplicación definida por:*

$$(e_1 \cdot e_2)(a) = e_1(a)e_2(a) \quad \forall a \in G$$

Llamamos a $\widehat{G}$ el grupo dual de G.

Demostración. Hay que ver que el grupo $\widehat{G}$ cumple las 4 propiedades de la estructura de grupos abelianos.
Asociatividad: Dados $e_1, e_2, e_3 \in \widehat{G}$, $e_1(a) \cdot (e_2 \cdot e_3)(a) = e_1(a) \cdot e_2(a) \cdot e_3(a) = (e_1 \cdot e_2)(a) \cdot e_3(a)$.
Identidad: La identidad de este grupo es el carácter trivial e_0 tal que para cada $a \in G$, $e_0(a) = 1$.
Inversa: Dado $e \in \widehat{G}$ tenemos que su inversa es $e^{-1} = \frac{1}{e}$ ya que $(e \cdot e^{-1})(a) = \frac{e(a)}{e(a)} = e_0(a)$ solo falta ver que $e^{-1} \in \widehat{G}$, Dados $a, b \in G$ se cumple que $e^{-1}(ab) = \frac{1}{e(ab)} = \frac{1}{e(a)}\frac{1}{e(b)} = e^{-1}(a)e^{-1}(b)$ y $|e^{-1}(a)| \leq 1$ para todo $a \in G$.
Conmutabilidad: Dados $e_1, e_2 \in \widehat{G}$ tenemos que $(e_1 \cdot e_2)(a) = e_1(a)e_2(a) = e_2(a)e_1(a) = (e_1 \cdot e_2)(a)$ ya que los valores de $e_1(a)$ y $e_2(a)$ están en $\mathbb{C}$. □

Por ejemplo, en nuestro caso, si tomamos $G = \mathbb{Z}(N)$, los caracteres de $\widehat{G}$ serán los mencionados anteriormente $e_0, ..., e_{N-1}$ que tomarán los valores $e_l(K) = e^{2\pi ilk/N}$ con $0 \leq l \leq N-1$.

Lema 1.6. *Los grupos $\widehat{\mathbb{Z}(N)}$ y $\mathbb{Z}(N)$ son isomorfos*

Demostración. Tenemos que encontrar un homomorfismo biyectivo entre los dos grupos. Definimos una función $f : \widehat{\mathbb{Z}(N)} \to \mathbb{Z}(N)$ tal que $f(e_l) = l$ donde $e_l(k) = \zeta^{lk}$. Entonces tenemos que

$$f(e_l \cdot e_k) = f(\zeta^l \zeta^k) = f(\zeta^{l+k}) = l + k = f(e_l) + f(e_k)$$

Ahora, si definimos $f' : \mathbb{Z}(N) \to \widehat{\mathbb{Z}(N)}$ tal que $f'(l) = e_l$ podemos ver que $f'(l+k) = e_{l+k} = \zeta^{l+k} = f'(l)f'(k)$. □

Lema 1.7. *Sea G un grupo finito abeliano, y $e : G \to \mathbb{C}\backslash\{0\}$ una función multiplicativa, tal que $e(a \cdot b) = e(a)e(b)$ $\forall a, b \in G$. Entonces, e es un carácter.*

Demostración. Como G es un grupo finito, tenemos que la función compleja e esta acotada por abajo y por arriba cuando va tomando valores $e(a)$ con $a \in G$. Asimismo, como $e(a \cdot b) = e(a)e(b)$ tenemos que $|e(a)^n| = |e(a)| \cdot |e(a)| \cdot ... \cdot |e(a)| = |e(a)|^n$. Como $|e(a)^n| = |e(a)|^n$ lo que implica que $|e(a)| = 1$ para todo $a \in G$. Por lo que podemos concluir que, $e(a) \in S^1$ para todo $a \in G$ □

Ahora, queremos ver que los caracteres forman una base ortonormal para el espacio vectorial $F(G,\mathbb{C})$ de las funciones sobre G. En concreto queremos ver que los caracteres sobre el grupo $\mathbb{Z}(N)$ que son $e_0, ..., e_{N-1}$ forman la base ortonormal del espacio vectorial $F(\mathbb{Z}(N),\mathbb{C})$. Para el caso general, tenemos que observar que habrán un número suficiente de caracteres que será igual al orden del grupo.

2.3.4. Las relaciones ortogonales

Sea $F(G,\mathbb{C})$ el espacio vectorial de funciones complejas sobre un grupo abeliano finito G, por el lema 1.4 la dimensión del espacio vectorial $F(G,\mathbb{C})$ es igual al orden del grupo $|G|$. Definimos, un producto Hermitiano interior en $F(G,\mathbb{C})$ como:

$$\langle f, g\rangle = \frac{1}{|G|}\sum_{a\in G} f(a)\overline{g(a)}$$

cuando $f, g \in F(G,\mathbb{C})$.

Teorema 1.4. *Los caracteres de G forman una familia ortonormal con respecto el producto interior recién definido.*

Demostración. Para comprobar que los caracteres forman una familia ortonormal se tiene que cumplir que: $\langle e, e\rangle = 1$ y $\langle e, e^{'}\rangle = 0$ con $e \neq e^{'}$. Primero vamos a comprobar que $\langle e, e\rangle = 1$. Por la demostración del lema anterior sabemos que $|e(a)| = 1$ para todo $a \in G$ por lo tanto,

$$\langle e, e\rangle = \frac{1}{|G|}\sum_{a\in G} e(a)\overline{e(a)} = \frac{1}{|G|}\sum_{a\in G} |e(a)|^2 = \frac{1}{|G|}(1+1+...+1) = \frac{|G|}{|G|} = 1$$

Para demostrar la segunda parte tenemos que introducir el siguiente lema.

Lema 1.8. *Si e es un carácter no trivial del grupo G, entonces* $\sum_{a\in G} e(a) = 0$.

Demostración. Sea $b \in G$ tal que $e(b) \neq 1$. Entonces tenemos que

$$e(b)\sum_{a\in G} e(a) = \sum_{a\in G} e(b)\overline{e(a)} = \sum_{a\in G} e(ab) = \sum_{a\in G} e(a)$$

Hay que tener en cuenta que $b \in G$ y $a \in G$ por lo tanto $ab \in G$ y como hemos definido $e(b) \neq 1$ esta igualdad solo se puede cumplir si $\sum_{a\in G} e(a) = 0$. □

Ahora, supongamos que e' es un carácter distinto de e como $e(e')^{-1}$ es un carácter no trivial por el lema 1.8, tenemos que:

$$\langle e, e'\rangle = \frac{1}{|G|}\sum_{a\in G} e(a)(e'(a))^{-1} = \frac{1}{|G|}\sum_{a\in G} e(e')^{-1}(a) = 0$$

□

Como los caracteres forman una base ortonormal tenemos que son linealmente independientes. Asimismo, como la dimensión de $F(G,\mathbb{C})$ sobre $\mathbb{C}$ es $|G|$ se tiene que el orden del grupo dual de G, $\widehat{G}$, será menor o igual al orden de G, $|\widehat{G}| \leq |G|$. Por último, vamos a comprobar que de hecho $|\widehat{G}| = |G|$.

2.3.5. Caracteres como una familia total

Primero tenemos que introducir unos conceptos que nos serán útiles más adelante. En particular las transformaciones unitarias, que nos darán una aplicación ideal en $F(G,\mathbb{C})$ para definir los caracteres.

Definición 1.4 (**Transformaciones unitarias**). *Supongamos que V es un espacio vectorial de dimensión d con producto interior $(\cdot,\cdot)$. Decimos que una transformación $T : V \to V$ es unitaria si conserva el producto interior, es decir, $(Tv, Tw) = (v, w) \quad \forall v, w \in V$.*

Proposición 2. *Toda transformación unitaria es diagonalizable por lo tanto existe una base $\{v_1, ..., v_d\}$ de V tal que $T(v_i) = \lambda_i v_i$ donde $\lambda_i \in \mathbb{C}$. Llamamos a $\{v_1, ..., v_d\}$ valores propios y a los λ_i los vectores propios asociados a cada v_i*

Proposición 3. *Sea M_T la matriz diagonal asociada a la transformación unitaria T entonces,*

$$M_T M_T^t = I_d$$

donde M_T^t es la matriz transpuesta de M_T y I_d es la matriz identidad de dimensión d.

Lema 3.1 (**Teorema de descomposición espectral**). *Existe una base ortonormal de V que consiste en los vectores propios de T. La descomposición espectral de una transformación T con una base ortonormal de vectores propios, se obtiene agrupando los vectores que correspondes al mismo valor propio. A estos subespacios los denotaremos como V_λ. Donde*

$$V_\lambda = \{v \in V : T(v) = \lambda v\}$$

Como consecuencia de esto tenemos el teorema de descomposición espectral que dicta lo siguiente: V es la suma directa ortogonal de los espacios V_λ

$$V = V_{\lambda_1} \oplus \cdots \oplus V_{\lambda_s}$$

Referencias: [2] y [5].

Una vez conocemos lo que son las transformaciones unitarias podemos pasar al teorema importante de este apartado, que nos dará acceso a encontrar una base ortonormal de nuestro espacio vectorial $F(G,\mathbb{C})$.

Teorema 3.1. *Los caracteres de un grupo finito abeliano forman una base del espacio vectorial de las funciones en G.*

Demostración. La demostración de este teorema se basa en el siguiente lema.

Lema 3.2. *Supongamos que $\{T_1, .., T_k\}$ es una familia conmutativa de transformaciones unitarias en el espacio finito V, es decir:*

$$T_i T_j = T_j T_i$$

Entonces $T_1, .., T_k$ son diagonalizables simultáneamente, existe una base de V que consiste de vectores propios para cada $T_i, i = 1, ..., k$

Demostración. Lo demostraremos por inducción sobre k. El caso $k = 1$ queda demostrado por el teorema de descomposición espectral.

Suponemos que el teorema es cierto para cualquier familia de $k-1$ transformaciones unitarias conmutativas. Ahora aplicamos el teorema de descomposición espectral a T_k y tenemos que

$$V = V_{\lambda_1} \oplus \cdots \oplus V_{\lambda_s}$$

donde $V_{\lambda_i} = \{v \in V : \lambda_i v = T_k(v)\}$ es el subespacio de todos los vectores propios de T_k con valor propio asociado λ_i. Por lo tanto, hemos encontrado una base de $F(G, \mathbb{C})$ formado por vectores propios asociados a T_k. Comprobamos ahora que cada una de las $T_1, \ldots, T_{k-1}$ envía cada subespacio V_{λ_i} a si mismo $T_j : V_{\lambda_i} \to V_{\lambda_i}$. Es decir, para cada $v \in V_{\lambda_i}$, $T_j(v) \in V_{\lambda_i}$ con $1 \leq j \leq k-1$, efectivamente por que:

$$T_k(T_j(v)) = T_k T_j(v) = T_j T_k(v) = T_j(T_k(v)) = T_j(\lambda_i v) = \lambda_i T_j(v)$$

Definimos la aplicación S_j como la restricción de cada T_j a V_{λ_i} con $1 \leq j \leq k-1$, $S_j : V_{\lambda_i} \to V_{\lambda_i}$, que como acabamos de demostrar son unitarias. Entonces, tenemos una familia $S_1, S_2, \ldots, S_{k-1}$ de transformaciones unitarias restringidas a cada subespacio V_{λ_i}. Aplicando la hipótesis de inducción existe una base de V_{λ_i} formada por los vectores propios de cada S_j y a su vez de $T_1, T_2, \ldots, T_{k-1}$ ya que

$$T_k(S_j(v)) = T_k S_j(v) = S_j T_k(v) = S_j(T_k(v)) = S_j(\lambda_i v) = \lambda_i S_j(v)$$

que son justamente los vectores propios de T_j restringidos a V_{λ_i}. Además, por definición sabemos que los vectores de V_{λ_i} son los vectores propios de T_k.

Para finalizar la demostración, como $V = V_{\lambda_1} \oplus \cdots \oplus V_{\lambda_s}$ y cada subespacio V_{λ_i} esta restringida a una familia de transformaciones unitarias lineales conmutativas $T_1, ..., T_k$ por la hipótesis de inducción podemos afirmar, que son simultáneamente diagonalizables en cada subespacio V_{λ_i} y por lo tanto en V. □

Una vez concluida la demostración del lema, podemos continuar con la demostración. Tenemos $F(G,\mathbb{C})$ un espacio vectorial de dimensión $|G|$. Para cada $a \in G$ definimos la siguiente transformación lineal $T_a : F(G,\mathbb{C}) \to F(G,\mathbb{C})$ como

$$(T_a f)(x) = f(a \cdot x) \quad \forall x \in G$$

Como G es abeliano y los valores que toma la función f a lo largo de G están contenidos en el grupo, es decir, f permuta los valores de G, tendremos que $T_a T_b f(x) = T_a(T_b f(x)) = T_a f(bx) = f(abx) = f(bax) = T_b f(ax) = T_b(T_a f(x)) = T_b T_a f(x)$. Además, por como hemos definido el producto interior Hermitiano en $F(G,\mathbb{C})$, tenemos que T_a es unitario $\forall a \in G$:

$$< T_a f, T_b g >= \frac{1}{|G|} \sum_{b \in G} T_a f(b)\overline{T_a g(b)} = \frac{1}{|G|} \sum_{b \in G} f(a \cdot b)\overline{g(a \cdot b)} = \frac{1}{|G|} \sum_{b \in G} f(b)\overline{g(b)} =< f, g >$$

La penúltima igualdad se cumple ya que como b va tomando todos los valores de G, $a \cdot b$ también va tomando todos los valores de G. Por lo tanto, tenemos una familia de transformaciones unitarias conmutativas sobre nuestro espacio vectorial $F(G,\mathbb{C})$, $\{T_a\}_{a \in G}$. Por el lema 3.2, existe una base de $F(G,\mathbb{C})$, $\{v_b\}_{b \in G}$, formada por valores propios de cada T_a, tal que cada $v_b(x)$ es una función sobre T_a que cumple que $(T_a v_b) = \lambda_a v_b$ para cada $a \in G$ y con $\lambda_a \in \mathbb{C}$.

Cabe destacar que, para cada $a \in G$ y para todo $x \in G$, $v_b(x) \neq 0$. Supongamos que existe $x \in G$ tal que $v_b(x) = 0$. Entonces, para todo $y \in G$ escribimos $a = yx^{-1}$ y tenemos que $v_b(y) = v_b(ax) = T_a v_b(x) = 0$. Concretamente, sea v un elemento de una de estas bases y 1 el elemento unitario de G, $v(1) \neq 0$.

Por último, definimos la función $w(x) = \lambda_x = v(x)/v(1)$. Por lo mencionado anteriormente, $w(x) \neq 0$ para todo $x \in G$:

$$w(a \cdot b) = \frac{v(a \cdot b)}{v(1)} = \frac{T_a v(b)}{v(1)} = \lambda_a \frac{v(b)}{v(1)} = \lambda_a \frac{T_b v(1)}{v(1)} = \lambda_a \lambda_b \frac{v(1)}{v(1)} = w(a)w(b)$$

Invocando el lema 1.7 como G es un grupo abeliano finito y $w : G \to \mathbb{C}\backslash\{0\}$ es una función multiplicativa entonces w es un carácter de G que nos proporciona los elementos de la base de $F(G,\mathbb{C})$. Es decir, toda función $f \in F(G,\mathbb{C})$ que actúa sobre G se podrá escribir como combinación lineal de los caracteres w. Con esto concluimos la demostración. □

Resumiendo, hemos encontrado una base para nuestro espacio vectorial de funciones complejas $F(G,\mathbb{C})$ formada por los caracteres $e_0, ..., e_{N-1}$ que hemos definido anteriormente. Esto nos será muy útil a la hora de desarrollar el teorema de Fourier ya que sabemos que las funciones serán combinaciones lineales de la base formada por los caracteres mencionados.

2.3.6. La inversión de Fourier y la fórmula de Plancharel

Finalmente, con todos los subaspectos definidos podemos pasar a desarrollar la **expansión de Fourier** de funciones sobre grupos abelianos finitos G. Dada una función $f \in F(G, \mathbb{C})$ definida sobre el grupo G y un carácter e de G, definimos el **coeficiente de Fourier** de f con respecto a e como:

$$\widehat{f(e)} = \langle f, e \rangle = \frac{1}{G} \sum_{a \in G} f(a)\overline{e(a)}$$

Como podemos observar, esto concuerda con la definición del producto interior Hermitiano definido sobre el espacio $F(G, \mathbb{C})$ en el tema anterior. Y por lo tanto, la serie de Fourier de f será

$$f \sim \sum_{e \in \widehat{G}} \widehat{f(e)} e$$

Pero por los resultados obtenidos, sabemos que los caracteres de G forman una base del espacio vectorial, es decir, f se puede escribir como combinación lineal de los caracteres

$$f = \sum_{e \in \widehat{G}} c_e e$$

Donde c_e es un conjunto de constantes, si sustituimos f en el producto definido anteriormente

$$\langle f, e \rangle = \frac{1}{G} \sum_{a \in G} f(a)\overline{e(a)} = \frac{1}{G} \sum_{a \in G} (\sum_{e \in \widehat{G}} c_e e(a))\overline{e(a)} = c_e$$

Como los caracteres forman una base ortonormal todos los productos del sumatorio serán igual a 0 excepto uno, cuando $e = \overline{e}$ que en este caso el valor será c_e. Esto nos indica que los coeficientes de Fourier son exactamente los mismos que los coeficientes c_e de la función f con respecto a la base del espacio vectorial. Por lo tanto, se cumple que f es exactamente igual a su serie de Fourier

$$f = \sum_{e \in \widehat{G}} \widehat{f(e)} e$$

Vamos a resumir lo descrito en estos dos teoremas siguientes.

Teorema 3.2. *Sea G un grupo finito abeliano. Los caracteres de G forman una base ortonormal sobre el espacio vectorial $F(G, \mathbb{C})$ de funciones sobre G con producto interior*

$$\langle f, g \rangle = \frac{1}{G} \sum_{a \in G} f(a)\overline{g(a)}$$

En particular, cualquier función f de G es igual a su serie de Fourier

$$f = \sum_{e \in \widehat{G}} \widehat{f(e)} e$$

Demostración. Solo tenemos que analizar el proceso descrito anteriormente y ver que los coeficientes de la Serie de Fourier de f son los mismos que el conjunto de constantes c_e de f como combinación lineal de la base de $F(G, \mathbb{C})$ □

Teorema 3.3. *Si f es una función sobre G , entonces*

$$||f||^2 = \sum_{e \in \widehat{G}} |\hat{f}(e)|^2$$

Demostración. Como los caracteres forman una base ortonormal tenemos que

$$||f||^2 = \langle f, f \rangle = \sum_{e \in \widehat{G}} (\hat{f}(e)e)\overline{(\hat{f}(e)e)} = \sum_{e \in \widehat{G}} |\hat{f}(e)|^2$$

□

Capítulo 3

El teorema de Dirichlet

Una vez introducida la teoría de Fourier de series finitas, podemos introducir el **Teorema de Dirichlet**. Este resultado es un claro ejemplo de una de las muchas aplicaciones que tiene la teoría de Fourier. En este caso lo aplicaremos a la distribución de los números primos, en particular su presencia en las **progresión aritmética**.

Una progresión aritmética con término a y diferencia común m consiste en una sucesión de números reales de la siguiente forma

$$a + mk \quad k = 0, 1, 2, ...$$

Un ejemplo básico, es la progresión de los números impares $1, 3, 5, ...$ que corresponde a los números de la clase $1 + 2k$. Si a y m tienen un factor común d entonces todos los números de la progresión aritmética son divisibles por el factor común. A causa de esto, surgió la cuestión de si se puede encontrar una progresión aritmética que contenga infinitos números primos. Es decir, si $\gcd(a, m) = 1$ es condición suficiente para que la progresión $a + km$ contenga infinitos primos. Fue *Johann P. G. L. Dirichlet* el primero en demostrar este hecho, este resultado se conoce como el Teorema de Dirichlet y es una de las muchas demostraciones sobre un tema muy relevante en las matemáticas, la infinitud de los primos, que se remonta al siglo III a.c cuando Euclides dio la primera demostración de este hecho.

3.1. Teoría elemental de números

Para entender el Teorema de Dirichlet primero necesitaremos conocer unos conceptos básicos. En particular, nos interesa las propiedades de divisibilidad de enteros y especialmente las propiedades de los números primos. Nuestro principal objetivo en este apartado es demostrar

el **teorema fundamental de la aritmética**, que afirma que todo número entero se puede expresar de forma única como producto de números primos.

3.1.1. El teorema fundamental de la aritmética

Teorema 3.4 (**Algoritmo de Euclides**). *Para cualesquiera $a, b \in \mathbb{Z}$ con $b > 0$ existen dos enteros únicos q y r tales que:*

$$a = qb + r$$

Donde q representa el cociente de a entre b y r representa el resto de la división con $0 \leq r < b$

Demostración. Consideramos el conjunto $A = \{a - qb : q \in \mathbb{Z} \ \ \& \ \ a - qb > 0\}$. Es decir, A esta formado por los números naturales de la forma $a - qb$. Claramente $A \neq \emptyset$, ya que si $a \geq 0$ entonces $a - (-a)b = a(1 + b) \geq 0 \in A$. Si $a \leq 0$ entonces, $a - ab = a(1 - b) \geq 0 \in A$. Dado que A está acotado por abajo ya que todo $a \in A$ tenemos que $a \in \mathbb{N}$. Sea r el menor elemento de A, como $r \in A$ existe $q \in \mathbb{Z}$ tal que $a - qb = r$ por lo tanto, $a = qb + r$. Además, como $r \in A$ sabemos que $r \geq 0$. Si $r \geq b$ tenemos que:

$$0 \leq r - b = (a - qb) - b = a - (q + 1)b \in A$$

Esto no puede cumplirse ya que r es el menor elemento de A y claramente $r - b < r$, por lo que concluimos que $r < b$. Hemos encontrado la existencia de q y r ahora nos falta comprobar la unicidad de estos dos.

Supongamos que existen q' y r' de tal manera que, $a = q'b + r'$. Supongamos también que, $r' \geq r$. Como $a = q'b + r' = qb + r$ tenemos que

$$r' - r = (q - q')b$$

Pero la parte de la izquierda de la igualdad esta acotado por $0 \leq r' - r < b$ y la derecha solo puede tomar los valores $(q - q')b \leq 0$ o $(q - q')b \geq b$, entonces la igualdad de arriba solo se cumple si ambos lados son iguales a 0, o con otras palabras, $r = r'$ y $q = q'$ □

Decimos que b divide a a si existe otro entero c tal que $a = bc$ o equivalentemente que $r = 0$. En este caso, escribimos $b|a$ y llamamos a b un divisor de a. Cabe destacar que 1 divide a todos los enteros. Dado un entero positivo $p > 1$ decimos que p es un número primo si y solo si no tiene ningún divisor positivo excepto 1 y a si mismo.

Definición 3.1. *Llamamos máximo común divisor de dos enteros positivos a y b al entero más grande que divide a ambos. Expresaremos el máximo común divisor como* $\gcd(a, b)$.

Decimos que dos enteros a y b son coprimos si $\gcd(a,b) = 1$ es decir, el único entero positivo que divide a ambos es el 1.

Teorema 3.5 (**Lema de Beizout**). *Si* $\gcd(a,b) = d$, *entonces existen enteros* x *e* y *tal que*

$$ax + by = d$$

Demostración. Consideramos el conjunto S formado por todos los enteros positivos de la forma $ax + by$ donde $x, y \in \mathbb{Z}$. Obviamente, este conjunto no es vació. Sea s el menor elemento del conjunto. Vamos a comprobar que $s = d$. Como $s \in S$ existe dos enteros x e y tal que

$$ax + by = s$$

Como d es divisor tanto de a como de b entonces d es divisor de s también, si expresamos $a = dc_1$ y $b = dc_2$ tenemos que

$$ax + by = dc_1x + dc_2y = d(c_1x + c_2y) = dc_3 = s$$

Esto implica que $d \leq s$. Para terminar la demostración nos falta comprobar que s es divisor de a y de b. Aplicando el algoritmo de Euclides, podemos escribir a como $a = qs + r$ con $0 \leq r < s$. Entonces

$$r = a - qs = a - q(ax + by) = a(1 - qx) + b(-qy)$$

Esto implica que $r \in S$ pero como s era el menor elemento de S y $r < s$ esto implica que $r = 0$ y por lo tanto s es divisor de a. Similarmente aplicando el algoritmo de Euclides a b obtenemos que s divide a b también. □

Ahora pasamos a estudiar tres consecuencias más relevantes de este teorema.

Teorema 3.6 (**Euclides**). *Dados dos enteros positivos* a *y* b*:*

(i) a *y* b *son coprimos si y solo si existen* $x, y \in \mathbb{Z}$ *tales que* $ax + by = 1$.

(ii) Supongamos que a *y* b *son coprimos. Sea* $z \in \mathbb{Z}$ *entonces* a *divide* bz *si y solo si* a *divide* z.

(iii) Si p *es primo y divide al producto* $a_1 \cdots a_n$ *entonces* p *divide a algún* a_i *con* $i = 1, ..., n$.

Demostración. Vamos a demostrar los tres apartados individualmente:

(i) Si a y b son coprimos por el teorema 3.5 existen x e y tales que $ax + by = 1$. Además, si d es un entero que divide a a y a b entonces d divide a $ax + by = 1$ esto implica que d divide a uno o lo que es lo mismo $d = 1$.

(ii) Sean a y b coprimos y supongamos que $a|bz$ para un $z \in \mathbb{Z}$. Por el apartado (a), $1 = ax+by$. Multiplicando ambos lados por z obtenemos que

$$z = axz + byz = axz + acy = (xz + cy)a \rightarrow z = ca$$

es decir $a|z$. La otra implicación es obvia.

(iii) Aplicamos inducción sobre n. Para $n = 1$ es trivial $p|a_1$ suponemos que si p divide a $a_1 \cdots a_{n-1}$ entonces p divide a algún a_i. Tenemos el producto, $a_1 \cdots a_n = a_1 \cdots a_{n-1} \cdot a_n$ por lo tanto $p|a_1 \cdots a_{n-1} \rightarrow p|a_1 \cdots a_{n-1} \cdot a_n$ aplicando la hipótesis de inducción p divide a algún a_i con $i = 1, ..., n$

□

Una vez introducido algunos conceptos básicos de la divisibilidad de enteros y algunas propiedades de los números primos podemos demostrar el principal teorema de este apartado.

Teorema 3.7 (**Teorema fundamental de la aritmética**). *Todo entero mayor que 1 se puede factorizar de manera única como producto de primos*

Demostración. La demostración consta de dos partes, primero tenemos que demostrar que tal factorización existe y luego que es única.

La primera parte la demostraremos por contradicción. Suponemos que existe un conjunto S no vacío con todos los enteros mayores que 1 que no se pueden factorizar como producto de primos. Sea s el elemento minimal de este conjunto. Como s no es primo existen dos números a y b mayores que 1 tal que $s = ab$ pero $a < s$ y $b < s$, por lo tanto $a, b \notin S$. Esto implica que tanto a como b pueden factorizarse como producto de primos. Sin embargo, esto es una contradicción ya que por lo tanto s se puede expresar como producto de primos es decir $s \notin S$ que implica que el conjunto S es vacío.

Ahora pasaremos a demostrar que se puede factorizar de manera única. Supongamos que s tiene dos factorizaciones en primos

$$n = p_1 p_2 \cdots p_d = q_1 q_2 \cdot \cdot q_r$$

Esta igualdad implica que p_1 divide al producto $q_1 q_2 \cdot \cdot q_r$ por el teorema 3.6 apartado (c) sabemos que $p_1|q_i$ para algún $i = 1, ..., r$. Como q_i es primo entonces tenemos que $p_1 = q_i$. Si continuamos este argumento para cada p_i obtenemos que ambas factorizaciones son iguales. □

3.1.2. La infinitud de los primos

La infinitud, o no, de los números primos fue en la antigüedad un tópico de gran interés en la comunidad matemática, especialmente en la aritmética. Fue Euclides en el siglo III A.C el primero en aportar una demostración sencilla pero genial para resolver este problema. A lo largo de la historia se ha demostrado de varias maneras diferentes abarcando múltiples áreas de las matemáticas. Primero vamos a estudiar la demostración aportado por Euclides.

Teorema 3.8. *Hay un número infinito de primos*

Demostración. Supongamos que el conjunto de los número primos es finito, y sea $p_1, p_2, ..., p_n$ el conjunto completo de todos ellos. Definimos

$$N = p_1 \cdot p_2 \cdots p_n + 1$$

Claramente N es más grande que cualquier primo definido en el conjunto anterior, por lo tanto N no puede ser primo. Por el teorema 3.7, N es divisible por algún primo p_i del conjunto. Sin embargo, todos los primos del conjunto dividen el producto $p_1 \cdot p_2 \cdots p_n$ pero ninguno divide a 1. Esta contradicción concluye la demostración. □

El trabajo de encontrar todos los primos es extremadamente complicado, ya que a medida que vas tomando números más grandes el número de operaciones que hay que realizar para comprobar que un número es primo va creciendo. Sin embargo, si que se ha podido averiguar que los primos se pueden clasificar en dos clases dependiendo de si son de la forma $4m + 1$ o $4m + 3$.

Una pequeña modificación de la demostración de Euclides nos permite demostrar que hay infinitos primos de la forma $4m + 3$ con $m \in \mathbb{Z}$. Suponemos que hay una cantidad finita de primos de la clase $4m + 3$, empezamos enumerando cada uno de ellos excluyendo el 3

$$p_1 = 7, p_2 = 11, ..., p_n$$

y sea

$$N = 4p_1p_2 \cdots p_n + 3$$

Claramente N es de la forma $4m+3$ y N no puede ser primo ya que $N > p_n$. Como el producto de los números de la clase $4m + 1$ nos da otro de la forma $4m + 1$

$$(4m_1 + 1) \cdot (4m_2 + 1) = 16m_1m_2 + 4m_1 + 4m_2 + 1 = 4(4m_1m_2 + m_1 + m_2) + 1 = 4m_3 + 1$$

si descomponemos N en sus factores primos al menos uno de ellos debe ser de la forma $4m + 3$ llamemos a este primo p. Cabe destacar que $p \neq 3$ por como hemos definido el conjunto inicial de números primos. También, observamos que p no puede ser ninguno de los p_i definidos

anteriormente, ya que si no p no sería divisor de N porque no divide a 3 pero al producto $4p_1p_2\cdots p_n$ si. Esto es una contradicción ya que hemos asumido que había un número finito de primos de esta clase.

No se puede aplicar un argumento similar para demostrar que hay infinitos primos de la clase $4m+1$, debido a que el producto de dos enteros de la forma $4m+3$ nunca son de la forma $4m+3$. Sin embargo, **Legendre** formulo la siguiente afirmación:

Si q y l son coprimos entonces la secuencia

$$l + kq \quad k \in \mathbb{Z}$$

contiene infinitos primos

La condición de que q y l sean coprimos es absolutamente necesarias ya que si no todos los números de la progresión son divisibles por $\gcd(q, l) = d$ por lo tanto no habría ningún primo. La hipótesis planteado por Legendre era que cualquier progresión aritmética que contuviese al menos un primo necesariamente contiene infinitos de ellos.

La afirmación de Legendre fue demostrada más adelante por Dirichlet. Su demostración está basada en los resultados obtenidos por Euler que abarco el problema en cuestión de una manera más analítica. Euler encontró una función multiplicativa ζ que dado dos números coprimos m y n

$$\zeta(mn) = \zeta(m)\zeta(n)$$

Esta fórmula nos da una versión reforzada del teorema 3.8 y constituye uno de los fundamentos en los que se apoyaron los resultados descubiertos por Dirichlet.

3.2. La función zeta y el producto de Euler

Primero tenemos que introducir los productos infinitos. Sea $\{A_n\}_{n=1}^{\infty}$ una secuencia infinita de números reales, definimos el producto de la secuencia como

$$\prod_{n=1}^{\infty} A_n = \lim_{N\to\infty} \prod_{n=1}^{N} A_n$$

si el límite existe entonces el producto converge. La manera más simple de trabajar con productos es tomar logaritmos y transformar los productos en sumas. Vamos a resumir las propiedades más importantes de los logaritmos definidos en los números reales en el siguiente lema.

Lema 3.3. *La función logaritmo cumple las siguientes propiedades:*

(i) $\log(1+x) = x + E(x)$ *donde* $E(x) \leq x^2$ *si* $|x| < 1/2$.

(ii) Si $\log(1+x) = y$ *e* $|x| < 1/2$, *entonces* $|y| \leq 2|x|$.

Demostración. Vamos a demostrar cada propiedad individualmente.

(i) Vamos a necesitar la expansión en series de potencias de la función $\log(1+x)$ para $|x| < 1$

$$\log(1+x) = \sum_{n=1}^{\infty} \frac{(-1)^{n+1}}{n} x^n$$

Entonces, tenemos que

$$E(x) = \log(1+x) - x = -\frac{x^2}{2} + \frac{x^3}{3} - \frac{x^4}{4} + ...$$

Observa que el primer término del sumatorio, $n = 1$, es x que se anula con $-x$. Si tomamos valores absolutos y aplicando la desigualdad triangular tenemos que

$$\begin{aligned} |E(x)| &\leq \left|-\frac{x^2}{2}\right| + \left|\frac{x^3}{3}\right| + \left|-\frac{x^4}{4}\right| + ... \\ &\leq \frac{x^2}{2}(1 + |x| + |x|^2 + ...) \end{aligned}$$

Ahora como, $|x| \leq 1/2$ podemos utilizar la serie geométrica para simplificar la suma del lado derecho

$$|E(x)| \leq \frac{x^2}{2}\left(1 + \frac{1}{2} + \frac{1}{4} + \frac{1}{8}...\right) \leq \frac{x^2}{2}\left(\frac{1}{1-1/2}\right) \leq x^2$$

(ii) Si $x = 0$, la propiedad claramente se cumple $log(1) = 0 \rightarrow |y| = 0$
Por el apartado anterior, sabemos que $\log(1+x) = x + E(x)$, donde $|E(x)| \leq x^2$. Tomamos valores absolutos y por la desigualdad triangular tenemos que

$$|\log(1+x)| \leq |x| + |E(x)|$$

Si $x \neq 0$ y $|x| \leq 1/2$ podemos dividir entre x

$$\begin{aligned} \left|\frac{\log(1+x)}{x}\right| &\leq 1 + \left|\frac{E(x)}{x}\right| \\ &\leq 1 + |x| \\ &\leq 2 \end{aligned}$$

Y por lo tanto, obtenemos que $|\log(1+x)| \leq 2|x|$

□

Proposición 4. *Si $A_n = 1 + a_n$ y $\sum |a_n|$ converge, entonces el producto $\prod_n A_n$ también converge, y este producto se anula si y solo si uno de los factores A_n es nulo. También. si $a_n \neq 1$ para todo n, entonces $\prod_n 1/(1 - a_n)$ converge.*

Demostración. Si $\sum |a_n|$ converge, sabemos que la sucesión $S_N = \sum_{n=0}^{N} |a_n|$ es una sucesión convergente entonces el término general a_n tiende a 0. Por lo tanto, podemos asumir que para valores de n grandes $|a_n| \leq 1/2$. Es decir, existe $n_0 \in \mathbb{Z}$ tal que para todo $n > n_0$ $|a_n| \leq 1/2$. Para estudiar la convergencia del producto tenemos que ver que

$$\lim_{N\to\infty} \prod_{n=1}^{N} A_n = \lim_{N\to\infty} \prod_{n=1}^{N} (1 + a_n) = N$$

existe. Si descomponemos el producto como $\prod_{n=1}^{N}(1 + a_n) = \prod_{n=0}^{n_0}(1 + a_n) \prod_{n=n_0}^{N}(1 + a_n)$, a la hora de hacer el límite tenemos que

$$\lim_{N\to\infty} \left(\prod_{n=0}^{n_0} (1 + a_n) \cdot \prod_{n=n_0}^{N} (1 + a_n) \right) = \prod_{n=0}^{n_0} (1 + a_n) \lim_{N\to\infty} \sum_{n=n_0}^{N} (1 + a_n)$$

Como solo nos interesa estudiar el límite podemos asumir que $|a_n| \leq 1/2$ para todo n. Ahora, escribimos los productos parciales como

$$\prod_{n=1}^{N} A_n = \prod_{n=1}^{N} 1 + a_n = \prod_{n=1}^{N} e^{\log(1+a_n)} = e^{B_N}$$

donde $B_N = \sum_{n=1}^{N} b_n$ con $b_n = \log(1 + a_n)$. Tenemos que $|a_n| \leq 1/2$ aplicando la propiedad (ii) del lema 3.3 obtenemos que $|b_n| \leq 2|a_n| \to |b_n| \leq 1$. Entonces, la suma parcial $B_N = \sum_{n=1}^{N} b_n$ es un número real, si hacemos que $N \to \infty$ aplicando el criterio de comparación directa, como $\sum |a_n|$ converge y $|b_n| \leq 2|a_n|$ tenemos que $\lim_{N\to\infty} B_N$ converge a un número real que llamaremos B. Como la función exponencial es continua, concluimos que e^{B_N} converge a e^B cuando N tiende hacia el infinito. Luego, tenemos que

$$\lim_{N\to\infty} \prod_{n=1}^{N} A_n = e^{\lim_{N\to\infty} B_N} = e^{\lim_{N\to\infty} \sum_{n=1}^{N} b_n} = e^{\lim_{N\to\infty} B_n} = e^B$$

con esto concluimos la primera parte de de la demostración. Cabe destacar, que si $1 + a_n \neq 0$ para todo n entonces el producto converge a un límite distinto de cero ya que lo expresamos como e^B.

Ahora nos queda ver que si $a_n \neq 1$ para todo n entonces $\prod_n 1/(1-a_n)$ converge. Observemos que

$$\prod_n 1/(1 - a_n) = 1/\prod_n (1 - a_n)$$

y aplicando el mismo argumento obtenemos que el producto converge a un límite distinto de cero. □

Después de esta introducción, podemos empezar a definir la **función zeta** que también es conocida como **función zeta de Euler**. Dado un entero positivo definimos la función zeta como

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

Antes de comenzar a analizar la función, necesitamos introducir una sección para la aproximación de sumas mediante integrales que nos sera importante.

3.2.1. Aproximación de sumas mediante integrales

Dada una función $f(x)$ continua y decreciente podemos aproximar la suma de la función mediante integrales. Esto se debe a que la integral de Riemann de una función positiva y continua es equivalente al área de la gráfica de la función con el eje OX. Las sumas de Riemann aproximan dicha área partiéndola en n trozos rectangulares y sumando el área de cada rectángulo. Donde el rectángulo n-ésimo representa la suma $\sum_{n-1}^{n} f(x)$, como se puede observar en la figura 3.1.

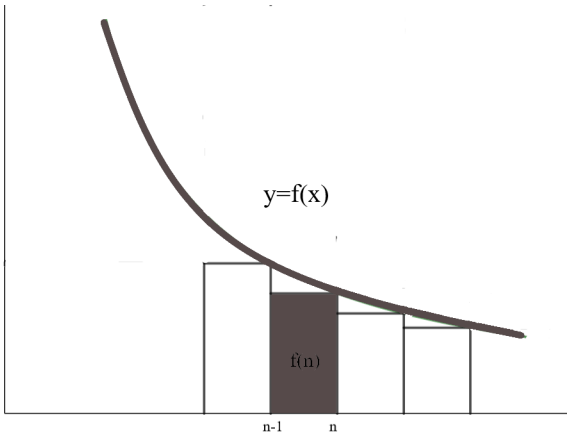

Figura 3.1: Aproximación de una suma con integrales

Vamos a compilar los resultados más importantes a la hora de estudiar la función zeta en los dos siguientes lemas.

Lema 4.1. *Dada la función zeta de Euler, si $s > 1$ la suma converge. Es más,*

$$\zeta(s) \leq \frac{1}{s-1}$$

Demostración. Vamos a utilizar la aproximación de sumas mediante integrales. Escogemos $f(x) = 1/x^s$ y tenemos que

$$\sum_{n=1}^{\infty} \frac{1}{n^s} \leq 1 + \sum_{n=2}^{\infty} \int_{n-1}^{n} \frac{dx}{x^s} = 1 + \int_1^{\infty} \frac{dx}{x^s}$$

Resolvemos la integral

$$\int_1^{\infty} \frac{dx}{x^s} = \lim_{N\to\infty} \int_1^N \frac{dx}{x^s} = \lim_{N\to\infty} \left[\frac{x^{1-s}}{1-s}\right]_1^N = \lim_{N\to\infty} \frac{1}{1-s}\left(N^{1-s} - 1\right) = \frac{1}{1-s} \lim_{N\to\infty} \left(\frac{1}{N^{s-1}} - 1\right)$$

Analizando el límite, como $s > 1$ el denominador de $\frac{1}{N^{s-1}}$ va creciendo y por lo tanto cuando $N \to \infty$ la división tiende a cero, por lo tanto el $\lim_{N\to\infty} \frac{1}{N^{s-1}} = 0$ y el resultado de la integral es

$$\frac{1}{1-s} \lim_{N\to\infty} \left(\frac{1}{N^{s-1}} - 1\right) = \frac{1}{1-s} \lim_{N\to\infty} \frac{1}{N^{s-1}} - \frac{1}{1-s} = \frac{1}{s-1}$$

□

Lema 4.2. *La suma*

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

no converge cuando $s \leq 1$

Demostración. Basta con estudiar el caso $s = 1$ ya que $\frac{1}{n^s} > \frac{1}{n}$ si $s < 1$. Para estudiar este caso, necesitamos introducir la siguiente proposición.

Proposición 5. *Si N es un entero positivo, entonces:*

(i) $\displaystyle\sum_{n=1}^{N} \frac{1}{n} = \int_1^N \frac{dx}{x} + O(1) = \log(N) + O(1)$

(ii) En especial, existe $\gamma \in \mathbb{R}$, conocida como la constante de Euler, tal que

$$\sum_{n=1}^{N} \frac{1}{n} = \log(N) + \gamma + O(1/N)$$

Demostración. Nos centraremos en la segunda propiedad ya que la primera es un caso particular. Sea

$$\gamma_n = \frac{1}{n} - \int_n^{n+1} \frac{dx}{x}$$

como $1/x$ es decreciente y continua cuando $x \neq 0$, tenemos que

$$0 \leq \gamma_n \leq \frac{1}{n} - \frac{1}{n+1} \leq \frac{1}{n^2}$$

como $\sum_{n=1}^{\infty} \frac{1}{n^2}$ converge y $\sum_{n=1}^{\infty} \gamma_n \leq \sum_{n=1}^{\infty} \frac{1}{n^2}$ y la serie $\sum_{n=1}^{\infty} \gamma_n$ converge también (criterio de comparación directa). Al límite de esta serie lo denotaremos como γ por lo tanto tenemos que

$$\begin{aligned}\gamma &= \sum_{n=1}^{\infty} \gamma_n \\ &= \sum_{n=1}^{N} \gamma_n + \sum_{n=N+1}^{\infty} \gamma_n\end{aligned}$$

pasando el segundo sumando al otro lado obtenemos que

$$\sum_{n=1}^{N} \gamma_n = \gamma - \sum_{n=N+1}^{\infty} \gamma_n$$

Cabe destacar, que la integral de una función $f(x)$ en un intervalo $[a, b]$ es igual a la suma de integrales de cada subintervalo es decir

$$\int_a^{a+1} f(x)dx + \int_{a+1}^{a+2} f(x)dx + \cdots + \int_{a+n}^{b} f(x)dx = \int_a^b f(x)dx$$

asi que la serie $\sum \gamma_n$ es igual a

$$\sum_{n=1}^{N} \gamma_n = \sum_{n=1}^{N} \left(\frac{1}{N} - \int_n^{N+1} \frac{dx}{x} \right) = \sum_{n=1}^{N} \frac{1}{N} - \int_1^N \frac{dx}{x} - \int_{N+1}^{\infty} \frac{dx}{x}$$

Seguidamente, si estimamos la serie $\sum f(x)$ con $f(x) = 1/x^2$ por $\int f(x)$, nos encontramos con que

$$\sum_{n=N+1}^{\infty} \gamma_n \leq \sum_{n=N+1}^{\infty} \frac{1}{n^2} \leq \int_{n=N+1}^{\infty} \frac{dx}{x} = O(1/N)$$

Por último, juntando todo tenemos que

$$\begin{aligned}\sum_{n=1}^{N} \frac{1}{N} - \int_1^N \frac{dx}{x} - \int_{N+1}^{\infty} \frac{dx}{x} &= \gamma - \sum_{n=N+1}^{\infty} \gamma_n \\ &= \gamma - \sum_{n=N+1}^{\infty} \gamma_n + \int_{N+1}^{\infty} \frac{dx}{x}\end{aligned}$$

donde $\int_1^N \frac{dx}{x} = \log(N)$ y si $N \to \infty$ entonces la integral es igual a $O(1/N)$ y obtenemos el resultado deseado. □

Para $s = 1$ tenemos que

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n} = \lim_{N\to\infty} \sum_{n=1}^{N} \frac{1}{n}$$

como n es un entero podemos aplicar la proposición 5 y obtenemos que

$$\lim_{N\to\infty} \sum_{n=1}^{N} \frac{1}{n} = \lim_{N\to\infty} (\log(N) + O(1))$$

donde el límite de $\log(N)$ tiene hacia el infinito y por lo tanto $\zeta(s)$ no converge para $s \leq 1$. □

Como hemos demostrado en el lema 4.1 la serie que define ζ converge para los valores $s > 1$ así que ζ es continua para estos valores de s. A continuación pasamos a estudiar los resultados más relevantes descubiertos por Euler con respecto a la función zeta.

Teorema 5.1 (**Fórmula de Euler**). *Para todo $s > 1$, tenemos que*

$$\zeta(s) = \prod_{p} \frac{1}{1 - 1/p^s}$$

donde el producto recorre todos los primos.

Demostración. Antes de comenzar con la demostración vamos a introducir un lema sobre el desarrollo del producto mencionado en el teorema.

Lema 5.1. *Si $s > 0$ entonces*

$$\prod_{p\leq N} \frac{1}{1 - p^{-s}} = \sum_{n=1}^{N} \frac{1}{n^s}$$

donde n son todos los enteros cuya factorización en números primos es menor a N.

Demostración. Si miramos atentamente los términos del producto, podemos ver que cada uno de ellos expresan una serie geométrica convergente, recordemos que son de la forma

$$1 + q + q^2 + ... + q^n + ... = \frac{1}{1 - q}$$

La series es convergente cuando $q < 1$. En nuestro caso, $q = 1/p^s$ que siempre es menor que 1 ya que $p > 1$ para todo p primo. Si descomponemos cada término en su serie geométrica correspondiente obtenemos

$$\frac{1}{1 - 1/p^s} = 1 + \frac{1}{p^s} + \frac{1}{p^{2s}} + ... + \frac{1}{p^{ns}} + ...$$

sustituyendo en el producto

$$\prod_{p_j}\left(1+\frac{1}{p_j^s}+\frac{1}{p_j^{2s}}+...+\frac{1}{p_j^{ns}}+...\right)$$

Donde el producto recorre todos los primos en orden ascendente $p_1 < p_2 < p_3 < ...$ A continuación, calculamos el producto como el sumatorio de términos. Para esto, escogemos un término $1/p_j^{ks}$, el término k-ésimo del sumatorio correspondiente a p_j, donde k depende de la j seleccionada y con $k = 0$ para j grandes. De este manera, un término se expresaría como

$$\frac{1}{(p_1^{k_1}p_2^{k_2}\cdots p_n^{k_n})^s}$$

Por el teorema fundamental de la aritmética todo entero mayor o igual a 1 se puede expresar de manera única como producto de primos, entonces $n = p_1^{k_1}p_2^{k_2}\cdots p_n^{k_n}$. Juntando todos los términos del producto anterior obtenemos que

$$\prod_{p_j}(1+\frac{1}{p_j^s}+\frac{1}{p_j^{2s}}+...+\frac{1}{p_j^{ns}}+...)=\sum_{n=1}^{\infty}\frac{1}{n^s}$$

En resumen, se puede escoger un número finito de factores, multiplicarlos y reagruparlos de manera que gracias al teorema fundamental de la aritmética nos proporciona una manera única de factorizar cada entero positivo n. Una vez explicado este resultado podemos comenzar con la demostración del teorema. □

Sean N, M dos enteros positivos con $M > N$. Como ya sabemos, todo entero positivo $n \leq N$ se puede expresar de manera única como producto de números primos $n = p_1^{a_1}p_2^{a_2}\cdots p_r^{a_r}$ donde cada primo del producto tiene que ser menor o igual a N y no se puede repetir más de M veces ya que si $p_1^{a_1}p_2^{a_2}\cdots p_r^{a_r} \geq N \geq n$. Por el lema 5.1 tenemos que

$$\begin{aligned}\sum_{n=1}^{N}\frac{1}{n^s} &\leq \prod_{p\leq N}\left(1+\frac{1}{p^s}+\frac{1}{p^{2s}}+...+\frac{1}{p^{Ms}}\right)\\ &\leq \prod_{p\leq N}\left(\frac{1}{1-p^{-s}}\right)\end{aligned}$$

Si N tiende hacia el infinito

$$\sum_{n=1}^{\infty}\frac{1}{n^s}\leq\prod_{p}\frac{1}{1-p^{-s}}$$

Ahora, vamos a desarrollar la desigualdad inversa, es decir

$$\prod_{p\leq N}(1+\frac{1}{p^s}+\frac{1}{p^{2s}}+...+\frac{1}{p^{Ms}})\leq\sum_{n=1}^{\infty}\frac{1}{n^s}$$

Si ahora M tiende hacia el infinito

$$\prod_{p\leq N}(\frac{1}{1-p^{-s}}) \leq \sum_{n=1}^{\infty}\frac{1}{n^s}$$

Entonces

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

Por consiguiente,

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

□

Para terminar, necesitamos introducir un último resultado que es la versión de Euler del teorema 3.8. Euler estudiando la serie armónica decidió separar los números primos del resto. Como esta serie diverge sabemos que hay infinitos enteros, en cambio si logramos ver que la serie armónica sobre todos los primos es divergente también, entonces tendríamos una demostración de que existen infinitos primos. Esta demostración fue el principal pilar en el que se apoyo Dirichlet para obtener sus propios resultados.

Proposición 6 (**Teorema de Euler**). *La serie*

$$\sum_{p} 1/p$$

diverge cuando tomamos el sumatorio sobre todos los primos.

Demostración. Como hemos mencionado anteriormente al aplicar logaritmos el producto pasa a ser un sumatorio ya que el logaritmo de un producto es igual a la suma de los logaritmos de los factores.

$$\begin{aligned}\log\left(\prod_{p}\left(\frac{1}{1-p^{-s}}\right)\right) &= \sum_{p}\log\left(\frac{1}{1-p^{-s}}\right)\\ &= \sum_{p}(\log(1)-\log(1-p^{-s}))\\ &= -\sum_{p}\log(1-p^{-s})\end{aligned}$$

Vamos a aplicar logaritmos en ambos lados de la fórmula de Euler, teorema 5.1. Para todo entero $s > 1$

$$-\sum_{p}\log(1-p^{-s}) = \log(\zeta(s))$$

Por el apartado (i) del lema 3.3 sabemos que $\log(1+x) = x+O(x)$ cuando $|x| \leq 1/2$. En nuestro caso, $x = -1/p^s$ y claramente $|1/p^s| \leq 1/2$ para todo p primo. Por lo tanto, sustituyendo en la ecuación anterior

$$\begin{aligned} -\sum_p \log(1-p^{-s}) &= -\sum_p [-1/p^s + O(1/p^{2s})] \\ &= \sum_p 1/p + O(1) \end{aligned}$$

Observemos que $\sum O(1/p^{2s}) = O(1)$ esto es debido a que $\sum_p 1/p^{2s} \leq \sum_n^\infty 1/n^2$ para $s > 1$ donde $\lim_{n\to\infty} \sum_n^\infty 1/n^2 = \frac{\pi^2}{6}$, este resultado se conoce como el problema de Basilea. Es decir, $\sum_p 1/p^{2s}$ converge a un número natural y por lo tanto $\sum O(1/p^{2s}) = O(1)$. La igualdad resultante es

$$\sum_p 1/p + O(1) = \log(\zeta(s))$$

Ahora hacemos s tender a 1 por la derecha $s \to 1^+$, por lo tanto $\zeta(s) \to \infty$ ya que se aproxima a la serie armónica, en otros términos $\sum_{n=1}^\infty 1/n^s \geq \sum_{n=1}^M 1/n^s$ para cualquier M, así que

$$\liminf_{s\to 1^+} \sum_{n=1}^\infty 1/n^s \geq \sum_{n=1}^M 1/n^s$$

Concluimos que $\sum_p 1/p^s \to \infty$ cuando $s \to 1^+$, y como $1/p > 1/p^s$ para todo $s > 1$, tenemos que

$$\sum_p 1/p = \infty$$

□

3.3. El teorema de Dirichlet

En este apartado vamos a introducir los pasos por los que se guió Dirichlet para demostrar su teorema.

Teorema 6.1. *Si q y l son dos enteros positivos coprimos entre ellos, entonces existen infinitos primos de la forma $l + kq$ con $k \in \mathbb{Z}$*

Como habíamos mencionado anteriormente cuando introducimos la función zeta de Euler, Dirichlet se baso en los resultados de Euler que demostró que

$$\sum_p \frac{1}{p}$$

divergía y por lo tanto existían infinitos primos, ya que si no el sumatorio sería convergente. Dirichlet demostró su teorema aplicando el mismo argumento pero modificado

$$\sum_{p\equiv l \mod q} \frac{1}{p}$$

es el mismo sumatorio que el empleado por Euler sin embargo, en vez de recorrer todos los primos, recorre todos los primos p congruentes a l módulo q. Es una demostración muy extensa que consta de varios pasos uno de ellos involucra el análisis de Fourier sobre el grupo $\mathbb{Z}^*(q)$ estudiada en el capítulo anterior.

No obstante, antes de comenzar con la demostración vamos a introducir la solución para el problema de la infinitud de los primos de la clase $4k+1$. Como podemos ver, es un caso particular del teorema de Dirichlet donde $q = 4$ y $l = 1$ que ilustra perfectamente todos los pasos relevantes de su demostración.

3.3.1. Estrategia de la demostración del teorema de Dirichlet para $q = 4$

El primer paso es definir el grupo sobre el cual vamos a trabajar y los caracteres que actuarán sobre este grupo, que son la clave para escoger solo los números que nos interesan. En este ejemplo son los números enteros positivos coprimos con 4, el grupo será $\mathbb{Z}^*(4) = \{1, 3\}$Elegimos el carácter χ que va actuar sobre el grupo $\chi : \mathbb{Z}(4) \to S^1$ tal que $\chi(1) = 1$ y $\chi(3) = -1$. Podemos extender este carácter a todo $\mathbb{Z}$ como

$$\chi(n) = \begin{cases} 0 & \text{si } n \text{ es par} \\ 1 & \text{si } n = 4k+3 \\ -1 & \text{si } n = 4k+1 \end{cases}$$

Hay que tener en cuenta que esta función es multiplicativa, $\chi(nm) = \chi(n)\chi(m)$ para todo $n, m \in \mathbb{Z}$, ya que el producto de cualquier entero por un número par es otra vez par por lo tanto $\chi(nm) = 0 = \chi(n)0 = 0$, el producto de dos números de la forma $4m+1$ son otra vez de la forma $4m+1$ demostrado en el apartado *La infinitud de los primos* así que $\chi(nm) = 1 \cdot 1 = \chi(n)\chi(m) = 1$ Ahora falta ver que $(4m+1)(4m'+3) = 4m''+3$ y que $(4m+3)(4m'+3) = 4m''+1$

$$(4m+1)(4m'+3) = 16mm' + 12m + 4m' + 3 = 4(4mm' + 3m + m') + 3 = 4m'' + 3$$

así que

$$\chi((4m+1)(4m'+3)) = \chi(4m+3) = -1 = \chi(4m+1)\chi(4m'+3)$$

Y por último

$$\begin{aligned}(4m+3)(4m'+3) &= 16mm' + 12m + 12m' + 9 \\ &= 16mm' + 12m + 12m' + 2 \cdot 4 + 1 \\ &= 4(4mm' + 3m + 3m' + 2) + 1 = 4m'' + 1\end{aligned}$$

y entonces

$$\chi((4m+3)(4m'+3)) = \chi(4m+1) = 1 = (-1)\cdot(-1) = \chi(4m+3)\chi(4m'+3)$$

El siguiente paso es definir la función L de Dirichlet para un entero s y un carácter χ, la definición exacta de esta función la daremos más adelante. Definimos

$$L(s,\chi) = \sum_{n=1}^{\infty} \frac{\chi(n)}{n^s} = 1 - \frac{1}{3^s} + \frac{1}{5^s} - \frac{1}{7^s} + ...$$

Lema 6.1. *La serie*

$$L(1,\chi) = 1 - \frac{1}{3} + \frac{1}{5} - \frac{1}{7} + ...$$

es convergente

Demostración. Podemos ver que la serie es convergente gracias al **Criterio de Leibniz** para series alternadas que dice lo siguiente

Dada la serie alternada $\sum_{n=1}^{\infty}(-1)^n a_n$*, entonces la serie converge si la sucesión* $\{a_n\}_n$ *es monótona decreciente y el* $\lim_{n\to\infty} a_n = 0$.

Referencia: [4]

Primero tenemos que ver cual va a ser la sucesión $\{a_n\}_n$

$$1 - \frac{1}{3} + \frac{1}{5} - \frac{1}{7} + \ldots = \sum_{n=0}^{\infty}(-1)^n \frac{1}{2n+1}$$

La sucesión entonces es $\{a_n\}_n = \frac{1}{2n+1} = 1, \frac{1}{3}, \frac{1}{5}, \ldots$ que podemos ver es monótona decreciente ya que $a_n \geq a_{n+1}$.

A continuación nos falta comprobar que $\lim_{n\to\infty} a_n = 0$

$$\lim_{n\to\infty} a_n = \lim_{n\to\infty} \frac{1}{2n+1} = 0$$

el denominador va creciendo a medida que n toma valores más grandes por lo tanto el límite tiende a 0.

Gracias al criterio de Leibniz, la serie definida por $L(1,\chi)$ converge y además podemos afirmar que como es una serie alternada cuyos valores absolutos tienden a cero que $L(1,\chi) \neq 0$. □

Por último, adaptamos la demostración de la proposición 6 a la función $L(s,\chi)$ para ver que la suma de la inversa de los números coprimos a 4 diverge. Como χ es multiplicativa podemos aplicar el producto de Euler, lo demostraremos más adelante

$$L(s,\chi) = \sum_{n=1}^{\infty} \frac{\chi(n)}{n^s} = \prod_p \frac{1}{1-\chi(p)/p^s}$$

Tomando logaritmos a ambos lados de la ecuación

$$\log L(s,\chi) = \log(\prod_p \frac{1}{1-\chi(p)/p^s}) = \sum_p \frac{\chi_p}{p^s} + O(1)$$

El logaritmo del producto ya fue desarrollado en la demostración del teorema 6. Sabemos que $L(1,\chi) \neq 0$ si dejamos que $s \to 1^+$, esto implica que $\sum_p \frac{\chi_p}{p^s}$ esta acotada. Descomponemos el sumatorio en dos dependiendo si p es de la clase $4k+1$ en este caso $\chi(p) = 1$ o si es de la clase $4k+3$ entonces $\chi(p) = -1$

$$\sum_p \frac{\chi_p}{p^s} = \sum_{p\equiv 1} \frac{1}{p^s} - \sum_{p\equiv 3} \frac{1}{p^s}$$

Observemos que

$$\sum_p \frac{1}{p^s} + \sum_{p\equiv 1} \frac{1}{p^s} - \sum_{p\equiv 3} \frac{1}{p^s} = 2\sum_{p\equiv 1} \frac{1}{p^s}$$

La primera suma a la izquierda de la igualdad recorre todos los primos, tanto los de la clase $4k+1$ como los de la clase $4k+3$, como le estamos sumando otra vez los primos de la clase $4k+1$ y restado los de la clase $4k+3$ nos quedamos con 2 veces la suma de los primos de la clase $4k+1$. Remontando a la proposición 6, demostramos que $\sum_p p^{-s}$ no esta acotada cuando $s \to 1^+$. Por lo tanto,

$$2\sum_{p\equiv 1} \frac{1}{p^s}$$

tampoco estará acotada cuando $s \to 1^+$ lo que implica que $2\sum_{p\equiv 1} 1/p$ diverge y por consecuencia existen infinitos primos de la clase $4k+1$

3.3.2. Estrategia de la demostración del teorema de Dirichlet para el caso general

Para lo que queda de sección cuando escribamos el grupo G nos estaremos refiriendo al grupo $\mathbb{Z}^*(q)$. Para las fórmulas siguientes nos vamos a referir al orden del grupo G que hará referencia al número de enteros del grupo $\mathbb{Z}(q)$ que son coprimos con q. Llamamos a la función que nos proporciona este número la **función φ de Euler** en nuestro caso $\varphi(q) = |G|$.

Definimos la función característica de l como δ_l sobre G que nos indicará para todo $n \in \mathbb{Z}^*(q)$ si es coprimo con l.

$$\delta_l(n) = \begin{cases} 1 & \text{si } n \equiv l \mod q \\ 0 & \text{resto} \end{cases}$$

Una vez que hemos definido la función, por el teorema 3.2 y siguiendo los pasos descritos en el tema anterior vamos a expandir δ_l en su serie de Fourier.

$$\delta_l(n) = \sum_{e \in \hat{G}} \hat{\delta}_l(e) e(n)$$

Y los coeficientes de Fourier son

$$\hat{\delta}_l(e) = < \delta_l, e > = \frac{1}{|G|} \sum_{n \in G} \delta_l(n) \overline{e(n)} = \frac{1}{|G|} \overline{e(l)}$$

Este resultado se obtiene por la definición de δ_l ya que solo cogeremos los $m \in G$ que son congruentes l módulo q en ese caso $e(n) = e(l)$ en el resto de valores son igual a 0. Luego, la serie de Fourier será

$$\delta_l(n) = \frac{1}{|G|} \sum_{e \in \hat{G}} \overline{e(l)} e(n)$$

Podemos expandir la función a todo $\mathbb{Z}$ poniendo $\delta_l(n) = 0$ cuando n y q no son coprimos. Análogamente, la extensión de los caracteres $e \in \widehat{G}$ a todo $\mathbb{Z}$ está definida por

$$\chi(n) = \begin{cases} e(n) & \text{si } n \text{ y } q \text{ coprimos} \\ 0 & \text{resto} \end{cases}$$

llamamos a $\chi(n)$ los **caracteres de Dirichlet** módulo q. Como los caracteres descritos en el tema anterior definimos el carácter trivial como χ_0, tal que $\chi_0(n) = 1$ para todo n coprimo con q y 0 el resto. Como es un carácter tiene que cumplirse la condición de que es multiplicativa en todo $\mathbb{Z}$

$$\chi(nm) = \chi(n)\chi(m) \quad \text{para todo} \quad n, m \in \mathbb{Z}$$

Lema 6.2. *Los caracteres de Dirichlet son multiplicativos. Además,*

$$\delta_l(n) = \frac{1}{\varphi(q)} \sum_{\chi} \overline{\chi(l)} \chi(n)$$

donde el sumatorio actúa sobre todos los caracteres de Dirichlet.

Demostración. Dados $m, n \in \mathbb{Z}$ tenemos 3 casos:

1 Si m y n no son coprimos a q entonces nm tampoco lo es $\chi(nm) = 0 = \chi(n)\chi(m)$.

2 Si m es coprimo y n no es coprimo entonces nm no es coprimo $\chi(nm) = 0 = \chi(n)\chi(m)$.

3 Si los dos son coprimos con q, entonces por la propiedad (iii) del teorema 3.6 mn es coprimo con q y tenemos que $\chi(nm) = e(nm) = e(n)e(m) = \chi(n)\chi(m)$.

□

Lema 6.3. *Existen infinitos primos* $p \equiv l \mod q$, *es decir*

$$\sum_{p \equiv l} \frac{1}{p}$$

diverge, si la suma $\sum_p \frac{\chi(p)}{p^s}$ *está acotada cuando* $s \to 1^+$.

Demostración. Como $\varphi_l(m)$ nos devuelve 1 si m es congruente con l módulo q, si extendemos esta función a todos los primos p tenemos la siguiente igualdad.

$$\begin{aligned}\sum_{p \equiv l} \frac{1}{p^s} &= \sum_p \frac{\delta_l(p)}{p^s} \\ &= \sum_p \frac{1}{p^s} \left[\frac{1}{\varphi(q)} \sum_\chi \overline{\chi(l)} \chi(p) \right] \\ &= \frac{1}{\varphi(q)} \sum_\chi \overline{\chi(l)} \sum_p \frac{\chi(p)}{p^s}\end{aligned}$$

Es decir, cogemos todos los primos que son congruentes con l y después expandimos φ_l en su serie de Fourier. Por esta igualdad, podemos entender el comportamiento del sumatorio a la izquierda de la igualdad si comprendemos como actúa el sumatorio $\sum_p \chi(p)/p^{-s}$ cuando $s \to 1^+$. Para esto, vamos a dividir el sumatorio de arriba en dos partes, la primera para el carácter trivial y la segundo para el resto

$$\sum_{p \equiv l} \frac{1}{p^s} = \frac{1}{\varphi(q)} \sum_p \frac{\chi_0(p)}{p^s} + \frac{1}{\varphi(q)} \sum_{\chi \neq \chi_0} \overline{\chi(l)} \sum_p \frac{\chi(p)}{p^s}$$

Como hay un número infinito de primos p que no dividen a q, $\chi_0(p) = 1$ y para el resto $\chi_0(p) = 0$, tenemos que

$$\sum_p \frac{\chi_0(p)}{p^s} = \sum_{\text{p no divide q}} \frac{1}{p^s}$$

por la proposición 6 la suma diverge cuando s tiende a 1 por la derecha. Por lo tanto, si la suma

$$\sum_p \frac{\chi(p)}{p^s}$$

está acotada para todo $\chi \neq \chi_0$ cuando $s \to 1^+$ entonces $\sum_{p \equiv l} \frac{1}{p^s}$ diverge y como $p^{-1} > p^{-s}$ para $s > 1$ implica que $\sum_{p \equiv l} \frac{1}{p}$ también diverge. □

3.3.3. Funciones L de Dirichlet

Al principio de este apartado, demostramos que la función zeta de Euler $\zeta(s) = \sum_n 1/n^s$ se podía expresar como un producto

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

Dirichlet encontró una manera análoga de expresar $\zeta(s)$ empleando los caracteres χ, se conocen como las **funciones L** tal que para todo $s > 1$

$$L(s, \chi) = \sum_{n=1}^{\infty} \frac{\chi(n)}{n^s}$$

Como se puede observar, es una versión adaptada a los caracteres de Dirichlet de la función zeta de Euler. Luego, empleando un razonamiento similar al de Euler, podemos expresar dicho sumatorio como un producto de primos.

Teorema 6.2. *Si χ es un carácter no trivial de Dirichlet, entonces la suma*

$$\sum_p \frac{\chi(p)}{p^s}$$

esta acotada cuando $s \to 1^+$

Demostración. Para demostrar el teorema primero tenemos que introducir un lema que lo volveremos a enunciar como el teorema 8.1 donde daremos la demostración formal.

Lema 6.4. *Si $s > 1$, entonces*

$$\sum_{n=1}^{\infty} \frac{\chi(n)}{n^s} = \prod_p \frac{1}{1 - \chi(p)p^{-s}}$$

donde el producto recorre todos los primos

Suponemos que χ es un carácter no trivial, empleamos la igualdad descrita en el lema 6.4. Tomando logaritmos a ambos lados de la igualdad obtenemos que

$$\log L(s, \chi) = -\sum_p \log(1 - \chi(p)p^{-s})$$

Seguidamente, gracias a que el $\log(1+x) = x + O(x^{2s})$ cuando $|x| < 1/2$ tenemos que

$$\begin{aligned} -\sum_p \log(1-\chi(p)p^{-s}) &= -\sum_p \left[-\frac{\chi(p)}{p^s} + O(\frac{1}{p^{2s}})\right] \\ &= \sum_p \frac{\chi(p)}{p^s} + O(1) \end{aligned}$$

Para terminar, como $L(1,\chi)$ es convergente distinto de 0, entonces $\log L(s,\chi)$ esta acotada cuando $s \to 1^+$ y por lo tanto tenemos que

$$L(s,\chi) = \sum_{n=1}^{\infty} \frac{\chi(n)}{n^s} = \prod_p \frac{1}{1-\chi(p)p^{-s}} = \sum_p \frac{\chi(p)}{p^s}$$

esta acotada cuando $s \to 1^+$. □

Sin embargo, hay algunos inconvenientes a la hora de demostrar formalmente el teorema. El primero, consiste en que los caracteres de Dirichlet son funciones de números enteros a números complejos, $\chi : G \to \mathbb{C} - \{0\}$, por lo tanto tenemos que expandir los logaritmos a los números complejos de la forma $w = 1/(1-z)$ con $|z| < 1$. Después, tenemos que adaptar el argumento empleado arriba con el logaritmo sobre $\mathbb{C}$.

Seguidamente, tenemos que comprobar que podemos aplicar la definición de logaritmo para números complejos en ambos lados de la igualdad planteada por el teorema. El problema reside en el hecho de que los logaritmos sobre $\mathbb{C}$ no tienen un único valor, esto implica que el logaritmo de un producto no es igual a la suma de los logaritmos de cada término.

Por último, falta comprobar que $\log L(s,\chi)$ esta acotada cuando $\chi \neq \chi_0$ y $s \to 1^+$. Sin embargo, si logramos ver que $L(s,\chi)$ es continua en $s = 1$ entonces con demostrar que $L(1,\chi) \neq 0$ es condición suficiente para ver que esta acotada. Esta es la parte más complicada de demostrar.

En resumen, nos centraremos en los tres puntos siguientes:

1. Logaritmos complejos y productos infinitos

2. El estudio de $L(s,\chi)$

3. Demostrar que $L(1,\chi) \neq 0$ cuando $\chi \neq \chi_0$

3.4. Demostración del teorema de Dirichlet

Para demostrar el teorema en cuestión vamos a atacar las tres dificultades mencionadas individualmente. Primero empezaremos por los logaritmos especialmente el logaritmo para los números complejos.

3.4.1. Logaritmos (complejos)

Como hemos mencionado en el tema anterior para tratar la fórmula de Dirichlet necesitamos tomar logaritmos. Sin embargo, esto plantea serias dificultades ya que no podemos tomar los logaritmos que utilizábamos para la demostración de Euler, ya que solo tenían en cuenta los números reales. Para resolver este problema, vamos a necesitar definir dos logaritmos, uno para los $w \in \mathbb{C}$ de la forma $w = \frac{1}{1-z}$ con $|z| < 1$ y el segundo logaritmo para la función $L(s, \chi)$. Al primero lo denotaremos como Lg y al segundo como $\mathcal{L}$.

Para el primer logaritmo, definimos la siguiente función

$$H(t) = \sum_{k=1}^{\infty} \frac{t^k}{k}$$

Primero, tengamos en cuenta que el sumatorio a la derecha de la ecuación converge cuando $|t| < 1$ por lo tanto la función H solo esta bien definida para estos valores de t. Segundo, si $Re(w) > 1/2$ y $w = \frac{1}{1-z}$ entonces $|z| < 1$. Esto se puede observar en la figura 3.2 donde la linea azul representa la función $f(x) = \frac{1}{1-x}$ y podemos ver que la función esta por encima de $1/2$,linea roja, cuando x está en el intervalo $-1 < x < 1$.

Definición 6.1. *Para cada $w \in \mathbb{C}$ definimos la función* $\mathrm{Lg}(w) = H\left(\frac{1}{1-w}\right)$

Lema 6.5. *Si $w \in \mathbb{R}$ y $w > 1/2$ entonces* $\mathrm{Lg}(w) = \log\left(\frac{1}{1-w}\right)$

Demostración. Antes de demostrar este lema necesitaremos introducir el concepto de convergencia uniforme y algunas de las propiedades más importantes que cumplen las sucesiones que convergen uniformemente.

Definición 6.2 (**Convergencia uniforme de sucesiones**). *Sea $D \subset \mathbb{C}$ y $f_n : D \to \mathbb{C}$ una sucesión de funciones. Se dice que f_n converge uniformemente a la función f si y sólo si para todo $\epsilon > 0$ existe n_0 natural tal que si $n \geq n_0$ se cumple que*

$$|f_n(x) - f(x)| < \epsilon \text{ para todo } x \in D$$

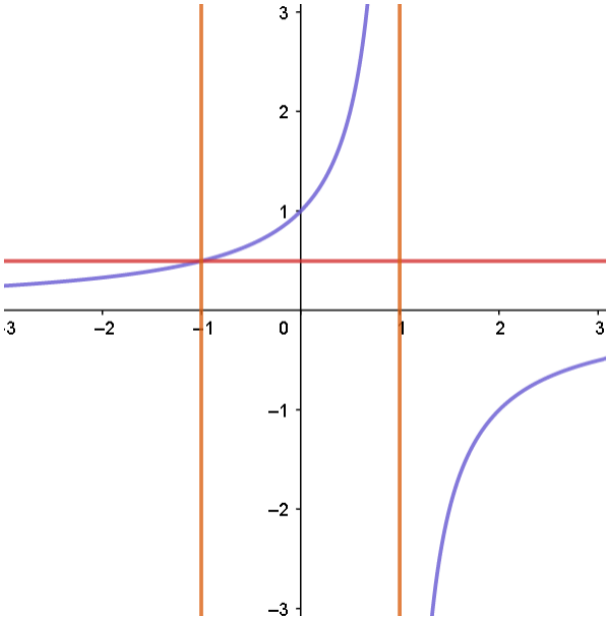

Figura 3.2: Región donde la función $H(t) > 1/2$

Lema 6.6. *Sea $I = [a, b]$ un intervalo tal que $f_n : I \to \mathbb{C}$ es una sucesión de funciones continuas que convergen uniformemente a la función $f \in I$. Entonces se cumplen las siguientes propiedades:*

(i) *f es continua*

(ii) $\lim_{n\to\infty} \int_a^b f_n(x)dx = \int_a^b f(x)dx$

(iii) *Si f_n tiene derivada continua y la serie de derivadas $\sum_n f_n'(x)$ converge uniformemente entonces $f'(x) = \sum_n f_n'(x)$*

Demostración. Demostraremos cada propiedad individualmente.

(i) Sea $x_0 \in I$ un punto. Para demostrar que $f(x)$ es continua en x_0 hay que comprobar que dado un $\epsilon > 0$ existe $\delta > 0$ tal que para todo $x \in I$ si

$$|x - x_0| < \delta \to |f(x) - f(x_0)| < \epsilon \tag{3.1}$$

Por hipótesis $f_n(x)$ es continua en I. Entonces

$$|f_n(x_0) - f(x_0)| < \epsilon/3 \text{ si } |x - x_0|\delta$$

Además f_n tiende a f uniformemente por lo tanto existe n_0 tal que

$$|f_n(x) - f(x)| < \epsilon/3 \text{ si } n \geq n_0 \text{ para todo } x \in I$$

y en x_0 tenemos que

$$|f_n(x_0) - f(x_0)| < \epsilon/3 \text{ si } n \geq n_0$$

Si restamos y sumamos $f_n(x_0)$ y $f_n(x)$ en la ecuación 3.1

$$\begin{aligned} |f(x) - f(x_0)| &= |f(x) - f_n(x) + f_n(x) - f_n(x_0) + f_n(x_0) - f(x_0)| \\ &\leq |f(x) - f_n(x)| + |f_n(x) - f_n(x_0)| + |f_n(x_0) - f(x_0)| \\ &\epsilon/3 + \epsilon/3 + \epsilon/3 = \epsilon \end{aligned}$$

Con esto concluimos con la demostración de la primera propiedad.

(ii) Por la propiedad (i) sabemos que f es continua en I lo que implica que la integral $\int_a^b f(x)dx$ existe. Sea $\epsilon > 0$ como f_n tiende a f uniformemente, existe n_0 natural tal que

$$|f_n(x) - f(x)| < \epsilon \text{ si } n \geq n_0 \text{ para todo } x \in I$$

Entonces tomando integrales y aplicando la propiedad que la resta de integrales es igual a la integral de la resta, observamos que

$$\begin{aligned} \int_a^b f_n(x)xd - \int_a^b f(x)dx &= \int_a^b \left(f_n(x) - f(x)\right) dx \\ &\leq \int_a^b |f_n(x) - f(x)|\, dx < \frac{\epsilon}{b-a} \int_a^b dx \\ &= \frac{\epsilon}{b-a}(b-a) = \epsilon \end{aligned}$$

Es decir, $\lim_{n\to\infty} \int_a^b f_n(x)dx = \int_a^b f(x)dx$

(iii) Por hipótesis f_n' converge uniformemente llamemos g a la función tal que $f_n' \to g$ por la propiedad (ii) tenemos que

$$\int_a^b f_n'(t)dt \to \int_a^b g(t)dt$$

como podemos observar

$$f_n(x) = K + f_n(a) + \int_a^b f_n(t)dt$$

donde la constante $K = 0$ si $x = a$ si tomamos limites

$$\begin{aligned} \lim_{n\to\infty} f_n(x) &= f_n(a) + \lim_{n\to\infty} \int_a^b f_n(t)dt \\ f(x) &= f_n(a) + \int_a^b g(t)dt \end{aligned}$$

Derivando la ultima igualdad obtenemos que $f'(x) = g(x)$

□

Una vez demostrado el lema, vamos a continuar con la demostración. Definimos la serie de funciones $\sum_{n=0}^{\infty} x^n$ en el intervalo $I = [-1, 1]$ como podemos ver esta serie equivale a la serie geométrica, es decir, $\sum_{n=0}^{\infty} x^n = \frac{1}{1-x}$. Por lo que podemos decir que $\sum_{n=0}^{\infty} x^n$ converge uniformemente a la función $f(x) = \frac{1}{1-x}$ con $x \in I$. Además, como la serie de derivadas $\sum_{n=0}^{\infty} nx^{n-1} = \frac{1}{(1-x)^2}$ por la propiedad (iii) $f(x)$ es derivable y $f'(x) = \sum_{n=0}^{\infty}(x^n)'$. Por lo tanto, si integramos a ambos lados obtenemos que

$$\int_0^x \frac{1}{1-x} = \sum_{n=0}^{\infty} \int_0^t x^n(t)dt$$

$$-\log(1-x) = \log\left(\frac{1}{1-x}\right) = \sum_{n=0}^{\infty} \frac{x^n}{n}$$

Concluimos, que $H(t) = \mathrm{Lg}(w) = \log\left(\frac{1}{1-z}\right)$ para $|z| < 1$. Cabe destacar que $\mathrm{Lg}(w)$ nos proporciona una extensión del logaritmo habitual, $\log(x)$ para los valores reales x cuando $x > 1/2$. □

Seguidamente, vamos a analizar las propiedades de Lg que como veremos son similares a las que demostramos en la proposición 3.3.

Proposición 7. *La función logarítmica* Lg *satisface las siguientes propiedades para* $|z| < 1$*:*

(i) $e^{\mathrm{Lg}(\frac{1}{1-z})} = \frac{1}{1-z}$

(ii) $\mathrm{Lg}(\frac{1}{1-z}) = z + E_1(z)$ *con* $|E_1(z)| \leq |z|^2$ *si* $|z| < 1/2$

(iii) Si $|z| \leq 1/2$*, entonces*

$$\left|\mathrm{Lg}(\frac{1}{1-z})\right| \leq 2|z|$$

Demostración. La demostración de las propiedades (ii) y (iii) son iguales a las del lema 3.3. Se considera la expansión en series de potencias de la función

$$\mathrm{Lg}\left(\frac{1}{1-z}\right) = \sum_{k=0}^{\infty} \frac{z^k}{k}$$

Poniendo $E(z) = \mathrm{Lg}(\frac{1}{1-z})$ se tiene que

$$E(z) - z = \frac{z^2}{2} + \frac{z^3}{3} + \frac{z^4}{4} + \ldots$$

por la desigualdad triangular el valor absoluto del error es menor que la suma de valores absolutos y por últimos utilizando la serie geométrica ya que $|z| \leq 1/2$ obtenemos que

$$|E(z)| \leq \frac{z^2}{2}\left(1 + \frac{1}{2} + \frac{1}{4} + \dots\right) \leq \frac{z^2}{2}\left(\frac{1}{1-1/2}\right) = z^2$$

Por lo tanto, tenemos que demostrar la propiedad (i) que es más compleja.

Primero, tomamos la fórmula de Euler para números complejos de manera que $z = re^{i\theta}$ con $0 \leq r < 1$. Notemos que solo nos hace falta demostrar que

$$(1-z)e^{\mathrm{Lg}\left(\frac{1}{1-z}\right)} = (1 - re^{i\theta})e^{\sum_{k=1}^{\infty}(re^{i\theta})^k/k} = 1 \tag{3.2}$$

Para esto vamos a derivar la parte de la izquierda de la función con respecto a r

$$\left[\left(1 - re^{i\theta}\right)e^{\sum_{k=1}^{\infty}\left(re^{i\theta}\right)^k/k}\right]' =$$

$$-e^{i\theta}e^{\sum_{k=1}^{\infty}(re^{i\theta})^k/k} + \left(1 - re^{i\theta}\right)e^{\sum_{k=1}^{\infty}\left(re^{i\theta}\right)^k/k} \cdot \left(\sum_{k=1}^{\infty}\left(re^{i\theta}\right)^k/k\right)' =$$

$$\left[-e^{i\theta} + \left(1 - re^{i\theta}\right)\left(\sum_{k=1}^{\infty}\left(re^{i\theta}\right)^k/k\right)'\right]e^{\sum_{k=1}^{\infty} re^{i\theta}}$$

Vamos a derivar el sumatorio. Como la serie $\sum \frac{z^k}{k} = \sum (re^{i\theta})^k/k$ converge en el intervalo que hemos escogido $|z| < 1$ podemos asegurar que la derivada de la suma es igual a la suma de las derivadas.

$$\begin{aligned}\left(\sum_{k=1}^{\infty}\left(re^{i\theta}\right)^k/k\right)' &= \sum_{k=1}^{\infty}\left(r^k\frac{e^{i\theta k}}{k}\right)' \\ &= \sum_{k=1}^{\infty} kr^{k-1}\frac{e^{i\theta k}}{k} \\ &= e^{i\theta}\sum_{k=1}^{\infty}\left(re^{i\theta}\right)^{k-1}\end{aligned}$$

Observemos que la serie resultante es la serie geométrica y como hemos restringido que $0 \leq r < 1$ tenemos que

$$\sum_{k=1}^{\infty}(re^{i\theta})^{k-1} = \frac{1}{1 - re^{i\theta}}$$

Ahora juntando todo

$$-e^{i\theta} + (1 - re^{i\theta})e^{i\theta}\sum_{k=1}^{\infty}(re^{i\theta})^{k-1} = -e^{i\theta} + (1 - re^{i\theta})e^{i\theta}\frac{1}{1 - re^{i\theta}} = -e^{i\theta} + e^{i\theta}\frac{1 - re^{i\theta}}{1 - re^{i\theta}} = 0$$

Por lo tanto, hemos visto que la derivada es igual a 0 es decir que el lado izquierdo de la ecuación 3.2 es constante. Si ponemos esta constante igual a 1 que es lo mismo que decir que $r = 0$ obtenemos el resultado deseado. □

Una vez demostradas estas 3 propiedades podemos pasar a estudiar la convergencia de productos infinitos, esta vez con números complejos. La demostración es similar a la de la proposición 4 pero utilizando Lg.

Proposición 8. *Si* $\sum |a_n|$ *converge y* $a_n \neq 1$ *para todo n, entonces*

$$\prod_{n=1}^{\infty}(\frac{1}{1-a_n})$$

también converge y es más este producto es distinto de cero

Demostración. Como demostramos en la proposición 4, para valores de n grandes $|a_n| < 1/2$, podemos asumir sin pérdida de generalidad que esto se cumple para todo $n \geq 1$. Entonces, por la propiedad (i) de la proposición 7 tenemos que

$$\prod_{n=1}^{N}\left(\frac{1}{1-a_n}\right) = \prod_{n=1}^{N} e^{\operatorname{Lg}(1/(1-a_n))} = e^{\sum_{n=1}^{N}\operatorname{Lg}(1/(1-a_n))}$$

Ahora como $|a_n| < 1/2$ podemos aplicar la propiedad (iii) de la proposición 7

$$\left|\operatorname{Lg}(\frac{1}{1-a_n})\right| \leq 2|a_n|$$

Tenemos que $\sum |a_n|$ converge, por lo tanto $\lim_{N\to\infty}\sum_{n=1}^{N}|a_n| = L$. Esto implica que

$$\sum_{n=1}^{N}\left|\operatorname{Lg}(\frac{1}{1-a_n})\right| \leq 2\sum_{n=1}^{N}|a_n| = 2L$$

como la serie de valores absolutos converge podemos asumir que la series sin valores absolutos converge también es decir, el límite

$$\lim_{N\to\infty}\operatorname{Lg}\left(\frac{1}{1-a_n}\right) = A$$

existe. Por lo tanto, tenemos que

$$e^{\sum_{n=1}^{\infty}\operatorname{Lg}(1/(1-a_n))} = e^{\lim_{N\to\infty}\sum_{n=1}^{\infty}\operatorname{Lg}\left(\frac{1}{1-a_n}\right)} = e^{A}$$

Como estamos tratando con exponentes sabemos no puede tomar el 0 como valor. Por lo tanto, hemos demostrado que el producto converge y es distinto de cero. □

Ahora que ya hemos introducido los elementos necesarios, procedemos a demostrar la fórmula de Dirichlet.

Teorema 8.1 (**Fórmula de Dirichlet**). *Si $s > 1$ entonces*

$$\sum_{n=1}^{\infty} \frac{\chi(n)}{n^s} = \prod_p \frac{1}{1 - \chi(p)P^{-s}}$$

donde el producto recorre todos los primos.

Demostración. Para simplificar denotaremos la serie de la izquierda como $L = \sum_n \frac{\chi(n)}{n^s}$ y el producto como $\Pi = \prod_p \frac{1}{1-\chi(p)P^{-s}}$. Ahora cogemos la suma y el producto parcial respectivamente

$$S_N = \sum_{n \leq N} \frac{\chi(n)}{n^s} \quad \text{y} \quad \Pi_N = \prod_{p \leq N} \frac{1}{1 - \chi(p)p^{-s}}$$

Aplicando la proposición 8 sabemos que Π_N converge ya que si definimos $a_n = \chi(p)p^{-s}$ con $s > 1$ entonces $\sum |\chi(p)p^{-s}|$ converge y también podemos observar que $|\chi(p)p^{-s}| \leq 1/2$ para todo p primo. Por esta razón, tenemos que el producto infinito $\Pi = \lim_{N\to\infty} \Pi_N = \prod_p \frac{1}{1-\chi(p)p^{-s}}$.

Por otro lado, utilizando también que $|\chi(p)p^{-s}| \leq 1/2$ podemos descomponer Π_N como el producto de series geométricas tal que

$$\Pi_N = \prod_{p \leq N} \left(1 + \frac{\chi(p)}{p^s} + \frac{\chi(p^2)}{p^{2s}} + \frac{\chi(p^3)}{p^{3s}} + \dots\right)$$

Dado un entero M tal que $M \geq N$ definimos

$$\Pi_{N,M} = \prod_{p \leq N} \left(1 + \frac{\chi(p)}{p^s} + \frac{\chi(p^2)}{p^{2s}} + \frac{\chi(p^3)}{p^{3s}} + \dots + \frac{\chi(p^M)}{p^{Ms}}\right)$$

Vamos a tomar limites para ver que L y Π son iguales. Dado un $\epsilon > 0$ escogemos un valor de N lo suficientemente grande tal que

$$|S_N - L| < \epsilon \quad \text{y} \quad |\Pi_N - \Pi| < \epsilon$$

y como $M > N$ tenemos que

$$|S_N - \Pi_{N,M}| < \epsilon \quad \text{y} \quad |\Pi_{N,M} - \Pi_N| < \epsilon$$

La primera igualdad se cumple gracias a que los caracteres de Dirichlet son multiplicativos y, como vimos en la demostración del teorema 5.1, podemos reagrupar y multiplicar los términos de $\Pi_{N,M}$ tal que gracias al teorema fundamental de la aritmética nos proporciona el inverso de cada entero n menor que N lo que implica que el $\lim_{M\to\infty} \Pi_{N,M} = S_N$. La segunda desigualdad

se cumple ya que cuando $M \to \infty$ entonces $\lim_{M\to\infty} \Pi_{N,M} = \Pi_N$ por definición. Aplicando la desigualdad triangular tenemos que

$$|L - \Pi| \leq |L - S_N| + |S_N - \Pi_{N,M}| + |\Pi_{N,M} - \Pi_N| + |\Pi_N - \Pi| < 4\epsilon$$

Entonces, la diferencia entre Π y L es de 4ϵ. Esto implica que $\Pi = L$ ya que si escogemos $\epsilon = |L - \Pi|/2$ entonces tendríamos que $|L - \Pi| < 4\epsilon = 4|L - \Pi|/2 = 2|L - \Pi|$ que es claramente una contradicción. □

3.4.2. Funciones L

Acabamos de ver como tratar el producto en la fórmula de Dirichlet utilizando una función definida sobre los complejos que actúa como una extensión de la función logaritmo. Cuando introdujimos las dificultades que hay al demostrar el teorema de Dirichlet, una de ellas era el estudio de la función L de Dirichlet

$$L(s, \chi) = \sum_{n=1}^{\infty} \frac{\chi(n)}{n^s}$$

que era una fórmula análoga de la función zeta de Euler. Especialmente, el estudio se vuelve complicado cuando s tiende a 1 y los caracteres de Dirichlet son no triviales, $\chi \neq \chi_0$. En el caso $L(s, \chi_0)$ el estudio es similar al de la función zeta. Formalizamos este idea en la siguiente proposición.

Proposición 9. *Supongamos que χ_0 es el carácter trivial de Dirichlet*

$$\chi_0(n) = \begin{cases} 1 & \textit{si } n \textit{ y } q \textit{ coprimos} \\ 0 & \textit{resto} \end{cases}$$

y $q = p_1^{a_1} \dots p_n^{a^N}$ la factorización en primos de q. Entonces

$$L(s, \chi_0) = (1 - p_1^{-s})(1 - p_2^{-s}) \dots (1 - p_N^{-s})\zeta(s)$$

Y por lo tanto, $L(s, \chi_0) \to \infty$ cuando $s \to 1^+$

Demostración. Vamos a estudiar las dos partes de la igualdad individualmente y ver si coinciden.

$$\begin{aligned} L(s, \chi_0) &= \sum_{n=1}^{\infty} \frac{\chi_0(n)}{n^s} \\ &= \prod_{p \equiv 1 \text{ mód } q} \frac{1}{1 - p^{-s}} \end{aligned}$$

Es decir, tenemos la suma de los $n = p$ coprimos a q ya que para el resto de valores $\chi_0(n) = 0$. Por otro lado, tenemos

$$(1 - p_1^{-s})(1 - p_2^{-s}) \dots (1 - p_N^{-s})\zeta(s)$$

Aplicando el teorema 5.1

$$\begin{aligned}(1 - p_1^{-s})(1 - p_2^{-s}) \dots (1 - p_N^{-s})\zeta(s) &= (1 - p_1^{-s})(1 - p_2^{-s}) \dots (1 - p_N^{-s}) \prod_p \frac{1}{1 - p^{-s}} \\ &= (1 - p_1^{-s})(1 - p_2^{-s}) \dots (1 - p_N^{-s}) \prod_p \frac{1}{1 - p^{-s}} \\ &= \prod_{p \equiv 1 \mod q} \frac{1}{1 - p^{-s}}\end{aligned}$$

Los $p_1, p_2, \dots, p_N$ se cancelan y son justamente los p del producto que no son coprimos a q. Para finalizar, como $\zeta(s) \to \infty$ cuando $s \to 1^+$ entonces $L(s, \chi_0) \to \infty$ también. □

Nos centramos, en el estudio de las funciones L cuyos caracteres son no triviales. Una propiedad destacable es que estas funciones están definidas y son continuas cuando $s > 0$ es decir, la suma $\sum_n \chi_n n^{-s}$ converge cuando $s > 0$. Introduciremos tres conceptos que no demostraremos y un lema para tratar la suma finita de caracteres no triviales, necesarias para la demostración de la proposición 10.

Lema 9.1 (**Suma por partes**). *Sean $\{f_k\}$ y $\{g_k\}$ dos secuencias entonces*

$$\sum_{k=m}^{N} f_k(g_{k+1} - g_k) = f_N g_N - f_m g_{m-1} - \sum_{k=m}^{N-1} (f_{N+1} - f_N) g_N$$

Lema 9.2 (**teorema del valor medio**). *Si f es una función continua en un intervalo cerrado $[a, b]$ y diferenciable en el intervalo abierto (a, b) entonces existe un punto c en (a, b) tal que la recta tangente en el punto c es paralela a la recta secante que pasa por los puntos$(a, f(a))$ y $(b, f(b))$, esto es*

$$f'(c) = \frac{f(b) - f(a)}{b - a}$$

Lema 9.3 (**prueba M de Weierstrass**). *Sea $\{f_n\}$ una sucesión de funciones de variable real o compleja definidas en un conjunto A, y supongamos que para cada $\{f_n\}$ existe una constante positiva M_n tal que $|f_n(x)| \leq M_n$ para todo $n \leq 1$ y todo x en A. Supongamos también que la serie $\sum_{n=1}^{\infty} M_n$ converge. Entonces la serie $\sum_{n=1}^{\infty} f_n(x)$ converge uniformemente en A*

Referencia: [4]

Por último antes de enunciar la proposición, vamos a introducir la propiedad de cancelación que poseen los caracteres no triviales de Dirichlet. Como veremos, esto es una propiedad de

los caracteres que ya fue mencionada en el capítulo anterior, lema 1.8, donde vimos que los caracteres e se cancelaban si no son triviales. Es una demostración similar pero aplicada a los caracteres de Dirichlet.

Lema 9.4. *Si χ es un carácter no trivial de Dirichlet, entonces*

$$\left|\sum_{k=1}^{k} \chi(n)\right| \leq q \quad \textit{para cualquier } k$$

Demostración. Primero tenemos que ver que

$$\sum_{n=1}^{q} \chi(n) = 0$$

Sea S el resultado de la suma y $a \in \mathbb{Z}^*(q)$, por la propiedad multiplicativa de los caracteres de Dirichlet

$$\chi(a)S = \chi(a)\sum_{n} \chi(n) = \sum_{n} \chi(a)\chi(n) = \sum_{n} \chi(n) = S$$

Esto se cumple ya que $a, n \in \mathbb{Z}^*(q)$ por lo tanto $an \in \mathbb{Z}^*(q)$ es decir, estamos permutando los elementos de la suma. Sin embargo, esto es una contradicción porque la igualdad solo se cumple si $\chi(a) = 1$ pero $\chi \neq \chi_0$ por lo tanto $\chi(a) \neq 1$ para algún $a \in \mathbb{Z}^*(q)$. Reescribimos k como $k = aq + b$ con $0 < b < q$ y obtenemos que

$$\sum_{n=1}^{k} \chi(n) = \sum_{n=1}^{aq} \chi(n) + \sum_{aq<n<aq+b} \chi(n) = 0 + \sum_{aq<n<aq+b} \chi(n) = \sum_{aq<n<aq+b} \chi(n)$$

No hay más de q elementos en ese sumatorio y $|\chi(n)| < 1$. □

Proposición 10. *Si χ es un carácter no trivial de Dirichlet, entonces la serie*

$$\sum_{n} \chi(n)n^{-s}$$

converge para todo $s > 0$, y denotamos la suma como $L(s, \chi)$. Además

(i) La función $L(s, \chi)$ es continua diferenciable para $0 < s < \infty$

(ii) Existen constantes $c, c' > 0$ tal que

$$L(s, \chi) = 1 + O(e^{-cs}) \quad \textit{cuando} \quad s \to \infty$$

$$L(s, \chi) = O(e^{-c's}) \quad \textit{cuando} \quad s \to \infty$$

Demostración. Sea $s_k = \sum_{n=1}^{k} \chi(n)$ y $s_0 = 0$. Sabemos que $L(s,\chi)$ esta definida para $s > 1$ por la serie

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

Por lo estudiado anteriormente sabemos que $\sum_{n=1}^{\infty} \frac{1}{n^s}$ converge para $s > 1$. Aplicando el lema 9.4 sabemos que $\left|\sum_{k=1}^{k} \chi(n)\right| \leq q$ lo que implica que $\sum \left|\frac{\chi(n)}{n^s}\right| = \sum \frac{|\chi(n)|}{n^s} \leq q \sum \frac{1}{n^s}$ entonces $\sum_{n=1}^{\infty} \frac{\chi(n)}{n^s}$ converge absolutamente para $s > \delta > 1$. Aplicando el mismo argumento, la serie derivada

$$L'(s,\chi) = \sum_{n=1}^{\infty} -s\frac{\chi(n)}{n^{s+1}} = -s\sum_{n=1}^{\infty} \frac{\chi(n)}{n^{s+1}}$$

converge absolutamente para $s > \delta > 1$ ya que $\sum \frac{|\chi(n)|}{n^s} \leq q \sum \frac{1}{n^{s+1}}$ entonces como la derivada existe y es continua la función $L(s,\chi)$ es continuamente diferenciable para $s > 1$.

Vamos a utilizar el lema 9.1 para extender este resultado para $s > 0$. En nuestro caso, $\{f_k\} = \sum_{k=1}^{N} \frac{1}{k^s}$ y $\{g_k\} = \sum_{k=1}^{N} \chi(k) = s_N$. Entonces tenemos que

$$\begin{aligned}
\sum_{k=1}^{N} \frac{\chi(k)}{k^s} &= \sum_{k=1}^{N} \frac{s_k - s_{k-1}}{k^s} \\
&= \frac{s_N}{N^s} - \frac{s_0}{1^s} - \sum_{k=1}^{N-1} (\frac{1}{(k+1)^s} - \frac{1}{k^s}) s_k \\
&= \frac{s_N}{N^s} + \sum_{k=1}^{N-1} (\frac{1}{(k)^s} - \frac{1}{(k+1)^s}) s_k \\
&= \sum_{k=1}^{N-1} f_k(s) + \frac{s_N}{N^s}
\end{aligned}$$

donde hemos denotado $f_k(s) = (\frac{1}{(k)^s} - \frac{1}{(k+1)^s}) s_k$ como una función dependiente de k. Si $g(x) = x^{-s}$ entonces $g'(x) = -sx^{-s-1}$, si aplicamos el lema 9.2 en el intervalo $(k, k+1)$

$$g'(k) = \frac{(k+1)^{-s} - k^{-s}}{k+1-k} = (k+1)^{-s} - k^{-s}$$

y utilizando el hecho de que $|s_k| \leq q$ obtenemos que

$$|f_k(s)| = |s_k((k+1)^{-s} - k^{-s})| \leq q g'(k) = qsk^{-s-1}$$

Por el lema 9.3 si escogemos la sucesión $\{f_k(s)\}$ y la constante positiva $M_n = qsk^{-s-1}$ podemos ver que $\sum_{k=1}^{\infty} qsk^{-s-1}$ converge ya que s y q son constantes y el denominador va creciendo por lo tanto el $lim_{N\to\infty} \sum_{k=1}^{N} qsk^{-s-1} = A$ existe. Podemos asumir que la serie $\sum f_k(s)$ converge

absoluta y uniformemente para $s > \delta > 0$ que consecuentemente implica que $L(s,\chi)$ es continua para $s > 0$. Nos falta comprobar que también es continuamente diferenciable para $s > 0$. Por el lema 6.6 si $L(s,\chi) = \sum \chi(n)n^{-s}$ converge uniformemente y el término de la suma es derivable entonces la derivada de la función es igual a la suma de las derivadas

$$L'(s,\chi) = \sum n^{-s}\log(n)\chi(n) = \sum \log(n)\frac{\chi(n)}{n^s}$$

Otra vez, utilizaremos el sumatorio por partes para reescribir la serie, esta vez $\{f_k\} = \sum_{k=1}^{N} \frac{\log(n)}{k^s}$ y $\{g_k\} = \sum_{k=1}^{N} \chi(k) = s_N$ y obtenemos

$$\begin{aligned}\sum \log(n)\frac{\chi(n)}{n^s} &= \sum_k \log(n)\frac{s_k - s_{k-1}}{k^s} \\ &= \sum_k s_k[\log(k)k^{-s} - \log(k+1)(k+1)^{-s}] + \frac{S_N}{N^s}\end{aligned}$$

Denotamos a la función $f(k) = s_k[\log(k)k^{-s} - \log(k+1)(k+1)^{-s}]$, aplicamos el teorema del valor medio a la función $g(x) = x^{-s}\log(x)$ en el intervalo $(k, k+1)$ y tenemos que

$$g'(c) = g(k+1) - g(k) = (k+1)^{-s}\log(k+1) - k^{-s}\log(k) = -sc^{-s-1}\log(c) + c^{-s}\frac{1}{c}$$

y obtenemos que

$$\begin{aligned}|s_k f(k)| &\leq q(-sc^{-s-1}\log(c) + c^{-s}\frac{1}{c}) \\ &\leq qc^{-\delta}\left(\log(c) + c^{-1}\right) \\ &\leq O\left(k^{-\delta/2}\left(\log(k) + k^{-1}\right)\right)\end{aligned}$$

Estudiando cada término por separado vemos que $O\left(k^{-\delta/2}k^{-s}\right) = O\left(k^{-\delta/2-1}\right)$ y como la función logaritmo crece a una velocidad notablemente menor que la función exponencial cuando $\frac{\log(k)}{k^{\delta/2}} < \frac{1}{k^{\delta/2-1}} = O\left(k^{-\delta/2-1}\right)$. Es decir, la función $f(k)$ está acotada por $O\left(k^{-\delta/2-1}\right)$ y aplicando un razonamiento similar al anterior vemos que $\sum f(k)$ converge absolutamente para $s > \delta > 0$ y por lo tanto es continua para $s > 0$. Por consecuencia, como la derivada de $L(s,\chi)$ existe y es continua podemos verificar que es continuamente diferenciable. □

Una vez estudiado el comportamiento de $L(s,\chi)$ podemos volver al problema inicial, definir un logaritmo para las funciones L. Para esto, vamos a integrar su derivada logarítmica. Es decir, si χ es un carácter no trivial de Dirichlet y $s > 0$ entonces definimos

$$\mathcal{L}\left(L(s,\chi)\right) = -\int_s^\infty \frac{L'(t,\chi)}{L(t,\chi)}dt$$

Teorema 10.1 (**Teorema fundamental del cálculo**). *Si f es continua en un intervalo $[a,b]$, la función g, definida por*

$$g(x) = \int_a^b f(t)dt$$

es continua en $[a,b]$ y diferenciable en (a,b), además $g'(x) = f(x)$

Referencia: [4]

Por la proposición 10 cuando $s \to \infty$ tenemos que

$$\frac{L'(s,\chi)}{L(s,\chi)} = \frac{O(e^{-c's})}{1+O(e^{-cs})} = O(e^{-cs})$$

luego como

$$\int_s^\infty e^{-ct}dt$$

converge entonces

$$\int_s^\infty \frac{L'(t,\chi)}{L(t,\chi)}dt = \int_s^\infty e^{-ct}dt$$

también converge lo que implica que es continua. Por lo tanto, podemos aplicar el teorema 10.1 para ver que

$$\mathcal{L}\left(L(s,\chi)\right) = -\int_s^\infty \frac{L'(t,\chi)}{L(t,\chi)}dt$$

La siguiente proposición enlaza los dos logaritmos definidos en este apartado, que nos será de utilidad más en adelante cuando empleemos logaritmos en la demostración de Dirichlet.

Proposición 11. *Si $s > 1$ entonces*

$$e^{\mathcal{L}(L(s,\chi))} = L(s,\chi)$$

Es más,

$$\mathcal{L}\left(L(s,\chi)\right) = \sum_p \mathrm{Lg}\left(\frac{1}{1-\chi(p)p^{-s}}\right)$$

Demostración. Para la primera parte de la demostración, nos basta con comprobar que la derivada de $e^{-\mathcal{L}(L(s,\chi))}L(s,\chi)$ con respecto a s es 0 con lo que $e^{-\mathcal{L}(L(s,\chi))}L(s,\chi)$ es constante y ver que esa constante es igual a 1. Aplicamos la regla de la cadena y el hecho que la derivada y la integral se anulan

$$-\frac{L'(s,\chi)}{L(s,\chi)}e^{-\mathcal{L}(L(s,\chi))}L(s,\chi) + e^{-\mathcal{L}(L(s,\chi))}L'(s,\chi) = 0$$

Por la proposición 10 sabemos que $L'(s,\chi)$ y su derivada tienden a 1 cuando $s \to \infty$. Esto concluye la primera parte de la demostración.

En cuanto a la segunda igualdad, tomamos exponentes a ambos lados. En la parte izquierda por lo que acabamos de demostrar obtenemos que $e^{\mathcal{L}(L(s,\chi))} = L(s,\chi)$. Y en la parte derecha por la propiedad (i) de la proposición 7

$$\prod_p e^{\mathrm{Lg}\left(\frac{1}{1-\chi(p)p^{-s}}\right)} = \prod_p \left(\frac{1}{1-\chi(p)p^{-s}}\right)$$

Después, aplicando la fórmula de Dirichlet, teorema 8.1, tenemos que

$$\prod_p \left(\frac{1}{1-\chi(p)p^{-s}}\right) = \sum_n \frac{\chi(n)}{n^s} = L(s,\chi)$$

Dos potencias complejas son iguales si los exponentes difieren por un número múltiplo de $2\pi i$. Es decir,

$$e^{\mathcal{L}(L(s,\chi))} = e^{\sum \mathrm{Lg}(\frac{1}{1-\chi(p)p^{-s}})}$$

son iguales si

$$\mathcal{L}\left(L(s,\chi)\right) - \sum_p \mathrm{Lg}\left(\frac{1}{1-\chi(p)p^{-s}}\right) = 2\pi i M(s)$$

donde $M : \mathbb{R} \to \mathbb{Z}$ es una función tal que para cada $s \in \mathbb{R}$ le asignamos un entero $M(s)$. Si logramos demostrar que la función M es continua entonces, como $\mathbb{R}$ es un conjunto conexo $M(\mathbb{R})$ tiene que ser conexo también pero los únicos conjuntos conexos en $\mathbb{Z}$ son los puntos, es decir $M(s)$ es constante para todo $s \in \mathbb{R}$.

Si tomamos $a_p = \chi(p)p^{-s}$ como $|a_p| < 1$ entonces $\sum_n |a_p|$ converge. Como vimos en la demostración de la proposición 8 el

$$\lim_{N\to\infty} \sum_{p\leq N} \mathrm{Lg}\left(\frac{1}{1-a_n}\right) = A$$

existe y por lo tanto, $\sum_p \mathrm{Lg}\left(\frac{1}{1-\chi(p)p^{-s}}\right)$ toma un valor real lo que implica que la función Lg es continua, ya que si para algún p_0 la función $\mathrm{Lg}\left(\frac{1}{1-\chi(p)p^{-s}}\right)$ no es continua entonces $\lim p \to p_0 \mathrm{Lg}\left(\frac{1}{1-\chi(p)p^{-s}}\right) = \infty$.

Utilizando un razonamiento similar, como

$$L(s,\chi) = \sum_n \frac{\chi(n)}{n^s} = \prod_p \left(\frac{1}{1-\chi(p)p^{-s}}\right) = \sum_n \mathrm{Lg}\left(\frac{1}{1-\chi(p)p^{-s}}\right)$$

sabemos que converge y es distinto de cero lo que implica que $\mathcal{L}(L(s,\chi))$ es continua. Por lo tanto, $\mathcal{L}(L(s,\chi))$ es continua en s. Por último, la resta de dos funciones continuas en un punto s también es continua en ese punto que implica que $M(s)$ es continua en s.

Concluimos la demostración con el hecho de que a medida que $s \to \infty$ $\sum_n \frac{\chi(n)}{n^s}$ se aproxima a cero, tanto Lg como $\mathcal{L}$ son iguales a 1. Así que $M(s) = 0$ cuando $s \to \infty$. □

Recordemos porque por la fórmula de Euler

$$L(s,\chi) = \prod_p \left(\frac{1}{1-\chi(p)p^{-s}}\right)$$

ahora una vez definidos los dos logaritmos tenemos que

$$\mathcal{L}(L(s,\chi)) = \sum_p \mathrm{Lg}\left(\frac{1}{1-\chi(p)p^{-s}}\right)$$

Como $|\frac{\chi(p)}{p^s}| < 1$ podemos aplicar la propiedad (i) de la proposición 7 y obtenemos que

$$\begin{aligned}\sum_p \mathrm{Lg}\left(\frac{1}{1-\chi(p)p^{-s}}\right) &= \sum_p \frac{\chi(p)}{p^s} + O\left(\sum_p \left(\frac{\chi(p)}{p^s}\right)^2\right) \\ &= \sum_p \frac{\chi(p)}{p^s} + O\left(\sum_p \frac{1}{p^{2s}}\right) \\ &= \sum_p \frac{\chi(p)}{p^s} + O(1)\end{aligned}$$

Ahora si $L(1,\chi) \neq 0$ para un carácter no trivial de Dirichlet, entonces la integral que utilizamos para definir $\mathcal{L}$ no se cancela y permanece acotada cuando $s \to 1^+$ ya que tanto $L(s,\chi)$ como su derivada están acotadas. Por consiguiente, aplicando la igualdad de la proposición anterior

$$\mathcal{L}(L(s,\chi)) = \sum_p \mathrm{Lg}\left(\frac{1}{1-\chi(p)p^{-s}}\right) = \sum_p \frac{\chi(p)}{p^s} + O(1)$$

Como $\mathcal{L}(L(s,\chi))$ permanece acotada cuando $s \to 1^+$ entonces $\sum_p \frac{\chi(p)}{p^s}$ también lo está. Que es el resultado que nos interesa para la demostración del teorema de Dirichlet, como se puede observar en el ejemplo de la demostración para los primos de la clase $4k+1$. Por último, nos queda demostrar que de hecho, $L(1,\chi) \neq 0$ para un carácter no trivial de Dirichlet.

3.4.3. Las funciones L no se anulan

Recogemos la información más relevante sobre este apartado en la demostración del siguiente teorema.

Teorema 11.1. *Si $\chi \neq \chi_0$ entonces $L(1,\chi) \neq 0$.*

La demostración se separa en dos casos, dependiendo si χ toma valores reales o complejos. Los caracteres de Dirichlet reales toman los valores $+1, -1$ o 0 si no, toma valores complejos. En otras palabras, χ es real si y solo si $\chi(n) = \overline{\chi(n)}$ para todo entero n ya que la inversa de $+1, -1$ o 0 son ellos mismos.

Caso I: Caracteres complejos de Dirichlet.

Este es el caso más sencillo de los dos. Se demuestra por contradicción y vamos a necesitar los dos siguientes lemas.

Lema 11.1. *Si $s > 1$, entonces*

$$\prod_{\chi} L(s,\chi) \geq 1$$

donde el producto recorre todos los caracteres de Dirichlet. En particular el producto tiene un valor real.

Demostración. En la proposición 11 hemos demostrado que

$$\mathcal{L}\left(L(s,\chi)\right) = \sum_{p} \mathrm{Lg}\left(\frac{1}{1-\chi(p)p^{-s}}\right)$$

si tomamos exponentes a ambos lados tenemos

$$L(s,\chi) = \exp\left(\sum_{p} \mathrm{Lg}\left(\frac{1}{1-\chi(p)p^{-s}}\right)\right)$$

Ahora si hacemos el producto de todos los caracteres de Dirichlet a ambos lados

$$\begin{aligned}\prod_{\chi} L(S,\chi) &= \prod_{\chi} \exp\left(\sum_{p} \mathrm{Lg}\left(\frac{1}{1-\chi(p)p^{-s}}\right)\right) \\ &= \exp\left(\sum_{\chi}\sum_{p} \mathrm{Lg}\left(\frac{1}{1-\chi(p)p^{-s}}\right)\right)\end{aligned}$$

Aplicando definición de Lg que recordemos era

$$\mathrm{Lg}\left(\frac{1}{1-z}\right) = \sum_{k=1}^{\infty} \frac{z^k}{k}$$

con $z = \frac{\chi(p)}{p^s}$ tenemos que

$$\begin{aligned}\prod_{\chi} L(S,\chi) &= \prod_{\chi} \exp\left(\sum_{p} \operatorname{Lg}\left(\frac{1}{1-\chi(p)p^{-s}}\right)\right) \\ &= \exp\left(\sum_{\chi}\sum_{p} \operatorname{Lg}\left(\frac{1}{1-\chi(p)p^{-s}}\right)\right) \\ &= \exp\left(\sum_{\chi}\sum_{p}\sum_{k=1}^{\infty}\left(\frac{\chi(p)}{p^s}\right)^k \frac{1}{k}\right) \\ &= \exp\left(\sum_{\chi}\sum_{p}\sum_{k=1}^{\infty}\frac{\chi(p)^k}{p^{ks}}\frac{1}{k}\right) \\ &= \exp\left(\sum_{p}\sum_{k=1}^{\infty}\sum_{\chi}\frac{\chi(p^k)}{p^{ks}}\frac{1}{k}\right)\end{aligned}$$

Para terminar, aplicamos el lema 6.2 con $l = 1$ donde demostrábamos que los caracteres de Dirichlet son multiplicativos. Es más demostrábamos que

$$\delta_l(n) = \frac{1}{\varphi(q)}\sum_{\chi}\overline{\chi(l)}\chi(m)$$

en nuestro caso escogemos $l = 1$ ya que así $\overline{\chi(1)} = 1$ y $m = p^k$ obtenemos que

$$\begin{aligned}\delta_1(p^k) &= \frac{1}{\varphi(q)}\sum_{\chi}\chi(p^k) \\ \sum_{\chi}\chi(p^k) &= \delta_1(p^k)\varphi(q)\end{aligned}$$

sustituyendo en la igualdad anterior

$$\prod_{\chi} L(s,\chi) = \exp\left(\varphi(q)\sum_{p}\sum_{k=1}^{\infty}\frac{\delta_1(p^k)}{p^{ks}}\frac{1}{k}\right) \geq 1$$

porque los términos en el exponentes son positivos. □

Lema 11.2. *Las tres siguientes propiedades se cumplen:*

(i) Si $L(1,\chi) = 0$, entonces $L(1,\overline{\chi}) = 0$.

(ii) Si χ es un carácter no trivial de Dirichlet y $L(1,\chi) = 0$, entonces

$$|L(s,\chi)| \leq C|s-1|$$

cuando $1 \leq s \leq 2$.

(iii) Para el carácter trivial de Dirichlet χ_0, tenemos que

$$|L(s,\chi_0)| \leq \frac{C}{|s-1|}$$

cuando $1 < s \leq 2$.

Demostración. La primera propiedad es inmediata ya que

$$L(s,\overline{\chi}) = \sum_{n=1}^{\infty} \frac{\overline{\chi(n)}}{n} = \sum_{n=1}^{\infty} \frac{1}{\chi(n)n} = \overline{L(s,\chi)}$$

Para la segunda propiedad aplicamos el teorema del valor medio sobre el intervalo $(1,s)$ ya que por la proposición 10 sabeos que $L(s,\chi)$ es continuamente diferenciable para $s > 0$ cuando χ es un carácter no trivial.

$$\begin{aligned} L_0'(s,\chi) &= \frac{L(s,\chi) - L(1,\chi)}{s-1} \\ (s-1)L_0'(s,\chi) &= L(s,\chi) - L(1,\chi) \\ L(s,\chi) &= L(1,\chi) + (s-1)L_0'(s,\chi) \end{aligned}$$

Por la propiedad triangular

$$|L(s,\chi)| \leq |L(1,\chi)| + |(s-1)L_0'(s,\chi)| \leq |s-1|C$$

ya que por la proposición 10 $L'(s,\chi) = O(e^{-cs})$. Para finalizar, la última propiedad se cumple por la proposición 9

$$L(s,\chi_0) = (1-p_1^{-s})(1-p_2^{-s})\dots(1-p_N^{-s})\zeta(s)$$

y recordemos que en el lema 4.1 la función zeta cumplía que

$$\zeta(s) \leq 1 + \frac{1}{s-1}$$

y por lo tanto

$$L(s,\chi_0) \leq (1-p_1^{-s})(1-p_2^{-s})\dots(1-p_N^{-s})\left(1+\frac{1}{s-1}\right)$$

otra vez aplicando la propiedad triangular

$$\begin{aligned} |L(s,\chi_0)| &\leq C + \left|\frac{C}{s-1}\right| \\ &\leq C + \frac{C}{|s-1|} \end{aligned}$$

□

Una vez demostrados los dos lemas podemos pasara a terminar la demostración de que $L(1,\chi) \neq 0$ para χ no trivial. Supongamos que $L(1,\chi) = 0$, entonces por la propiedad (i) del lema anterior $L(1,\overline{\chi}) = 0$ y como χ es no trivial $\chi \neq \overline{\chi}$. Por lo tanto hay al menos dos términos en el producto

$$\prod_{\chi} L(s,\chi)$$

que decrecen como $|s-1|$ por la propiedad (ii) cuando $s \to 1^+$. Sin embargo, el único término que crece cuando $s \to 1^+$ es $L(s,\chi_0)$ y este crecimiento es por la propiedad (iii) como mucho $O(1/|s-1|)$, nos encontramos con que el producto tiende a cero cuando s se aproxima a 1 por la derecha. Esto es una contradicción por lo demostrado en el lema 11,1.

Caso II: Caracteres reales de Dirichlet.

La demostración de $L(1,\chi) \neq 0$ para los caracteres no triviales reales de Dirichlet es muy distinta a la de los caracteres complejos. Necesitaremos introducir el **teorema de división de Dirichlet** como ejemplo para el método de suma a lo largo de hipérbolas que después, adaptaremos a las funciones $L(s,\chi)$ para acabar demostrando que $L(1,\chi) \neq 0$.

Proposición 12. *Si N es un entero positivo, entonces*

$$\begin{aligned}\sum_{n=1}^{N} \frac{1}{n^{1/2}} &= \int_1^N \frac{dx}{x^{1/2}} + c' + O(1/N^{1/2}) \\ &= 2N^{1/2} + c + O(1/N^{1/2})\end{aligned}$$

Demostración. La demostración es muy parecida a la de la proposición anterior. En este caso tenemos que

$$\gamma_n = \frac{1}{n^{1/2}} - \int_n^{n+1} \frac{dx}{x^{1/2}}$$

y después aplicando el teorema del valor medio a la función $f(x) = x^{-1/2}$ en el intervalo $[n, n+1]$ obtenemos que

$$f'(x) = -1/2x^{-3/2} = (n+1)^{-1/2} - n^{-1/2} \to \left| \frac{1}{n^{1/2}} - \frac{1}{(n+1)^{1/2}} \right| \leq \frac{C}{n^{3/2}}$$

Por lo tanto, $\sum \gamma_n$ converge y denotamos al límite como γ. Después, estimando la serie a integrales obtenemos que

$$\sum_{n=N+1}^{\infty} n^{-3/2} \leq \int_N^{\infty} \frac{dx}{x^{3/2}} = O(1/n^{1/2})$$

Por último, separando la serie e igualándola a γ

$$\sum_{n=1}^{N} \frac{1}{n^{1/2}} - \int_1^N \frac{dx}{x^{-1/2}} = \gamma - \sum_{n=N+1}^{\infty} \gamma_n + \int_N^{N+1} \frac{dx}{x^{-3/2}}$$

donde $\int_1^N \frac{dx}{x^{-1/2}} = 2N^{1/2} + 2$ y si $N \to \infty$ entonces la última integral es $O(1/N^{1/2})$ □

Sumas hiperbólicas.

Dada una función F con dos variables enteras positivas (m, n), donde sumamos cada par de enteros (m, n) de manera que

$$S_N = \sum \sum F(m, n)$$

Las dos maneras más tradicionales de calcular este sumatorio son:

1. *Verticalmente* Para cada valor de m recorremos los valores $1 \leq n \leq N/m$

$$S_N = \sum_{m=1}^{N} \left(\sum_{n=1}^{N/m} F(m, n) \right)$$

2. *Horizontalmente* Para cada valor de n recorremos los valores $1 \leq m \leq N/n$

$$S_N = \sum_{m=1}^{N} \left(\sum_{n=1}^{N/m} F(m, n) \right)$$

Otro método para calcular esta suma consiste en tomar hipérbolas. Es decir, para cada valor $1 \leq k \leq N$ recorremos todos las posibles combinaciones de (m, n) tal que $mn = k$

$$S_N = \sum_{k=1}^{N} \left(\sum_{nm=k} F(m, n) \right)$$

Se puede comprobar a mano que de hecho el resultado de la suma dada por los tres métodos es la misma. Vamos a aplicar este resultado al problema del divisor.

Problema del divisor.

Queremos estudiar el comportamiento de la función $d(k)$ que para cada entero positivo k nos devuelve su número de divisores. Uno podría razonar que a medida que k toma valores más grande el valor de $d(k)$ también crece. Sin embargo, y como ya hemos visto, existen infinitos primos así que para algunos valores de k muy grandes $d(k) = 2$. Por lo tanto, para entender el comportamiento de la función, nos interesa averiguar el tamaño medio, es decir averiguar el valor de

$$\frac{1}{N} \sum_{k=1}^{N} d(k) \quad \text{cuando } N \to \infty$$

La respuesta a esta pregunta fue averiguada por Dirichlet, empleando el uso de sumas hiperbólicas. De hecho, podemos ver que

$$d(k) = \sum_{nm=k} 1$$

con n, m enteros positivos, claramente estamos sumando una vez todos las posibles combinaciones de divisores de k que es justamente $d(k)$.

Teorema 12.1. *Si k es un entero positivo, entonces*

$$\frac{1}{N}\sum_{k=1}^{N} d(k) = \log(N) + O(1)$$

Demostración. Sea $S_N = \sum_{k=1}^{N} d(k)$. Como ya hemos mencionado si escogemos $F = 1$ y sumamos a lo largo de hipérbolas obtenemos S_N. Sumando verticalmente obtenemos que

$$S_N = \sum_{m=1}^{N}\sum_{n=1}^{N/m} 1$$

Si observamos el segundo sumatorio, vemos que para cada m sumamos 1 N/M veces es decir $\sum_{n=1}^{N/m} 1 = N/m + O(1)$ y por lo tanto

$$S_N = \sum_{m=1}^{N} (N/m + O(1)) = N\left(\sum_{m=1}^{N} 1/m\right) + O(N)$$

Por último si dividimos S_N entre N tenemos que

$$\frac{S_N}{N} = \sum_{m=1}^{N} 1/m + O(1)$$

y aplicando la propiedad (i) de la proposición 5

$$\sum_{m=1}^{N} 1/m = \log(N) + O(1)$$

□

La función L no se anula.

Finalmente, ya hemos llegado al último apartado de esta sección que concluirá con la demostración del teorema de Dirichlet. Aplicaremos la suma a lo largo de hipérbolas para ver

que $L(1,\chi) \neq 0$ para los caracteres no triviales de Dirichlet reales. Dado un carácter de los mencionados definimos

$$F(n,m) = \frac{\chi(n)}{(nm)^{1/2}}$$

y

$$S_N = \sum\sum F(m,n)$$

donde la suma recorre todos los pares de enteros positivos (m,n) tal que $mn = N$.

Proposición 13. *Sea χ un carácter real, las dos siguientes afirmaciones son ciertas:*

(i) $S_N \geq c\log(N)$ *para alguna constante* c

(ii) $S_N = 2N^{1/2}L(1,\chi) + O(1)$

Como podemos observar, si demostramos la proposición entonces la suposición de que $L(1,\chi) = 0$ sería una contradicción.

Demostración. Primero sumamos a lo largo de hipérbolas

$$\sum_{nm=k} \frac{\chi(n)}{(nm)^{1/2}} = \sum_{nm=k} \frac{\chi(n)}{k^{1/2}} = \frac{1}{k^{1/2}} \sum_{n|k} \chi(n)$$

Para demostrar la propiedad (i) nos bastará con demostrar el siguiente lema.

Lema 13.1.

$$\sum_{n|k} \chi(n) \geq \begin{cases} 0 & \textit{para todo } k \\ 1 & \textit{si } k = l^2 \textit{ para algún } l \in \mathbb{Z} \end{cases}$$

Demostración. Si $k = p^a$ donde p es primo entonces los divisores de k serán $1, p, p^2, \ldots, p^a$ y tenemos que

$$\begin{aligned} \sum_{n|k} \chi(n) &= \chi(1) + \chi(p) + \cdots + \chi(p^a) \\ &= 1 + \chi(p) + \chi(p)^2 + \cdots + \chi(p)^a \end{aligned}$$

Como χ es un carácter no trivial de Dirichlet real solo puede tomas los valores $1, -1$ o 0. Por lo tanto,

$$\sum_{n|k} \chi(n) = \begin{cases} a+1 & \text{si } \chi(p) = 1 \\ 1 & \text{si } \chi(p) = -1 \text{ y } a \text{ es par} \\ 0 & \text{si } \chi(p) = -1 \text{ y } a \text{ es impar} \\ 1 & \text{si } \chi(p) = 0 \text{ o sea } p|q \end{cases}$$

Si tenemos $k = l^2$ un cuadrado perfecto entonces, su descomposición en primos es igual a $k = p_1^{a_1} \dots p_N^{a_N}$ donde a_i con $1 \leq i \leq N$ son pares. Si aplicamos la propiedad multiplicativa de χ obtenemos que

$$\sum_{n|k} \chi(n) = \prod_{i=1}^{N} \left(\chi(1) + \chi(p_i) + \chi(p_i)^2 \cdots + \chi(p_i)^{a_i}\right)$$

donde cada término del producto será distinto de 0 porque a_i es par. Y cero para el resto de valores de k. □

Para demostrar la segunda parte de la demostración, vamos a dividir la gráfica de la función $nm = N$ en 3 regiones, como se puede apreciar en la figura 3.3. Estas regiones están definidas de la siguiente manera

$$I = \{1 \leq m < N^{1/2}, N^{1/2} < n \leq N/m\},$$
$$II = \{1 \leq m \leq N^{1/2}, 1 \leq n \leq N^{1/2}\},$$
$$III = \{N^{1/2} < m \leq N/n, 1 \leq n \leq N^{1/2}\}$$

Reescribimos $S_N = S_I + (S_{II} + S_{III})$. Primero evaluaremos S_I verticalmente y luego la suma $(S_{II} + S_{III})$ horizontalmente. Sin embargo, vamos a necesitar el siguiente lema para realizar los cálculos

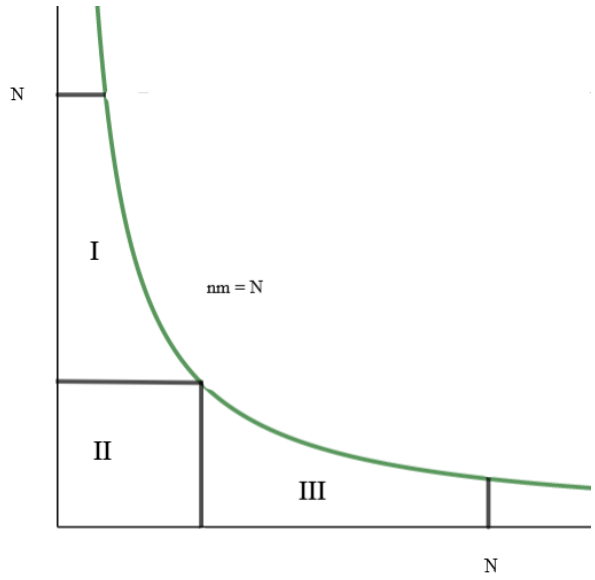

Figura 3.3: División de la función $nm = N$ en tres regiones

Lema 13.2. *Para todos los enteros $0 < a < b$ tenemos que*

(i) $\sum_{n=a}^{b} \frac{\chi(n)}{n^{1/2}} = O(a^{-1/2})$

(ii) $\sum_{n=a}^{b} \frac{\chi(n)}{n} = O(a^{-1})$

Demostración. Demostraremos la primera propiedad ya que la demostración es similar para ambas. Sea $s_n = \sum_{k=1}^{n} \chi(k)$. Recordemos que, por el lema 9.4 $|s_n| \leq q$ para todo n. Utilizamos sumas por partes, donde $f(k) = k^{-1/2}$ y $g(k) = s_k$. Tenemos que

$$\begin{aligned}\sum_{k=a}^{b} \frac{\chi(k)}{k^{1/2}} &= \sum_{k=a}^{b} \frac{s_{k+1} - s_k}{k^{1/2}} \\ &= \sum_{k=a}^{b-1} s_k \left[k^{-1/2} - (k+1)^{-1/2}\right] - \frac{s_b}{b^{1/2}} + \frac{s_a}{a^{1/2}}\end{aligned}$$

Primero se puede observar que $\left|\frac{s_a}{a^{1/2}} - \frac{s_b}{b^{1/2}}\right| \leq \frac{C}{a^{1/2}} = O(a^{-1/2})$. Segundo, en la demostración de la proposición 12 vimos que $\left|k^{-1/2} - (k+1)^{-1/2}\right| \leq \frac{C}{k^{3/2}}$ por lo tanto el sumatorio $\sum_{k=a}^{b-1} s_k \left[k^{-1/2} - (k+1)^{-1/2}\right] \leq \sum_{k=a}^{\infty} \frac{s_k}{n^{3/2}} = O\left(\sum_{k=a}^{\infty} n^{-3/2}\right)$. Para finalizar, si estimamos la suma $\sum_{k=a}^{\infty} n^{-3/2}$ con la integral de $f(x) = x^{-3/2}$, tenemos que

$$\sum_{k=a}^{\infty} n^{-3/2} \leq \int_a^{\infty} \frac{dx}{x^{3/2}} \leq \frac{C}{a^{1/2}} = O(a^{-1/2})$$

y por lo tanto llegamos a que

$$\sum_{k=a}^{b} \frac{\chi(k)}{k^{1/2}} = O(a^{-1/2}) + O(a^{-1/2}) = O(a^{-1/2})$$

□

Sumando verticalmente S_I tenemos que

$$S_I = \sum_{m=1}^{N^{1/2}} \left(\sum_{n=N^{1/2}}^{N/m} \frac{\chi(n)}{(nm)^{1/2}} \right) = \sum_{m=1}^{N^{1/2}} \frac{1}{m^{1/2}} \left(\sum_{n=N^{1/2}}^{N/m} \frac{\chi(n)}{n^{1/2}} \right)$$

por el lema anterior la suma de dentro es igual a $O(a^{-1/2})$ y por la proposición 12 la suma de fuera es igual a $2N^{1/4} + c + O(N^{-1/2})$ juntando todo podemos ver que

$$s_I = \sum_{m=1}^{N^{1/2}} \frac{1}{m^{1/2}} \left(\sum_{n=N^{1/2}}^{N/m} \frac{\chi(n)}{n^{1/2}} \right) \leq C = O(1)$$

Por último, sumamos horizontalmente

$$\begin{aligned} S_{II}+S_{III} &= \sum_{n=1}^{N^{1/2}} \frac{\chi(n)}{n^{1/2}} \left(\sum_{m=1}^{N^{1/2}} \frac{1}{m^{1/2}} \right) + \sum_{n=1}^{N^{1/2}} \frac{\chi(n)}{n^{1/2}} \left(\sum_{m=N^{1/2}}^{N/n} \frac{1}{m^{1/2}} \right) \\ &= \sum_{n=1}^{N^{1/2}} \frac{\chi(n)}{n^{1/2}} \left(\sum_{m=1}^{N^{1/2}} \frac{1}{m^{1/2}} + \sum_{m=N^{1/2}}^{N/n} \frac{1}{m^{1/2}} \right) \\ &= \sum_{n=1}^{N^{1/2}} \frac{\chi(n)}{n^{1/2}} \left(\sum_{m=1}^{N/n} \frac{1}{m^{1/2}} \right) \end{aligned}$$

por la proposición 12 el sumatorio de dentro es igual a $2(N/n)^{1/2}+c+O\left((n/N)^{1/2}\right)$, sustituyendo

$$\begin{aligned} S_{II}+S_{III} &= \sum_{n=1}^{N^{1/2}} \frac{\chi(n)}{n^{1/2}} \left\{ 2(N/n)^{1/2}+c+O\left((n/N)^{1/2}\right) \right\} \\ &= \sum_{n=1}^{N^{1/2}} \frac{\chi(n)}{n^{1/2}} \left(2\left(\frac{N}{n}\right)^{1/2} \right) + c\sum_{n=1}^{N^{1/2}} \frac{\chi(n)}{n^{1/2}} + O(\sum_{n=1}^{N^{1/2}} \frac{\chi(n)}{n^{1/2}} \left(\left(\frac{n}{N}\right)^{1/2} \right) \\ &= 2N^{1/2} \sum_{n=1}^{N^{1/2}} \frac{\chi(n)}{n} + c\sum_{n=1}^{N^{1/2}} \frac{\chi(n)}{n^{1/2}} + O\left(\frac{1}{N^{1/2}} \sum_{n=1}^{N^{1/2}} \chi(n) \right) \\ &= A+B+C \end{aligned}$$

Por la definición de la función L A es igual a $2N^{1/2}L(1,\chi)+O(1)$. El segundo término, gracias a la propiedad (i) del lema 13.2, $B = c \cdot O(1^{-1/2}) = O(1)$ y por último, podemos ver que $C = O(1)$ ya que $|\sum \chi(n)| \leq q$. Con esto concluimos el lema y demostramos que $L(1,\chi) \neq 0$ para los caracteres no triviales de Dirichlet □

Finalmente, hemos demostrado las tres dificultades que se planteaban para poder demostrar el teorema de Dirichlet que recordemos eran:

1 Definir logaritmos complejos para tratar productos infinitos.

2 El estudio de la función $L(s,\chi)$ especialmente en el caso $s \to 1^+$

3 Demostrar que $L(1,\chi) \neq 0$ para caracteres no triviales de Dirichlet

Ahora que hemos comprobado los tres aspectos del problema, podemos explicar la demostración del teorema de Dirichlet. Recordemos el enunciado.

Teorema 13.1. *Si q y l son dos enteros positivos coprimos entre ellos, entonces existen infinitos primos de la forma $l + kq$ con $k \in \mathbb{Z}$*

Demostración. Para la demostración solo tenemos que aplicar el lema 6.3 ya que por la proposición 13 sabemos que $L(s, \chi) = \sum_{n=0}^{\infty} \frac{\chi(p)}{p^s}$ está acotada cuando $s \to 1^+$ □

Capítulo 4

Conclusiones

Durante la realización del Trabajo de Final de Grado he logrado tener un conocimiento más extenso sobre la investigación matemática, un tópico en el cual no se profundiza mucho durante el grado, y el trabajo realizado por los académicos para redactar libros y documentos académicos. También, ha servido para poner en práctica los conocimientos adquiridos y retar al estudiante a no solo comprender conceptos nuevos si no ha transmitirlos de una manera coherente y adecuada. En conclusión, este proyecto me ha dado una visión inicial del trabajo realizado por los matemáticos a un nivel académico.

Respecto al contenido, me ha agradado poder visualizar como un concepto generalmente asociado al análisis matemático puede ser trasladado y utilizado en otras áreas. Además, de la gran utilidad y versatilidad de la teoría de Fourier de la cual no era conocedor hasta la realización del trabajo. No obstante, aunque algunas de las demostraciones y conceptos han sido complicados de entender, investigar y leer libros sobre diferentes tópicos ha sido de gran agrado y me a abierto puertas a nuevos conceptos.

Por último, quiero agradecer a mi tutor Jorge Galindo Pastor, por el apoyo y la guía que me ha dado a lo largo de la realización del trabajo. Siempre ha estado dispuesto tanto a atender mis dudas como ha recomendarme libros o documentos en los cuales podría encontrar soluciones a los diferentes problemas que fueron surgiendo.

Bibliografía

[1] T.W. Körner. *Fourier Analysis*. Cambridge University Press, 1988. Capítulo 6.

[2] Serge Lang. *Graduate Texts in Mathematics, Algebra*. Springer, 2002. Capítulo 15.6.

[3] Gabriel Navarro. *Un curso de álgebra*. Universidad de Valencia, 2016. Capítulos 1-3.

[4] James Stewart. *Cálculo. Trascendentes tempranas*. Thomson, 1999.

[5] Juan R. Torregosa y Cristina Jordán. *Álgebra lineal y sus aplicaciones*. McGraw-Hill, 1987. Capítulo 3.

[6] E.M. Stein y R. Shakarchi. *Fourier analysis*. Princeton University Press, 2003. Capítulos 7 - 8.